RESUMEN – TRABAJO DE GRADO

AUTORES	KATHEDRIN SÁNCHEZ ARIAS
FACULTAD	FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS	INGENIERÍA DE SISTEMAS
DIRECTOR	YESENIA ARENÍZ ARÉVALO
TÍTULO DE LA TESIS	DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA MUNICIPAL DE RÍO DE ORO, CESAR

RESUMEN

(70 palabras aproximadamente)

EN EL PRESENTE PROYECTO SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA MUNICIPAL DE RÍO DE ORO (CESAR), CON EL OBJETIVO DE PROTEGER LA INFORMACIÓN Y DEMÁS ACTIVOS IMPORTANTES PARA ESTA, MEDIANTE LA IMPLEMENTACIÓN DE ESTA GUÍA, QUE INCLUYE LAS MEDIDAS DE SEGURIDAD NECESARIAS QUE CONTRIBUIRÁN A MANTENER LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LOS DATOS, A TRAVÉS DE LA REALIZACIÓN DE SUS LABORES DIARIAS.

CARACTERÍSTICAS

PÁGINAS: 319	PLANOS:	ILUSTRACIONES:	CD-ROM: 1

DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA MUNICIPAL DE RÍO DE ORO, CESAR

KATHEDRIN SÁNCHEZ ARIAS

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
OCAÑA
2014

DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA MUNICIPAL DE RÍO DE ORO, CESAR

KATHEDRIN SÁNCHEZ ARIAS

Trabajo de Grado presentado para optar al título de Ingeniero de Sistemas

Directora
Yesenia Areníz Arévalo
Especialista en Auditoria de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
OCAÑA
2014

RESUMEN

En el presente proyecto se establecen las Políticas de Seguridad de la Información para la Alcaldía Municipal de Río de Oro (Cesar), con el objetivo de proteger la información y demás activos importantes para esta, mediante la implementación de esta guía, que incluye las medidas de seguridad necesarias que contribuirán a mantener la integridad, confidencialidad y disponibilidad de los datos, a través de la realización de sus labores diarias.

AGRADECIMIENTOS

A Dios por ser quien me da la fortaleza espiritual para enfrentar cada día nuevos retos y haberme permitido culminar con éxito esta etapa de mi vida. Guiando mis pasos por el sendero de la sabiduría.

A mi Madre por haberme brindando la oportunidad de ser una profesional. Por impulsarme día a día con sus consejos.

Debo agradecer de manera especial y sincera a la Esp. Yesenia Areníz Arévalo, por el gran apoyo que me brindó a lo largo de la realización de este proyecto. Por haberme transmitido una gran confianza y orientación en mí trabajo.

Al Alcalde Manuel Rodolfo Márquez Páez y a los funcionarios de la Alcaldía Municipal de Río de Oro (Cesar), por permitir el buen desarrollo de este proyecto.

A mis docentes por la sabiduría y el conocimiento otorgado durante estos años.

A mis compañeros de carrera por ser amigos a lo largo de este gran camino, aprendiendo mutuamente.

Gracias a todos.

KATHEDRIN SÁNCHEZ ARIAS

DEDICATORIA

A mis Madre Aida Lucia Arias Portillo, por el apoyo incondicional en todo momento y en cada etapa de mi vida, por su constancia y dedicación, por ser un ejemplo a seguir. Gracias a sus enseñanzas que me han ayudado en mi crecimiento personal y profesional.

A mis hermanos Karen Yulisa Sánchez Arias y Luis Gustavo Sánchez Arias, por demostrarme siempre que son mi fuerza para superar todos los obstáculos y salir adelante por ellos.

A mi marido Andrés Alfonso Pacheco Solano, por compartir esta inmensa alegría conmigo y apoyarme en todo momento.

KATHEDRIN SÁNCHEZ ARIAS

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

La seguridad informática siempre ha sido necesaria, desde los inicios de los computadores, pero ahora se ha agudizado más la importancia de contar con buenos mecanismos de seguridad debido a que los riesgos y amenazas que no solamente se presentan desde el área física, sino que ahora también existen riesgos de robo o accesos no autorizados a información mediante las diferentes redes que interconectan a los computadores o a cualquier equipo tecnológico utilizado para transmitir información digital.

Aunque muchas entidades públicas y privadas le restan valor al aspecto de seguridad, no se puede dudar que las pérdidas por la falta de seguridad pueden ser realmente caras, tanto en materia económica como en cuanto a prestigio, problemas legales, entre otros.

En vista de la importancia que tiene la seguridad en las tecnologías de la información, no es suficiente estudiar buenas prácticas y consejos sabios de personas que llevan una gran trayectoria en el área de la informática, sino que más aún, Normas Internacionales, son un beneficio de grandes magnitudes para cualquier organización con necesidades relacionadas con la seguridad de las tecnologías de la información, mediante la implementación de acciones y procedimientos necesarios que garanticen la confidencialidad, integridad y disponibilidad de la información.

Pero aunque ningún conjunto de controles puede lograr la seguridad completa, sí es posible reducir al máximo los riesgos que amenacen con afectar la seguridad en una organización, por lo que no pueden quedar estáticos para siempre, sino que por el contrario, tienen que ser continuamente revisados y actualizados para que se mantengan en condiciones favorables y en concordancia con los cambios tecnológicos o cualquier tipo de cambio que se dé a través del tiempo.

La determinación de estos controles debe realizarse de forma particular por cada organización, aprobado por la administración y luego publicado y comunicado a todo el personal y las partes externas relevantes.

Pero antes de la creación de estos, se deberá realizar un análisis de riesgos y controles actualmente aplicados, que definirán los lineamientos a implementar, para minimizar los riesgos a los cuales se encuentra expuesta la información en la actualidad.

Con el presente proyecto se pretende establecer una Política de Seguridad de la Información para la Alcaldía Municipal de Río de Oro (Cesar), compuesta de una serie de lineamiento de implementación, que contiene una clara definición de seguridad de la información, sus objetivos y alcances generales, importancia, intención de la administración en cuanto al tema de seguridad de la información, estructuras de evaluación y gestión de riesgos, definición de las responsabilidades individuales en cuanto a la seguridad, entre otras. Determinando un alto compromiso de la Alcaldía con el proceso de gestión responsable de su información.

1. DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA MUNICIPAL DE RÍO DE ORO (CESAR).

1.1PLANTEAMIENTO DEL PROBLEMA

EL Municipio de Río de Oro está divido territorialmente en doce (12) corregimientos, que integran 48veredas. Se localiza al SUR del Departamento del Cesar, tiene una extensión aproximada de 613.3 Km^2, área que corresponde a 661.330 hectáreas; con coordenadas geográficas; Latitud Norte, 8° 17´ 40"Longitud Oeste a 73° 23´ 18"de Greenwich. Limita al NORTE; con el Departamento del Norte de Santander y el Municipio de González, por el SUR; con el Municipio de San Martín, los Departamentos del Norte de Santander y Santander del Sur, al ORIENTE; con la Provincia de Ocaña, perteneciente al Departamento del Norte de Santander, al OCCIDENTE; con el Municipio de Aguachica. Su consolidación como Municipio se cumple en el año de 1.658.

El municipio de Río de Oro avanzará en la garantía de derechos a niños, niñas y adolescentes, haciendo extensivas las acciones y programas a todos los grupos poblacionales urbano y rurales, con un enfoque inclusivo, diferencial, con equidad de género y participativo; promoviendo la convivencia; la sana recreación y el deporte y mejorando la prestación de servicios de salud y educación. Debido a que la Alcaldía Municipal de Río de Oro (Cesar) maneja la información referente a su Filosofía Institucional, Trámites y Servicios, Planeación de Planes, Programas y Proyectos, Presupuesto y Finanzas, Participación, Atención a la Ciudadanía, Contratación, Normatividad, Inventario de Bienes Inmuebles, entre otros, y se halla interconectada a la red de Internet por medio de su aplicación web.

La Alcaldía Municipal de Río de Oro (Cesar), como toda institución maneja gran cantidad de información confidencial. En algunas oportunidades, no se tiene la certeza del grado de seguridad que manejan los sistemas informáticos, lo que puede generar una mala imagen institucional, inconsistencias y pérdida de activos.

Además, en una encuesta aplicada a la secretaria del alcalde del municipio, se dedujo que la falta de cultura organizacional por parte del personal podría poner en riesgo los recursos de información y la tecnología, frente a amenazas, internas o externas, deliberadas o accidentales. (Ver Anexo A)

1.2 FORMULACIÓN DEL PROBLEMA

¿Un conjunto de políticas de seguridad de la información constituirá un instrumento que le facilite a la Alcaldía Municipal de Río de Oro (Cesar), la protección, conservación y buen uso de la información y los recursos tecnológicos?

1.3 OBJETIVOS DEL ESTUDIO

1.3.1 Objetivo General.

Diseñar las Políticas de Seguridad de la Información para la Alcaldía Municipal de Río de Oro (Cesar).

1.3.2 Objetivos Específicos.

- Realizar un reconocimiento dela estructura organizacional, el direccionamiento estratégico y componente tecnológico de la Alcaldía Municipal de Río de Oro (Cesar).

- Evaluar las normas COBIT 4.1, ITIL v3 e ISO/IEC 27002 y mediante un cuadro comparativo determinar cuál es la más pertinente para el establecimiento de las Políticas de Seguridad de la Información en la Alcaldía Municipal de Río de Oro (Cesar).

- Proponer un Manual de las Políticas de Seguridad de la Información para la Alcaldía Municipal de Río de Oro (Cesar) con base a la norma seleccionada.

- Redactar un Artículo donde se expongan la tabulación de resultados de las encuestas aplicadas en la Alcaldía de Río de Oro (Cesar).

1.4 JUSTIFICACIÓN

Cada día es mayor la importancia de la información, especialmente relacionada con sistemas basados en el uso de tecnologías de la información y comunicaciones, por lo que el impacto de los fallos, los accesos no autorizados, la divulgación de la información, y otras incidencias, tienen un impacto mucho mayor que hace unos años.

Las políticas y estándares de Seguridad de la Información tienen como objetivo establecer medidas técnicas, de organización de las tecnologías de información y de las personas que interactúan haciendo uso de los servicios informáticos que proporciona la Alcaldía Municipal de Río de Oro (Cesar), contribuyendo con la mejora y complimiento de metas institucionales. Además, el tener en claro el diseño de las políticas de seguridad de la información, permite que esta no se pierda, no se altere, esté segura y disponible cuando se le requiera, para el correcto y normal funcionamiento de las actividades que se realizan en la Alcaldía, dando así una mayor credibilidad y confianza a todos los usuarios.

Es por lo anterior que se plantea el diseño de las políticas de seguridad de la información para la Alcaldía municipal de rio de oro, ya que la seguridad de la información y el estudio de amenazas de riesgos de la información proporcionan ventajas para implantar procedimientos, métodos y controles con el objeto de administrar, proteger y salvaguardar uno de los activos más importantes, como es la información. También repercute en el uso de recursos de hardware y el acceso controlado a las necesidades del usuario para cumplir

eficientemente con sus actividades. Una política de seguridad de la información es una forma de comunicarse con los usuarios, pues las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la Institución.

Con la aplicación de la identificación de riesgos en la Alcaldía y una propuesta de seguridad en la información, se evaluaron las prácticas de seguridad informática dentro de ella, la cual llegaron a obtener el control total de la información y se crearon la responsabilidad de cada persona que la manipula, de lo anterior existe un sentido de conciencia del funcionamiento adecuado dela Alcaldía, el cual permite el control de los datos de ésta.

1.5 HIPÓTESIS

Con el establecimiento de las políticas de seguridad de la información se logrará minimizar los factores de riesgo para la Alcaldía Municipal de Río de Oro (Cesar).

1.6 DELIMITACIÓN DEL PROBLEMA

1.6.1 Geográficas. Este proyecto se desarrolló en la Alcaldía Municipal de Río de Oro (Cesar).

1.6.2 Temporal. El proyecto de investigación se llevó a cabo en un lapso de 5 meses en donde se desarrollaron paso a paso los objetivos propuestos.

1.6.3 Conceptual. Los conceptos que se manejaron en esta investigación se relacionaron con la Seguridad de la Información, Políticas de Seguridad, Riesgos y Amenazas en la Información, Incidencias, Controles.

1.6.4 Operativa. Este documento sobre las Políticas de Seguridad de la Información es de voluntaria aplicación para todos los funcionarios, proveedores y personal externo que desempeñen labores o le proporcionen algún tipo de servicio o producto a la Alcaldía Municipal de Río de Oro (Cesar).

2. MARCO REFERENCIAL

2.1 MARCO HISTÓRICO

2.1.1 Reseña Histórica del Municipio de Río de Oro (Cesar). No se tiene una fecha clara y precisa sobre la fundación del Sitio de Río de Oro, como en un inicio fue denominado, pero según historiadores se cree que comenzó a ser poblado desde 1658 a raíz de la llegada del sagrado lienzo de la Virgen del Rosario, donado por encomenderos españoles a la orden de los Agustinos Calzados cuyo claustro y capilla quedaba precisamente en lo que hoy es el Convento de los Agustinos (patrimonio departamental) y la Iglesia Nuestra Sra. del Rosario respectivamente en el parque principal del municipio.

Se sostiene que los primeros encomenderos en hacer su aparición en estas tierras fueron: Mateo Corzo, Juan de Gálvez Caballero y Catalina Gálvez de Caballero. Quienes donaron tierras; también se habla de Luis Téllez Blanco y Gaspar Barbosa de Marín Pedroso, herederos del sagrado lienzo y quienes lo donaron a la orden religiosa.

Se habla entonces de construcción o poblamiento más no de fundación. Y como a partir de la llegada de la virgen el 1º. De Agosto de 1658 se comenzaron a construir las primeras casas alrededor de la ermita, se tomó como referencia esta fecha para celebrar los cumpleaños del municipio.

Sellada la independencia de la Nueva Granada en 1819 y formada la Gran Colombia es cuando el organizador civil de la República, el General Francisco de Paula Santander designa como su primer alcalde a Don Rafael Antonio de los Dolores Patiño en el año de 1820. Desde entonces ha sufrido varias transformaciones político-administrativas así:

- 1849: por medio de la Ley 64 del 29 de mayo, se denomina Distrito Parroquial Río de Oro, perteneciente a la provincia de Ocaña.

- 1857: pasa a la provincia de Mompox y luego al estado del Magdalena.

- 1868: la Ley 142 crea el departamento del Banco con capital Río de Oro.

- 1910: Entra a conformar el departamento del Magdalena.

- 1867: El 21 de diciembre, se convierte en municipio del nuevo departamento del Cesar.

El 1º. De Agosto de cada año, Río de Oro celebra su poblamiento.

A Nivel Internacional.

2.1.2 Políticas de Seguridad Informática a través de la Oficina de Gobierno Electrónico e Informático. Presidencia del Consejo de Ministros. Lima, Perú 2013. La implementación de políticas de seguridad informática impulsadas por la Presidencia del

Consejo de Ministros, a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), ha permitido que muchas entidades del Estado de Perú se desarrollen con una visión de corto, mediano y largo plazo. El Gobierno Electrónico implica la innovación en la reforma del Estado, el uso de la tecnología para agilizar procesos, fomentar la competitividad del país y acercar servicios a los ciudadanos. De igual forma, involucra el impulso de la Sociedad de la Información. Además se logrará que se incluyan a los gobiernos regionales y locales dentro de esta política que persigue la utilización de las herramientas digitales para el logro de los objetivos nacionales. Esta medida debe incluir el uso de las nuevas tecnologías de la información[1].

2.1.3 Reglamento sobre Seguridad Informática. Ministerio de la Informática y las Comunicaciones. La Habana, Cuba 2012. El presente Reglamento tiene por objeto establecer los principios, criterios y requerimientos de Seguridad Informática que garanticen la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce y conserva mediante el uso de las tecnologías de información, siendo el Jefe máximo de cada entidad pública el responsable del cumplimiento de todo lo que en él se dispone[2].

A Nivel Nacional.

2.1.4 Política de Seguridad de la Información para la Alcaldía de Bucaramanga. Santander, Colombia. La Alcaldía de Bucaramanga, para el cumplimiento de su misión, visión, objetivo estratégico y apegado a sus valores corporativos, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

Minimizar el riesgo en las funciones más importantes de la entidad, cumplir con los principios de seguridad de la información, cumplir con los principios de la función administrativa, mantener la confianza de sus usuarios y servidores públicos, apoyar la innovación tecnológica, implementar el Plan de Copias de seguridad de la información, proteger los activos tecnológicos, establecer las políticas, procedimientos e instructivos en materia de seguridad de la información, fortalecer la cultura de seguridad de la información en los servidores públicos, practicantes y usuarios de la administración municipal y garantizar la continuidad de los procesos de la administración frente a incidentes de la plataforma tecnológica[3].

2.1.5 Modelo Política de Seguridad de la Información del Municipio de Sotaquirá. Boyacá, Colombia. La Alcaldía de Sotaquirá ha decidido definir, implementar, operar y

[1] PRESIDENCIA DEL CONSEJO DE MINISTROS DE PERU. Políticas de Seguridad Informática a través de la Oficina de Gobierno Electrónico e Informático. Lima. Perú. 2013. 15h. [en línea]. http://www.enterese.net/entidades-del-estado-se-modernizan-con-politicas-de-seguridad-informatica/

[2] MINISTERIO DE LA INFORMATICA Y LAS COMUNICACIONES. Reglamento sobre Seguridad Informática. La Habana. Cuba. 2012. 15h. [en línea]. http://fcmfajardo.sld.cu/seguridad_informatica/resol_y_dispos_del_mic/reglamento_seguridad_informatica.pdf

[3] ALCALDÍA MUNICIPAL DE BUCARAMANGA. Política de Seguridad de la Información para la Alcaldía de Bucaramanga. Bucaramanga. Colombia. 2012. 3h. [en línea]. http://www.bucaramanga.gov.co/documents/Politica_de_Seguridad_de_la_Informacion.pdf

mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros, alineados a las necesidades de la Entidad, y a los requerimientos regulatorios. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores o terceros[4].

2.1.6 Políticas de Seguridad de la Información para la Alcaldía de Floridablanca. Santander, Colombia. Consciente de sus necesidades actuales, la Alcaldía de Floridablanca Implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales y regulatorios vigentes[5].

A nivel Regional.

2.1.7 Políticas de Seguridad de la Información para el Sitio Web de la Alcaldía Municipal de Mutiscua, Norte de Santander, Colombia 2009. Definir los lineamientos para la implementación efectiva de las políticas y estándares asociados, como la política de actualización del sitio Web (donde deberán estar involucradas las diversas áreas, direcciones y/o programas de la entidad), política de uso aceptable delos Servicios de la Red y de Internet, política de servicio por medios electrónicos, política de privacidad y condiciones de uso y política de seguridad del sitio Web entre otros[6].

2.1.8 Política de Actualización de Contenidos del Portal Web www.durania-nortedesantander.gov.co, como una iniciativa por parte de la Estrategia de Gobierno en Línea. Durania, Norte de Santander, Colombia. Con el objetivo de optimizar el acceso a la información y reglamentar su uso en todos los niveles que conforman la página web del Municipio de Durania se trazó esta Política Editorial (son características que deben considerar las entidades al momento de publicar contenidos en medios electrónicos), que está orientada a lograr un manejo adecuado de la información, la actualización de la misma y la prestación de un servicio mucho más ágil y adecuado para los ciudadanos. La actualización, manejo y publicación de contenidos estará a cargo del Líder de Gobierno en Línea designado por el Alcalde Municipal y bajo la supervisión del Comité Territorial de Gobierno en Línea, del Municipio de Durania[7].

---

[4] ALCALDÍA MUNICIPAL DESOTAQUIRÁ. Modelo Política de Seguridad de la Información del Municipio de Sotaquirá. Sotaquirá, Colombia. 2009. 3h. [en línea]. http://sotaquira-boyaca.gov.co/apc-aa-files/32383063636332366139383566353635/politica-de-seguridad-de-la-informacin-sotaquir.pdf

[5] ALCALDÍA MUNICIPAL DE FLORIDABLANCA. Políticas de Seguridad de la Información para la Alcaldía de Floridablanca. Floridablanca. Colombia. 2013. 3h. [en línea]. http://floridablanca.gov.co/wp-content/uploads/2013/06/POLITICA-DE-LA-SEGURIDAD-DE-LA-INFORMACION-1.pdf

[6] ALCALDÍA MUNICIPAL DE MUTISCUA. Políticas de Seguridad de la Información para el Sitio Web de la Alcaldía Municipal de Mutiscua, Mutiscua. Colombia. 2009. 6h. [en línea]. http://mutiscua-nortedesantander.gov.co/apc-aa-files/63366536346631323039323934613532/DECRETO_N__28_DE_09_NOVIEMBRE_DE_2009.pdf

[7] ALCALDÍA MUNICIPAL DE DURANIA. Política de Actualización de Contenidos del Portal Web www.durania-nortedesantander.gov.co, como una iniciativa por parte de la Estrategia de Gobierno en Línea.

A nivel Local.

2.1.9 Plan de Acción Municipio de Ocaña. Norte de Santander, Colombia. Frente a los compromisos de la implementación de la Estrategia Gobierno en línea la Alcaldía Municipal de Ocaña, teniendo en cuenta: "La metodología para la elaboración de diagnósticos para la implementación de la estrategia de gobierno en línea" (dirección de articulación y gestión) programa gobierno en línea, ha efectuado las siguientes disposiciones previas al acompañamiento y capacitación para el cumplimiento de la fase de información y el avance en la fase de interacción:

1. Actualización del sitio web, con el fin de brindar información actualizada a la comunidad.

2. Publicitar el sitio web Municipal a través de diferentes mecanismos de socialización, para dar a conocer el municipio a nivel Nacional e
Internacional.

3. Dinamizar el turismo del municipio, por medio del aprovechamiento del sitio web, como medio para dar a conocer los diferentes atractivos turísticos, gastronómicos y culturales[8].

2.2 MARCO CONTEXTUAL

El desarrollo de la investigación se llevó a cabo en la Alcaldía Municipal de Rio de Oro (Cesar) Colombia, donde se estudió el modelo de negocio de los procesos de la misma, su estructura orgánica, sus recursos informáticos y de software, y se realizó el Manual de las Políticas de Seguridad de la Información.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades, importante ayuda para la gestión de las actividades de la Alcaldía.

En la gestión efectiva de la seguridad, toma parte activa toda la Alcaldía apoyada por su máximo representante, tomando en consideración también a los habitantes y visitantes. El modelo de gestión de la seguridad contempla políticas y procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.
El Sistema de gestión de seguridad de la información (SGSI) ayudo a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la Alcaldía, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia Alcaldía ha decidido asumir.

Durania, Colombia. 2009. 18h. [en línea]. http://durania-nortedesantander.gov.co/apc-aa-files/33666536313963356239323539346563/Politica_Editorial_Sitio_Web.pdf

[8] ALCALDÍA MUNICIPAL DE OCAÑA. Plan de Acción Municipio de Ocaña. Ocaña. Colombia. 2010. 17h. [en línea]. http://ocana-nortedesantander.gov.co/apc-aa-files/61643230666336653165633566373234/Plan_de_Accion_GEL___si_Oca_a__.pdf

Con un sistema SGSI, la Alcaldía conoce los riesgos a los que está sometida su información y activos y los asume, minimiza, transfiere o controla mediante una metodología definida, documentada y conocida por todos, que se revisa y mejora constantemente.

La línea de investigación de Gobernabilidad de TI, tiene establecido un macro proyecto titulado: "Establecimiento de criterios de Gobernabilidad de TI en las empresas Colombianas", el cual se está trabajando para el contexto de Norte de Santander, en su parte inicial Ocaña y la Provincia, por sectores de empresas.

Actualmente existe la necesidad de crear un ámbito de evaluación y seguimientos de los procesos y la seguridad de la información; con miras al mejoramiento de la calidad y las buenas prácticas en la realización de los procesos de las empresas, se busca determinar el grado de madurez en que se encuentra las diferentes dependencias para así medir y realizar un autoanálisis de cómo se están realizando los procesos, un estudio del nivel de madurez a las tecnologías de información permitirá definir donde debe estar, estableciendo oportunidades de mejora y optimización de los procesos alineándolos con las estrategias y objetivos de la empresa y con los requerimientos, permitiendo establecer pautas para tomar decisiones en cuanto a la inversión necesaria para avanzar y lograr el grado de madurez deseado. La finalidad del proyecto consisto en incorporar prácticas de buen gobierno de TI, en el sector educativo y público en el caso específico la Alcaldía Municipal de Rio de Oro (Cesar) y de este modo contribuir con la línea de investigación Gobernabilidad de TI que se viene desarrollando en la Especialización de Auditoria de Sistemas de la UFPSO[9].

2.3 MARCO CONCEPTUAL

Para propósitos de este proyecto, se aplican los siguientes términos y definiciones.

Acceso autorizado: Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

Acceso lógico: Provee medios técnicos para controlar la información que los usuarios pueden utilizar, los programas que pueden ejecutar y las modificaciones que pueden hacer. Los controles pueden estar en el sistema operativo, aplicaciones, bases de datos, o dispositivos de red.

Acceso físico: Restringen la entrada y salida de personal, equipos y medios de áreas como edificios, centros de datos o cuartos de servidores.
Activo: Cualquier cosa que tenga valor para la organización.

Activo de Información: Corresponde a elementos tales como bases de datos, documentación, manuales de usuarios, entre otros[10].

[9] PACHECO SOLANO, Andrés Alfonso y TORO RUEDA, Mileidy. Políticas de Seguridad de la Información para la Unidad de Almacén de la Universidad Francisco de Pula Santander Ocaña. Ocaña, Colombia. 2013. 232h. Trabajo de grado (Profesional en Ingeniería de Sistemas). Universidad Francisco de Pula Santander Ocaña. Facultad de Ingenierías.
[10] UNIVERSIDAD LIBRE. Acuerdo No. 05 (Noviembre 17 de 2009). Colombia. 2009. 85h. [en línea]. http://www.unilibre.edu.co/images/pdf/acd_05-09.pdf

Amenaza: Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información. Pueden ser de origen externo (agresiones técnicas, naturales o humanos) o de origen interno (negligencia del propio personal o las condiciones técnicas, procesos operativos internos).Generalmente se distingue y divide tres grupos: a) Criminalidad, b) Sucesos de origen físico, c) Negligencia y decisiones institucionales[11].

Análisis de Riesgos: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Auditoria: Examinar de forma independiente los log's del sistema y actividades para comprobar la eficiencia y controlar la integridad de los datos.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Autorización: Garantizar que todos los accesos a datos y/o medios, cumplan con los niveles de autorización correspondientes para su utilización y divulgación.

Backup's: Son copias de respaldo o de seguridad del sistema o de los datos, que puede ser utilizada en caso de producirse un fallo generalizado, caída del sistema, o el daño o eliminación accidental de archivos. Gracias a la información contenida en el Backup's, se podrá restaurar el sistema al estado en que se encontraba en el momento de realizar la copia de seguridad.

Bitácora: Libro donde se registran las observaciones de un evento.

COBIT: Es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. Una vez implementado, los ejecutivos pueden asegurarse de que sea justa de manera eficaz con los objetivos del negocio y dirigir mejor el uso de TI para obtener ventajas comerciales. COBIT brinda un lenguaje común a los ejecutivos de negocios para comunicar las metas, objetivos y resultados a los profesionales de auditoría, informática y otras disciplinas[12].

[11] ERB, Markus. Gestión de Riesgo en la Seguridad Informática. Amenazas y Vulnerabilidades. España. 3h. [en línea]. http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

[12] GOVERNANCE INSTITUTE, OFICINA GUBERNAMENTAL DE COMERCIO y THE STATIONERY OFFICE. Alineando COBIT 4.1, ITIL V3 e, ISO/IEC 27002 en beneficio del negocio. Estados Unidos e Inglaterra. 2010. 130h. [en línea]. http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf.

Comité de Seguridad de la Información: Es un cuerpo integrado por representantes de todas las áreas sustantivas de la Alcaldía, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

Confidencialidad: es la garantía de que la información sea accesible solo aquellas personas autorizadas a tener acceso a ella.

Contraseña: Conjunto de caracteres que permite el ingreso a un recurso informático.

Controles: Políticas o procedimientos que aplican a una vulnerabilidad.

Control de acceso: Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Comunicación: Transmisión de información desde un equipo a cualquier otro. Para que se pueda realizar una transmisión de información, son necesarios tres elementos: El emisor, quien origina la información; el medio de transmisión: que permite la transmisión de esa información; el receptor: quien recibe la información.
Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Correo electrónico: También conocido como "E-mail". Es un software que puede utilizarse para el envío y recepción de mensajería entre usuarios, entendiendo por mensajería cualquier texto, archivo, programa, etc.

Cortafuegos: Parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Desastre o Contingencia: Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Direccionamiento Estratégico: Conjunto de instrucciones, pautas o criterios establecidos por la Alta Dirección para el logro de los objetivos y metas de la Alcaldía[13].
Disponibilidad: es la garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella cada vez que se requiera.

[13] ALCALDIA MAYOR DE BOGOTA D.C. Direccionamiento Estratégico. Gestión Estratégica y Planes Institucionales. Bogotá. Colombia. 2013. 7h. [en línea].
http://www.patrimoniocultural.gov.co/descargas/nosotros/mapa-de-procesos/DE-P01%20GESTION%20ESTRATEGICA%20Y%20PLANES%20INST.pdf

Estructura organizacional: Puede ser definida como las distintas maneras en que puede ser dividido el trabajo dentro de una organización para alcanzar luego la coordinación del mismo orientándolo al logro de los objetivos.

Filtración de datos: Sucede cuando se compromete un sistema, exponiendo la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, que tratan de adquirir información confidencial que puede utilizarse con fines delictivos o con otros fines malintencionados.

Hardware: El hardware está formado por los componentes físicos. Es la parte "dura", es decir, las partes que configuran la máquina y que le dan una serie de características.

Impacto: Daño potencial sobre un sistema cuando una amenaza se presenta[14].

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que afecta a un sistema de información, a una red, o la violación o inminente amenaza de violación de una política o norma o de seguridad.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Integridad: es la salvaguarda de la exactitud y totalidad de la información y los métodos de procesamiento de la misma.

ISO/IEC 27002: El objetivo del estándar es brindar información a los responsables de la implementación de seguridad de la información de una organización. En él se definen las estrategias de 133 controles de seguridad organizados bajo 11 dominios. La norma subraya la importancia de la gestión del riesgo y deja claro que no es necesario aplicar cada parte, sino sólo aquellas que sean relevantes.

ITIL: La gestión de servicios de TI se refiere a la planificación, aprovisionamiento, diseño, implementación, operación, apoyo y mejora de los servicios de TI que sean apropiados a las necesidades del negocio. ITIL proporciona un marco de trabajo de mejores prácticas integral, consistente y coherente para la gestión de servicios de TI y los procesos relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de TI.

LAN: (Local Área Network): Se refiere a redes de computadoras que no traspasan de un ámbito delimitado por un área física determinada, como por ejemplo un edificio, una compañía, etc.

[14]UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. Modulo Evaluación de la Seguridad de la Información. Ocaña. Colombia. 2012. 65h.

Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

No repudio: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Políticas: Es el conjunto de grandes orientaciones y lineamientos que guían las acciones a desarrollar por la institución, a fin de mejorar su funcionamiento; directrices que se traducen en los objetivos y metas que un sistema se propone alcanzar dentro de un futuro determinado, asociados a la indicación de los medios más generales que deberán ser utilizados para alcanzarlos[15].

Política de Seguridad de la Información: Es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de la Alcaldía, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.

Procedimiento de seguridad: Proporcionan las instrucciones detalladas para llevar a cabo las tareas relacionadas con la seguridad de la información. Los procedimientos tienen un ámbito reducido de actuación y tienen siempre carácter operativo. Los procedimientos complementan los estándares de seguridad aportando la operativa necesaria para cumplirlas.

Proveedor: Persona que provee o abastece a otra persona de lo necesario o conveniente para un fin determinado. Empresa que se dedica a proveer o abastecer de productos necesarios a una persona o empresa.

Recursos informáticos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas académicas y administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Alcaldía.

Redes sociales: Las Redes son formas de interacción social, definida como un intercambio dinámico entre personas, grupos e instituciones en contextos de complejidad. Un sistema abierto y en construcción permanente que involucra a conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos.

Registro: Es una evidencia que permite presentar que se está cumpliendo con lo acordado.

Riesgo: Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización.

[15] MANUAL DE SEGURIDAD. [En línea]. [15 Mayo 2013]. Disponible En: https://euskadi.net/r47-contbp2z/es/contenidos/informacion/bp_segurtasuna/es_dit/adjuntos/MSPLATEA_c.pdf

Routers: Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas.

Seguridad Física: Consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Servidor: Computadora que ejecuta un programa que realiza alguna tarea en beneficio de otras aplicaciones llamadas clientes.

Sistema de información: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Software: El software está compuesto por los programas que dirigen el funcionamiento de un ordenador. Es la "parte lógica" de la máquina que permite enlazar todos los elementos de hardware de la manera más efectiva posible, permitiéndole realizar cualquier tipo de trabajo.

Software malicioso: (malware) Es un término común que se utiliza al referirse a cualquier programa malicioso o inesperado o a códigos móviles como virus, troyanos, gusanos o programas de broma.

Switch: Es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa de enlace de datos, Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro.

Terceros: Persona que es reconocida por ser independiente de las partes involucradas concerniente al tema.

TI: Tecnología de la Información.

UPS: Sistema de alimentación ininterrumpida. Fuente ininterrumpida de energía. Es un dispositivo eléctrico que puede proporcionar energía eléctrica ante un apagón gracias a sus baterías internas que almacenan energía eléctrica.

Usuarios: Se refiere a todos los empleados, proveedores, contratistas, o cualquier otra persona o entidad que por razón de su trabajo se le permita acceso, se le asignen derechos de uso y utilicen los recursos que componen los medios electrónicos de almacenamiento y transmisión de datos.

Virus: Son pequeños programas de computadora cuya principal cualidad es la de poder auto replicarse, está escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este para producir efectos dañinos.

Vulnerabilidades: Es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. Es decir, la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño. Están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño. Puede agrupar en grupos característicos: Ambiental, Física, Económica, Social, Educativa, Institucional y Política.

WAN: (Redes de Área Extensa). Al ampliarse el alcance de las LAN, traspasando las fronteras que delimitan su espacio físico, se convierten en una red de área extensa (WAN). Generalmente se denomina WAN a un conjunto de redes LAN situadas en espacios físicos distantes, que se interconectan entre sí mediante medios de transmisión de datos (enlaces de radio, fibra óptica, microondas, cable, MODEM, etc.).

2.4 MARCO TEÓRICO

Cada organización necesita ajustar la utilización de estándares y prácticas a sus requerimientos individuales.

La creciente adopción de mejores prácticas de TI se explica porque la industria de TI requiere mejorar la administración de la calidad y la confiabilidad de TI en los negocios y para responder a un creciente número de requerimientos regulatorios y contractuales.

Sin embargo, existe el peligro de que las implementaciones de estas mejores prácticas, potencialmente útiles, puedan ser costosas y desenfocadas si son tratadas como guías puramente técnicas. Para ser más efectivos, las mejores prácticas deberían ser aplicadas en el contexto del negocio, enfocándose donde su utilización proporcione el mayor beneficio a la organización. La alta dirección, los gerentes, auditores, oficiales de cumplimiento y directores de TI, deben trabajar en armonía para estar seguros que las mejores prácticas conduzcan a servicios de TI económicos y bien controlados.
Las mejores prácticas de TI posibilitan y soportan:

• Una mejor gestión de TI, lo que es crítico para el éxito de la estrategia de la empresa.

• Un gobierno eficaz de las actividades de TI.
• Un marco de referencia eficaz para la gestión de políticas, controles internos y prácticas definidas, lo que es necesario para que todos sepan lo que hay que hacer.

• Muchos otros beneficios, incluyendo ganancia de eficiencias, menor dependencia de expertos, menos errores, mejora de la confianza de los socios de negocios y de reguladores.

Para lograr el alineamiento de las mejores prácticas con los requerimientos del negocio, se deben utilizar procesos formales que soporten el buen gobierno de TI.

COBIT puede ser utilizado en los más altos niveles de gobierno de TI, proporcionando un marco de referencia global de control basado en el modelo de procesos de TI que el ITGI pretende se pueda adaptar a cada empresa. También hay una necesidad de procesos detallados y estandarizados para profesionales.

El ITGI y la OGC continuarán actualizando sus guías para mejorar el alineamiento de la terminología y el contenido con otros documentos, facilitando la integración y reflejando las mejores prácticas más recientes.

A continuación, una breve descripción ISO/IEC 27002, COBIT y ITIL.

NTC-ISO/IEC 27002, proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios: Política de Seguridad de la Información, Organización de la Seguridad de la Información, Gestión de Activos de Información, Seguridad de los Recursos Humanos, Seguridad Física y Ambiental, Gestión de las Comunicaciones y Operaciones, Control de Accesos, Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, Gestión de Incidentes en la Seguridad de la Información, Gestión de Continuidad del Negocio y Cumplimiento.

COBIT, proporciona las herramientas para dirigir y supervisar todas las actividades relacionadas con las TI, basado en estándares de la industria y las mejores prácticas, puede ajustarse de manera eficaz con los objetivos del negocio y dirigir mejor el uso de TI para obtener ventajas comerciales.

Es un marco de trabajo que organiza la gestión del gobierno de TI, los objetivos de control y las mejores prácticas de los procesos y dominios de TI, y los relaciona con las necesidades del negocio. Contiene un conjunto de 34 objetivos de control de alto nivel, uno para cada proceso de TI, agrupados en cuatro dominios: Planificar y Organizar, Adquirir e Implementar, Entregar y dar soporte, Monitorear y Evaluar.

ITIL, proporciona un marco de trabajo de mejores prácticas integral, consistente y coherente para la gestión de servicios de TI y los procesos relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de TI. El papel de este marco de trabajo es describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas y su roles brindar orientación en el nivel organizacional más bajo que pueda aplicarse. De

manera similar, los procesos de ITIL pueden ser utilizados para lograr y demostrar el cumplimiento con los objetivos de control COBIT[16].

2.5 MARCO LEGAL

2.5.1 Constitución Política de 1991. En los artículos 209 y 269 se fundamenta el sistema de control interno en el Estado Colombiano, el primero establece: "La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley" y en el 269, se soporta el diseño del sistema: "En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas".

2.5.2 Leyes Informáticas Colombianas[17].

2.5.3 Ley estatutaria 1266 del 31 de diciembre de 2008. Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

2.5.4 Ley 1273 del 5 de enero de 2009. Delitos informáticos. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

2.5.5 Ley 1341 del 30 de julio de 2009. Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

2.5.6 Ley estatutaria 1581 de 2012. Entró en vigencia la Ley 1581 del 17 de octubre 2012 de **PROTECCIÓN DE DATOS PERSONALES**, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y

[16] GOVERNANCE INSTITUTE, OFICINA GUBERNAMENTAL DE COMERCIO y THE STATIONERY OFFICE. Alineando COBIT 4.1, ITIL V3 e, ISO/IEC 27002 en beneficio del negocio. Estados Unidos e Inglaterra. 2010. 130h. [en línea]. http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf.

[17] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Gerencia de Innovación y Desarrollo Tecnológico. Última actualización el Lunes, 22 de Abril de 2013 09:05. [en línea]. http://www.unad.edu.co/gidt/index.php/leyesinformaticas

reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

Aspectos claves de la normatividad:

1. Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.

2. Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

3. Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.

4. Crea una especial protección a los datos de menores de edad.

5. Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.

6. Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.

7. Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.

8. Crea el Registro Nacional de Bases de Datos.

9. Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

2.5.7 Ley 603 de 2000. Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

El Derecho de Autor[18].

[18] MINISTERIO DEL INTERIOR Y DE JUSTICIA DE COLOMBIA. Dirección Nacional del Derecho de Autor. Unidad Administrativa Especial. [en línea].
http://www.propiedadintelectualcolombia.com/Site/LinkClick.aspx?fileticket=yDsveWsCdGE%3D&tabid=

2.5.8 Constitución Política de 1991. En su artículo 61, que expresa: "El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley".

2.5.9 Decisión 351 de 1993, o Régimen Común Andino sobre Derecho de Autor y Derechos Conexos. Es de aplicación directa y preferente a las leyes internas de cada país miembro del Grupo Andino.

2.5.10 Ley 23 de 1982. Contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia.

2.5.11 Ley 44 de 1993 (febrero 15). Modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.

2.5.12 DECRETO 1360 DE 1989(junio 23)."Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor".

2.5.13 Decreto 460 de 1995. Por la cual se reglamenta el Registro Nacional de Derecho de Autor.

2.5.14 DECRETO 1474 DE 2002(Julio 15)."Por el cual se promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996)".

2.5.15 Ley 734 de 2002, Numeral 21 y 22 del Art. 34. Son deberes de los servidores Públicos "vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente", y "responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización"[19].

2.5.16 Habeas Data. Tiene por objeto desarrollar el derecho constitucional que tienen todas las persona a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

[19] SUPERINTENDENCIAS DE SOCIEDADES. Manual Manejo y Control Administrativo de los Bienes de Propiedad. Bogotá D.C., Colombia, 2009. 29h. [en línea].
http://www.supersociedades.gov.co/web/Ntrabajo/SISTEMA_INTEGRADO/Documentos%20Infraestructura/DOCUMENTOS/GINF-M-001%20MANUAL%20ADMINISTRATIVO.pdf

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

Para llevar a cabo el presente proyecto se utilizó el tipo de estudio descriptivo y aplicativo. La investigación aplicada se identifica porque busca la aplicación o utilización de los conocimientos que se adquieren, en este caso en la aplicación del marco conceptual de seguridad de la información en la Alcaldía Municipal de Rio de Oro (Cesar). El otro tipo de investigación que se utilizará será descriptiva, ya que los estudios descriptivos utilizan el método de análisis para lograr caracterizar un objeto de estudio o una situación concreta, señalar sus características y propiedades, combinada con ciertos criterios de clasificación, sirve para ordenar, agrupar o sistematizar los objetos propuestos.

3.2 POBLACIÓN Y MUESTRA

3.2.1 Universo. Para este proyecto, el universo lo conformaron la comunidad del Municipio de Río de Oro (Cesar), con 14.300 habitantes de los cuales el 40% equivalente al área urbana y el 60% restantes al área rural.

3.2.2 Población. La población la conformaron todos los empleados que hacen parte del organigrama de la Alcaldía de Rio de oro, es decir 31 personas distribuidas entre empleados de planta y OPS.

3.2.3 Muestra. Es una parte de la población, que reúne todas las condiciones o características de la población objetivo, para determinar el direccionamiento estratégico de la Alcaldía. Para el caso se tomó como muestra el 67% de la población involucrada en el proceso, que equivale a 21 de los funcionarios que laboran en la Alcaldía, de los cuales 13 son empleados de planta y 8 son empleados OPS.

3.3 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

3.3.1 Técnicas de Recolección. Las técnicas e instrumentos de recolección empleados para la obtención de la información necesaria para el desarrollo del proyecto, fueron la observación, la encuesta y la revisión documental.

La observación directa permitió obtener información clara y precisa, a partir del detalle en tiempo real de los hechos y situaciones sociales, que se presentan y llevan a cabo normalmente en la Alcaldía.

La encuesta, está compuesta de un cuestionario, que contiene una serie de preguntas enfocadas al manejo de la información, en cuya formulación se observa el problema que se deseó estudiar. A través de ellas se especifican los requerimientos del presente proyecto y fueron aplicadas a los funcionarios de la Alcaldía Municipal de Río de Oro (Cesar), con el propósito de hallar posibles soluciones. (Ver anexos)

Con el apoyo de la revisión documental se consultaron textos e información en línea (consultas de sitios y páginas Web) con la finalidad de ampliar los conocimientos necesarios para alcanzar los objetivos propuestos y definir el marco teórico.

3.4 ANALISIS DE LA INFORMACION RECOLECTADA

Los resultados de las encuestas se tabularon, se graficaron y se analizaron cuantitativa y cualitativamente de acuerdo a los resultados, tomando solo la información relevante que contribuyo al buen desarrollo y ejecución de este proyecto, con la finalidad de ser base a la construcción de conocimiento a personas que en un futuro utilicen este proyecto como guía para el Diseño de Políticas de Seguridad de la Información.

Tomando como referencia los resultados obtenidos en la encuesta preliminar realizada a la secretaria del Alcalde Municipal para el inicio del proyecto, se detallan los aspectos esenciales para el diseño y la creación de las políticas de seguridad de la información a utilizar. En esta fase se plantearon alternativas de solución al problema detectado, analizando la situación actual de la Alcaldía Municipal de Río de Oro (Cesar) y tomando en cuenta los recursos con los que se cuenta. (Ver Anexo A)

A continuación se muestran los resultados obtenidos de esta encuesta.

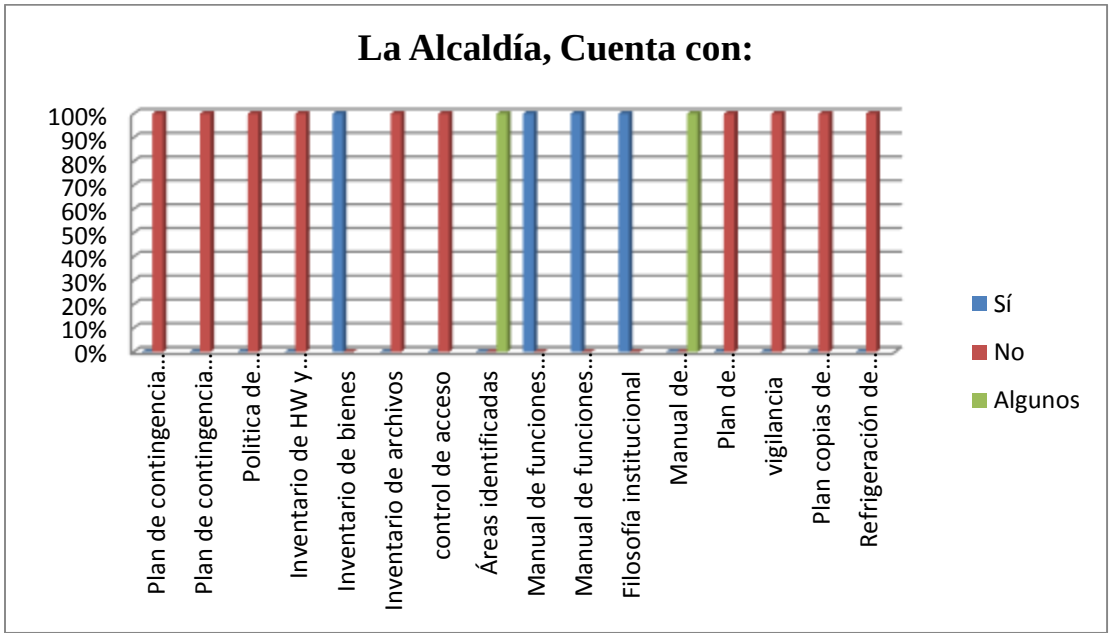
Tabla 1. La Alcaldía de Río de Oro, cuenta con:

	FRECUENCIA				**PORCENTAJE**			
	Sí	**No**	**Alguno**	**Total**	**Sí**	**No**	**Alguno**	**Total**
Plan de contingencia para eventualidad natural	0	1	0	**1**	0%	100%	0%	**100%**
Plan de contingencia para eventualidad criminal	0	1	0	**1**	0%	100%	0%	**100%**
Política de privacidad y confidencialidad de sus empleados	0	1	0	**1**	0%	100%	0%	**100%**
Inventario de hardware y software	0	1	0	**1**	0%	100%	0%	**100%**
Inventario de bienes muebles e inmuebles	1	0	0	**1**	100%	0%	0%	**100%**
Inventario de archivos	0	1	0	**1**	0%	100%	0%	**100%**
Control de acceso a personal, visitantes y demás	0	1	0	**1**	0%	100%	0%	**100%**
Identificación de sus áreas	0	0	**1**	**1**	0%	0%	100%	**100%**

Manual de funciones y competencias del personal de planta	1	0	0	**1**	100%	0%	0%	**100%**
Manual de funciones y competencias del personal OPS	1	0	0	**1**	100%	0%	0%	**100%**
Filosofía institucional	1	0	0	**1**	100%	0%	0%	**100%**
Manual de procedimientos a usuarios	0	0	**1**	**1**	0%	0%	100%	**100%**
Plan de mantenimiento de equipos	0	1	0	**1**	0%	100%	0%	**100%**
Vigilancia en las instalaciones	0	1	0	**1**	0%	100%	0%	**100%**
Plan de copias de respaldo de la información	0	1	0	**1**	0%	100%	0%	**100%**
Sistema de refrigeración para los equipos	0	1	0	**1**	0%	100%	0%	**100%**

Fuente: Autora

Figura 1. La Alcaldía, cuenta con:



Fuente: Autora

La Figura 1. Muestra que la Alcaldía cuenta con inventario de bienes muebles e inmuebles, manual de funciones y competencias del personal de planta, manual de funciones y competencias del personal OPS y filosofía institucional.

Además, no cuenta plan de contingencia para eventualidad natural o criminal, política de privacidad y confidencialidad de sus empleados, inventario de hardware y software, inventario de archivos, control de acceso a personal, visitantes y demás, plan de mantenimiento de equipos, vigilancia en las instalaciones, plan de copias de respaldo de la información, ni sistema de refrigeración para los equipos.

Pero solo algunas de sus áreas se encuentran identificadas y cuenta con algunos manuales de procedimientos a usuarios.

Tabla 2. En su estructura orgánica, ¿Cuenta con personal encargado del área de sistemas?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	0	0%
No	1	100%
Total	**1**	**100%**

Fuente: Autora

Figura 2. Personal de sistemas

Fuente: Autora

Con respecto a la figura 2. La Alcaldía no cuenta con personal encargado del área de sistemas dentro de su estructura orgánica, lo que para el desarrollo de este proyecto es de vital importancia su existencia, pues es directamente responsable de la buena ejecución de políticas de seguridad de la información.

De acuerdo a las encuestas realizadas al personal de la Alcaldía y a la identificación de la norma más pertinente para el establecimiento de las políticas de la seguridad de la Información, se aplicaron encuestas en base a la norma ISO/IEC 27002 seleccionada. (Ver Anexo B)

A continuación se reflejan y detallan los resultados de la investigación anteriormente descrita.

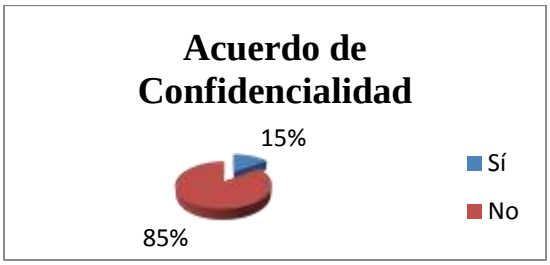
3.4.1 Encuesta de Seguridad de la Información Dirigida al Personal de Planta de la Alcaldía Municipal de Río de Oro (Cesar).

Tabla 3. ¿Cuenta con un acuerdo de confidencialidad de la información?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	2	15%
No	11	85%
Total	**13**	**100%**

Fuente: Autora

Figura 3. Acuerdo de confidencialidad



Fuente: Autora

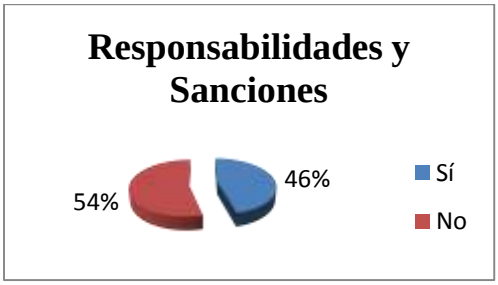
Se observa que el 85% de los empleados de planta de la Alcaldía, no cuenta con un acuerdo de confidencialidad de la información establecido por la administración, mientras el 15% restante sí cuenta con uno, pero solo de forma verbal.

Tabla 4. ¿Tiene usted conocimiento de sus responsabilidades y sanciones, frente a la seguridad de la información?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	6	46%
No	7	54%
Total	**13**	**100%**

Fuente: Autora

Figura 4. Responsabilidades y sanciones.



Fuente: Autora

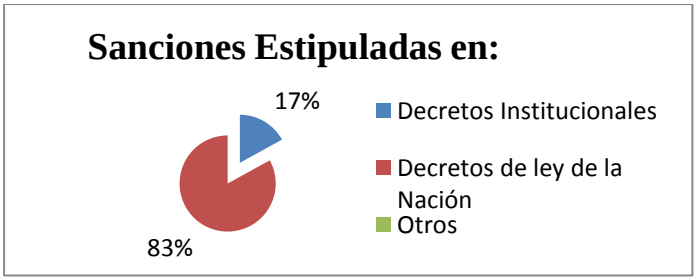
De los encuestados el 54%, no tiene conocimiento de sus responsabilidades y sanciones, frente a la seguridad de la información, lo que se analizaría como un alto porcentaje de riesgos que afectarían gravemente la gestión de la seguridad de la información.

Tabla 5. Estas sanciones se encuentra estipuladas en:

RESPUESTA	FRECUENCIA	PORCENTAJE
Decretos o resoluciones institucionales	1	17%
Decretos de ley de la nación	5	83%
Otros	0	0%
Total	**6**	**100%**

Fuente: Autora

Figura 5. Sanciones estipuladas en:



Fuente: Autora

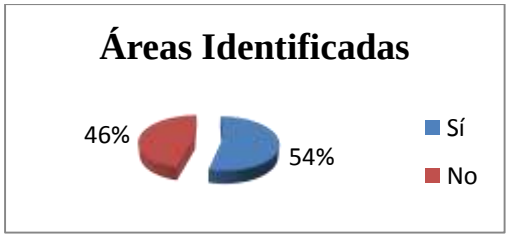
De la figura 5. Se interpreta que: El 83% de los empleados que tiene conocimiento de sus responsabilidades y sanciones, afirman que se encuentran estipuladas en Decretos de Ley de la Nación, a diferencia del 17% que afirma se encuentran estipuladas en Decretos o resoluciones Institucionales, y el 0% opinan que se estipulan en otros Documentos.

Tabla 6. ¿El área en la cual labora, se encuentra debidamente identificada?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	7	54%
No	6	46%
Total	**13**	**100%**

Fuente: Autora

Figura 6. Áreas identificadas.



Fuente: Autora

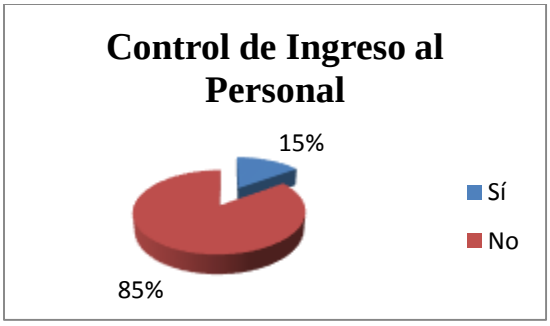
El 54% de los empleados afirma que el área en la cual labora se encuentra debidamente identificada, mientras que el 46% afirma que no lo está, lo que impide que los visitantes identifiquen las áreas y encuentren la que buscan.

Tabla 7. ¿Su área cuenta con controles de ingreso al personal?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	2	15%
No	11	85%
Total	**13**	**100%**

Fuente: Autora

Figura 7. Control de ingreso al personal.



Fuente: Autora

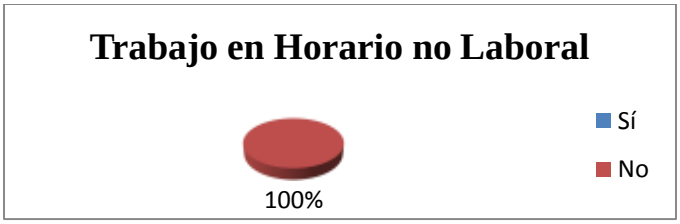
En lo relacionado con el control de Ingreso al Personal en las áreas en las cuales laboran los encuestados, el 85% de estás no cuenta con tal control, mientras que el otro 15% de estas áreas si cuenta con dicho control de acceso, es decir, los empleados puede ampliar o disminuir su jornada laboral diaria por sí mismos.

Tabla 8. ¿Se controla el trabajo, fuera del horario laboral definido?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	0	0%
No	13	100%
Total	**13**	**100%**

Fuente: Autora

Figura 8. Trabajo en horario no laboral.



Fuente: Autora

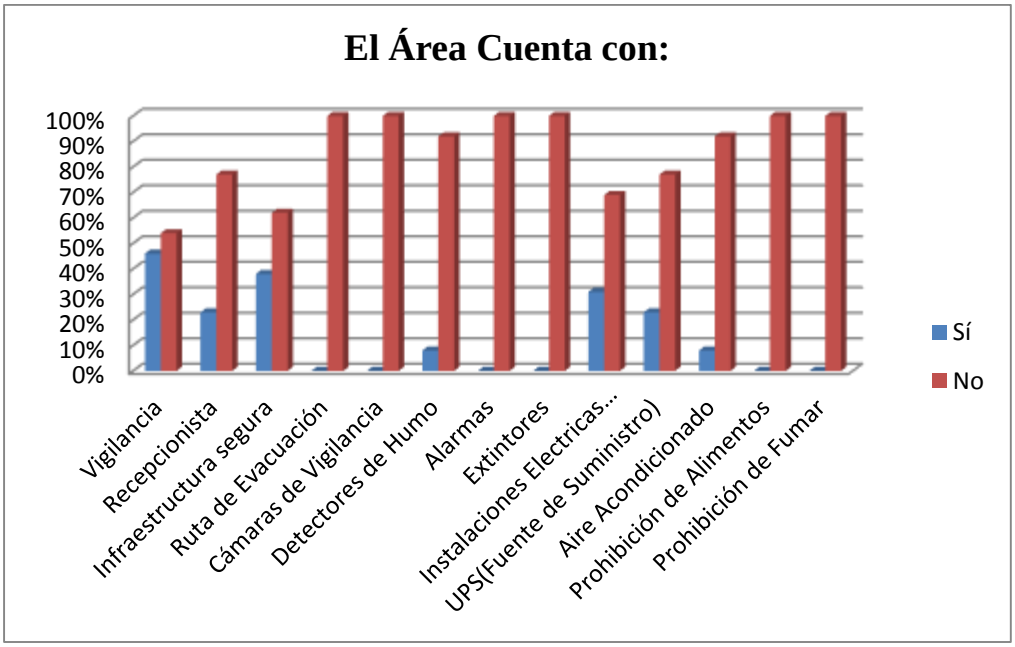
Se muestra en la figura 8, que el 100% de los trabajadores concuerdan en que no se controla su trabajo fuera del horario laboral definido, por la administración.

Tabla 9. El área cuenta con:

	FRECUENCIA			PORCENTAJE		
	Sí	**No**	**Total**	**Sí**	**No**	**Total**
Vigilancia	6	7	**13**	46%	54%	**100%**
Recepcionista	3	10	**13**	23%	77%	**100%**
Infraestructura sólida y segura	5	8	**13**	38%	62%	**100%**
Ruta de Evacuación	0	13	**13**	0%	100%	**100%**
Cámaras de vigilancia	0	13	**13**	0%	100%	**100%**
Detectores de Humo	1	12	**13**	8%	92%	**100%**
Alarmas	0	13	**13**	0%	100%	**100%**
Extintores	0	13	**13**	0%	100%	**100%**
Instalaciones eléctricas ideales	4	9	**13**	31%	69%	**100%**
UPS(Fuentes de suministro eléctrico)	3	10	**13**	23%	77%	**100%**
Aire acondicionado	1	12	**13**	8%	92%	**100%**
Prohibición de Alimentos y bebidas	0	13	**13**	0%	100%	**100%**
Prohibición de Fumar en el área	0	13	**13**	0%	100%	**100%**

Fuente: Autora

Figura 9. El área cuenta con:



Fuente: Autora

La Figura 9. Muestra que el 46% de las áreas, cuenta con vigilancia, mientras que el 23% de estas cuenta con un recepcionista.

Además, solo el 38% de estas áreas son consideradas por los trabajadores como una infraestructura sólida y segura, pero en ninguno de los casos se cuenta con una ruta de evacuación debidamente señalizada.

Las áreas de trabajo de los empleados no cuentan con cámaras de vigilancia, Alarmas o Extintores, y solo el 8% de estas, cuenta con detectores de humo.

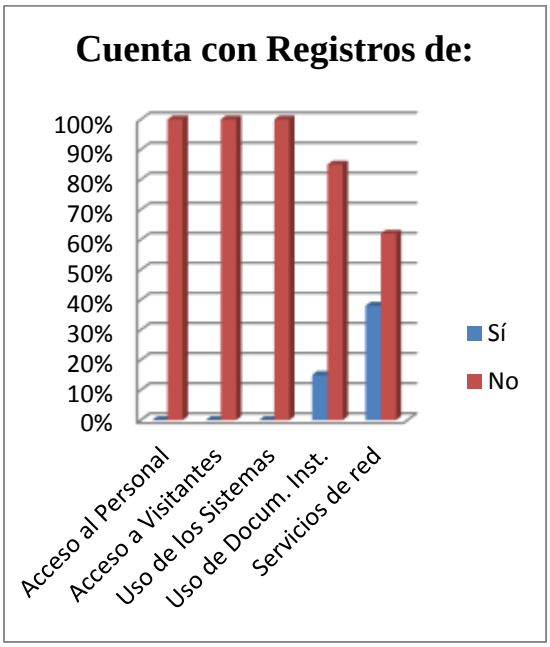
El 31% de las áreas de trabajo, cuentan con instalaciones eléctricas ideales, pero solo el 23% de ellas cuenta con UPS (Fuente de Suministro Eléctrico) y un 8% hace uso de aire acondicionada, mientras que en ninguna de estas se prohíbe el consumo de alimentos y bebidas, además de no prohibirse fumar en las instalaciones.

Tabla 10. Sabe usted si la Alcaldía cuenta con registros de:

	FRECUENCIA			PORCENTAJE		
	Sí	**No**	**Total**	**Sí**	**No**	**Total**
Acceso al personal	0	13	**13**	0%	100%	**100%**
Acceso de visitantes	0	13	**13**	0%	100%	**100%**
Uso de los sistemas	0	13	**13**	0%	100%	**100%**
Uso de documentos institucionales	2	11	**13**	15%	85%	**100%**
Servicios de red	5	8	**13**	38%	62%	**100%**

Fuente: Autora

Figura 10. Cuenta con registros de:



Fuente: Autora

En la figura 10. Se aprecia que la Alcaldía Municipal no cuenta en un 100% con el registro de acceso a sus instalaciones del personal y los visitantes, ni del uso de los sistemas por alguien distinto al empleado en específico.

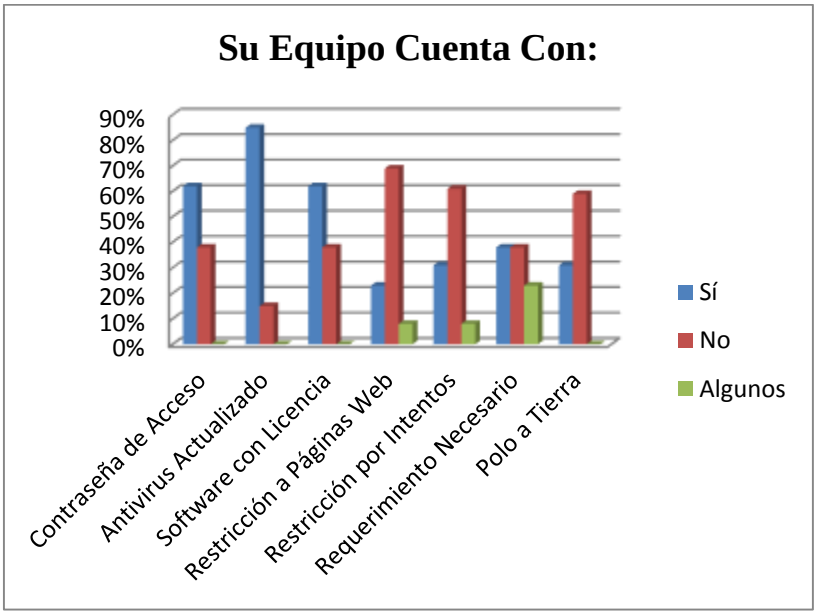
Además, el uso de los documentos institucionales solo se registra en un 15% y el uso de los servicios de red en un 38%.

Tabla 11. El equipo de cómputo a su disposición, cuenta con:

	FRECUENCIA				PORCENTAJE			
	Sí	**No**	**Alguno**	**Total**	**Sí**	**No**	**Alguno**	**Total**
Contraseña de acceso	8	5	0	**13**	62%	38%	0%	**100%**
Antivirus actualizado	11	2	0	**13**	85%	15%	0%	**100%**
Software con licencia	8	5	0	**13**	62%	38%	0%	**100%**
Restricción a páginas web	3	9	1	**13**	23%	69%	8%	**100%**
Restricción por intentos	4	8	1	**13**	31%	61%	8%	**100%**
Requerimientos necesarios	5	5	**3**	**13**	38%	38%	23%	**100%**
Polo a tierra	4	9	**0**	**13**	31%	59%	0%	**100%**

Fuente: Autora

Figura 11. Su equipo cuenta con:



Fuente: Autora

En lo relacionado con los controles de seguridad de la información aplicados en cada equipo, cabe mencionar que el 62% de los equipos de los empleados encuestados cuenta con una contraseña (para permitir el acceso de usuarios a los sistemas), mientras que el 85% de estos, mantiene el antivirus actualizado, el 62% cuenta con su Software licenciado e indistintamente el 59%, carece de polo a tierra.

Las restricciones de acceso a páginas web (redes sociales, etc.) en los equipos de los empleados encuestados son del 23% para todas, del 69% para ninguna y el 8% para algunas de estas.
Por otra parte el acceso restringido a las aplicaciones después de varios intentos es de total uso en el 23% de los equipos, nulo en el 61% y parcial en el 8%.

Además, el 38% de los encuestados consideran que su equipo cuenta con los requerimientos necesarios para la realización optima de sus labores, al igual que una misma fracción de estos considera que no, pero indistintamente un 8%, considera que cuenta con solo algunos de estos requerimientos.

Tabla 12. El equipo de cómputo que actualmente está a su disposición, ¿Es utilizado por otro funcionario?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	6	50%
No	6	50%
Total	**12**	**100%**

Fuente: Autora

Figura 12. ¿Es utilizado por otro funcionario?

Fuente: Autora

La figura 12. Muestra el 50% de los equipos de cómputo que actualmente se encuentran a disposición de los empleados encuestados, son utilizados por otros funcionarios por motivos laborales, mientras que el otro 50%, solo es utilizado por un funcionario en específico.

Tabla 13. ¿Cuenta con manuales de procedimientos para la operación de cada uno de los sistemas de cómputo del área?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	1	8%
No	10	84%
Algunos	1	8%
Total	**12**	**100%**

Fuente: Autora

Figura 13. ¿Cuenta con manuales de procedimiento?

Fuente: Autora

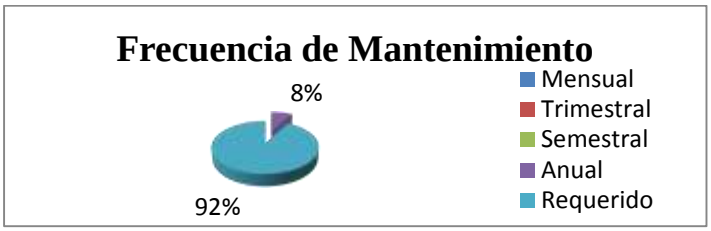
El 84% de los encuestados afirma que no cuenta con manuales de procedimiento para la operación de cada uno de los sistemas de cómputo de su área, mientras que un 8% afirma que si cuenta con ellos y en igual fracción se afirma que se cuenta con solo algunos de ellos.

Tabla 14. ¿Con que frecuencia el equipo de cómputo a su disposición recibe mantenimiento?

RESPUESTA	FRECUENCIA	PORCENTAJE
Mensualmente	0	0%
Trimestralmente	0	0%
Semestralmente	0	0%
Anualmente	1	8%
Cuando lo requiere	11	92%
Total	**12**	**100%**

Fuente: Autora

Figura 14. Frecuencia de Mantenimiento.



Fuente: Autora

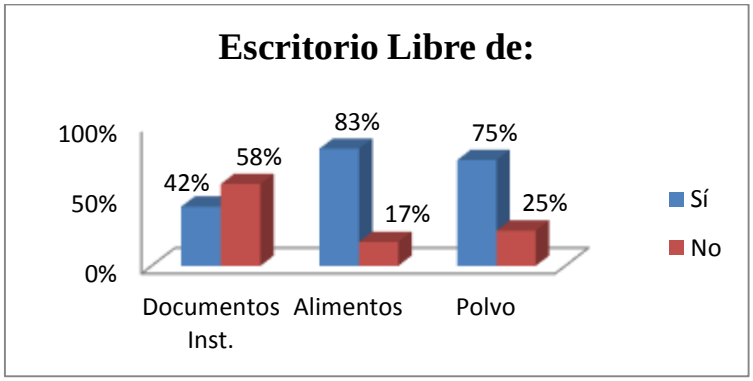
En cuanto a la frecuencia con la que los equipos a disposición de los encuestados, recibe mantenimiento, el 92% de los equipos recibe mantenimiento solo cuando este lo requiere y el 8% de ellos lo recibe cada año.

Tabla 15. Su escritorio personal, permanece libre de:

	FRECUENCIA			PORCENTAJE		
	Sí	**No**	**Total**	**Sí**	**No**	**Total**
Archivos o documentos institucionales	5	7	**12**	45%	58%	**100%**
Alimentos	10	2	**12**	83%	17%	**100%**
Polvo	9	3	**12**	75%	25%	**100%**

Fuente: Autora

Figura 15. Escritorio libre de:



Fuente: Autora

En lo referente a la política de escritorio limpios, 58% los empleados afirman que su escritorio no permanece libre de archivos o documentos institucionales.

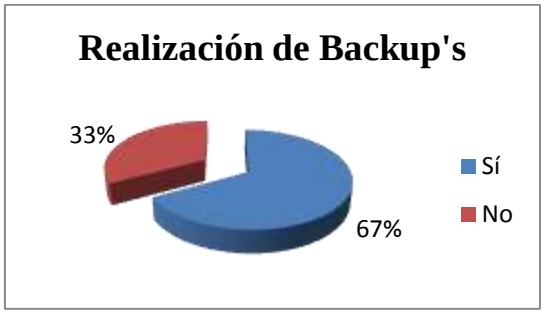
El 83% de ellos mantiene su escritorio libre de alimentos y el 75%, libre de polvo.

Tabla 16. ¿Realiza backup's (copias de seguridad) de la información a su disposición?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	8	67%
No	4	33%
Total	**12**	**100%**

Fuente: Autora

Figura 16. Realización de backup's.



Fuente: Autora

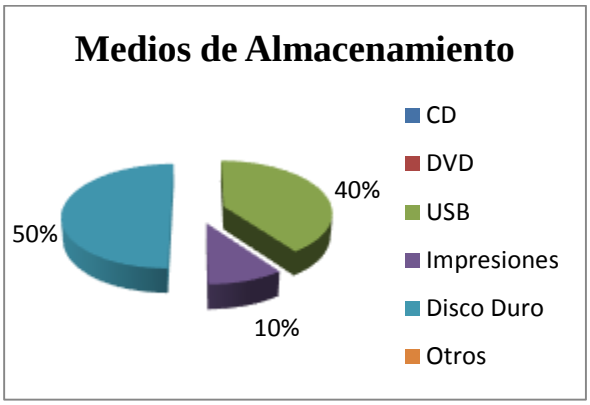
La figura 16. Muestra que el 67% de los encuestados realiza Backup's (Copias de Seguridad) de la información a su disposición, mientras que el otro 33% no las realiza.
De este 67% de los empleados que respondieron afirmativamente esta pregunta, se pretendió conocer cual medio preferían para realizar el almacenamiento de esta información.

Tabla 17. ¿En qué medio almacena esta información?

RESPUESTA	FRECUENCIA	PORCENTAJE
CD	0	0%
DVD	0	0%
Memorias USB	4	40%
Impresiones	1	10%
Disco Duro	5	50%
Otras	0	0%
Total	**10**	**100%**

Fuente: Autora

Figura 17. Medios de almacenamiento.



Fuente: Autora

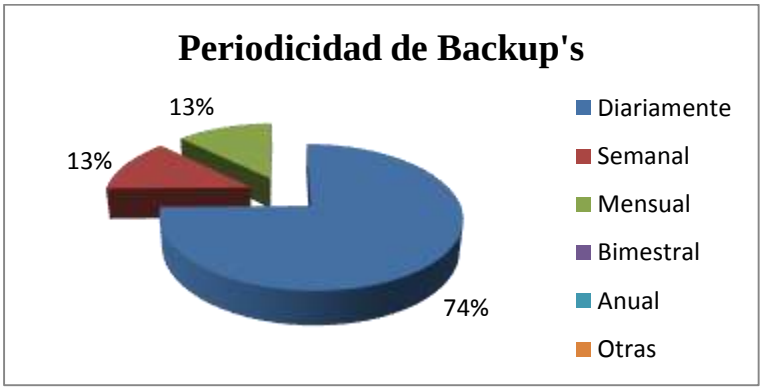
El resultado que se obtuvo fue, que el 40% de los empleados encuestados, prefieren almacenar sus backup's en memorias USB, mientras que el 50% prefiere los Discos Duros e indistintamente un 10% prefiere imprimirlas.

Tabla 18. ¿Con que periodicidad se realizan?

RESPUESTA	FRECUENCIA	PORCENTAJE
Diariamente	6	74%
Semanalmente	1	13%
Mensualmente	1	13%
Bimestralmente	0	0%
Anualmente	0	0%
Otras	0	0%
Total	**8**	**100%**

Fuente: Autora

Figura 18. Periodicidad de backup's.



Fuente: Autora

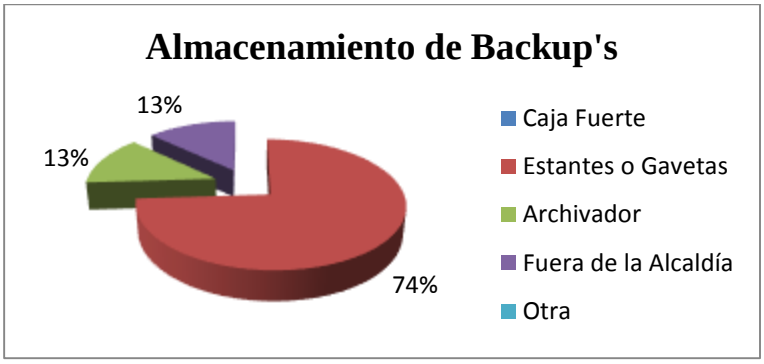
En la figura 18. Se observa que los empleados encuestados realizan sus backup's con una periodicidad diaria en un 74%, mientras que semanalmente y mensualmente, se realizan en un 13%.

Tabla 19. Las copias de respaldo de la información es almacenada en:

RESPUESTA	FRECUENCIA	PORCENTAJE
Caja fuerte o bóveda	0	0%
Estantes o gavetas	6	74%
Muebles con cerradura o archivador	1	13%
Fuera de la Alcaldía	1	13%
Otras	0	0%
Total	**8**	**100%**

Fuente: Autora

Figura 19. Almacenamiento de backup's.



Fuente: Autora

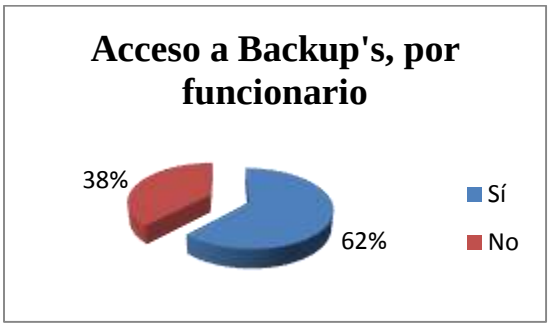
En cuanto al almacenamiento de Backup's, el 74% de los encuestados prefiere resguardar su información en estantes o gavetas, mientras que el 13% prefiere muebles con cerradura o archivadores, y con igual fracción se prefiere un sitio fuera de las instalaciones de la Alcaldía, para prevenir la perdida de datos en caso de incidencias.

Tabla 20. ¿El acceso a estas copias de respaldo o documentos institucionales es restringido, según el rol en la institución?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	5	38%
No	3	62%
Total	**8**	**100%**

Fuente: Autora

Figura 20. Acceso a backup's por funcionario.



Fuente: Autora

Debido a que la información mantenerse segura, el 62% de los encuestados opina que el acceso a las copias de respaldo o documentos institucionales es restringido, según el rol del funcionario dentro de la Alcaldía, mientras que el 38% restante opina que no lo es.

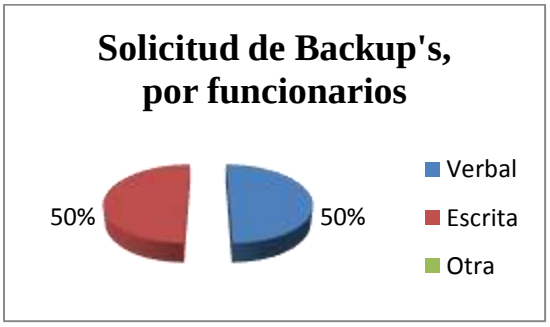
En relación al acceso de funcionarios a estos documentos, ¿Cómo se debe realizar la respectiva solicitud?

Tabla 21. ¿Cómo se permite el acceso a estas?

RESPUESTA	FRECUENCIA	PORCENTAJE
Mediante solicitud verbal	4	50%
Mediante solicitud escrita	4	50%
Otras	0	0%
Total	**8**	**100%**

Fuente: Autora

Figura 21. Solicitud de backup's por funcionarios.



Fuente: Autora

La respectiva solicitud de acceso a los backup's o documentos institucionales oscila en un 50%, mediante forma verbal o escrita.

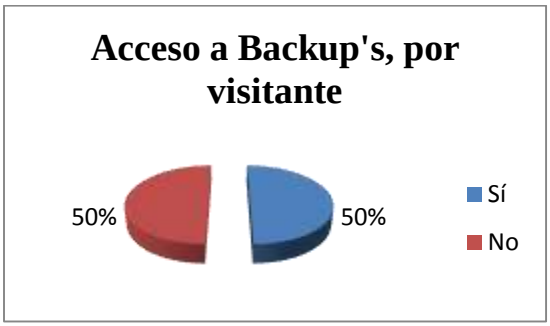
Pero que sucede si el solicitante a estos Backup's, no es un funcionario de la Alcaldía; Si por el contrario es una persona ajena a esta y requiere la información. ¿Cómo accede a ella?

Tabla 22. ¿El acceso a estas copias de respaldo o documentos institucionales es restringido, a usuarios externos a la institución?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	4	50%
No	4	50%
Total	**8**	**100%**

Fuente: Autora

Figura 22. Acceso a backup's por visitante.



Fuente: Autora

Aunque la Alcaldía es un establecimiento público, que debe brindar la disponibilidad de la información ante la solicitud del interesado, existe cierta información que debe ser confidencial para evitar incidencias que pongan en peligro su integridad.

Por tal razón, el 50% de los encuestados concuerdan en que cierta información no debe ser divulgada.

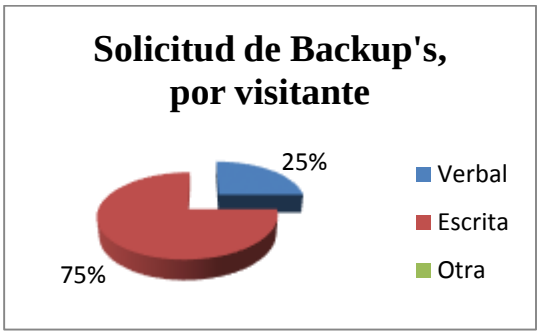
En cuanto a esa información que es disponible al interesado, ¿Cómo debe realizar la respectiva solicitud?

Tabla 23. ¿Cómo se permite el acceso a estas?

RESPUESTA	FRECUENCIA	PORCENTAJE
Mediante solicitud verbal	3	75%
Mediante solicitud escrita	1	25%
Otras	0	0%
Total	**4**	**100%**

Fuente: Autora

Figura 23. Solicitud de backup's por visitante.



Fuente: Autora

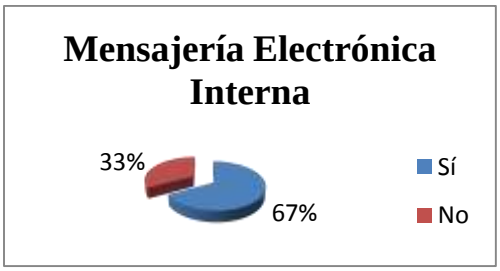
Para realizar la respectiva solicitud de acceso a Backup's y documentos institucionales a terceros, el 75% de los empleados encuestados opina que debe realizarse de forma escrita, mientras el otro 25%, opina se deben realizar de forma verbal.

Tabla 24. ¿Cuenta con mensajería electrónica interna para sus labores diarias?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	8	67%
No	4	33%
Total	**12**	**100%**

Fuente: Autora

Figura 24. Mensajería electrónica interna.



Fuente: Autora

El 67% de los empleados, cuenta con algún tipo de mensajería electrónica interna para la efectiva realización de sus labores diarias, mientras que el 33% restante no.

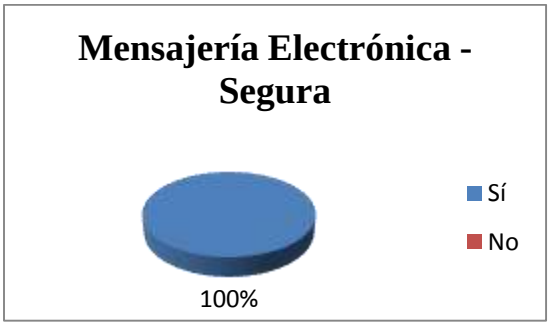
Pero de este 67%, cuantos consideran este tipo de mensajería como segura.

Tabla 25. ¿Este tipo de mensajería se podría considerar segura?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	8	100%
No	0	0%
Total	**12**	**100%**

Fuente: Autora

Figura 25. Mensajería electrónica – segura.



Fuente: Autora

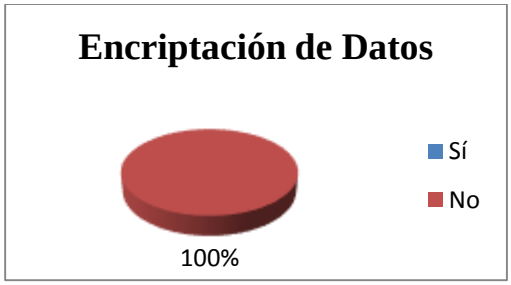
En la figura 25. Se detalla que el 100% de los empleados que cuentan con mensajería electrónica interna, la consideran segura.

Tabla 26. ¿Cuenta con programas para la encriptación (camuflar información a destinatarios no deseados) de datos?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	0	0%
No	12	100%
Total	**12**	**100%**

Fuente: Autora

Figura 26. Encriptación de datos.



Fuente: Autora

Según el 100% de los empleados encuestados, no cuentan con ningún tipo de aplicación que les permita encriptar su información de destinatarios no deseados.

Tabla 27. ¿La Alcaldía cuenta con un procedimiento formal para reportes de incidentes (robos de información, perdida de datos, accesos no permitidos, etc.)?}

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	0	0%
No	12	100%
Total	**12**	**100%**

Fuente: Autora

Figura 27. Reporte de incidentes.

Fuente: Autora

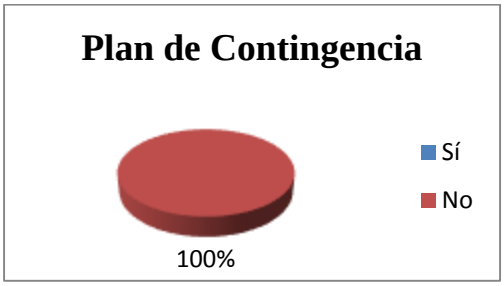
En la figura 28. Se aprecia que la Alcaldía no cuenta con un procedimiento formal para reporte de incidente (robos de información, perdida de datos, accesos no permitidos, etc.).

Tabla 28. ¿Al presentarse un incidente de seguridad en la Alcaldía, se cuenta con un plan de contingencia?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	0	0%
No	12	100%
Total	**12**	**100%**

Fuente: Autora

Figura 28. Plan de contingencia.



Fuente: Autora

Al presentarse cualquier tipo de incidente de seguridad en las instalaciones de la Alcaldía, esta no cuenta con un plan de contingencia que le permita mantener sus funciones, en un estado de continuidad.

Tabla 29. ¿Se investigan y recolectan evidencias sobre el incidente de seguridad de la información?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	0	0%
No	12	100%
Total	**12**	**100%**

Fuente: Autora

Figura 29. Investigación de incidentes.

Fuente: Autora

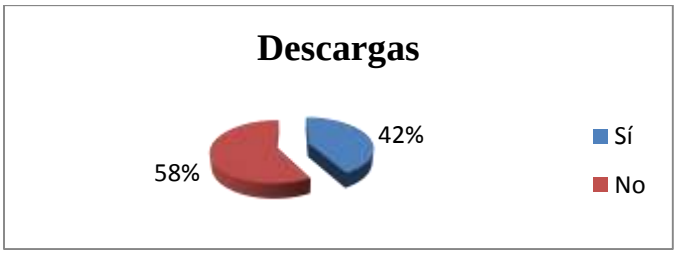
Hasta el momento no se realizan investigaciones, ni recolección de evidencias sobre incidentes de seguridad de la información, que se presenten en la Alcaldía.

Tabla 30. ¿Acostumbra utilizar programas de descarga de archivos de usuario (música, películas, programas…)?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	5	42%
No	7	58%
Total	**12**	**100%**

Fuente: Autora

Figura 30. Descargas.



Fuente: Autora

El 42% de los encuestados realiza descargas de música, películas, programas entre otros, lo que pone en riesgo la seguridad de la información a su cargo, debido a virus al descargar.

3.4.2 Encuesta de Seguridad de la Información Dirigida al Personal de OPS de la Alcaldía Municipal de Río de Oro (Cesar).

Tabla 31. ¿Cuenta con un acuerdo de confidencialidad de la información?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	3	38%
No	5	62%
Total	**8**	**100%**

Fuente: Autora

Figura 31. Acuerdo de confidencialidad.

Fuente: Autora

Se observa que el 62% de los empleados de OPS de la Alcaldía, no cuentan con un acuerdo de confidencialidad de la información establecido por la administración, mientras el 38% restante sí cuenta con uno, pero solo de forma verbal.

Tabla 32. ¿Tiene usted conocimiento de sus responsabilidades y sanciones, frente a la seguridad de la información?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	4	50%
No	4	50%
Total	**8**	**100%**

Fuente: Autora

Figura 32. Responsabilidades y sanciones.

Fuente: Autora

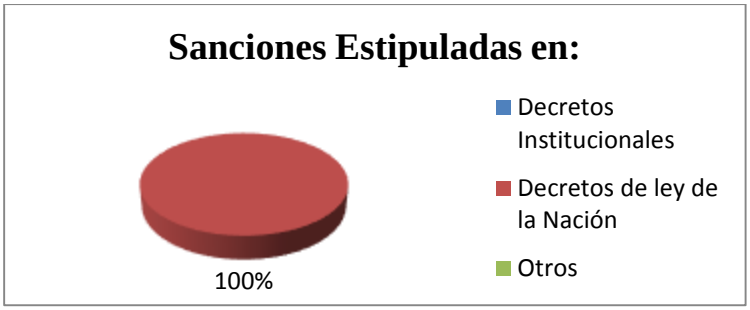
De los encuestados el 50%, no tiene conocimiento de sus responsabilidades y sanciones, frente a la seguridad de la información, mientras que el 50% restante, cuenta con pleno conocimiento de estas.

Tabla 33. Estas sanciones se encuentra estipuladas en:

RESPUESTA	FRECUENCIA	PORCENTAJE
Decretos o resoluciones institucionales	0	0%
Decretos de ley de la nación	4	100%
Otros	0	0%
Total	**4**	**100%**

Fuente: Autora

Figura 33. Sanciones estipuladas en:



Fuente: Autora

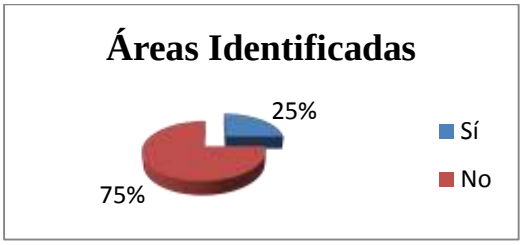
De la figura 33. Se interpreta que: El 100% de los empleados que tiene conocimiento de sus responsabilidades y sanciones, afirman que se encuentran estipuladas en Decretos de Ley de la Nación.

Tabla 34. ¿El área en la cual labora, se encuentra debidamente identificada?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	2	25%
No	6	75%
Total	**8**	**100%**

Fuente: Autora

Figura 34. Áreas identificadas.



Fuente: Autora

El 25% de los empleados afirma que el área en la cual labora se encuentra debidamente identificada, mientras que el 75% afirma que no lo está, lo que impide que los visitantes identifiquen las áreas y encuentren la que buscan.

Tabla 35. ¿Su área cuenta con controles de ingreso al personal?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	0	0%
No	8	100%
Total	**8**	**100%**

Fuente: Autora

Figura 35. Control de ingreso al personal.

Fuente: Autora

En lo relacionado con el control de Ingreso al Personal en las áreas en las cuales laboran los encuestados, el 100% de estás no cuenta con dicho control de acceso, es decir, los empleados puede ampliar o disminuir su jornada laboral diaria por sí mismos.

Tabla 36. ¿Se controla el trabajo, fuera del horario laboral definido?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	2	25%
No	6	75%
Total	**8**	**100%**

Fuente: Autora

Figura 36. Trabajo en horario no laboral.

Fuente: Autora

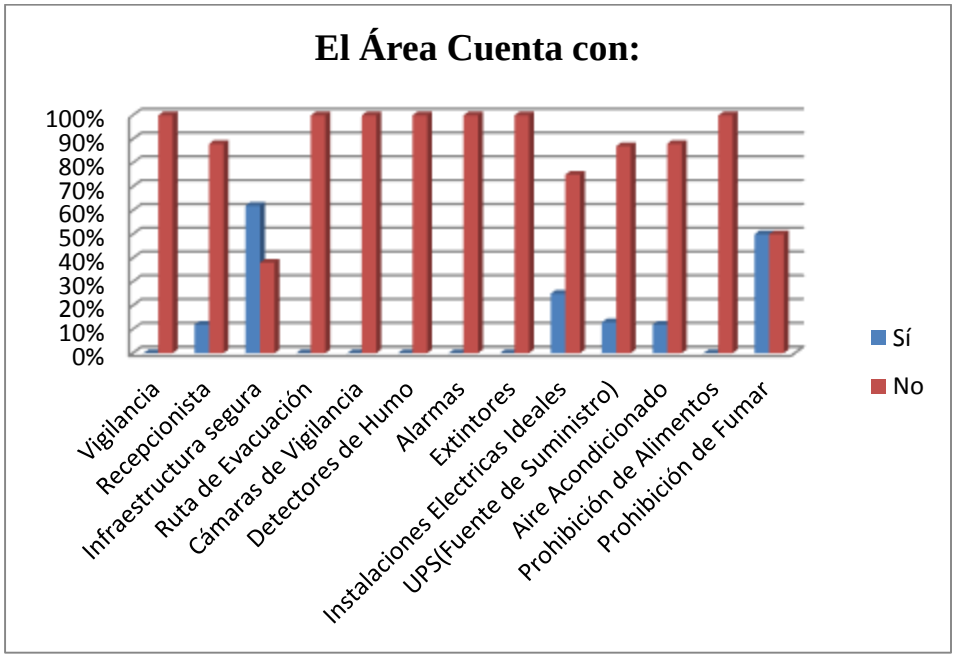
Se muestra en la figura 36, que el 75% de los trabajadores concuerdan en que no se controla su trabajo fuera del horario laboral definido, por la administración, mientras que el 25% restante sí.

Tabla 37. El área cuenta con:

	FRECUENCIA			PORCENTAJE		
	Sí	**No**	**Total**	**Sí**	**No**	**Total**
Vigilancia	0	8	**8**	0%	100%	**100%**
Recepcionista	0	8	**8**	12%	88%	**100%**
Infraestructura sólida y segura	5	3	**8**	62%	38%	**100%**
Ruta de Evacuación	0	8	**8**	0%	100%	**100%**
Cámaras de vigilancia	0	8	**8**	0%	100%	**100%**
Detectores de Humo	0	8	**8**	0%	100%	**100%**
Alarmas	0	8	**8**	0%	100%	**100%**
Extintores	0	8	**8**	0%	100%	**100%**
Instalaciones eléctricas ideales	2	6	**8**	25%	75%	**100%**
UPS(Fuentes de suministro eléctrico)	1	7	**8**	12%	88%	**100%**
Aire acondicionado	1	7	**8**	12%	88%	**100%**
Prohibición de Alimentos y bebidas	0	8	**8**	0%	100%	**100%**
Prohibición de Fumar en el área	4	4	**8**	50%	50%	**100%**

Fuente: Autora

Figura 37. El área cuenta con:



Fuente: Autora

La Figura 37. Muestra que el 100% de las áreas, no cuenta con vigilancia, mientras que el 88% de estas no cuenta con un recepcionista.

Además, solo el 62% de estas áreas son consideradas por los trabajadores como una infraestructura sólida y segura, pero en ninguno de los casos se cuenta con una ruta de evacuación debidamente señalizada.

Además, se observa que ninguna de las áreas de trabajo de los empleados cuenta con cámaras de vigilancia, detectores de humo, alarmas o Extintores.

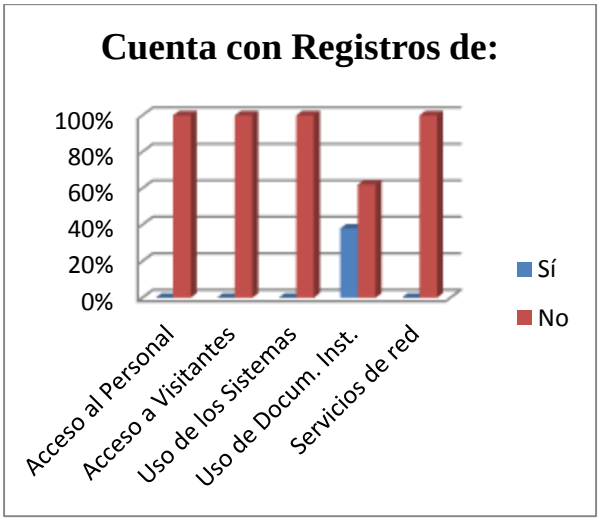
El 75% de las áreas de trabajo, no cuentan con instalaciones eléctricas ideales, pero solo el 12% de ellas cuenta con UPS (Fuente de Suministro Ininterrumpido) y un 12% hace uso de aire acondicionado, mientras que en ninguna de estas se prohíbe el consumo de alimentos y bebidas, además el 50% no prohíbe fumar en las instalaciones.

Tabla 38. Sabe usted si la Alcaldía cuenta con registros de:

	FRECUENCIA			PORCENTAJE		
	Sí	**No**	**Total**	**Sí**	**No**	**Total**
Acceso al personal	0	8	**8**	0%	100%	**100%**
Acceso de visitantes	0	8	**8**	0%	100%	**100%**
Uso de los sistemas	0	8	**8**	0%	100%	**100%**
Uso de documentos institucionales	3	5	**8**	38%	62%	**100%**
Servicios de red	0	8	**8**	0%	100%	**100%**

Fuente: Autora

Figura 38. Cuenta con registros de:



Fuente: Autora

En la figura 38. Se aprecia que la Alcaldía Municipal no cuenta en un 100% con el registro de acceso a sus instalaciones del personal y los visitantes, ni del uso de los sistemas por alguien distinto al empleado en específico.

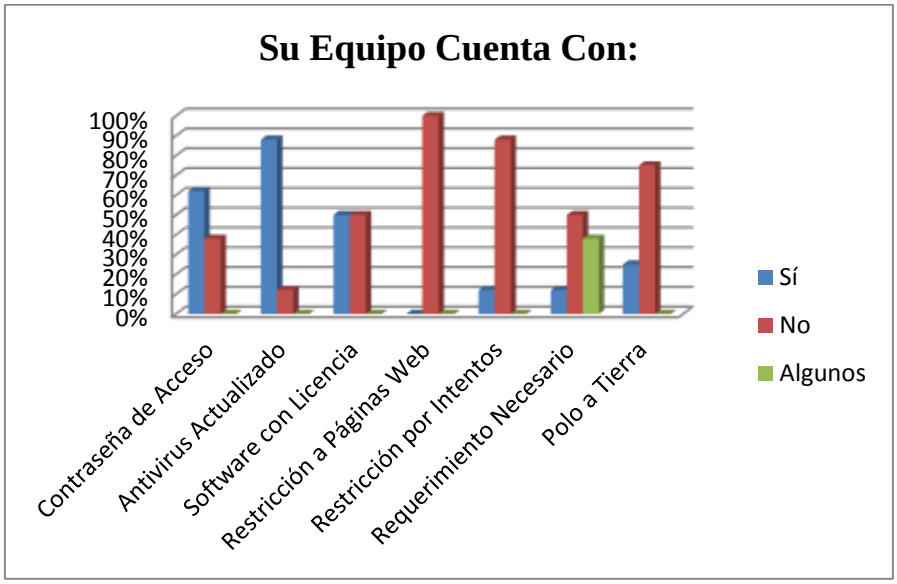
Además, el uso de los documentos institucionales solo se registra en un 38% y el uso de los servicios de red el 0%.

Tabla 39. El equipo de cómputo a su disposición, cuenta con:

	FRECUENCIA				PORCENTAJE			
	Sí	**No**	**Alguno**	**Total**	**Sí**	**No**	**Alguno**	**Total**
Contraseña de acceso	5	3	0	**8**	62%	38%	0%	**100%**
Antivirus actualizado	7	1	0	**8**	88%	12%	0%	**100%**
Software con licencia	4	4	0	**8**	50%	50%	0%	**100%**
Restricción a páginas web	0	8	0	**8**	0%	100%	0%	**100%**
Restricción por intentos	1	7	0	**8**	12%	88%	0%	**100%**
Requerimientos necesarios	1	4	3	**8**	12%	50%	38%	**100%**
Polo a tierra	2	6	0	**8**	25%	75%	0%	**100%**

Fuente: Autora

Figura 39. Su equipo cuenta con:



Fuente: Autora

En lo relacionado con los controles de seguridad de la información aplicados en cada equipo, cabe mencionar que el 62% de los equipos de los empleados encuestados cuenta con una contraseña (para permitir el acceso de usuarios a los sistemas), mientras que el 88% de estos, mantiene el antivirus actualizado, el 50% cuenta con su Software licenciado.

Las restricciones de acceso a páginas web (redes sociales, etc.) en los equipos de los empleados encuestados son del 0% para todas, del 100% para ninguna y el 0% para algunas de estas.

Por otra parte el acceso restringido a las aplicaciones después de varios intentos es de total uso en el 12% de los equipos, nulo en el 88% y parcial el 0%.

Además, el 12% de los encuestados consideran que su equipo cuenta con los requerimientos necesarios para la realización óptima de sus labores, pero el 50% de estos considera que no, aunque indistintamente un 38% considera que cuenta con solo algunos de estos requerimientos, e indistintamente el 25%, carece de polo a tierra.

Tabla 40. El equipo de cómputo que actualmente está a su disposición, ¿Es utilizado por otro funcionario?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	3	38%
No	5	62%
Total	**8**	**100%**

Fuente: Autora

Figura 40. ¿Es utilizado por otro funcionario?

Fuente: Autora

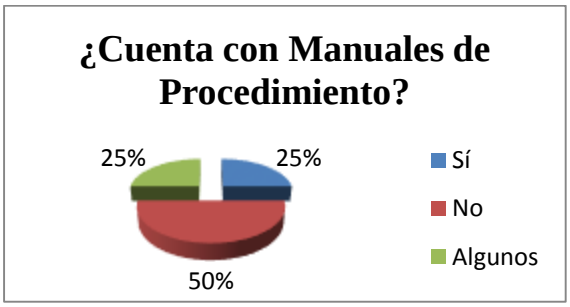
La figura 41. Muestra el 38% de los equipos de cómputo que actualmente se encuentran a disposición de los empleados encuestados, son utilizados por otros funcionarios por motivos laborales, mientras que el 62% restante, solo es utilizado por un funcionario en específico.

Tabla 41. ¿Cuenta con manuales de procedimientos para la operación de cada uno de los sistemas de cómputo del área?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	2	25%
No	4	50%
Algunos	2	25%
Total	**8**	**100%**

Fuente: Autora

Figura 41. ¿Cuenta con manuales de procedimiento?



Fuente: Autora

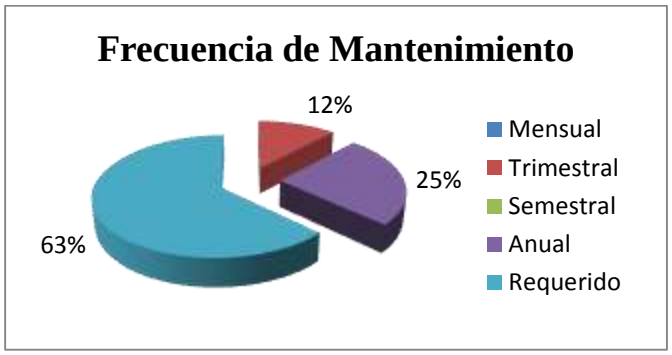
El 50% de los encuestados afirma que no cuenta con manuales de procedimiento para la operación de cada uno de los sistemas de cómputo de su área, mientras que un 25% afirma que si cuenta con ellos y en igual fracción se afirma que se cuenta con solo algunos de ellos.

Tabla 42. ¿Con que frecuencia el equipo de cómputo a su disposición recibe mantenimiento?

RESPUESTA	FRECUENCIA	PORCENTAJE
Mensualmente	0	0%
Trimestralmente	1	12%
Semestralmente	0	0%
Anualmente	2	25%
Cuando lo requiere	5	63%
Total	**8**	**100%**

Fuente: Autora

Figura 42. Frecuencia de Mantenimiento.



Fuente: Autora

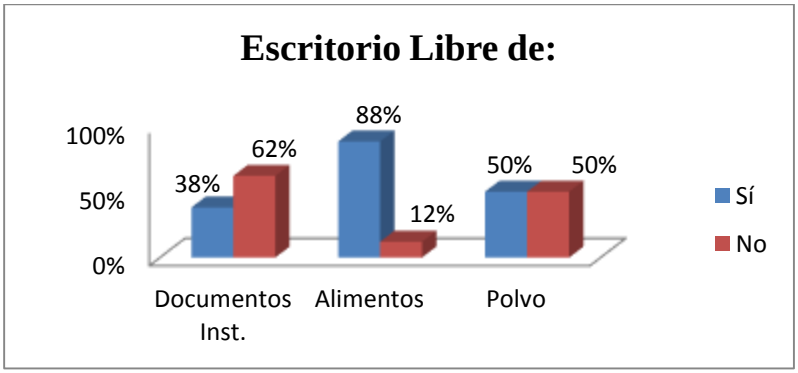
En cuanto a la frecuencia con la que los equipos a disposición de los encuestados, recibe mantenimiento, es del 63% cuando este lo requiere, el 25% Anualmente y el 12% Trimestralmente.

Tabla 43. Su escritorio personal, permanece libre de:

	FRECUENCIA			PORCENTAJE		
	Sí	**No**	**Total**	**Sí**	**No**	**Total**
Archivos o documentos institucionales	3	5	**8**	38%	62%	**100%**
Alimentos	7	1	**8**	88%	12%	**100%**
Polvo	4	4	**8**	50%	50%	**100%**

Fuente: Autora

Figura 43. Escritorio libre de:



Fuente: Autora

En lo referente a la política de escritorio limpios, 38% los empleados afirman que su escritorio no permanece libre de archivos o documentos institucionales.

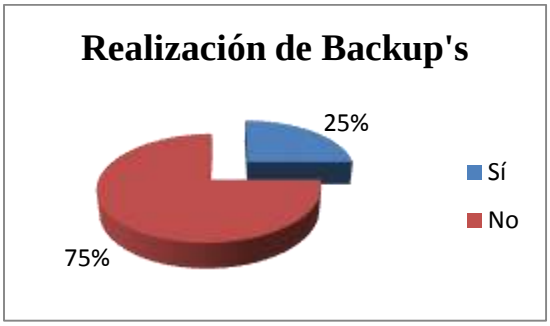
El 88% de ellos mantiene su escritorio libre de alimentos y el 50%, libre de polvo.

Tabla 44. ¿Realiza backup's (copias de seguridad) de la información a su disposición?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	2	25%
No	6	75%
Total	**8**	**100%**

Fuente: Autora

Figura 44. Realización de backup's.



Fuente: Autora

La figura 44. Muestra que el 25% de los encuestados realiza Backup's (Copias de Seguridad) de la información a su disposición, mientras que el otro 75% no las realiza.

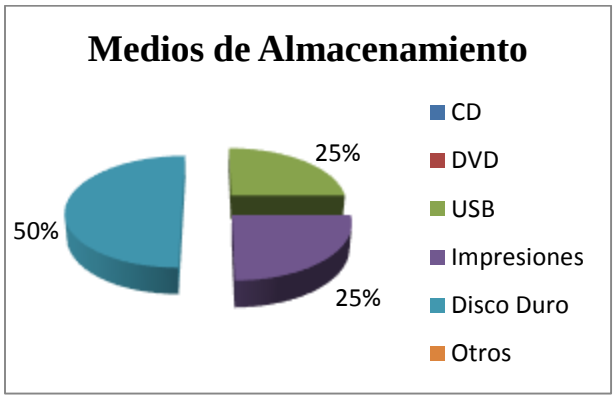
De este 25% de los empleados que respondieron afirmativamente esta pregunta, se pretendió conocer cual medio preferían para realizar el almacenamiento de esta información.

Tabla 45. ¿En qué medio almacena esta información?

RESPUESTA	FRECUENCIA	PORCENTAJE
CD	0	0%
DVD	0	0%
Memorias USB	1	25%
Impresiones	1	25%
Disco Duro	2	50%
Otras	0	0%
Total	**4**	**100%**

Fuente: Autora

Figura 45. Medios de almacenamiento.



Fuente: Autora

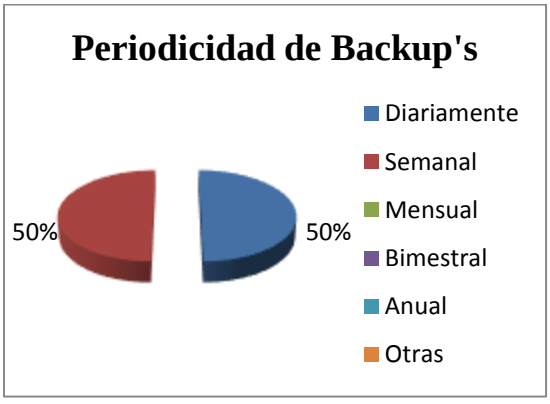
El resultado que se obtuvo fue, que el 25% de los empleados encuestados, prefieren almacenar sus backup's en memorias USB, mientras que el 50% prefiere los Discos Duros e indistintamente un 25% prefiere imprimirlas.

Tabla 46. ¿Con que periodicidad se realizan?

RESPUESTA	FRECUENCIA	PORCENTAJE
Diariamente	1	50%
Semanalmente	1	50%
Mensualmente	0	0%
Bimestralmente	0	0%
Anualmente	0	0%
Otras	0	0%
Total	**2**	**100%**

Fuente: Autora

Figura 46. Periodicidad de backup's.



Fuente: Autora

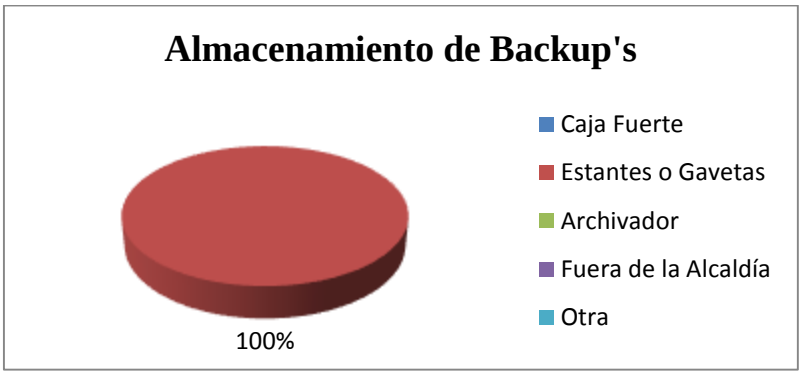
En la figura 46. Se observa que los empleados encuestados realizan sus backup's con una periodicidad diaria en un 50%, mientras que semanalmente se realizan en el 50% restante.

Tabla 47. Las copias de respaldo de la información es almacenada en:

RESPUESTA	FRECUENCIA	PORCENTAJE
Caja fuerte o bóveda	0	0%
Estantes o gavetas	2	100%
Muebles con cerradura o archivador	0	0%
Fuera de la Alcaldía	0	0%
Otras	0	0%
Total	**2**	**100%**

Fuente: Autora

Figura 47.Almacenamiento de backup's.



Fuente: Autora

En cuanto al almacenamiento de Backup's, el 100% de los encuestados prefiere resguardar su información en estantes o gavetas.

Tabla 48. ¿El acceso a estas copias de respaldo o documentos institucionales es restringido, según el rol en la institución?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	2	100%
No	0	0%
Total	**2**	**100%**

Fuente: Autora

Figura 48.Acceso a backup's por funcionario.

Fuente: Autora

Debido a que la información mantenerse segura, el 100% de los encuestados opina que el acceso a las copias de respaldo o documentos institucionales es restringido, según el rol del funcionario dentro de la Alcaldía.

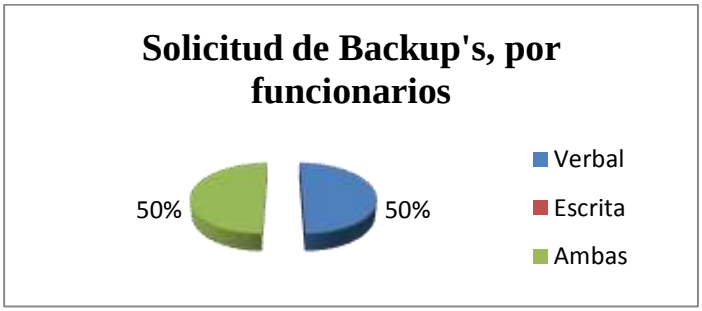
En relación al acceso de funcionarios a estos documentos, ¿Cómo se debe realizar la respectiva solicitud?

Tabla 49. ¿Cómo se permite el acceso a estas?

RESPUESTA	FRECUENCIA	PORCENTAJE
Mediante solicitud verbal	1	50%
Mediante solicitud escrita	0	0%
Otra (Ambas)	1	50%
Total	**2**	**100%**

Fuente: Autora

Figura 49. Solicitud de backup's por funcionarios.



Fuente: Autora

La respectiva solicitud de acceso a los backup's o documentos institucionales mediante solicitud verbal es del 50%, pero en igual fracción la solicitud debe ser realizada mediante solicitud verbal o escrita, depende el caso.

Pero que sucede si el solicitante a estos Backup's, no es un funcionario de la Alcaldía; Si por el contrario es una persona ajena a esta y requiere la información. ¿Cómo accede a ella?

Tabla 50. ¿El acceso a estas copias de respaldo o documentos institucionales es restringido, a usuarios externos a la institución?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	2	100%
No	0	0%
Total	**2**	**100%**

Fuente: Autora

Figura 50. Acceso a backup's por visitante.

Fuente: Autora

Aunque la Alcaldía es un establecimiento público, que debe brindar la disponibilidad de la información ante la solicitud del interesado, existe cierta información que debe ser confidencial para evitar incidencias que pongan en peligro su integridad.

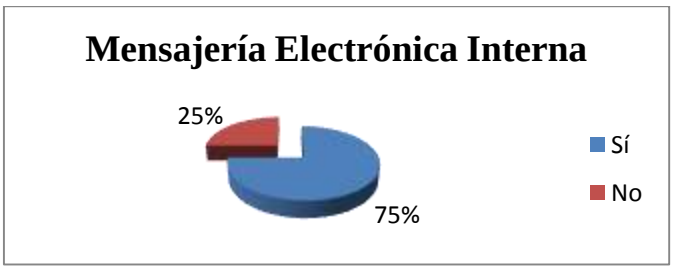
Por tal razón, el 100% de los encuestados concuerdan en que cierta información no debe ser divulgada.

Tabla 51. ¿Cuenta con mensajería electrónica interna para sus labores diarias?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	6	75%
No	2	25%
Total	**8**	**100%**

Fuente: Autora

Figura 51. Mensajería electrónica interna.



Fuente: Autora

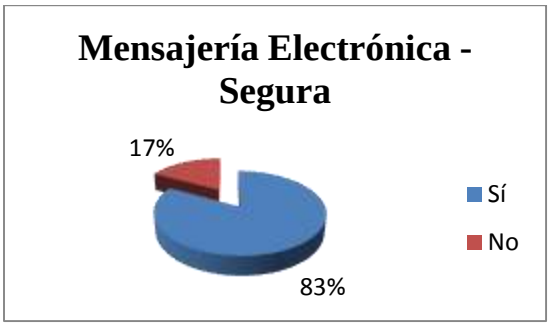
El 75% de los empleados, cuenta con algún tipo de mensajería electrónica interna para la efectiva realización de sus labores diarias, mientras que el 25% restante no.

Tabla 52. ¿Este tipo de mensajería se podría considerar segura?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	5	83%
No	1	17%
Total	**6**	**100%**

Fuente: Autora

Figura 52.Mensajería electrónica – segura.



Fuente: Autora

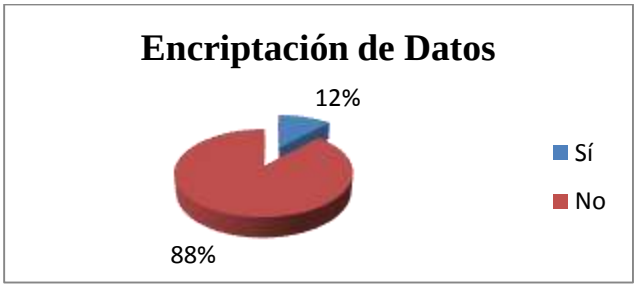
En la figura 52. Se detalla que el 83% de los empleados que cuentan con mensajería electrónica interna, la consideran segura.

Tabla 53. ¿Cuenta con programas para la encriptación (camuflar información a destinatarios no deseados) de datos?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	1	12%
No	7	88%
Total	**8**	**100%**

Fuente: Autora

Figura 53.Encriptación de datos.



Fuente: Autora

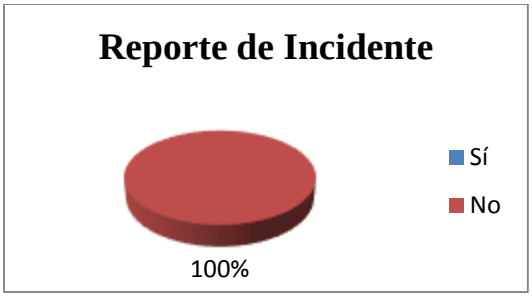
Según el 88% de los empleados encuestados, no cuentan con ningún tipo de aplicación que les permita encriptar su información de destinatarios no deseados.

Tabla 54. ¿La Alcaldía cuenta con un procedimiento formal para reportes de incidentes (robos de información, perdida de datos, accesos no permitidos, etc.)?}

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	0	0%
No	8	100%
Total	**8**	**100%**

Fuente: Autora

Figura 54. Reporte de incidentes.



Fuente: Autora

En la figura 54. Se aprecia que la Alcaldía no cuenta con un procedimiento formal para reporte de incidente (robos de información, perdida de datos, accesos no permitidos, etc.).

Tabla 55. ¿Al presentarse un incidente de seguridad en la Alcaldía, se cuenta con un plan de contingencia?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	0	0%
No	8	100%
Total	**8**	**100%**

Fuente: Autora

Figura 55. Plan de contingencia.

Fuente: Autora

Al presentarse cualquier tipo de incidente de seguridad en las instalaciones de la Alcaldía, esta no cuenta con un plan de contingencia que le permita mantener sus funciones, en un estado de continuidad.

Tabla 56. ¿Se investigan y recolectan evidencias sobre el incidente de seguridad de la información?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	0	0%
No	8	100%
Total	**8**	**100%**

Fuente: Autora

Figura 56. Investigación de incidentes.

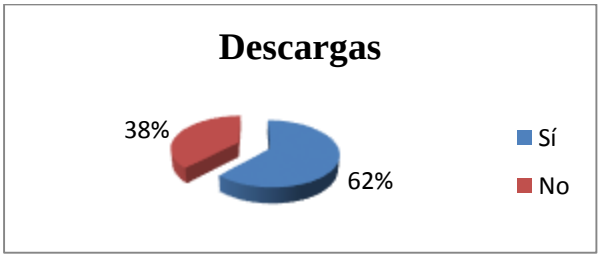
Fuente: Autora

Hasta el momento no se realizan investigaciones, ni recolección de evidencias sobre incidentes de seguridad de la información, que se presenten en la Alcaldía.

Tabla 57. ¿Acostumbra utilizar programas de descarga de archivos de usuario (música, películas, programas…)?

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	5	62%
No	3	38%
Total	**8**	**100%**

Figura 57. Descargas.



Fuente: Autora

Solo el 62% de los encuestados realiza descargas de música, películas, programas entre otros, lo que pone en riesgo la seguridad de la información a su cargo, debido a virus al descargar.

A continuación se detallan las conclusiones generales de esta investigación, tras la tabulación de los resultados obtenidos en las encuestas aplicadas.

1. La Alcaldía Municipal de Río de Oro, no realiza controles al horario de trabajo fuera del plan laboral definido, ni el respectivo registro de acceso del personal y visitantes, uso de los sistemas y documentos institucionales o servicio de red. No controla de acceso en la mayoría de sus áreas y no cuenta con planes de contingencias en caso de presentarse un incidente de seguridad. Solo si es de tipo criminal es investigado por las autoridades (policía).

2. De las áreas pertenecientes a la Alcaldía, sólo algunas se encuentran debidamente identificadas, cuentan con una recepcionista y son consideradas sólidas y seguras. Mientras que en su totalidad no cuentan con una ruta de evacuación señalizada, cámaras de vigilancia, alarmas, extintores o UPS, ni se prohíbe el consumo de alimentos y bebidas, o fumar. Solo una cuenta con detector de humo y otra con aire acondicionado. Y la vigilancia es solo en horas de la noche.

3. Sus empleados, no cuentan con acuerdos de confidencialidad de la información y no se encuentran debidamente informados de sus responsabilidades y posibles sanciones, en caso de una violación a la seguridad de la información a su cargo. Cuentan con escasos manuales de procedimiento para la operación de los sistemas de su área. Solo algunos realizan backup’s, preferiblemente mediante impresiones, memorias USB y Discos Duros, con una periodicidad diaria o semanal. Estas son preferiblemente almacenadas en estantes y archivadores. Algunos consideran que los backup´s son restringidos al personal, de acuerdo al rol que desempeña, y la respectiva petición de estos, puede realizarse de forma verbal o escrita. Pero en cambio el acceso de estos, a personas no funcionarias de la Alcaldía, debe realizarse preferiblemente de forma escrita, para su respectiva aprobación, esto en caso de que la información solicitada sea de carácter confidencial o privado; de lo contrario su solicitud será verbal, para el caso de la información pública o general que maneja la Alcaldía. En cuanto a la comunicación, algunos de ellos realizan el proceso de mensajería electrónica interna, mediante correos electrónicos los cuales son considerados en algunos casos como seguros. Pero algunos acostumbran realizar descargas de archivos, que son poco seguros y recomendables.

4. Pocos equipos de cómputo de la Alcaldía, mantienen una contraseña de acceso, cuentan con sistema operativo y software empresarial licenciado, mantienen restricciones de acceso a páginas web y a las aplicaciones luego de varios intentos y cuentan con los requerimientos necesarios para que los empleados realicen sus labores diarias de manera óptima. La mayoría mantiene un antivirus actualizado. Pero algunos cuentan con polo a tierra y son usados por otros funcionarios. Y en cuanto al mantenimiento, generalmente lo reciben cuando lo requieren.

5. Los escritorios, en su gran mayoría permanecen con documentos institucionales sobre ellos, pero pocos de ellos mantienen alimentos, bebidas y polvo.

Con el propósito de enfocar el diseño de las políticas de seguridad de la información a las necesidades actuales de la Alcaldía municipal de Río de Oro (Cesar), se realizó el respectivo análisis de riesgos y amenazas a las que se exponen sus activos.

1. Definición de Activos. Un activo, es cualquier cosa que sea importante para una organización. Para el caso en particular, la Alcaldía cuenta con 3 grupos de activos, definidos de la siguiente forma:

- Datos e Información: Agrupa todos los documentos institucionales relacionados con proyectos, planes, evaluaciones e informes pertenecientes a la Alcaldía así como directorios, correos, bases de datos y páginas web.
- Sistemas e Infraestructura: Agrupa todos los equipos de redes y comunicaciones, software, edificios y vehículos.
- Personal: Agrupa todo el personal de la Alcaldía y personal externo a ella que desarrollan labores que igualmente la exponen.

2. Clasificación de Activos. Los activos de la Alcaldía se clasifican de la siguiente forma:

2.1. Datos e Información.

- Confidencial, Privado, Sensitivo: Hace referencia a los activos con un alto grado de criticidad para la Alcaldía, en cuanto a su publicación no autorizada.
- Obligación por ley / Contrato / Convenio: Hace referencia a los activos de los cuales está obligada la Alcaldía mantener y cumplir, a través contratos, convenios o por la ley.
- Costo de Recuperación: Hace referencia a los activos de los cuales su recuperación representa costos de tiempo, materiales, imagen o económica para la Alcaldía, en caso de ocurrir cualquier eventualidad.

2.2. Sistemas e Infraestructura.

- Acceso Exclusivo: Hace referencia al acceso especial de esta clase de activos, solo a personal autorizado.
- Acceso limitado: Hace referencia al acceso establecido de estos activos, a un grupo mayor pero con sus respectivos lineamientos.
- Costo de Recuperación: Enmarca los activos de los cuales su costo de recuperación puede medirse en tiempo, material, imagen o economía para la Alcaldía.

2.3. Personal.

- Imagen pública de Alto nivel: Corresponde al personal indispensable para el funcionamiento de la Alcaldía orientado a sus líderes.
- Perfil Medio: Corresponde al personal que la labora (interno o externo) en la Alcaldía y representa a aquellos expertos en el área.

- Perfil Bajo: Se enfoca en el personal no indispensable para el funcionamiento normal de las actividades que se desarrollan en la Alcaldía.

3. Magnitud de Daño: Los activos de la Alcaldía se encuentran expuestos a amenazas que los ponen en riesgo de daño, provocando un impacto a la misma. La magnitud de daño de los activos a la Alcaldía debido a su exposición, se divide de la siguiente forma:

[1] - Insignificante: No causa ningún tipo de impacto o daño a la Alcaldía.
[2] - Baja: Causa daño aislado, que no perjudica a ningún componente.
[3] - Mediana: Provoca la desarticulación de un componente de la Alcaldía. Si no se atiende a tiempo, a largo plazo puede provocar su desarticulación.
[4] - Alta: En corto plazo desarticulara a la Alcaldía.

4. Probabilidad de Amenaza: Los activos se encuentra expuestos a toda clase de riesgos, de los cuales mantienen un nivel probable de amenaza:

[1] - Insignificante: El impacto provocado a la Alcaldía por ataque a los activos, es mínimo o nulo para el desempeño de sus actividades.
[2] - Bajo: Se presenta cuando existen condiciones que hacen muy lejana la posibilidad de ataque.
[3] - Mediano: Existen condiciones que hacen poco probable un ataque en el corto plazo, pero no son suficientes para evitarlo en largo plazo.
[4] - Alto: Ocurre en casos donde el ataque es inminente, debido a que no existen condiciones internas y externas que impidan el desarrollo del ataque.

5. Amenazas: Las amenazas a las cuales se encuentran expuestos los activos se dividen en 3 grandes grupos, que son:

- **Actos originados por la criminalidad común y motivación pública:** Incluye allanamientos, persecución, secuestro, sabotaje, vandalismo, extorción, fraude, robo (físico y electrónico), intrusión, infiltración, virus y violación de derechos de autor.
- **Sucesos de Origen físico:** Incluye incendios, inundación, sismos, polvo, falta de ventilación, electromagnetismo, sobrecarga eléctrica, apagones y fallas del sistema.
- **Sucesos derivados de la impericia, negligencia usuarios/as y decisiones institucionales:** falta de capacitación, mal manejo de sistemas y herramientas, uso de software pirata, falta de pruebas a software nuevo, perdida de datos, infección de sistemas por falta de escaneo, manejo inadecuado de datos críticos, unidades portables sin cifrado, manejo inadecuado de contraseñas, exposición o extravío de equipos, sobrepaso de autoridades, falta de definición de perfil, falta de mantenimiento, falta de actualización de software, fallas en permisos de usuarios, acceso electrónico no autorizado, red cableada e inalámbrica expuesta, dependencia a servicio técnico externo, falta de normas y reglas claras, falta de mecanismos de verificación de amenazas y ausencia de documentación.

6. Elementos de Información. A continuación se relaciona la definición de activos, su clasificación y magnitud de daño.

6.1. Datos e Información.

Elementos de información	Clasificación			Magnitud de daño			
Datos e información	**Confidencial, Privado, sensitivo**	**Obligación por ley/ contrato/ convenio**	**Costo de recuperación (tiempo, económico, material, imagen, emocional)**	**Insignificante (ninguno)**	**Bajo**	**Mediano**	**Alto**
Documentación Institucional	✓	✓	✓				✓
Directorio de Contactos	✓		✓				✓
Productos Institucionales	✓		✓			✓	
Correo Electrónico	✓					✓	
Bases de Datos	✓		✓				✓
Página Web	✓	✓			✓		
Respaldos	✓		✓				✓
Infraestructura			✓				✓
Navegación en Internet	✓					✓	
Chat interno	✓					✓	
Chat externo	✓						✓
Llamadas Telefónicas Internas	✓				✓		
Llamadas Telefónicas Externas	✓						✓

6.2. Sistemas e Infraestructura.

Elementos de información	Clasificación			Magnitud de daño			
Sistemas e Infraestructura	**Acceso exclusivo**	**Acceso limitado**	**Costo de recuperación (tiempo, económico, material, imagen, emocional)**	**Insignificante (ninguno)**	**Bajo**	**Mediano**	**Alto**
Equipos de Red Cableada	✓		✓				✓
Equipos de Red Inalámbricos	✓		✓				✓
Cortafuego			✓				✓
Servidores	✓		✓				✓
Computadores		✓	✓				✓
Portátiles		✓	✓				✓
Programas de Administración	✓		✓				✓
Programas de Manejo de Proyectos	✓		✓				✓
Programas de Comunicaciones	✓		✓				✓
Impresora	✓		✓			✓	
Memorias Portátiles			✓				✓
Celulares	✓				✓		
Edificio		✓	✓				✓
Vehículos	✓		✓	✓			

6.3. Personal.

Elementos de información	Clasificación			Magnitud de daño			
Personal	**Imagen pública de alto perfil, indispensable para el funcionamiento institucional**	**Perfil medio, experto en su áreas**	**Perfil bajo, no indispensable para el funcionamiento institucional**	**Insignificante (ninguno)**	**Bajo**	**Mediano**	**Alto**
Dirección	✓						✓
Administración		✓					✓
Personal Técnico		✓				✓	
Recepción		✓			✓		
Conductor			✓	✓			
Soporte Técnico Externo		✓					✓
Soporte Técnico Interno		✓			✓		
Servicio de Limpieza de Planta			✓	✓			
Servicio de Mensajería de Propio		✓			✓		
Servicio de Mensajería de Externo		✓				✓	

7. Valoración de Probabilidad de Amenaza.

7.1. Actos Originados por la Criminalidad Común y Motivación Política.

Tipo de Amenaza o Ataque	Clasificación			
Actos Originados por la Criminalidad Común y Motivación Política	**Insignificante (ninguno)**	**Bajo**	**Mediano**	**Alto**
Allanamiento (ilegal, legal)		✓		
Persecución (civil, fiscal, penal)		✓		
Orden de secuestro / Detención		✓		
Sabotaje (ataque físico y electrónico)			✓	
Daños por vandalismo			✓	
Extorción		✓		
Fraude / estafa				✓
Robo / hurto (físico)				✓
Robo / hurto de información electrónica			✓	
Intrusión a red interna				✓
infiltración		✓		
Virus / ejecución no autorizada de programas				✓
Violación de Derechos de Autor		✓		

7.2. Sucesos de Origen Físico

Tipo de Amenaza o Ataque	Clasificación			
Sucesos de Origen Físico	**Insignificante (ninguno)**	**Bajo**	**Mediano**	**Alto**
Incendio				✓
Inundación / deslave		✓		
Sismo		✓		
Polvo			✓	
Falta de ventilación				✓
Electromagnetismo		✓		
Sobrecarga eléctrica			✓	
Falla de corriente (apagones)			✓	
Falla de sistema / Daños disco duro			✓	

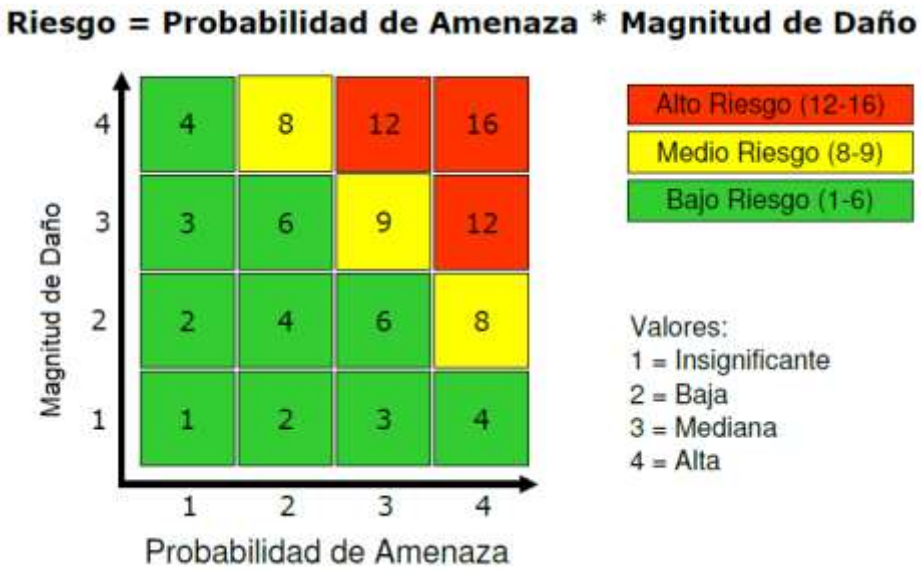
7.3. Sucesos Derivados de la Impericia, Negligencia de Usuarios/as y Decisiones Institucionales

Tipo de Amenaza o Ataque	Clasificación			
Sucesos Derivados de la Impericia, Negligencia de Usuarios/as y Decisiones Institucionales	**Insignificante (ninguno)**	**Bajo**	**Mediano**	**Alto**
Falta de inducción, capacitación y sensibilización sobre riesgos				✓
Mal manejo de sistemas y herramientas			✓	
Utilización de programas no autorizados / software 'pirateado'				✓
Falta de pruebas de software nuevo con datos productivos			✓	
Perdida de datos				✓
Infección de sistemas a través de unidades portables sin escaneo				✓
Manejo inadecuado de datos críticos (codificar, borrar, etc.)				✓
Unidades portables con información sin cifrado				✓
Transmisión no cifrada de datos críticos			✓	
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)				✓
Compartir contraseñas o permisos a terceros no autorizados			✓	
Transmisión de contraseñas por teléfono		✓		
Exposición o extravío de equipo, unidades de almacenamiento, etc				✓
Sobrepasar autoridades		✓		
Falta de definición de perfil, privilegios y restricciones del personal			✓	
Falta de mantenimiento físico (proceso, repuestos e insumos)				✓
Falta de actualización de software (proceso y recursos)				✓
Fallas en permisos de usuarios (acceso a archivos)			✓	
Acceso electrónico no autorizado a sistemas externos		✓		
Acceso electrónico no autorizado a sistemas internos		✓		
Red cableada expuesta para el acceso no autorizado				✓
Red inalámbrica expuesta al acceso no autorizado				✓
Dependencia a servicio técnico externo				✓
Falta de normas y reglas claras (no institucionalizar el estudio de				✓

los riesgos)				
Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control				✓
Ausencia de documentación				✓

8. Matriz de Riesgo. Mediante una matriz, basada en la clasificación, probabilidad de amenaza y magnitud de daño de los datos e información, así como de sistemas e infraestructura y del personal.

Los resultados de este estudio, se ven reflejando en las gráficas mediante un estándar de colores definido así:



8.1. Datos e Información.

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																				
Datos e Información	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común y motivación política												Sucesos de origen físico								
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)		Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
					2	2	2	3	3	2	4	4	3	4	2	4	2	4	2	2	3	4	2	3	3	3
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	x	x	x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Directorio de Contactos	x		x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	x		x	3	6	6	6	9	9	6	12	12	9	12	6	12	6	12	6	6	9	12	6	9	9	9
Correo electrónico	x			3	6	6	6	9	9	6	12	12	9	12	6	12	6	12	6	6	9	12	6	9	9	9
Bases de datos internos	x		x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Página Web externa	x	x		2	4	4	4	6	6	4	8	8	6	8	4	8	4	8	4	4	6	8	4	6	6	6
Respaldos	x		x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Infraestructura (Planes, Documentación, etc.)			x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Navegación en Internet	x			3	6	6	6	9	9	6	12	12	9	12	6	12	6	12	6	6	9	12	6	9	9	9
Chat interno	x			3	6	6	6	9	9	6	12	12	9	12	6	12	6	12	6	6	9	12	6	9	9	9
Chat externo	x			4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Llamadas telefónicas internas	x			2	4	4	4	6	6	4	8	8	6	8	4	8	4	8	4	4	6	8	4	6	6	6
Llamadas telefónicas externas	x			4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																							
Datos e Información	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																							
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)		Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
					4	3	4	3	4	4	4	4	3	4	3	2	4	2	3	4	4	3	2	2	4	4	4	4	4	4
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	x	x	x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Directorio de Contactos	x		x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	x		x	3	12	9	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	6	6	12	12	12	12	12	12
Correo electrónico	x			3	12	9	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	6	6	12	12	12	12	12	12
Bases de datos internos	x		x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Página Web externa	x	x		2	8	6	8	6	8	8	8	8	6	8	6	4	8	4	6	8	8	8	4	4	8	8	8	8	8	8
Respaldos	x		x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Infraestructura (Planes, Documentación, etc.)			x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Navegación en Internet	x			3	12	9	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	6	6	12	12	12	12	12	12
Chat interno	x			3	12	9	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	6	6	12	12	12	12	12	12
Chat externo	x			4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Llamadas telefónicas internas	x			2	8	6	8	6	8	8	8	8	6	8	6	4	8	4	6	8	8	8	4	4	8	8	8	8	8	8
Llamadas telefónicas externas	x			4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16

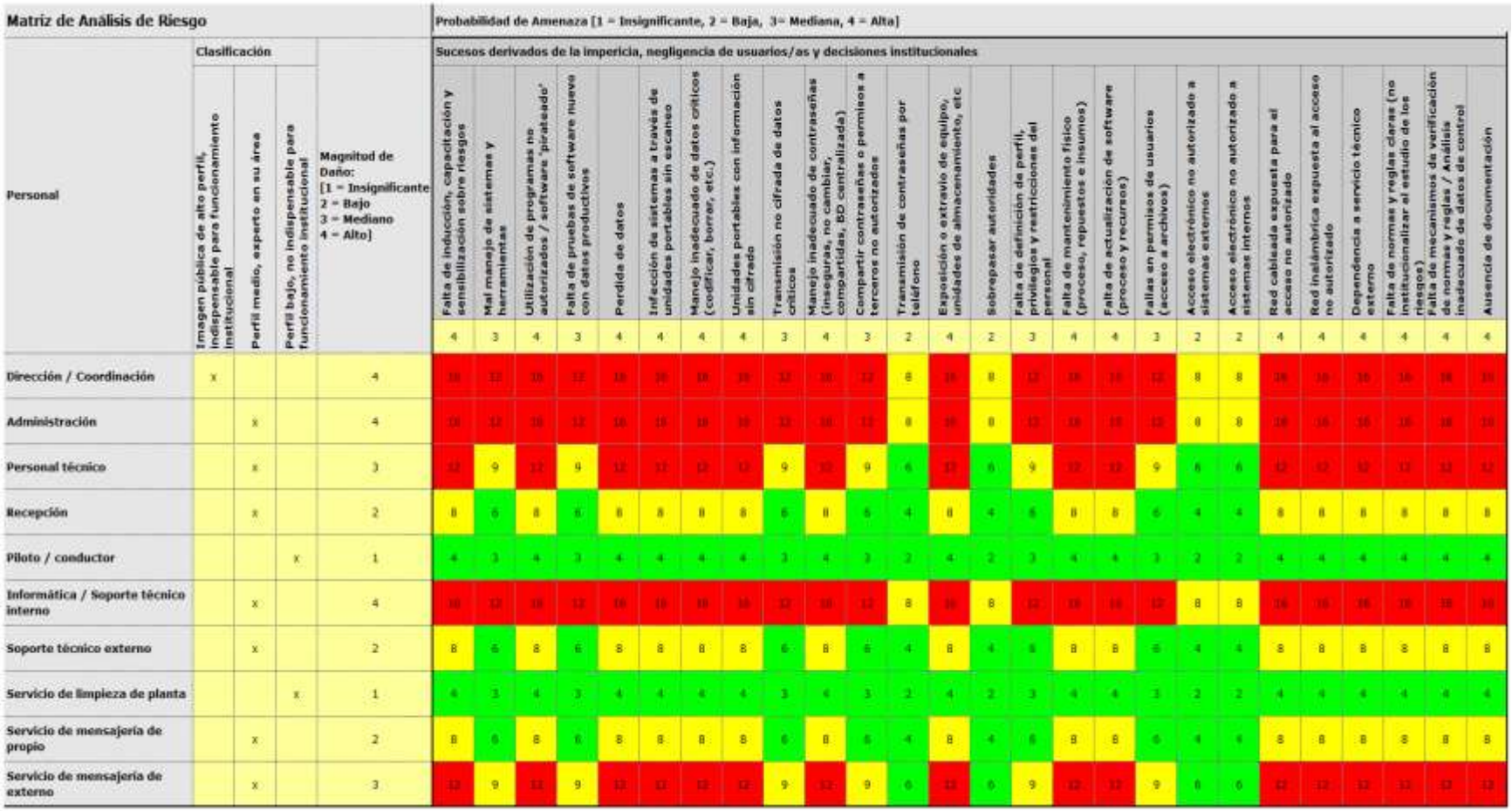
8.2. Sistemas e Infraestructura.

Matriz de Análisis de Riesgo	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																				
					Actos originados por la criminalidad común y motivación política													Sucesos de origen físico								
Sistemas e Infraestructura	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen, emocional)		Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / desfase	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
					2	2	2	3	3	2	4	4	3	4	2	4	2	4	2	2	3	4	2	3	3	3
Equipos de la red cableada (router, switch, etc.)	x		x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Equipos de la red inalámbrica (router, punto de acceso, etc.)	x		x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Cortafuego			x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Servidores	x		x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Computadoras		x	x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Portátiles		x	x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Programas de administración (contabilidad, manejo de personal, etc.)	x		x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Programas de manejo de proyectos	x		x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	x		x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Impresoras	x		x	3	6	6	6	9	9	6	12	12	9	12	6	12	6	12	6	6	9	12	6	9	9	9
Memorias portátiles			x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Celulares	x			2	4	4	4	6	6	4	8	8	6	8	4	8	4	8	4	4	6	8	4	6	6	6
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)		x	x	4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Vehículos	x		x	1	2	2	2	3	3	2	4	4	3	4	2	4	2	4	2	2	3	4	2	3	3	3

Matriz de Análisis de Riesgo	Clasificación				Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																									
					Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																									
Sistemas e Infraestructura	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Tranamisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Tranamisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de fotos de control	Ausencia de documentación
					4	3	4	3	4	4	4	4	3	4	3	2	4	2	3	4	4	3	2	2	4	4	4	4	4	4
Equipos de la red cableada (router, switch, etc.)	x		x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Equipos de la red inalámbrica (router, punto de acceso, etc.)	x		x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Cortafuego			x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Servidores	x		x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Computadoras		x	x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Portátiles		x	x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Programas de administración (contabilidad, manejo de personal, etc.)	x		x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Programas de manejo de proyectos	x		x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	x		x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Impresoras	x		x	3	12	9	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	6	6	12	12	12	12	12	12
Memorias portátiles			x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Celulares	x			2	8	6	8	6	8	8	8	8	6	8	6	4	8	4	6	8	8	6	4	4	8	8	8	8	8	8
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)		x	x	4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Vehículos	x		x	1	4	3	4	3	4	4	4	4	3	4	3	2	4	2	3	4	4	3	2	2	4	4	4	4	4	4

8.3. Personal.

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																				
	Clasificación				Actos originados por la criminalidad común y motivación política												Sucesos de origen físico								
Personal	Imagen pública de alto perfil, indispensable para funcionamiento institucional	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
					2	2	2	3	3	2	4	4	3	4	2	4	2	4	2	2	3	4	2	3	3	3
Dirección / Coordinación	x			4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Administración		x		4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Personal técnico		x		3	6	6	6	9	9	6	12	12	9	12	6	12	6	12	6	6	9	12	6	9	9	9
Recepción		x		2	4	4	4	6	6	4	8	8	6	8	4	8	4	8	4	4	6	8	4	6	6	6
Piloto / conductor			x	1	2	2	2	3	3	2	4	4	3	4	2	4	2	4	2	2	3	4	2	3	3	3
Informática / Soporte técnico interno		x		4	8	8	8	12	12	8	16	16	12	16	8	16	8	16	8	8	12	16	8	12	12	12
Soporte técnico externo		x		2	4	4	4	6	6	4	8	8	6	8	4	8	4	8	4	4	6	8	4	6	6	6
Servicio de limpieza de planta			x	1	2	2	2	3	3	2	4	4	3	4	2	4	2	4	2	2	3	4	2	3	3	3
Servicio de mensajería de propio		x		2	4	4	4	6	6	4	8	8	6	8	4	8	4	8	4	4	6	8	4	6	6	6
Servicio de mensajería de externo		x		3	6	6	6	9	9	6	12	12	9	12	6	12	6	12	6	6	9	12	6	9	9	9



Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																							
Personal	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																							
	Imagen pública de alto perfil, indispensable para funcionamiento institucional	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional		Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
					4	3	4	3	4	4	4	4	3	4	3	2	4	2	3	4	4	3	2	2	4	4	4	4	4	4
Dirección / Coordinación	x			4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Administración		x		4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Personal técnico		x		3	12	9	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	6	6	12	12	12	12	12	12
Recepción		x		2	8	6	8	6	8	8	8	8	6	8	6	4	8	4	6	8	8	6	4	4	8	8	8	8	8	8
Piloto / conductor			x	1	4	3	4	3	4	4	4	4	3	4	3	2	4	2	3	4	4	3	2	2	4	4	4	4	4	4
Informática / Soporte técnico interno		x		4	16	12	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	8	8	16	16	16	16	16	16
Soporte técnico externo		x		2	8	6	8	6	8	8	8	8	6	8	6	4	8	4	6	8	8	6	4	4	8	8	8	8	8	8
Servicio de limpieza de planta			x	1	4	3	4	3	4	4	4	4	3	4	3	2	4	2	3	4	4	3	2	2	4	4	4	4	4	4
Servicio de mensajería de propio		x		2	8	6	8	6	8	8	8	8	6	8	6	4	8	4	6	8	8	6	4	4	8	8	8	8	8	8
Servicio de mensajería de externo		x		3	12	9	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	6	6	12	12	12	12	12	12

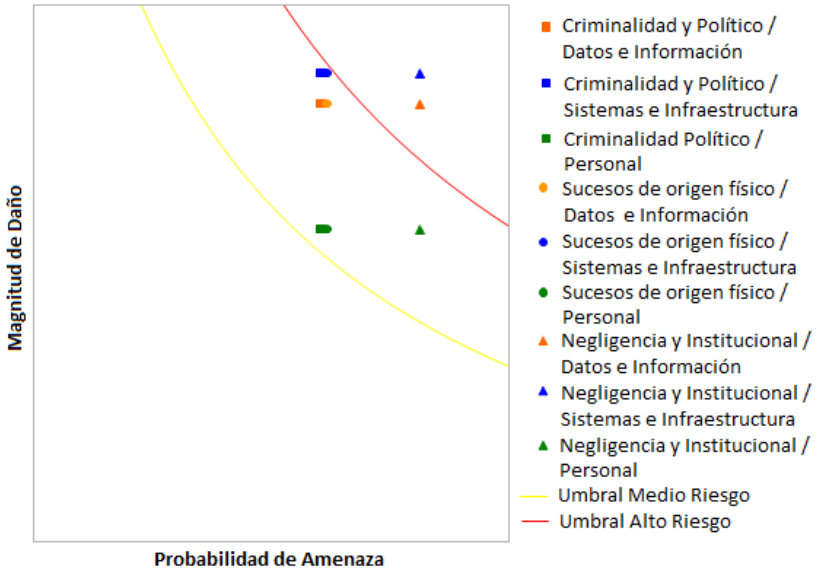
Figura 58. Análisis de Riesgo Promedio

		Probabilidad de Amenaza		
		Criminalidad y Político	**Sucesos de Origen Físico**	**Negligencia y Institucional**
Magnitud de Daño	**Datos e Información**	9,6	9,8	11,7
	Sistemas e Infraestructura	10,2	10,3	12,4
	Personal	7,4	7,5	9,0

Fuente: Autora del Proyecto

La probabilidad de que ocurran amenazas de tipo criminal, natural o por negligencia, se divide en tres (3) magnitudes de daño: baja, Mediana y Alta. La magnitud de daño baja se presenta cuando existen condiciones que hacen muy lejana la posibilidad de ataque, Mediana cuando existen condiciones que hacen poco probable un ataque en el corto plazo, pero que no son suficientes para evitarlo en el largo plazo, y Alta en casos donde el ataque es inminente, debido a que no existen condiciones internas y externas que impidan el desarrollo del ataque.

Figura 59. Análisis de Factores



Fuente: Autora del Proyecto

La figura anterior, corresponde a los factores (actos criminales, sucesos físicos y negligencia) que originan o hacen efectiva la amenaza a los activos (Datos e información, sistemas e infraestructura y el personal) de la Alcaldía, evaluados en un umbral de riesgo.

Bajo: corresponde a una probabilidad de amenaza baja que origina una magnitud de riesgo igualmente baja, debido a que existen condiciones que hacen muy lejana la posibilidad de ataque, manteniendo un nivel aceptable de riesgo para los activos de la Alcaldía.

Medio: hace referencia a una probabilidad de amenaza mediana que origina una magnitud de riesgo igualmente mediana, debido a que existen condiciones que hacen poco probable un ataque en el corto plazo, pero no son suficientes para evitarlo en largo plazo, provocando una alerta de riesgo para los activos de la Alcaldía, la cual debe ser monitoreada y evaluada constantemente aplicando medidas correctivas que disminuyan la amenaza y la orienten a un nivel aceptable o nulo.

Alto: refleja una probabilidad de amenaza alta originando una magnitud de riesgo igualmente alta, donde el ataque es inminente, debido a que no existen condiciones internas y externas que impidan el desarrollo del ataque.

4. PRESENTACIÓN DE RESULTADOS

4.1 RECONOCIMIENTO DE LA ALCALDÍA MUNICIPAL DE RÍO DE ORO (CESAR)

4.1.1 Direccionamiento Estratégico

4.1.1.1 Misión. El municipio de Río de Oro es una entidad estatal de corte social, cuyo objetivo es el desarrollo humano y social, a través de una adecuada ejecución financiera para la construcción de obras de desarrollo social, la eficiente prestación de servicios masivos domiciliarios, el acceso equitativo a más y mejores oportunidades, la generación de empleo, el impulso a la iniciativa empresarial con fortalezas ambientales y culturales para ser aprovechadas de forma sostenible.

4.1.1.2 Visión. En el 2032 Río de Oro será un municipio prospero, incluyente y participativo, con altas estándares de calidad en la prestación de los servicios de salud, educación y domiciliarios, que le permitirán gozar a sus habitantes de un buen nivel de vida, plenas garantías de sus derechos y cumplidores de sus deberes.

4.1.1.3 Reseña Histórica. No tiene una fecha clara y precisa sobre la fundación del Sitio de Río de oro, como en un inicio fue denominado, y según historiadores se cree que comenzó a ser poblado desde 1658 por encomenderos españoles. Se sostiene que los primeros encomenderos en hacer su aparición en estas tierras fueron: Mateo Corzo, Juan de Gálvez Caballero y Catalina Gálvez de Caballero. También se habla de Luís Téllez Blanco y Gaspar Barbosa de Marín Pedroso como primeros pobladores; pero se habla de construcción, más no de fundación. También se afirma que las primeras construcciones se realizaron en tierras que fueron donadas por Antón García de Bonilla. Tampoco existe una fuente precisa de la fundación del convento de los agustinos calzados, de quienes se dice que fundaron a Río de Oro en 1658.

En síntesis se habla de construcción más no de fundación, lo que lógicamente ha debido tener lugar con antelación, al año citado, ya que a comienzos de la conquista Ambrosio Alfinger, llegó hasta las tribus de los carates o caretas en los puntos llamados después Río de Oro y Gonzáles.

4.1.1.4 Objetivos. El municipio de Río de Oro avanzará en la garantía de derechos a niños, niñas y adolescentes, haciendo extensivas las acciones y programas a todos los grupos poblacionales urbano y rurales, con un enfoque inclusivo, diferencial, con equidad de género y participativo; promoviendo la convivencia; la sana recreación y el deporte y mejorando la prestación de servicios de salud y educación.

4.1.1.5 Principios.

Principios del Control Interno

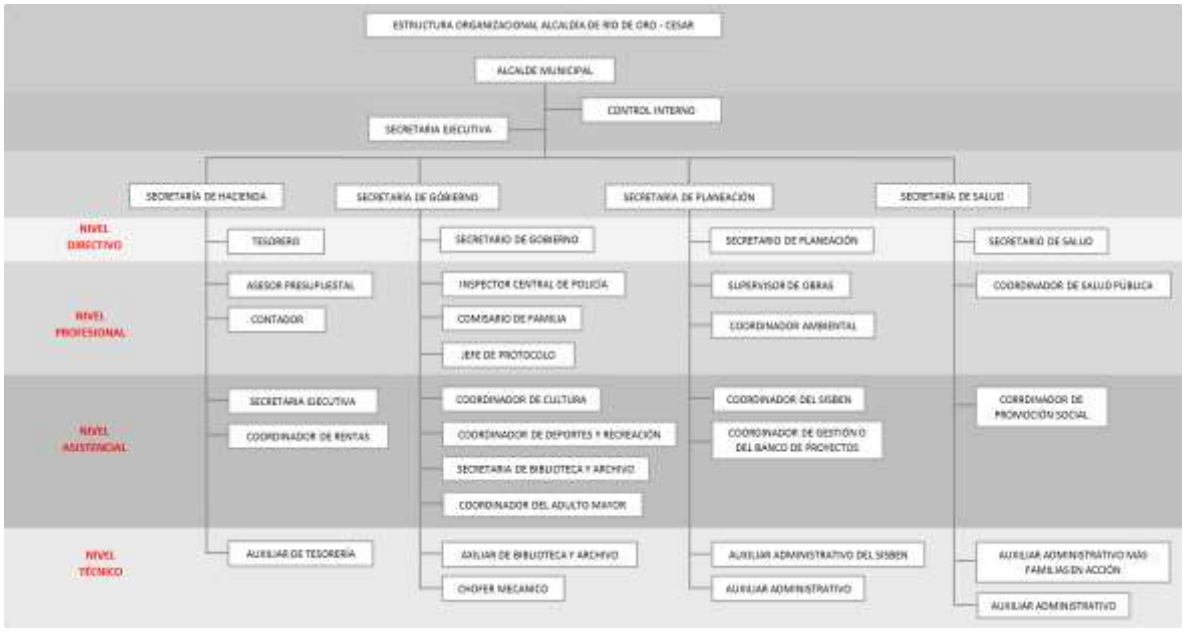
La Constitución Política de 1991, estableció los principios que deben cumplirse en el ejercicio de la Función Pública de Administrar el Estado, constituyéndose en los preceptos fundamentales definidos para encaminar su desarrollo y otorgar orientación estratégica a la toma de decisiones.

Están presentes en todos los procesos, actividades o tareas emprendidas por la entidad pública a fin de cumplir con su propósito institucional.

Lo anterior, relacionado con el cumplimiento de los objetivos de la institución pública, de los cuales el Control Interno se constituye en el medio para llegar a este fin, obliga a que estos principios deben tomarse como la base sobre la cual establecer el Control Interno, a fin de apoyar a la entidad a cumplir sus objetivos y coordinar sus actuaciones hacia el logro de los fines esenciales del Estado. (Ver Anexo C)

4.1.1.6 Estructura Orgánica de la Alcaldía Municipal de Río de Oro (Cesar).

Figura 60. Estructura Orgánica de la Alcaldía.



Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

4.1.2 Modelo de Negocios para la Alcaldía Municipal de Río de Oro (Cesar).

(Ver Anexo D, Anexo E)

4.1.3 Modelado de procesos del negocio

Procesos Direccionales: Son los procesos gestionados por la administración municipal y están relacionados con la planeación estratégica, políticas, objetivos y suministros de los recursos del sistema de gestión de la calidad. Entre esto se encuentra los procesos generales de carrera administrativa, control disciplinarios y de jefatura del personal y revisión por la dirección.

Procesos Misionales: Estos procesos relacionados con los servicios que brinda la Administración Municipal a la comunidad; entre estos se encuentran las siguientes: Procesos de Educación, Salud Pública, Deporte, Saneamiento Básico, Desarrollo Urbano, Transporte, Orden Público, Desarrollo Programas de Inversión, Planeación Tributaria, Presupuestales, Planeación Financiera y Hacienda.

Procesos de Apoyo: Estos procesos contribuyen con la gestión de los procesos direccionales, misionales y de evaluación; entre estos se encuentran los siguientes: Gestión de Contratación, Gestión de Talento Humano, Gestión Jurídica, Gestión Financiera, Gestión de Recursos Físicos, Servicio de Información.

Procesos de Evaluación: Incluye aquellos procesos para medir y recopilar datos destinados a realizar el análisis del desempeño y la mejora continua del sistema de gestión de la calidad, entre esto se encuentran los siguientes procesos: Proceso de control interno, proceso de evaluación y de mejora continua.

- PROCESOS.

La Administración Municipal ha descrito o caracterizado cada uno de sus procesos con el fin de poder normalizarlos, controlarlos y disminuir la variación en los mismos, para ello se define el objetivo, alcance, los proveedores, entradas, actividades, salidas y usuario, responsables, parámetros, medición y seguimiento, puntos de control, documentos internos y externos, requisitos legales y de la NTCGP 1000:2004 aplicables; que permitan mantener un monitoreo y mejoramiento continuo.

Diagrama de Actividades

La Alcaldía ejecuta sus procesos utilizando las cadenas de valor diseñadas para el direccionamiento estratégico para el logro de las competencias constitucionales y legales de la entidad.

Figura 61. Cadena de Valor – Macro Procesos

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 62. Cadena de Valor – Procesos Principales del Macro Proceso Estratégico

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

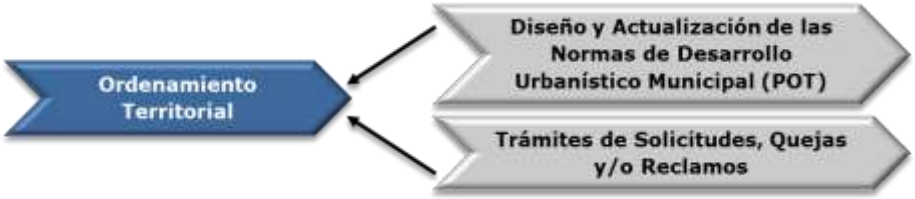
Figura 63. Cadena de Valor – Subprocesos del Proceso Principal Planeación y Direccionamiento Estratégico

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 64. Cadena de Valor – Procedimientos del Subproceso Planeación y Direccionamiento.

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 65. Cadena de Valor – Procedimientos del Subproceso Ordenamiento Territorial



Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

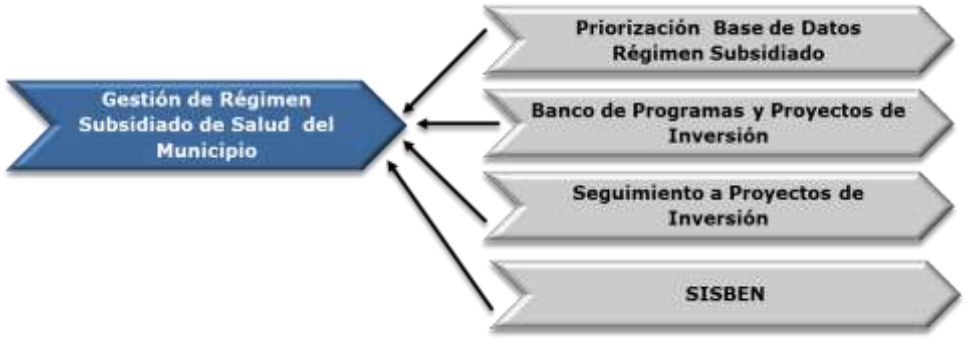
Figura 66. Cadena de Valor – Procesos Principales del Macro Proceso Misional

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 67. Cadena de Valor – Subprocesos del Proceso Principal Salud

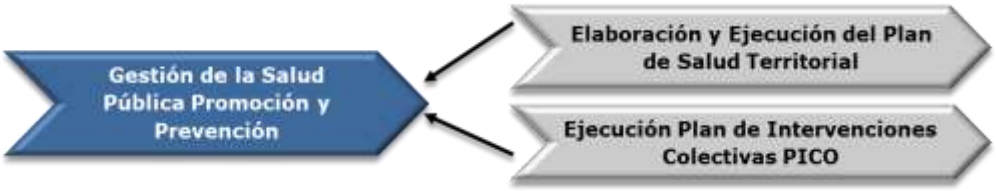
Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 68. Cadena de Valor – Procedimientos del Subproceso Gestión de Régimen Subsidiado de Salud del Municipio



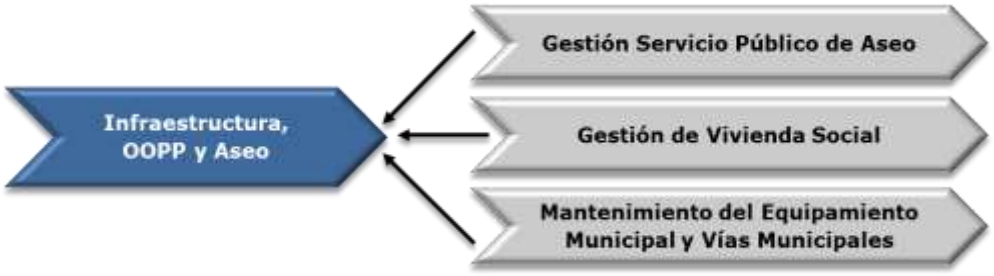
Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 69. Cadena de Valor – Procedimientos del Subproceso Gestión de la Salud Pública Promoción y Prevención



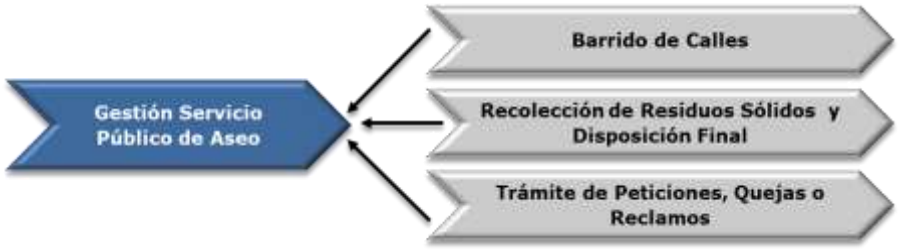
Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 70. Cadena de Valor – Subprocesos del Proceso Principal Infraestructura, OOPP y Aseo



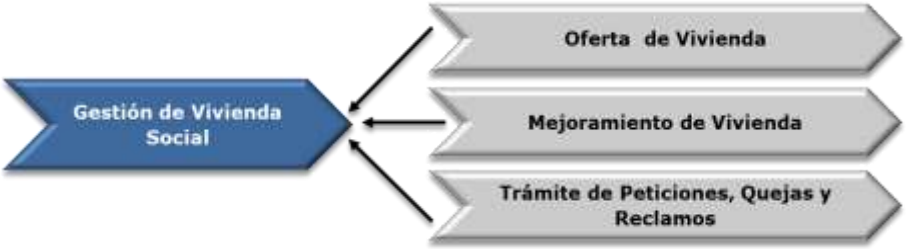
Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 71. Cadena de Valor – Procedimientos del Subproceso Gestión Servicio Público de Aseo



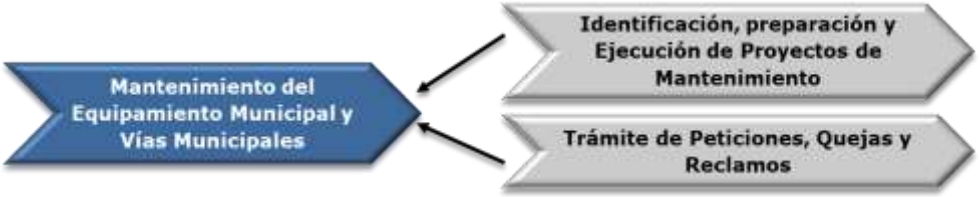
Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 72. Cadena de Valor – Procedimientos del Subproceso Gestión de Vivienda Social



Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 73. Cadena de Valor – Procedimientos del Subproceso Mantenimiento del Equipamiento Municipal y Vías Municipales



Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 74. Cadena de Valor – Subprocesos del Proceso Principal Promoción y Desarrollo de la Educación

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

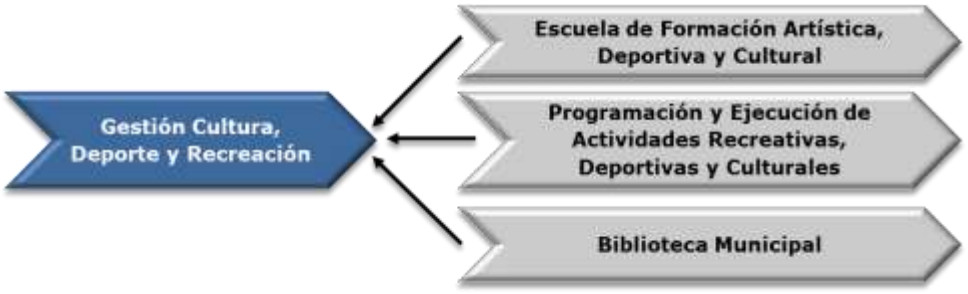
Figura 75. Cadena de Valor – Procedimientos del Subproceso Calidad de la Educación

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 76. Cadena de Valor – Subprocesos del Proceso Principal Gestión Cultura, Deporte y Recreación

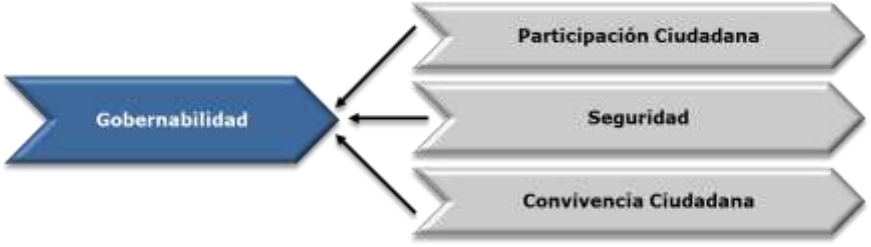
Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 77. Cadena de Valor – Procedimientos del Subproceso Gestión Cultura, Deporte y Recreación



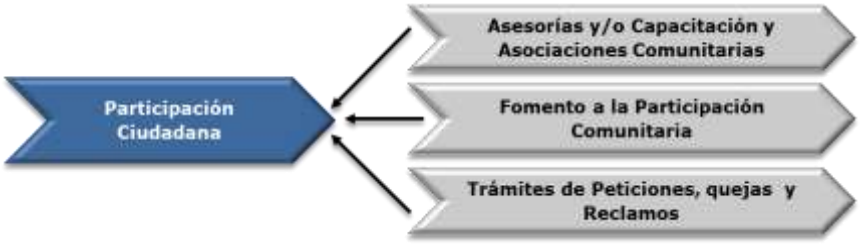
Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 78. Cadena de Valor – Subprocesos del Proceso Principal Gobernabilidad



Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 79. Cadena de Valor – Procedimientos del Subproceso Participación Ciudadana



Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 80. Cadena de Valor – Procedimientos del Subproceso Seguridad

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

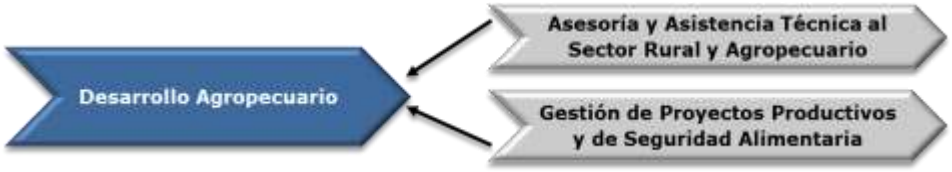
Figura 81. Cadena de Valor – Procedimientos del Subproceso Convivencia Ciudadana

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 82. Cadena de Valor – Subprocesos del Proceso Principal Promoción del Crecimiento Económico

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 83. Cadena de Valor – Procedimientos del Subproceso Desarrollo Agropecuario



Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 84. Cadena de Valor – Subprocesos del Proceso Principal Gestión Ambiental

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

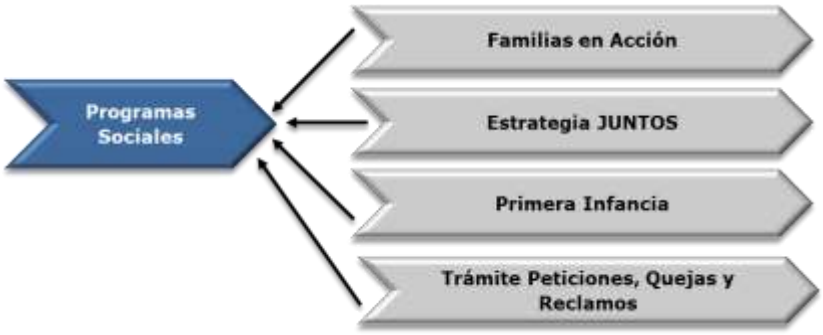
Figura 85. Cadena de Valor – Procedimientos del Subproceso Gestión Medio Ambiente

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 86. Cadena de Valor – Subprocesos del Proceso Principal Gestión Social

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 87. Cadena de Valor – Procedimientos del Subproceso Programas Sociales

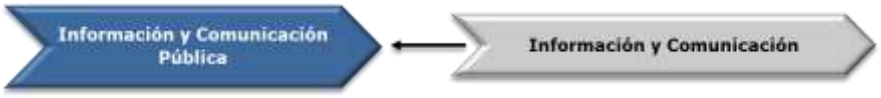


Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 88. Cadena de Valor – Procesos Principales del Macro Proceso Apoyo

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Ilustración 89. Cadena de Valor – Subprocesos del Proceso Principal Información y Comunicación Pública

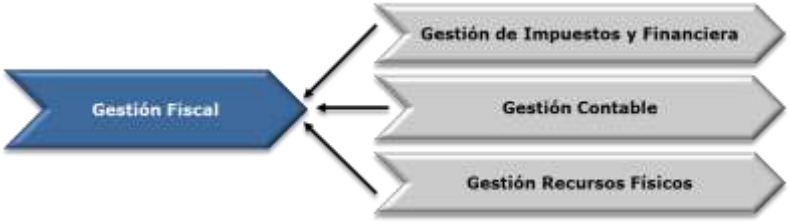


Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 90. Cadena de Valor – Procedimientos del Subproceso Información y Comunicación

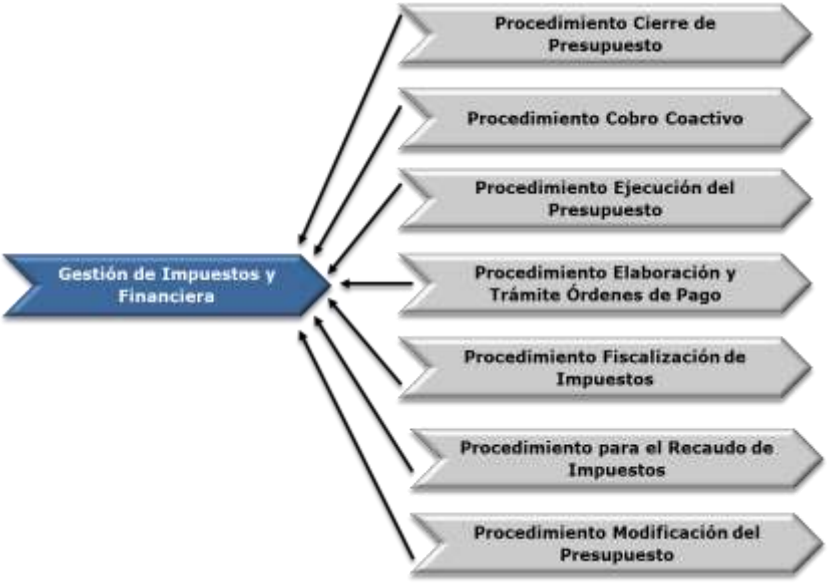
Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 91. Cadena de Valor – Subprocesos del Proceso Principal Gestión Fiscal



Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 92. Cadena de Valor – Procedimientos del Subproceso Gestión de Impuestos y Financiera



Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

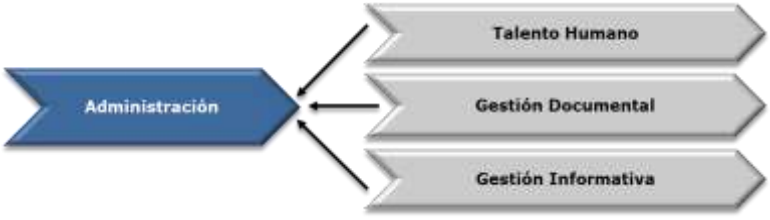
Figura 93. Cadena de Valor – Subprocesos del Proceso Principal Gestión Contable

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 94. Cadena de Valor – Procedimientos del Subproceso Gestión Recursos Físicos

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 95. Cadena de Valor – Subprocesos del Proceso Principal Administración

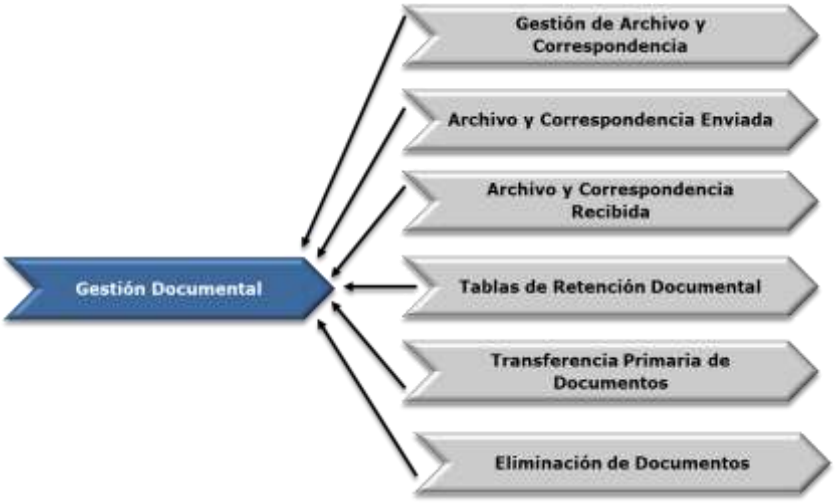


Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 96. Cadena de Valor – Procedimientos del Subproceso Talento Humano

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 97. Cadena de Valor – Procedimientos del Subproceso Gestión Documental



Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

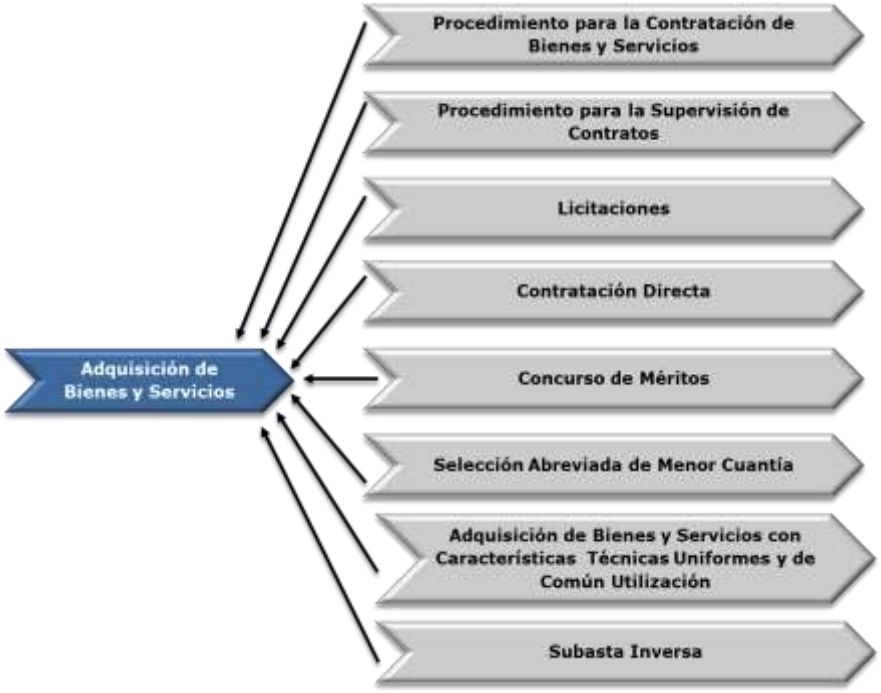
Figura 98. Cadena de Valor – Procedimientos del Subproceso Gestión Informativa

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 99. Cadena de Valor – Subprocesos del Proceso Principal Contratación

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 100. Cadena de Valor – Procedimientos del Subproceso Adquisición de Bienes y Servicios



Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 101. Cadena de Valor – Procesos Principales del Macro Proceso Evaluación

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Figura 102. Cadena de Valor – Subprocesos del Proceso Principal Medición, Análisis y Mejora

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

4.1.4 Infraestructura tecnológica.

La Alcaldía Municipal de Río de Oro (Cesar), cuenta con equipos de cómputo en las áreas de trabajo. Se relaciona las características de los dispositivos para la ejecución de los procesos de la misma.

4.1.4.1 Equipos de Cómputo. (Ver Anexo F)

4.1.4.2 Equipos de Oficina. (Ver Anexo G)

4.1.4.3 Dispositivos de Comunicaciones. (Ver Anexo H)

La Alcaldía se encuentra interconectada en cinco (5) nodos en su único edificio de dos plantas.

- **Planos de Arquitectura Física y de Red.**

Figura 103. Plano – Primer piso

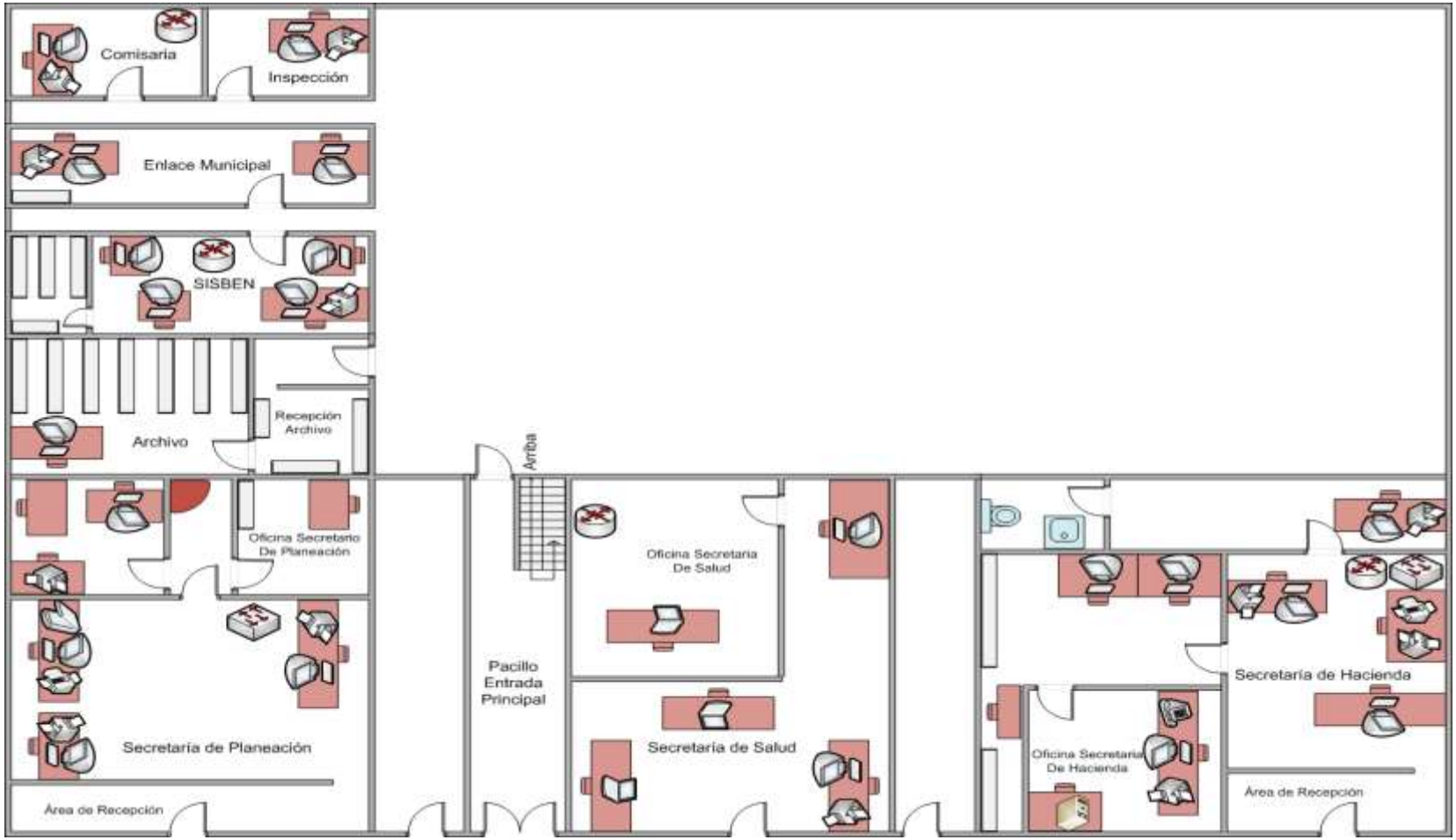
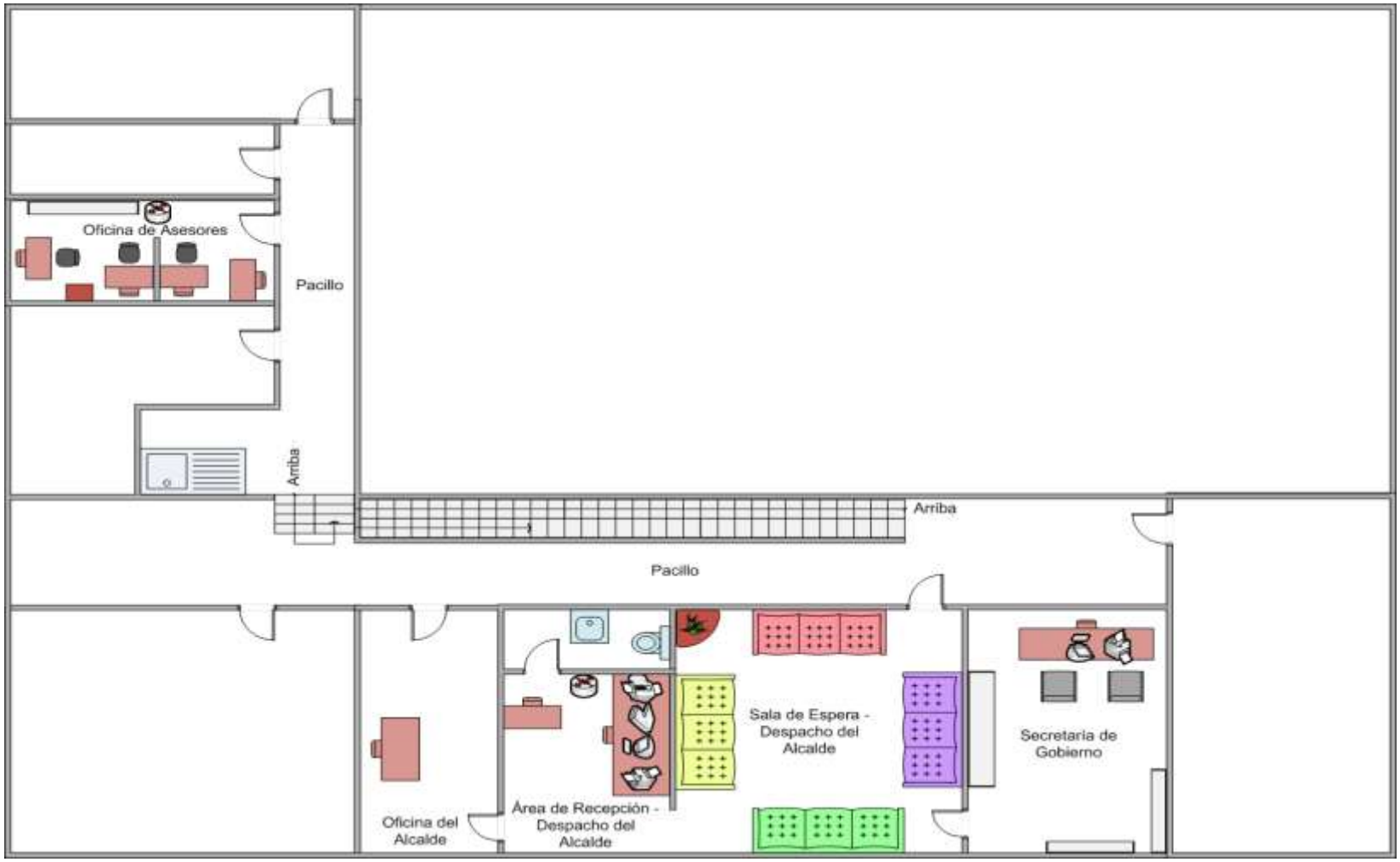


Figura 104. Plano – Segundo Piso



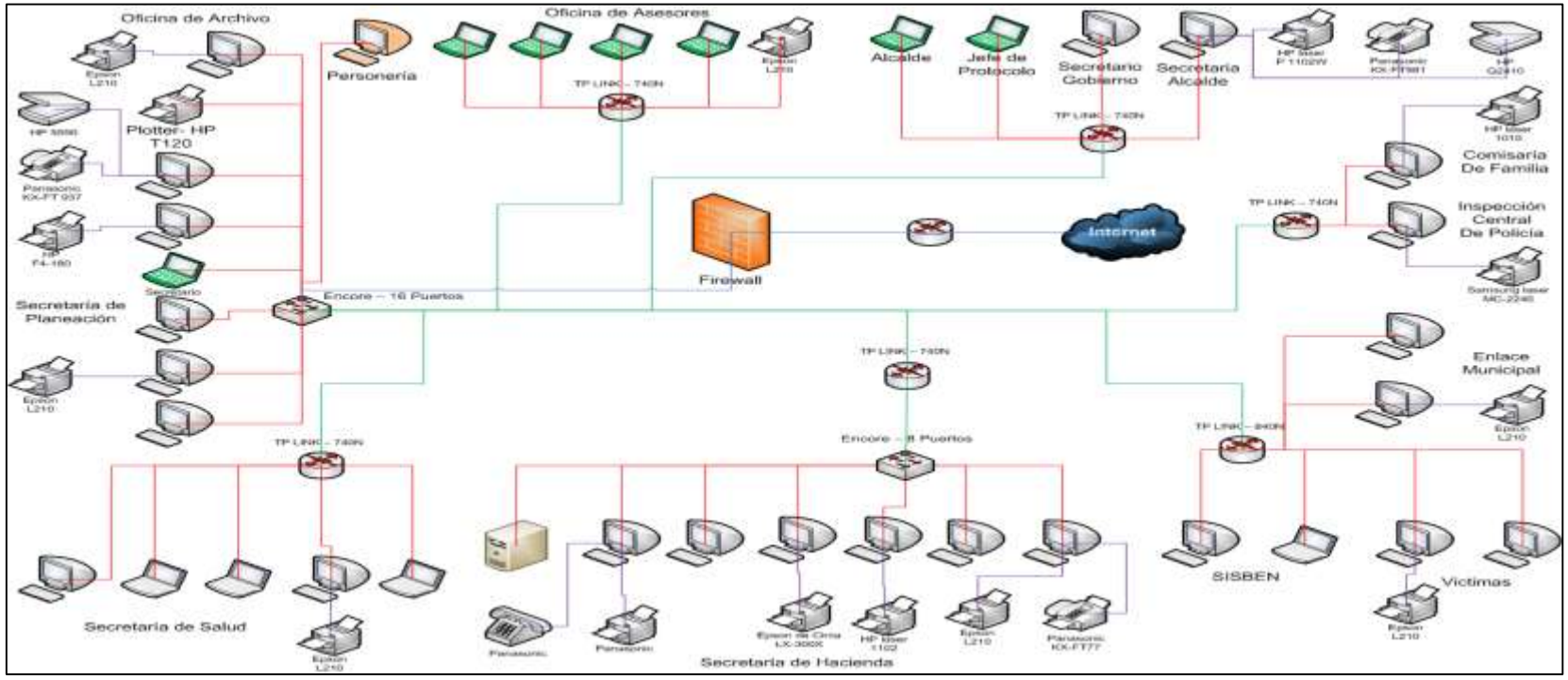
4.1.4.4 Tipo de Red.

Referente al tipo de red, la Alcaldía Municipal cuenta con una red LAN Fast Ethernet 100/1000.

4.1.4.5 Topología.

La topología presente en la Alcaldía es estrella extendida, utilizando para las conexiones cable UTP categoría 5e.

Figura 105. Esquema de red de la Alcaldía Municipal de Río de Oro (Cesar).



El proveedor de servicios de internet es RYO Comunicaciones S.A.S. contratado para conectar las diferentes dependencias de la Alcaldía.

4.1.4.6 Sistemas Operativos. (Ver Anexo I)

4.1.4.7 Software Empresarial. (Ver Anexo J)

Sistema Contable y Administrativo Integrado (Visual TNS) – Sector Oficial

Características: Diseño claro, fácil de entender para que los usuarios puedan aprovechar al máximo todo lo que ofrece el sistema, cubriendo sus necesidades de disposición de información precisa oportuna y veraz.

Además se caracteriza por estar en continua adaptación a los cambios que se presentan por legislación o mejoras técnicas como rendimiento, seguridad, facilidades de operación y acoplamiento a nuevas plataformas.

Módulos que lo componen: Contabilidad, Administración de Tesorería y Manejo de Presupuesto Oficial.

- **Módulo de Contabilidad:** Diseñado para llevar en forma oportuna la información contable, se caracteriza por manejar múltiples empresas, no requerir de cierres (períodos abiertos). Registra los asientos de Egresos, Ingresos, Notas de Contabilidad y Comprobantes de
Contabilidad.

Permite además las siguientes funciones:

- Definición del plan de cuentas en múltiples niveles.
- Manejo de Centros de Costos y Áreas administrativas.
- Permite manejar múltiples empresas.
- Evita los procesos de redigitación de información ya que se encuentra integrado en línea con los demás módulo operativos y permite sacar copias de documentos a partir de otros similares.
- Lleva un registro completo de terceros y su historial de movimientos por año.

Suministra los siguientes informes:

- Balances de Comprobación.
- Balance General.
- Estados de Ganancias y Pérdidas.
- Libro Diario, Libros Auxiliares y Mayor y Balances.
- Expide los certificados de Retención en la Fuente y Rete IVA.

- Genera medios magnéticos Exógena, archivos del CHIP1 y CHIP2, CGR a la contraloría, archivos SIA y los demás reportes para rendir cuentas a las Entidades de Control como el FUT y SIDEF.

- **Módulo de Administración de Tesorería:** Facilita el control de Ingresos, Egresos de efectivo y cheques a la institución en forma sincronizada con el programa de contabilidad. Maneja diferentes cuentas bancarias, imprime múltiples formatos de cheques, genera los informes de saldos y estado de bancos, flujo de caja; informes de Cuentas por Pagar de otras vigencias y el informe de operaciones efectivas de caja.

Permite además:

- Elaborar Comprobantes de Egreso, Recibos de Caja y Traslados bancarios.
- Boletín de bancos discriminando el saldo.
- Ejecución mensual y acumulada del PAC.
- Imprimir Relación de ingresos y egresos por Banco y concepto.
- Resumen y movimientos detallados por conceptos.
- Saldos de definitivas por pagar y ejecuciones presupuestales de pagos a rubros.

- **Módulo de Presupuesto Oficial:** Registra las transacciones de ejecución presupuestal de Ingresos y Gastos de Otros recursos y Recursos nacionales. Genera los informes de Ejecución Mensual de Ingresos y Gastos, Planilla Diaria de Compromisos y Giros, y los Libros de Ejecución Presupuestal exigidos por las Entidades de Control.

- Permite crear rubros de ingresos y egresos multinivel, permitiendo mayorizar los saldos en cualquier estructura jerárquica que se configure.
- Los rubros se pueden parametrizar para la integración contable, generación SIDEF, FUT, Planeación, CGR, SIA, Desplazados y Regalías.
- Maneja Fuentes de Recurso, Centros de Costos, Áreas administrativas.
- Maneja la creación del presupuesto inicial.
- Modificaciones al presupuesto: Incorporaciones/reducciones, Créditos/Contracréditos, Liberaciones/Aplazamientos.
- Control del PAC mensual y acumulado por rubro desde la disponibilidad, registro o definitiva.
- Control de PAC por cada registro para programación de pagos.
- Generación e impresión de Disponibilidades, Registros Presupuestales y Definitivas de pagos.
- Se pueden realizar ajustes de saldo a las disponibilidades, registros, definitivas y pagos.
- Imprime ejecuciones de Gastos e Ingresos mensual y acumulado.
- Ejecución Mensual y Acumuladas del PAC.
- Planillas diarias de Disponibilidades, registros y definitivas.
- Impresión de Saldos de disponibilidades, registros y definitivas.
- Libro auxiliar de Movimientos de Rubros.

- Conciliación Presupuestal para control de pagos de definitivas con sus comprobantes de egreso.

4.2 COMPARATIVA ENTRE ISO/IEC 27002, ITIL V3 Y COBIT 4.1

Actualmente existen varios estándares certificables que garantizan la protección de los Sistemas Informáticos, así como un buen uso de la información. Poseer alguno de estos estándares significa cumplir con la Ley Orgánica de Protección de Datos (LOPD), ya que impone controles más restrictivos que esta ley.

El principal estándar de seguridad informática y de la información, que define los requisitos de auditoría y sistemas de gestión de seguridad de la información es el ISO/IEC 27001. Este estándar puede usarse en conjunción con el ISO/IEC 27002, el cual se conforma como un código internacional de buenas prácticas de seguridad informática y de la información.

Existen otros estándares de carácter más general que también cubren la seguridad informática como parte del desarrollo de una infraestructura de tecnología de la información completa. Ejemplos de este tipo son COBIT (Objetivos de Control de la Tecnologías de la Información) e ITIL (Biblioteca de Infraestructura de Tecnologías de Información). Estos estándares surgen como buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información.

4.2.1 ISO/IEC 27002

El ISO/IEC 27002, también conocido como ISO 17799, es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización.

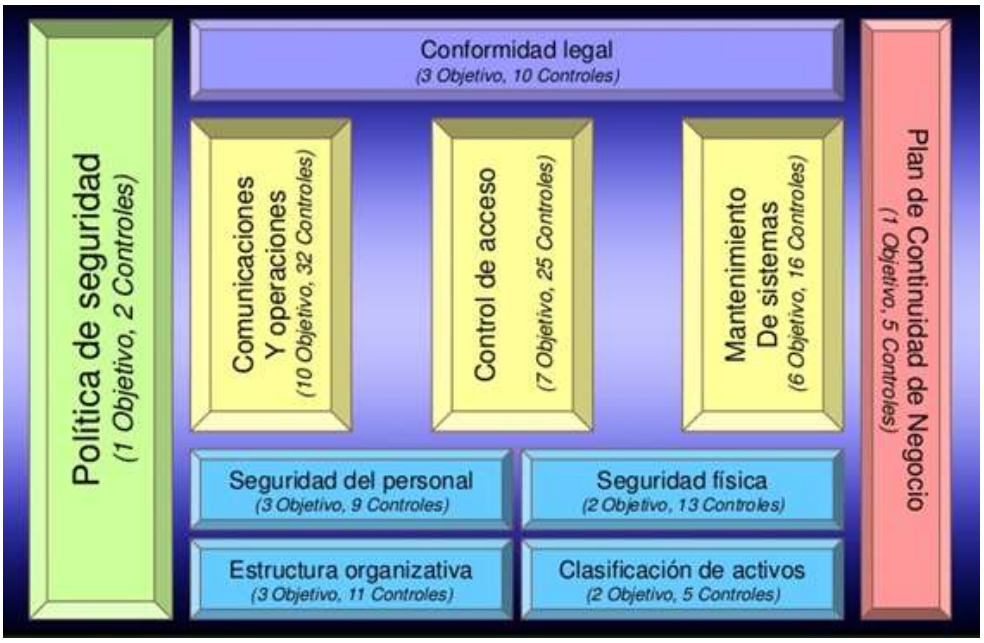
El objetivo de la norma ISO/IEC 27002 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

Se trata de una norma no certificable, pero que recoge la relación de controles a aplicar para establecer un SGSI.

Estructura del estándar:

El ISO/IEC 27002 contiene 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridad principales.
A continuación se detallan las diferentes cláusulas con sus categorías y los objetivos que persiguen cada una de ellas:

Figura 106. Modelo de Procesos ISO/IEC 27002



Fuente. Mapa de Procesos 27002.

1. Política de Seguridad

- **Política de seguridad de la información.** Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.

2. Organización de la Seguridad de la Información

- **Organización interna.** Manejar la seguridad de la información dentro de la organización.

- **Grupos o personas externas.** Mantener la seguridad de la información y los medios de procesamiento de información de la organización que son ingresados, procesados, comunicados o manejados por, grupos externos.

3. Gestión de Activos

- **Responsabilidad por los activos.** Lograr y mantener una apropiada protección de los activos organizacionales.

- **Clasificación de la información.** Asegurar que la información reciba un nivel de protección apropiado.

4. Seguridad de Recursos Humanos

- **Antes del empleo.** Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados, y reducir el riesgo de robo, fraude y mal uso de los medios.

- **Durante el empleo.** Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

- **Finalización o cambio de empleo.** Asegurar que los usuarios empleados, contratistas y terceras personas salgan de la organización o cambien de empleo de una manera ordenada.

5. Seguridad Física y Ambiental

- **Áreas seguras.** Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

- **Equipo de seguridad.** Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.

6. Gestión de Comunicaciones y Operaciones

- **Procedimientos y responsabilidades operacionales.** Asegurar la operación correcta y segura de los medios de procesamiento de la información.

- **Gestión de la entrega del servicio de terceros.** Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros.

- **Planificación y aceptación del sistema.** Minimizar el riesgo de fallos en el sistema.
- **Protección contra el código malicioso y móvil.** Proteger la integridad del software y la integración.

- **Copia de Seguridad.** Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

- **Gestión de seguridad de la red.** Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

- **Gestión de medios.** Evitar la divulgación no autorizada, la modificación, eliminación o destrucción de activos y la interrupción de las actividades comerciales.

- **Intercambio de información.** Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa.

- **Servicios de comercio electrónico.** Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro.

- **Monitorización.** Detectar las actividades de procesamiento de información no autorizadas.

7. Control de Acceso

- **Requerimiento del negocio para el control del acceso.** Controlar el acceso a la información.

- **Gestión de acceso del usuario.** Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.

- **Responsabilidades del usuario.** Evitar el acceso de usuarios no autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.

- **Control de acceso a la red.** Evitar el acceso no autorizado a los servicios de la red.

- **Control del acceso al sistema operativo.** Evitar el acceso no autorizado a los sistemas operativos.

- **Control de acceso a la aplicación y la información.** Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.

- **Computación y tele-trabajo móvil.** Asegurar la seguridad de la información cuando se utiliza medios de computación y tele-trabajo móvil.

8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

- **Requerimientos de seguridad de los sistemas de información.** Garantizar que la seguridad sea una parte integral de los sistemas de información.

- **Procesamiento correcto en las aplicaciones.** Prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.

- **Controles criptográficos.** Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos.

- **Seguridad de los archivos del sistema.** Garantizar la seguridad de los archivos del sistema.

- **Seguridad en los procesos de desarrollo y soporte.** Mantener la seguridad del software y la información del sistema de aplicación.

- **Gestión de la Vulnerabilidad Técnica.** Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

9. Gestión de Incidentes de Seguridad de la Información

- **Informe de los eventos y debilidades de la seguridad de la información.** Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

- **Gestión de los incidentes y mejoras en la seguridad de la información.** Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

10. Gestión de la Continuidad del Negocio

- **Aspectos de la seguridad de la información de la gestión de la continuidad del negocio.** Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallos importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

11. Cumplimiento

- **Cumplimiento de los requerimientos legales.** Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

- **Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico.** Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

- **Consideraciones de auditoría de los sistemas de información.** Maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información.

4.2.2 COBIT 4.1

El modelo COBIT (Objetivos de Control para la Información y Tecnología Relacionada) es el marco aceptado internacionalmente de buenas prácticas para el control de la información TI y los riesgos que conllevan. COBIT se usa para implementar el gobierno de TI y mejorar los controles de TI. De igual manera, contiene objetivos de control, directrices de aseguramiento, mediciones de desempeño y resultados, factores críticos de éxito y modelos de madurez.

Para apoyar a las organizaciones a satisfacer exitosamente los desafíos de los negocios actualmente, el IT Governance Institute (ITGI) publicó la versión de COBIT 4.1.

Figura 107. Modelo COBIT 4.1

Fuente: www.fedeac.com

COBIT es un marco de Gestión de TI y un conjunto de herramientas de soporte para el gobierno de TI, que permite a los gerentes cubrir la brecha entre los requisitos de control, los aspectos técnicos y riesgos de negocio.

COBIT hace viable el desarrollo de una política clara y buenas prácticas para los controles de TI a través de las organizaciones.

COBIT hace énfasis en la conformidad de regulaciones, ayuda a las organizaciones a incrementar el valor alcanzado desde la TI, permite el alineamiento y simplifica la implementación de COBIT.

El Marco de Referencia de COBIT 4.1, está conformado por 34 Objetivos de Control de alto nivel, todos diseñados para cada uno de los Procesos de TI, los cuales están agrupados en cuatro grandes secciones mejor conocidos como dominios, estos se equiparán a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

- Dominio Planear y Organizar (PO). Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir mejor con los objetivos del negocio. Es importante mencionar que la realización de la visión estratégica requiere ser

planeada, comunicada y administrada desde diferentes perspectivas; y finalmente, la implementación de una estructura organizacional y tecnológica apropiada.

La gerencia espera cubrir la alineación de la estrategia de TI con el negocio, optimizar el uso de recursos, el entendimiento de los objetivos de TI por parte de la organización, la administración de riesgos y calidad en los sistemas de TI para las necesidades del negocio.

- Dominio Adquirir e Implementar (AI). Con el fin de cumplir una estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas, como también implementadas e integradas en los proceso del negocio. Además, el cambio y el mantenimiento de los sistemas existentes serán cubiertos para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.
La gerencia con este dominio pretende cubrir, que los nuevos proyectos generen soluciones que satisfagan las necesidades del negocio, que sean entregados en tiempo y dentro del presupuesto, que los nuevos sistemas una vez implementados trabajen adecuadamente y que los cambios no afecten las operaciones actuales del negocio.

- Dominio Entregar y Dar Soporte (DS). Involucra la entrega en sí de los servicios requeridos, incluyendo la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte a los usuarios del servicio, la administración de los datos y de las instalaciones operativas.

El objetivo es lograr que los servicios de TI se entreguen de acuerdo con las prioridades del negocio, la optimización de costos, asegurar que la fuerza de trabajo utilice los sistemas de modo productivo y seguro, implantar de forma correcta la confidencialidad, la integridad y la disponibilidad.

- Dominio Monitorear y Evaluar (ME). La totalidad de los proceso de TI deben de ser evaluados regularmente en el tiempo, para conocer su calidad y cumplimiento de los requerimientos de control. Este dominio incluye la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

Con esto se obtendrá de manera oportuna la detección de problemas por medio de la medición del desempeño, se garantiza que los controles internos sean efectivos y eficientes, la vinculación del desempeño de TI con las metas del negocio así como la medición y reporte de riesgos, además del control, cumplimiento y desempeño.

4.2.3 ITIL V3

La Biblioteca de Infraestructura de Tecnologías de la Información ITIL está basada en un conjunto de mejores prácticas para la gestión de servicios de tecnologías de la información en lo referente a personas, procesos y tecnología, las cuales fueron desarrolladas por la OGC (Oficina Gubernamental de Comercio) del Reino Unido, y que describe los procesos necesarios para administrar el área de TI eficazmente con el fin de optimizar beneficios y garantizar la integración de los servicios en la cadena de valor de las unidades de negocio.

El conjunto de mejores prácticas de ITIL permite hacer más eficiente la gestión de servicio de TI, generar orden, lenguaje y procesos comunes, que establecen la mejor manera de hacer las cosas. Este estándar no es una solución en sí; para lograrlo es fundamental contar con personas con el conocimiento para aplicar las recomendaciones y procesos necesarios. La metodología ITIL se asienta sobre la base de una decena de procesos, cuyos objetivos principales son: el incremento de la calidad de servicio y el control eficaz de los costes.

Figura 108. Modelo de ITIL V3.

Fuente: Mapa de procesos TI.

ITIL v3 consta de cinco libros de referencia que se irán complementando tanto con publicaciones más específicas sobre mercados verticales e industrias (Sector Público, Servicios Financieros), como con una constante aportación de material en la Web. Los cinco libros de referencia de ITIL v3 son los siguientes:

- Estrategia del servicio (ServiceStrategy)
- Diseño del servicio (ServiceDesing)
- Transición del servicio (ServiceTransition)
- Operación del servicio (ServiceOperation)
- Mejora continua del servicio (ContinualService)

El principal aporte de ITIL V3 es la vertebración de los libros en torno al ciclo de vida del servicio. Con ello se pretenden obtener beneficios tales como establecer la integración de la estrategia de negocio con la estrategia de los servicios de TI, facilitar el diseño de servicios ágiles y el cálculo del ROI, y proporcionar modelos de transición de servicios que sean válidos para una gran variedad de innovaciones. También se pretende mejorar la gestión de los proveedores de servicio según los modelos de subcontratación, así como la facilidad de implantación y de gestión de servicios, según las actuales necesidades de negocio, y la medición y demostración del valor de los servicios de TI. En general, lo que se ha perseguido es solventar las actuales deficiencias de ITIL.

Figura 109. Ciclo de Vida del Servicio ITIL V3.

Fuente. Ciclo de Vida ITIL.

ITIL V3 está orientado al Ciclo de Vida del Servicio. Según la perspectiva empresarial, los servicios de TI, al igual que los productos, también se encuentran condicionados a un ciclo de vida típico, que empieza con la introducción del servicio al mercado y finaliza con la exclusión del mismo del portafolio de servicios. Cada una de las cinco disciplinas principales de ITIL está enfocada a una fase específica dentro del Ciclo de Vida del Servicio:

- En el marco de la Estrategia del Servicio se determina qué clase de servicios deben ofrecerse a determinados clientes y/o mercados.

- En la fase del Diseño del Servicio se determinan los requisitos concretos. El Diseño del Servicio se ocupa de desarrollar soluciones adecuadas a estos requisitos, de proyectar nuevos servicios y de modificar y/o mejorar los ya existentes.

- En la fase de la Transición del Servicio se amplían y extienden los servicios nuevos o modificados.

- La Operación del Servicio se encarga de realizar todas las tareas operacionales que se vayan presentando.

- En el marco de Mejora Continua del Servicio se aplican métodos de la gestión de calidad con el fin de aprender de los éxitos y fracasos del pasado. Mediante este proceso se pone en marcha un circuito regulador cerrado para mejorar continuamente la efectividad y eficiencia de servicios y procesos de TI.

4.2.4 Factores de comparación

En el cuadro que se muestra a continuación se muestra un comparativo de los modelos COBIT 4.1, ITIL V3 e ISO/IEC 27002 basado en las funciones, las áreas de cobertura, la organización que creó el modelo, para qué se implementa y quienes los orientan (evalúan). Es importante concluir que un modelo no será mejor que otro, debido a que inicialmente hay que evaluar la pertinencia, la cobertura (áreas) y ante todo que cada organización, cada empresa tiene su particularidad, por ende, lo importante será adoptar un modelo pertinente, tomar los elementos que sean aplicables y adaptar el modelo de referencia para generar un modelo propio para la empresa.

Tabla 58. Factores de Comparación COBIT 4.1, ITIL V3 e ISO/IEC 27002.

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Significado de las Siglas:	Objetivos de Control para la Información y Tecnología Relacionada.	Biblioteca de Infraestructura de Tecnologías de la Información.	Organización Internacional de Normalización y Comisión Electrotécnica Internacional.
Creado por:	La Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y el Instituto de Administración de las Tecnologías de la Información (ITGI).	La Organización Gubernamental de Comercio (OGC).	La Organización Internacional de Normalización (ISO) y Comisión Electrotécnica Internacional (IEC).
Carácter de Fundamentación:	Marco de mejores prácticas.	Marco de mejores prácticas.	Marco de Mejores Prácticas. Es un anexo del Estándar 27001 para la seguridad de la información.
Definición:	Es un marco de referencia para la dirección de TI, así como también de herramientas de soporte que permite a la alta dirección reducir la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del negocio.	Es una colección de guías especializadas en temas organizacionales enfocadas a la planeación, el suministro y soporte de servicios de TI. Resume las mejores prácticas para el área de gerencia de servicios de TI, orientadas especialmente a describir **Qué** funciones o procesos son los que se recomienda desarrollar, más no en el **Cómo** desarrollarlos; para este último, es responsabilidad de la	Es un estándar de seguridad que proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Definición:		organización definir las estrategias y métodos necesarios para implementarla, siempre y cuando se adapten al tamaño, a la cultura y a las necesidades internas de la organización.	
Estructura	Está definida por 34 objetivos de alto nivel que cubren 318 objetivos de control clasificados en 4 dominios.	Contiene 27 procesos detallados organizados en 5 procesos de alto nivel.	Está compuesta por 39 objetivos de control y 133 controles, agrupados en 11 dominios para seguridad de la información.
Características:	- Orientado al negocio - Alineado con estándares y regulaciones "de facto". - Basado en una revisión crítica y analítica de las tareas y actividades en TI. - Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA). - Enfatiza el cumplimiento regulatorio, ayuda a las organizaciones a incrementar el valor obtenido desde TI, permitiendo alinear y simplificar la implementación del marco de trabajo.	- Lista una serie de procesos y funciones que se recomienda implantar para una mejor entrega de los servicios que las áreas de TI proporcionan a sus usuarios. No Desarrollada Con Derechos De Propiedad: - Set trata de un modelo de aplicación basado en mejores prácticas independientemente de proveedores asociados a su aplicación. - Las mejores prácticas están basadas en procesos puestos en marcha y recopilados en estos volúmenes, no tienen derechos de uso por prácticas personales o	- Es la única norma que no sólo cubre la problemática de la seguridad TI sino que hace una aproximación holística a la seguridad de la información corporativa, abarcando todas las funcionalidades de una organización en cuanto a la seguridad de la información que maneja. - En distintos ámbitos, permite conocer qué se puede hacer para mejorar la seguridad de la información. - Expone, en distintos campos, una serie de apartados a tratar en relación a la seguridad, los objetivos de seguridad a

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Características:		empresariales únicas. De Dominio Público: - Transición de conocimiento libre. - Es de libre utilización. Cualquiera, independientemente de las características de la entidad puede ponerlo en práctica, incluso únicamente las partes que le apliquen. Compendio De Mejores Prácticas: - Se puede aplicar y obtener beneficios adaptando el modelo a las características de cada necesidad, creciendo constantemente porque se retroalimenta de nuevas mejores prácticas. - Estas mejores prácticas son el resultado de los resultados obtenidos por el trabajo diario de expertos y profesionales del mundo de las TI desde hace casi tres décadas.	perseguir, una serie de consideraciones (controles) a tener en cuenta para cada objetivo y un conjunto de "sugerencias" para cada uno de esos controles. - Facilita la integración de los sistemas de gestión, debido a que es una estructura de alto nivel, donde los términos y definiciones ayudan a implementar.

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Características:		Estándar Internacional: - Trata de establecer, al igual que se realizó en otras ciencias, una estandarización en los conceptos, lenguaje, estructura y formas de trabajo de las organizaciones en todo el mundo con respecto a las TI. - Está desarrollado y responde a la estructura común del lenguaje y su terminología, así como los documentos que se utilizan actualmente en el mundo empresarial (Servicios, procesos, estrategias, objetivos, responsabilidades, recursos, etc.).	
Funciones y Orientación	Mapeo de procesos de TI y orientado al Negocio.	Mapeo de niveles de gestión de servicios de TI.	Marco de referencia de seguridad de la información.
Objetivos:	Proporciona una guía a alto nivel sobre puntos en los que establecer controles internos con tal de: - Asegurar el buen gobierno, protegiendo los intereses de los stakeholders (clientes, accionistas, empleados, etc.). - Garantizar el cumplimiento normativo del sector al que	- Proponer la visión de TI como proveedor de servicios. - Generar mejoras en la calidad de suministros de los servicios de TI. - Fomentar la reducción de costos de los servicios de TI. - Alinear la prestación de servicios de TI con las necesidades actuales y futuras del negocio de las organizaciones,	-Establecer las guías y principios generales para iniciar, implementar, mantener, y mejorar la gestión de seguridad de la información en una organización. - Que sus objetivos de control y controles sean recomendados para cubrir los requerimientos de seguridad que han surgido luego

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Objetivos:	pertenezca la organización. - Mejorar la eficacia y eficiencia de los procesos y actividades de la organización. - Garantizar la confidencialidad, integridad y disponibilidad de la información.	además de mejorar la relación con los Clientes. - Estandarizar los procesos que forman parte de la Gestión de Servicios de TI. - Promover el uso de un lenguaje común por parte de las personas para mejorar la comunicación al interior de las organizaciones. - Servir de base para la certificación de las personas y de las organizaciones que desean adoptar este estándar. - Mejor la eficiencia, aumentando la efectividad. - Reducir los posibles riesgos que se pueden presentar.	de una evaluación de riesgos.
Permite:	- El desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones, además enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de TI. - Mejor alineación, con base en su enfoque de negocios. - Una visión, entendible para la	A las organizaciones : - Aprovechar por completo su inversión en TI. - Brindar la posibilidad de extraer todo el potencial de la TI y la experiencia de los profesionales para hacer el negocio más innovador y valioso. A La TI: - Sus profesionales desempeñan	- Flexibilidad de controles para su uso en la forma en que una organización quiere protegerse a sí mismo. - Aumentar la reputación de los negocios que han implementado la norma. - Proteger a las empresas mediante la identificación de riesgos y estableciendo controles para gestionarlos o reducirlos.

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Permite:	gerencia, de lo que hace TI. - Propiedad y responsabilidades claras, con base en su orientación a procesos. - Aceptación general de terceros y reguladores. - Entendimiento compartido entre todos los Interesados, con base en un lenguaje común. - Cumplimiento de los requerimientos COSO para el ambiente de control de TI. - A los gerentes, cerrar la brecha existente entre los requisitos de control, cuestiones técnicas y riesgos de negocio. - Desarrollar una política clara y buenas prácticas para controlar TI en las organizaciones.	un papel más enriquecedor y satisfactorio. A esto se suma que su visibilidad y la percepción de su valor para la compañía crecen, ya que los directivos empiezan a ver la TI como un factor de creación de valor para el negocio. A los responsables del negocio: - Una relación mucho más estrecha con la TI y una mejor comprensión de la capacidad de este departamento para aprovechar la tecnología en proyectos de innovación. - A través de la colaboración con la TI, pueden implantar nuevos procesos que incrementen su competitividad y, gracias a la innovación tecnológica, pueden abrir nuevas áreas de negocio previamente inalcanzables.	- Ayudar a los grupos de interés y aumentar la confianza del cliente, teniendo sus datos protegidos. - Aumentar las oportunidades de acceso a licitaciones mediante la demostración de cumplimiento y obtener un estatus como proveedor preferido.
Beneficios:	- Mantiene información de alta calidad para soportar las decisiones de negocio. - Alcanza los objetivos estratégicos y obtener los	- El suministro de los servicios de TI se orienta especialmente al Cliente y los acuerdos sobre la calidad del servicio mejoran la relación entre el departamento de	- Reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos. - Reducción de las amenazas hasta alcanzar un nivel asumible

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Beneficios:	beneficios de negocio a través del uso efectivo e innovador de TI. - Logra la excelencia operativa a través de una aplicación fiable y eficiente de la tecnología. - Mantiene los riesgos relacionados con TI a un nivel aceptable. - Optimiza el costo de servicios de TI y tecnología. - Apoya el cumplimiento de las leyes, reglamentos, acuerdos contractuales y las políticas.	TI y el Cliente. - Mejoramiento en los niveles de satisfacción de los Clientes por medio de medidas objetivas y eficacia en la disponibilidad y desempeño de la calidad de los servicios de TI. - Implantación de estándares que permitan realizar el control, la administración y operación de los recursos de la organización. - Los servicios ofrecidos son descritos en un lenguaje más cómodo y con mayores detalles para los clientes. - Se gestiona de una mejor manera la calidad, disponibilidad, fiabilidad y coste de los servicios ofrecidos en la organización. - Mejora en la comunicación con el departamento de TI al momento de acordar los puntos de contacto. - El departamento de TI genera una estructura clara, centrada en los objetivos corporativos de una manera eficaz. - Soporte a los procesos de negocios y las actividades de los	para la organización. - En caso de producirse una incidencia, los daños se minimizan y la continuidad del negocio está asegurada. - Ahorro de costes derivado de una racionalización de los recursos. - Eliminación de las inversiones innecesarias e ineficientes como las producidas por desestimar o sobrestimar riesgos. - Se Considera a la seguridad como un sistema, y esta se convierte en una actividad de gestión. - La seguridad deja de ser un conjunto de actividades más o menos organizadas y pasa a transformarse en un ciclo de vida metódico y controlado, en el que participa toda la organización. - Se asegura a la organización del cumplimiento de la legislación vigente y se evitan riesgos y costes innecesarios. - La entidad se asegura del

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Beneficios:		decisores de TI. - El departamento de TI cuenta con un mayor control sobre la infraestructura y los servicios que tiene a cargo, obteniéndose una visión clara de la capacidad del departamento; además, permite administrar los cambios de una manera sencilla y fácil de manejar. - Definición de funciones, roles y responsabilidades en el área de los servicios. - Posibilidad de identificar, a través de una estructura procedimental, la externalización de algunos de los elementos de los servicios de TI. - Minimización de costos en la definición de procesos, procedimientos e instructivos de trabajo. - Suministro de servicios de TI que satisfagan las necesidades del negocio de la organización. - Incremento y mejoras en la productividad y eficiencia organizacional a través de las	cumplimiento del marco legal que protege a la empresa de aspectos que probablemente no se habían tenido en cuenta anteriormente.

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Beneficios		experiencias vividas y los conocimientos adquiridos. - Generación de un cambio cultural hacia la provisión de servicios y sustenta la introducción de un sistema de gestión de calidad. - Establecimiento de un marco de trabajo coherente para las comunicaciones tanto internas como externas, permitiendo contar con la identificación y estandarización de los procedimientos a seguir. - Mejoras en la satisfacción del personal de la organización reduciendo notablemente su rotación. - Mejoras entra la comunicación en información entre el personal de TI y sus clientes. - Generación de intercambio de experiencias obtenidas con su adopción.	
Dominios:	- Planificación y Organización. - Adquisición e Implementación. - Entrega de servicios.	- La Perspectiva del Negocio. - Administración de Aplicaciones. - Entrega de Servicios de TI. - Soporte a los Servicios de TI.	- Política de Seguridad. - Organización de la Seguridad de la Información. - Gestión de Activos.

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Dominios:	- Soporte y Monitorización.	- Gestión de la Infraestructura.	- Seguridad de Recursos Humanos. - Seguridad Física y Ambiental. - Gestión de Comunicaciones y Operaciones. - Control de Acceso. - Adquisición, Desarrollo y Mantenimiento de Sistemas de Información. - Gestión de Incidentes de Seguridad de la Información. - Gestión de la Continuidad del Negocio. - Cumplimiento.
Para que se Implementa:	Auditoría de Sistemas de información.	Gestión de niveles de servicio.	Cumplimiento del estándar de seguridad de la información.
Quiénes lo Evalúan:	Compañías de contabilidad y compañías de consultoría en TI.	Compañías de consultoría en TI.	Compañías de consultoría en TI, Empresas de seguridad de información y consultores de seguridad en redes.
Ventajas:	- Es un marco de referencia de gobierno TI, aceptado mundialmente y basado en estándares y mejores prácticas de la industria. - Una vez implementado, es posible asegurarse de que TI se encuentra efectivamente	Para el Cliente/Usuario: - La provisión de servicios de TI se orienta más al cliente, y los acuerdos sobre la calidad del servicio mejoran la relación entre el departamento de TI y el cliente. - Se describen mejor los servicios, en un lenguaje más cómodo para	A la organización: - Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial. - Demuestra independientemente

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Ventajas:	alineado con las metas del negocio, y orientar su uso para obtener ventajas competitivas. - Suministra un lenguaje común que le permite a los ejecutivos de negocios comunicar sus metas, objetivos y resultados con Auditores, TI y otros profesionales. - Proporciona las mejores prácticas y herramientas para monitorear y gestionar las actividades de TI. - El uso de sistemas usualmente requiere de una inversión que necesita ser adecuadamente gestionada. - Ayuda a los ejecutivos a entender y gestionar las inversiones en TI a través de sus ciclo de vida, así como también proporcionándoles métodos para asegurarse que TI entregara los beneficios esperados. - Avances en la medición del desempeño; mejores objetivos de control; y una excelente	el cliente, y con mayor nivel de detalle. - Se manejan mejor la calidad y el coste del servicio. - Se mejora la comunicación con la organización de TI al acordar los puntos de contactos. Para la Organización: - La organización TI desarrolla una estructura más clara, se vuelve más eficaz y se centra más en los objetivos corporativos. - La dirección tiene más control y los cambios resultan más fáciles de manejar. - Su estructura de proceso eficaz brinda un marco para concretar de manera más adecuada la externalización de algunos de los elementos de los servicios de TI. - Seguir las mejores prácticas de ITIL alienta el cambio cultural hacia la provisión de servicios y sustenta la introducción de un sistema de gestión de calidad basado en las series ISO 9000. -ITIL establece un marco de	que se respetan las leyes y normativas que sean de aplicación. Al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial: - Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información. - Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información. - Al realizar procesos de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora. - Aumento de la seguridad efectiva de los sistemas de

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Ventajas:	alineación entre objetivos de negocio y de TI. - Enfatiza el cumplimiento normativo. - Ayuda a las organizaciones a incrementar el valor de TI. - Ayuda al alineamiento con el negocio y simplifica la implantación de COBIT.	referencia para la comunicación interna y la comunicación con los proveedores, así como la estandarización y la identificación de procedimientos.	información - Correcta planificación y gestión de la seguridad de la información. - Garantías de continuidad del negocio. - Mejora continua a través del proceso de auditoría interna. - Incremento de los niveles de confianza de los clientes. - Aumento del valor comercial y mejora de la imagen de la organización.
Desventajas:	- Esta versión no invalida el trabajo efectuado con las versiones anteriores del COBIT, sino que puede ser empleado para mejorar el trabajo previo. - No incluye los pasos del proceso y las tareas, pues es un marco de gestión y control y no un marco de proceso. - Se centra en lo que la empresa tiene que hacer, no cómo debe hacerlo y el público objetivo es la alta dirección, alta dirección de TI y los auditores. - Con el incremento de las	- Eleva las TI a un nivel estratégico, donde sólo las organizaciones que hayan madurado en experiencia con la versión anterior serán capaces de afrontar la nueva. - En organizaciones de pequeño y mediano tamaño la versión 3, es más compleja y no es tan apropiada. -Tiempo y esfuerzo necesario para su implementación. - Falta de presencia del cambio en la cultura de las áreas involucradas.	- Al iniciar este conjunto de tareas, no cabe duda que se está sobrecargando el ritmo habitual de trabajo de toda la organización, por lo tanto se debe ser consciente de que exigirá un esfuerzo adicional. -Independientemente de las tareas periódicas que implica, una vez lanzado el SGSI para los administradores del mismo, el mantenimiento del nivel alcanzado, requerirá inexorablemente un esfuerzo continuado de toda la

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Desventajas:	tecnologías de punta y la necesaria generalización de las aplicaciones informáticas de auditoría, el auditor tradicional debe enfrentarse al cambio, por lo que tendrá que vencer los retos que este cambio representa; entre ellos pueden señalarse los siguientes: Nueva Técnica Informática, su auditabilidad e impacto en los procedimientos y controles, adaptar conceptos clásicos de control a la nueva tecnología, desarrollo de nuevas técnicas y herramientas para obtener evidencias.	- Falta de una mejora reflejada, por falta de entendimiento sobre procesos, indicadores y como pueden ser controlados. -Que el personal no se involucre y se comprometa. -La mejora del servicio y la reducción de costos puede no ser visible. -Que la inversión en herramientas de soporte sea escasa. Los procesos podrán parecer inútiles y no se alcancen las mejoras en los servicios.	organización al completo. - Sea cual fuere la elección, el cúmulo de actividades realizadas exige un mantenimiento y mejora continua, sino deja de ser un SGSI, y ello salta a la vista en el muy corto plazo. Es decir no se puede dejar de lado, pues al abandonar un cierto tiempo el SGSI, requerirá un esfuerzo similar a lanzarlo de nuevo. - La implantación de ISO/IEC 27002 en una organización, es un proyecto que suele tener una duración entre seis y doce meses, dependiendo del grado de madurez en seguridad de la información. - Es recomendable la ayuda de consultores externos. - El equipo de proyectos de implantación, debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI.
Metas o Alcances:	- Investigar, desarrollar, hacer público y promover un marco	-Impulsar la adopción de procesos, de manera que puedan	- Establecer los lineamientos y principios generales para iniciar,

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Metas o Alcances:	de control de gobierno TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento. - Ser el modelo de control para la tecnología de información.	adaptarse para encajar tanto en organizaciones grandes como en pequeñas. - Integrar Niveles de Servicio de transparencia a sus procesos. -Aplicar ITIL especialmente en aquellas empresas que han integrado clientes y proveedores en sus operaciones a través de redes de datos, como internet. -Ofrecer un marco común para todas las actividades del departamento TI, como parte de la provisión de servicios, basado en la infraestructura TI.	implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. - Proporcionar un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados. - Ser implementada para satisfacer los requerimientos identificados por una evaluación del riesgo. - Servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas. - Ayudar a elaborar la confianza en las actividades inter-organizacionales.
Utilización:	- Generalmente como herramienta para uso conjunto con Sarbanes-Oaxley y otros estándares mundiales. - En las organizaciones reduce el riesgo en el manejo de las TI e incrementa el valor derivado	Sirve como guía y base para la definición de nuevas acciones de mejora de los servicios de TI.	Legislativo. - Protección de datos y privacidad de la información personal. - Protección de los registros organizacionales. - Derechos de propiedad

	COBIT 4.1	ITIL V3	ISO/IEC 27002
Utilización:	de su uso.		intelectual.
A Quién está Dirigida:	- A la alta dirección, que se está dando cuenta del impacto significativo que la información puede tener en el éxito de una empresa. - A la dirección ejecutiva, gerencia del negocio, gerencia de TI y auditores. - A Consultores, Auditores, Responsables de las áreas administrativas y de la Seguridad de la Información, que reconocen la dependencia crítica de muchos de los procesos de negocio sobre TI, el incremento de necesidades de cumplimientos legales y los beneficios de una gestión de riesgos efectiva. - Auditores de TI, administradores de TI, profesionales de calidad de TI, líderes de TI, desarrolladores de TI y administradores de firmas	- Al Personal directivo, gerencial y operativo de los departamentos de TI que estén directa o indirectamente involucrados con la prestación y soporte de servicios de TI.	- A oficiales de seguridad de la información. - A oficiales del cumplimiento. - A oficiales de la privacidad de datos. - Auditores internos. - A auditores que quieran liderar auditorías de certificación de Sistema de Gestión de Seguridad de la información (SGSI). - A gerentes de proyectos o consultores que quieren dominar los procesos de auditoría de Sistemas de Gestión de Seguridad de la Información (SGSI). - A altos directivos responsables de la dirección de una empresa y la gestión de sus riesgos. - A Miembros de un equipo de seguridad de la información. - A Instructores en seguridad de la información.

	COBIT 4.1	ITIL V3	ISO/IEC 27002
A Quién está Dirigida:	proveedoras de servicios de TI. - A responsables de la Gestión de TI: Administradores de sistemas o redes, directores de TI, analistas de negocios, especialistas en procesos, gerentes de desarrollo, analistas de sistemas y arquitectos de TI, encargados de seguridad, y general a los responsables de gestionar la entrega y soporte de servicios de TI.		
Herramientas Utilizadas:	-Perspectivas del negocio. -Dirección de la aplicación. -Entrega de servicios TI. -Soporte de servicio. -Gestión de infraestructura.	-Resumen ejecutivo. -Marco referencial. -Objetivos de control. -Guías de auditoría. -Conjunto de herramientas de implementación. -Guías gerenciales.	-Intercambio y movilidad (Red externa y red local). -Soportes físicos. -Servicios externos. -Seguridad física. -Desarrollo y Mantenimiento (Documentación, servidores, aplicaciones y puestos de trabajo). -Organización y Usuarios.
Confiabilidad:	Alta	Alta	Alta
Enfoque:	Operacional	Táctico	Táctico

Fuente: Alcaldía del Municipio de Río de Oro, Cesar.

Se seleccionó la norma ISO/IEC 27002, porque es un marco de trabajo de mejores prácticas internacionales que establece las guías y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en la Alcaldía Municipal de Río de Oro (Cesar). Sus objetivos de control y controles son recomendados para cubrir los requerimientos de seguridad que han surgido luego de una evaluación de riesgos.

4.3 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA MUNICIPAL DE RÍO DE ORO, CESAR

4.3.1 Política de Seguridad de la Información

La Política de seguridad establece las acciones necesarias y los procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información, así como los mecanismos utilizados para la implementación de los mismos.

Debe dedicarse un tiempo significativo para la creación de la Política de Seguridad de la Información de la empresa, proceso que estará orientado por el Comité de Seguridad de la información.

A continuación se desarrollará la Política de Seguridad de la Información para la Alcaldía Municipal de Río de Oro, Cesar:

Aprobación

Resolución No. ___

Por la cual se regulan las políticas de seguridad de la información y el uso adecuado de la tecnología para el procesamiento de la información en la Alcaldía Municipal de Río de Oro, Cesar.

EL ALCALDE MUNICIPAL MANUEL RODOLFO MARQUEZ PAEZ

En uso de sus facultades legales y estatutarias y

CONSIDERANDO

Que la Alcaldía Municipal de Río de Oro (Cesar), reconoce que la información es un activo valioso y que se requieren políticas adecuadas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la misma.

Que la Constitución Política en su Artículo 61 establece que el Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.

Que la Alcaldía Municipal de Río de Oro (Cesar) debe promover y proteger la producción intelectual de los miembros de su comunidad mediante el reconocimiento de los derechos morales y patrimoniales generados.

Que se hace necesario el establecimiento de las políticas de seguridad de la información que protejan, preserven y administren correctamente la información de la Alcaldía Municipal de Río de Oro (Cesar), junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

Que todos los servidores públicos y contratistas vinculados con la Alcaldía Municipal de río de Oro, Cesar, deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades.

Que el otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.

Que todas las prerrogativas para el uso de los sistemas de información de la Alcaldía Municipal de Río de Oro, Cesar, deben terminar inmediatamente después de que el servidor público o contratista cesa de prestar sus servicios a ella.

Que los proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

ALCANCE

Las políticas de seguridad, definidas en el presente documento, aplican a todos los servidores públicos y contratistas de la Alcaldía Municipal de Río de oro, Cesar, y otras personas vinculadas que utilicen los recursos informáticos de ella.

También describe todas las normas, políticas y estándares que se aplicarán de manera obligatoria por parte del personal con respecto a seguridad informática, para precautelar un correcto uso de equipos de cómputo y aplicaciones tecnológicas; para el presente manual se han considerado sugerencias y recomendaciones del estándar ISO/IEC 27002.

ISO/IEC 27002 hace énfasis en la integridad, confidencialidad y disponibilidad. Integridad se refiere a la necesidad de proteger la exactitud de la información, así como los métodos utilizados para procesarla. Confidencial se refiere a la garantía de que la información sólo puede ser visitada por las personas que tienen la autorización para hacerlo. Y la disponibilidad se refiere a la garantía de que aquellos que han sido autorizadas a hacer uso de la información tienen acceso a ella y todos los asociados activos cuando sea necesario.

Este manual, brindará información a los responsables de la implementación de seguridad de la información en la Alcaldía Municipal de Río de Oro, Cesar, y subraya la importancia de

la gestión de riesgos, mediante la descripción de nueve de los once dominios de este estándar, los cuales son:

- ✓ POLITICA DE SEGURIDAD
- ✓ ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
- ✓ GESTIÓN DE ACTIVOS
- ✓ SEGURIDAD DE LOS RECURSOS HUMANOS
- ✓ SEGURIDAD FÍSICA Y AMBIENTAL
- ✓ GESTIÓN DE COMUNICACIONES Y OPERACIONES
- ✓ CONTROL DE ACCESOS
- ✓ ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN
- ✓ GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Cada dominio incluye la política relacionada, así como el conjunto de controles respectivos considerados en cada caso.

PROPÓSITO

Se hace necesario el establecimiento de las Políticas de Seguridad de la Información que protejan, preserven y administren correctamente la información de la Alcaldía Municipal de Río de Oro, Cesar, junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

Que en mérito de lo expuesto,

RESUELVE:

4.3.2 Organización de la Seguridad de la Información

El Comité de Seguridad de la Información de la Alcaldía Municipal de Río de Oro (Cesar), estará integrado por:

- Alcalde Municipal
- Coordinador Control Interno
- Jefe del Área de Sistemas (Coordinador del Comité de Seguridad de la Información)
- Secretario de Gobierno (Cumpliendo además con las Funciones de Responsable del Área de Recursos Humanos)
- Secretario de Hacienda
- Secretario de Planeación
- Secretario de Salud

Los integrantes del Comité velarán por el cumplimiento de los siguientes objetivos de seguridad:

1) Revisar y proponer al Alcalde Municipal, para su consideración y posterior aprobación, las políticas de seguridad de la información para la Alcaldía Municipal de Río de Oro (Cesar) y las funciones generales en materia de seguridad de la información que fuera convenientes y apropiadas.

2) Monitorear cambios significativos en los riesgos que afectan a los recursos de la información frente a posibles amenazas, sean internas o externas.

3) Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios de la Alcaldía Municipal de Río de Oro (Cesar), sean preexistentes o nuevos.

4) Promover la difusión y cumplimiento de las Políticas de Seguridad establecidas para la Alcaldía Municipal de Río de Oro (Cesar).

5) Coordinar a las diferentes dependencias en materia de seguridad de la información y control de los activos (bienes muebles e inmuebles, elementos de consumo y componente tecnológico) de la Alcaldía Municipal de Río de Oro (Cesar).

6) Revisar anualmente la política de seguridad de la información.

Roles y responsabilidades

A continuación se enumeran los roles que intervienen en el Comité de Seguridad de la Información de la Alcaldía Municipal Río de Oro (Cesar).

- Alcalde Municipal.

Pertenece al Comité de Seguridad de la Información y cumplirá la función de cumplimiento a la implementación de esta política y de aprobar los controles necesarios para el aseguramiento de la información confidencial de la Alcaldía.

- Coordinador Control Interno

Pertenece al Comité de Seguridad de la Información y cumplirá la función de practicar auditorias periódicas de los sistemas y actividades vinculadas con la tecnología de la información.

- Coordinador del Comité Seguridad de la Información.

Será el responsable de coordinar las acciones del Comité de Seguridad de la Información, así como de impulsar la implementación y cumplimiento de la presente Política. Este rol recae sobre el Jefe del Área de Sistemas.

- Responsable del Área de Recursos Humanos.

Pertenece al Comité de Seguridad de la Información y cumplirá la función de implicar a todo el personal de la Alcaldía Municipal de Río de Oro (Cesar) en el conocimiento y cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan, así como de los cambios que en aquellas se produzcan. Igualmente, se responsabilizará de la implementación de los compromisos de confidencialidad que deban suscribir los empleados y de la capacitación continua de los mismos en materia de seguridad. Este rol es desempeñado por el Secretario de Gobierno.

- Secretarios

Pertenecen al Comité de Seguridad de la Información y cumplirán la función de velar por el cumplimiento de esta política por parte de todos y cada uno de los empleados (incluso ellos mismos) ligados a su secretaria. Este rol es desempeñado por el Secretario de Hacienda, el Secretario de Gobierno, el secretario de Planeación y el Secretario de Salud.

Acuerdos de Confidencialidad

Corresponde a la Administración Municipal, la creación y modificación de los acuerdos de confidencialidad o no divulgación, los cuales deben tener en cuenta el requerimiento que contempla las necesidades de protección de la información confidencial, de la Alcaldía Municipal. El cual debe ser anexo al contrato de trabajo e igualmente firmado, como compromiso de confidencialidad, que evitara la divulgación de información no autorizada a terceros.

Este acuerdo de confidencialidad y no divulgación, protegerá la información organizacional e informa a los firmantes de su responsabilidad de proteger, usar y divulgar información de una manera responsable y autorizada.

Para su elaboración se deben considerar los siguientes aspectos:

- Definir qué información es confidencial y debe protegerse.
- Permitir el uso de la información confidencial.
- Definir el proceso de notificación y reporte de divulgación no autorizada o incumplimiento del acuerdo de información confidencial.
- Definir responsabilidades y sanciones, al divulgarse información no autorizada o incumplirse este acuerdo, por parte del firmante.

La aplicación de acuerdos de confidencialidad y no divulgación debe ser extendida a todos los empleados, proveedores y demás personas, que hagan uso de la información crítica de la Alcaldía.

Contacto con las Autoridades y Grupos de Interés Especial

Corresponde a la Administración Municipal, mantener los contactos apropiados con las autoridades y grupos de interés especial pertinentes para asegurar la Información de la Alcaldía. Además de establecer procedimientos que especifiquen cuándo y cuáles autoridades (Policía, Bomberos, Defensa Civil, etc.) contactar, y cómo reportar los incidentes de seguridad de la información identificados de una manera oportuna en caso de sospecha, con el fin de preservar la continuidad de las funciones.

En caso de presentarse, ataques desde Internet se debe mantener el contacto con el proveedor del servicio de Internet o un operador de telecomunicaciones, para que tome las respectivas acciones contra la fuente de ataque.

Para la correcta ejecución, se debe considerar:

- Recibir advertencias tempranas de alertas, asesorías y avisos relacionados con ataques y vulnerabilidades.
- Obtener acceso a consultoría especializada de seguridad de la información.

4.3.3 Gestión de Activos

Sus objetivos son:

- Garantizar que los activos de información reciban un apropiado nivel de protección.
- Clasificar la información para señalar su sensibilidad y criticidad.
- Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

La Alcaldía Municipal de Río de Oro (Cesar), bajo supervisión del Comité de Seguridad de la Información debe elaborar y mantener un inventario de los activos de información que posee la misma, garantizando la disponibilidad, integridad y confidencialidad de los datos que la componen.

4.3.3.1 Responsabilidad por los Activos

La Administración Municipal deberá mantener sus activos inventariados y nombrar un responsable (Secretarios) para ellos. Los responsables deberán identificar todos los activos y deberán asignar la responsabilidad de mantener los controles apropiados. La implementación de controles específicos puede ser delegada por el responsable conforme

sea apropiado, pero este sigue siendo responsable por la protección apropiada de los activos.

Inventario de Activos

Se identificarán los activos importantes pertenecientes a la Alcaldía, sus respectivos responsables y su ubicación, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 2 meses.

El Secretario de Planeación será el encargado de elaborar el inventario y mantenerlo actualizado.

Debido a que existen muchos tipos de activos: Información, Software, Físicos, Servicios y Personas. La Administración Municipal deberá regular, que el inventario de activos se mantenga actualizado. Este inventario debe estar establecido de la siguiente forma:

Inventario de Hardware y Software: Este inventario deberá contener toda la información relacionada con las especificaciones de los equipos de cómputo, equipo de oficina, sistemas operativos y software empresarial, pertenecientes a la Alcaldía. Cada activo debe describir su nombre, responsable (asignado a su uso) y Dependencia en la cual se ubica.

- Inventario de Equipos de Cómputo: Este inventario deberá contener información específica de los equipos de cómputo, como: El modelo, fabricante, fecha de adquisición, resolución de pantalla, CPU (para el caso), color, capacidad de procesador, capacidad de RAM, capacidad de Disco Duro, tipo de Sistema Operativo y software empresarial (para el caso).

EQUIPO	CARACTERISTICAS	
NOMBRE DEL ACTIVO **Responsable** (Dependencia)	**HARDWARE**	
	Modelo	
	Fabricante	
	Fecha Adquisición	
	Pantalla	
	CPU	
	Color	
	Procesador	
	RAM	
	Disco Duro	
	SOFTWARE	
	Sistema Operativo	
	“SW Especifico”	

- Inventario de Equipos de Oficina: Este inventario deberá contener información específica de los equipos de oficina (impresora, teléfono, fax, escáner, plotter, etc.), como: El modelo, fabricante, fecha de adquisición y color.

EQUIPO	CARACTERISTICAS	
NOMBRE DEL ACTIVO **Responsable** (Dependencia)	**GENERALES**	
	Modelo	
	Fabricante	
	Fecha Adquisición	
	Color	

- Inventario de Sistemas Operativos: Este inventario deberá contener información específica de los sistemas operativos, como: La versión, fabricante y número de licencias.

SISTEMA OPERATIVO	CARACTERISTICAS	
NOMBRE – SISTEMA OPERATIVO	**GENERALES**	
	Versión	
	Fabricante	
	N° de Licencias	

- Inventario de Software Empresarial: En cuanto al inventario de software empresarial perteneciente a la Alcaldía, deberá contener: El fabricante, Descripción del software, módulos de los que se compone, fecha de adquisición, número de licencias, dependencia y responsable (asignado a su uso).

SOFTWARE EMPRESARIAL	CARACTERISTICAS	
NOMBRE- SOFTWARE EMPRESARIAL	**GENERALES**	
	Fabricante	
	Descripción	
	Módulos	
	Fecha Adquisición	
	Licencia	
	N° de Licencias	
	Dependencia	
	Responsable	

Inventario de Equipos de Comunicación: Este inventario deberá contener toda la información relacionada con las especificaciones de los Servidores, Router, Switch y demás equipos de red, que permite la comunicación entre las áreas de la Alcaldía.

- **Inventario de Servidores:** Este inventario deberá contener información específica de los servidores, como: Características específicas y licencia.

DISPOSITIVO	CARACTERISTICAS	
Servidor	**Especificas**	
	Licencia	

- Inventario de Switch: Este inventario deberá contener información específica de los switch, como: Fabricante, Puertos, Protocolo de Gestión Remota, Voltaje Necesario y Consumo Eléctrico.

SWITCH (Dependencia)	**GENERALES**	
	Fabricante	
	Puertos	
	Protocolo de Gestión Remota	
	Voltaje Necesario	
	Consumo Eléctrico	

- Inventario de Router: Este inventario deberá contener información específica de los router, como: Modelo, Fabricante, Puertos, Interfaces WAN y LAN.

ROUTER (Dependencia)	**GENERALES**	
	Modelo	
	Fabricante	
	TECNICAS	
	Puertos	
	Interfaces WAN	
	Interfaces LAN	

Inventario de Bienes Muebles e Inmuebles: Este inventario deberá contener el nombre, el detalle, la ubicación, el responsable y el serial, de cada uno de los activos bienes muebles e inmuebles, que pertenezcan a la Alcaldía.

ID	Nombre	Detalle	Dependencia	Persona a Cargo	Serial
1					
2					
3					

Inventario de Archivos: Este deberá contener el nombre (decreto, resolución, etc.), número, año (en que se creó), título, ubicación (estante, archivador, etc.) y dependencia en la cual se encuentra.

ID	Nombre	Número	Año	Título	Ubicación	Dependencia
1						
2						
3						

4.3.3.2 Clasificación de la Información

La información deberá ser clasificada para indicar la necesidad, prioridades y grado de protección necesario, cuando se maneje.

Lineamientos de Clasificación

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad:

- Confidencialidad.

0. Pública: Información de libre acceso, no requiere autorización.
1. Uso Interno: Información que puede ser conocida y utilizada por todos los empleados de la Alcaldía y externos debidamente autorizados, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la Alcaldía.
2. Privada: Información que sólo puede ser conocida y utilizada por un grupo de empleados, para el buen desarrollo de sus labores, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la Alcaldía.
3. Confidencial: Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la Administración Municipal, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves a la Alcaldía.

- Integridad.

0. Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatividad de la Alcaldía.
1. Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para a la Alcaldía.
2. Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la Alcaldía.
3. Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a la Alcaldía.

- Disponibilidad.

0. Información cuya inaccesibilidad no afecta la operatividad de la Alcaldía durante un mes.
1. Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para la Alcaldía.
2. Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la Alcaldía.
3. Información cuya inaccesibilidad permanente durante 2 horas podría ocasionar pérdidas significativas a la Alcaldía.

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

CRITICIDAD BAJA: ninguno de los valores asignados supera el 1.
CRITICIDAD MEDIA: alguno de los valores asignados es 2.
CRITICIDAD ALTA: alguno de los valores asignados es 3.

Etiquetado y Manipulado de la Información

Se definirán procedimientos para el etiquetado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

Copia.
Almacenamiento.
Transmisión electrónica (correo, fax, correo electrónico).
Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, entre otros).

- **Información Almacenada en Formato Digital.**

Todo medio de almacenamiento digital (CD´s, Disco Duro, USB, etc.) debe presentar una etiqueta con la clasificación correspondiente.

La información en formato digital clasificada como "Publica", puede ser almacenada en a en cualquier área de la Alcaldía. Sin embargo se deben tomar las medidas necesarias para no mezclar información "Pública" con Información correspondiente a otra clasificación.

Todo usuario, antes de transmitir información clasificada como "Privada" o "Confidencial", debe asegurarse que el destinatario de la información esté autorizado a recibir dicha información.

Todo usuario que requiere acceso a información clasificada como "Privada" o "Confidencial", debe ser autorizado por el jefe inmediato. Las autorizaciones de acceso a este tipo de información deben ser documentadas, es decir, presentadas en un formato físico.

La clasificación asignada a este tipo de información, solo puede ser modificada por el Comité de Seguridad de la Información, luego de justificar formalmente el cambio en dicha clasificación.

La información en formato digital, clasificada como "Privada", debe ser encriptada con un método aprobado por el Comité de Seguridad de la Información, cuando es almacenada en cualquier medio (CD´s, Disco Duro, USB, etc.).

Es recomendable el uso de técnicas de encriptación para la información clasificada como "Privada" o "Confidencial", transmitida a través de mensajería interna.

Toda transmisión de Información clasificada como "Privada", "Confidencial" o de "Uso Interno" realizada hacia o a través de mensajería externa a la Alcaldía, debe realizarse utilizando un medio de transmisión seguro o utilizando técnicas de encriptación aprobadas.

Todo documento en formato digital, debe presentar la clasificación correspondiente en la parte superior (cabecera) e inferior (píe de página) de cada página del documento.

Los medios de almacenamiento, incluyendo Discos Duros del Computador, que albergan información clasificada como "Restringida", deben ser ubicados en ambientes cerrados, diseñados para el almacenamiento de dicho tipo de información. En lugar de protección física, la información clasificada como "Restringida", podría ser protegida con técnicas de encriptación aprobadas por la Alcaldía.

- **Información Almacenada en Formato No Digital.**

Todo documento o contenedor de información, debe ser etiquetado como "Privada", "Confidencial", de "Uso Interno" o de Acceso "Publico", dependiendo de la clasificación asignada.

Todo documento que presente información clasificada como "Confidencial" o "Privada", debe ser etiquetada en la parte superior e inferior de cada página con la clasificación correspondiente.

Todo documentos clasificado como "Confidencial" o "Privado", debe contar con una caratula en la cual se muestre la clasificación de la información que contiene.

Los activos de información correspondientes a distintos niveles de clasificación, deben ser almacenados en distintos contenedores, de no ser posible dicha distinción, se asignará el nivel crítico de la información identificada a todo el contenedor de información.
El ambiente donde se almacena la información clasificada como "privada", debe contar con adecuados controles de acceso y asegurad cuando se encuentre sin vigilancia. EL acceso debe ser permitido solo al personal formalmente autorizado. El Personal de limpieza, debe ingresar al ambiente acompañado de personal autorizado.

Solo el personal formalmente autorizado, debe tener acceso a información clasificada como "Privada" o "Confidencial".

Los usuarios que utilizan documentos con información "Privada" o "Confidencial", deben asegurarse de almacenarlos en lugares adecuados, evitar que usuarios no autorizados accedan a dichos documentos y destruir los documentos si luego de su utilización, dejan de ser necesarios.

4.3.4 Seguridad de los Recursos Humanos

Sus objetivos son:

- Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.
- Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.
- Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Alcaldía, en el transcurso de sus tareas normales.
- Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las áreas de procesamiento de información.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

4.3.4.1 Antes del Empleo

Asegurar que los empleados conozcan sus responsabilidades en el cumplimiento de la política de seguridad antes de ser contratados para ejercer funciones en la Alcaldía, y reducir así el riesgo de robo, fraude y mal uso de los activos.

Funciones y Responsabilidades

Todas las funciones correspondientes a la seguridad de la información deben ser incluidas en la descripción de las responsabilidades de cada cargo.

Términos y Condiciones de Contratación

Como parte de sus términos y condiciones iniciales de empleo, los empleados firmarán un Acuerdo de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del área.

República de Colombia
Departamento Del Cesar
Alcaldía Municipal
RIO DE ORO

ACUERDO DE CONFIDENCIALIDAD No. ____
(Fecha)

"POR EL CUAL SE ADOPTAN LAS RESPONSABILIDADES Y SANCIONES, LIGADAS A LA VULNERABILIDAD DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN, ESTIPULADOS EN EL MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE RÍO DE ORO CESAR"

Yo, _____ identificada con cedula de ciudadanía número _____ de _____, por medio del presente dejo constancia de haber recibido accesos a los activos de clasificación "Confidencial", "Privada" y de "Uso Interno" de la Alcaldía de Río de Oro (Cesar). Comprometiéndome a aceptar y cumplir con todas las políticas, leyes, decretos, resoluciones, normas y estándares de seguridad informática de la Alcaldía y el Estado, y específicamente, a:

PRIMERO: No utilizar la información para fines contrarios a los intereses de la Alcaldía. El intento de acceso a recursos no asignados al mismo será considerado "Intento de Violación a la Seguridad" en el cual la Alcaldía se reserva el derecho de tomar las acciones pertinentes al caso.

SEGUNDO: No divulgar la información obtenida en la Alcaldía.

TERCERO: No revelar la contraseña otorgada. Modificar la contraseña al sospechar que esta haya sido descubierta.

CUARTO: Aceptar las responsabilidades sobre el uso de mi cuenta de usuario, y no permitir su uso a terceros.

QUINTO: Utilizar los activos de la Alcaldía únicamente para fines aprobados por ésta.

SEXTO: No realizar instalación de ningún tipo de software no aprobado por la Alcaldía.

SEPTIMO: Aceptar que toda la información conservada en los equipos informáticos (archivos y demás) es de propiedad de la Alcaldía, por lo que podrá ser administrada y/o monitoreada por los responsables del área de sistemas de acuerdo con las pautas de seguridad definidos.

OCTAVO: Efectuar la destrucción de todo mensaje cuyo origen es desconocido, y asumir la responsabilidad por las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos, no se deben contestar dichos mensajes y debe ser enviada una copia al Coordinador del Comité de Seguridad para que efectúe las tareas de seguimiento e investigación necesarias.

NOVENO: Desconectarse de la estación de trabajo correspondiente, cada vez que finalice con las tareas que en ella desarrolla, a fin de evitar el uso de la clave por otra persona.

En caso de incumplimiento de las obligaciones contenidas en este documento, reconozco el derecho de la ALCALDÍA para reclamar las indemnizaciones respectivas a través de todas las acciones judiciales contempladas en la legislación vigente y presentar inclusive las acciones penales a que hubiere lugar de acuerdo con lo dispuesto en la Ley de Propiedad Intelectual.

La terminación del presente acuerdo, por cualquier causa, no me libera de las obligaciones de confidencialidad adquiridas en virtud del mismo, respecto a la información que le haya sido revelada hasta la fecha de la terminación.

PUBLÍQUESE Y CÚMPLASE.

Dado en el Municipio de Río de Oro, Cesar, a los ___ días del mes de _____ de _____ (2.___).

_____
Nombre Completo del Empleado
Cedula de ciudadanía, ciudad

4.3.4.2 Durante el Empleo

La Administración Municipal se asegurara que los empleados estén al tanto de amenazas e inquietudes en relación a seguridad de la información, sus responsabilidades y obligaciones, en el transcurso de la realización de sus labores y reducir así el error humano.

Responsabilidades de la Gerencia

La Administración Municipal se asegurara que los empleados, estén apropiadamente informados sobre sus roles y responsabilidades de seguridad antes de otorgarles acceso a

información confidencial o a los sistemas de información, esto con el fin de evitar daños considerables en la Alcaldía.

Además debe lograr un nivel de conciencia sobre seguridad relevante para sus roles y responsabilidades dentro de la organización, brindarles motivación y lineamientos para establecer las expectativas de seguridad de su rol dentro de la organización.

Concienciación, Formación y Capacitación en Seguridad de la Información

Se desarrollará un proceso de inducción, enfocado a la capacitación y el conocimiento formal de las políticas, así como de las expectativas de seguridad de la Alcaldía, antes de otorgar acceso a la información. Con el objetivo de permitir a las personas reconocer los problemas e incidentes de la seguridad de la información, y responder de acuerdo a las necesidades de su rol en el trabajo.

El Comité de Seguridad desarrollará planes de capacitación de Seguridad de la Información, los cuales se deben realizar mínimo una capacitación por semestre, tanto a empleados, proveedores y personal externo, que desempeñen funciones en la misma.

Proceso Disciplinario

Se deberá realizar una verificación previa del incumplimiento de seguridad, antes de iniciar un proceso disciplinario.

El proceso disciplinario formal deberá asegurar el tratamiento correcto y justo para los empleados sospechosos de cometer incumplimientos de la seguridad, tomando a consideración factores como la naturaleza y gravedad del incumplimiento y su impacto en la Alcaldía, si esta es la primera vez que ocurre, si el culpable fue apropiadamente capacitado y otros factores que se puedan requerirse. En los casos serios, el proceso deberá permitir la remoción inmediata de los deberes, derechos de acceso y privilegios.

4.3.4.3 Finalización o Cambio de Empleo

Responsabilidades de Terminación

Los cambios en la responsabilidad o empleo deben ser manejados como la terminación de la responsabilidad o empleo respectivo, y la responsabilidad o empleo nuevo deberá ser controlada.

Devolución de Activos

Todos los empleados contratados, deberán devolver todos los activos de la Alcaldía que tengan en su posesión al momento de terminar su empleo, contrato o acuerdo.

Retirada de los Derechos de Acceso

Cuando un empleado se retire de la Alcaldía, el Jefe del Área de Sistemas, eliminará el usuario correspondiente a dicho empleado.

4.3.5 Seguridad Física y Ambiental

Sus objetivos son:

- Prevenir e impedir accesos no autorizados (carnet institucional y para terceros carnet de visitante), daños e interferencia a las sedes, instalaciones e información de la Alcaldía.
- Proteger el equipamiento de procesamiento de información crítica de la Alcaldía, ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.
- Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la Alcaldía.
- Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Para el acceso a los sitios y áreas restringidas (oficinas de la Alcaldía), debe notificarse en una bitácora de entradas y salidas para la autorización correspondiente, y así proteger la información y los bienes informáticos, muebles e inmuebles y elementos de consumo de la Alcaldía.

4.3.5.1 Áreas Seguras

Se deben implementar medidas de seguridad física para asegurar la integridad de las oficinas. Las medidas de protección deben ser consistentes con el nivel de clasificación de los activos y el valor de la información procesada y almacenada en las instalaciones de la Alcaldía.

Los medios de procesamiento de información crítica o confidencial deberán ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Deberán estar físicamente protegidos del acceso no autorizado, daño e interferencia con la información y las oficinas de la Alcaldía.

La protección suministrada deberá estar acorde con los riesgos identificados.

Perímetro de Seguridad Física

La protección física se llevará a cabo utilizando perímetros de seguridad, mediante la creación de diversas barreras o medidas de control físicas a las oficinas de la Alcaldía, área de archivo y biblioteca, donde se preserva la información y medios de procesamiento de esta; y demás áreas (de suministro de energía eléctrica) consideradas críticas para el correcto funcionamiento de la Alcaldía.

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por Comité de Seguridad de la Información, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

- Se deberán definir claramente los perímetros de seguridad, su ubicación y aseguramiento de acuerdo a la clasificación de los activos que resguarda y el nivel de riesgo evaluado.

- Deberán ser físicamente sólidos (es decir, no deberían existir brechas en el perímetro o áreas donde fácilmente pueda ocurrir un ingreso no autorizado). Las paredes externas deberán ser sólidas y todas las puertas externas adecuadamente protegidas contra accesos no autorizados mediante mecanismos de control. Por ejemplo, alarmas, etc... Las puertas y ventanas deberán ser seguras cuando están desatendidas y se deberá considerar una protección externa para las ventas, particularmente en el primer piso.

- Las áreas de trabajo compartidas por dos o más funcionarios, deberá ser delimitada con el espacio suficiente, por barreras formando cubículos de trabajo.

- Contar con un área de para controlar el acceso físico a la Alcaldía. El acceso a las oficinas deberá restringirse solamente al personal autorizado.

-Todas las puertas de emergencia del perímetro de seguridad deberán contar con alarmas, debidamente monitoreadas y probadas, así como las paredes.

- Se deberán instalar adecuados sistemas de detección de intrusos según, los cuales serán probados regularmente para abarcar todas las puertas externas y ventanas accesibles. Las áreas no ocupadas deberán contar con alarmas en todo momento.

- Las áreas con flujo constantes de visitantes, deberán contar con un espacio propio para la recepción, con el fin de separar el área de trabajo.

Un área segura puede ser una oficina con llave, o varias oficinas rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarios barreras y perímetros adicionales para controlar el acceso físico entre las áreas con diferentes requerimientos de seguridad dentro del perímetro de seguridad.

Controles de Ingreso Físico

Las áreas seguras deberían protegerse mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado.
Todos los sistemas de control de acceso, deben considerar 3 diferentes categorías de personal:

- Operadores: Personal que laboran en el área, con acceso continúo.
- Personal de Soporte: Personal de mantenimiento y soporte, requiere de acceso periódico.

- Otros: Visitantes debidamente identificados, con acceso muy rara vez.

Se deberán considerar los siguientes lineamientos:

- Implementar una bitácora de accesos de los empleados y visitantes, por área. Donde se especifique:

Empleado: Fecha, nombre completo, hora de entrada, hora de salida, más la firma correspondiente.

República de Colombia
Departamento Del Cesar
Alcaldía Municipal
RIO DE ORO

Bitácora de Acceso del Personal - Área

ID	Fecha	Empleado	Hora de Entrada	Hora de Salida	Firma
1	D/M/A		H:M am	H:M am	
2	D/M/A		H:M am	H:M am	

Visitante: Fecha, nombre completo, cédula de ciudadanía, motivo de la visita, hora de entrada, hora de salida, más la firma correspondiente.

República de Colombia
Departamento Del Cesar
Alcaldía Municipal
RIO DE ORO

Bitácora de Acceso de Visitantes - Área

ID	Fecha	Visitante	Motivo	Hora de Entrada	Hora de Salida	Firma
1	D/M/A			H:M am	H:M am	
2	D/M/A			H:M am	H:M am	

- Se deberá registrar en la bitácora de accesos a los visitantes, los cuales serán supervisados por el personal, a no ser que su acceso haya sido previamente aprobado. Sólo se les deberá permitir acceso por propósitos específicos y autorizados y se deberá emitir las instrucciones sobre los requerimientos de seguridad del área y sobre los procedimientos de emergencia.

- El acceso a áreas críticas se deberá controlar y restringir sólo a personas autorizadas.

- Se deberá requerir que todos los empleados usen identificación visible. Deberá notificarse si un visitante a áreas seguras no se encuentra debidamente acompañado, o que no usa una identificación visible.

- Los derechos de acceso a áreas seguras deberán ser revisados y actualizados regularmente, y revocados cuando sea necesario.

Seguridad de Oficinas, Despachos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad.

Protección Contra Amenazas Externas e Internas

Se deberá asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

Se deberá prestar cuidado a cualquier amenaza contra la seguridad presentada por estructuras vecinas.

Se deberán considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

- **Explosiones:** Los materiales peligrosos o combustibles deberían ser almacenados a una distancia prudente del área asegurada.

- **Fuego:** Mantener siempre a la mano extintores debidamente recargados y probados, además de contar con detectores de calor y humo.

- **Inundaciones:** Contar con diferentes niveles del suelo, barreras, desagües y pisos falsos, para evitar el rápido avances del agua a las oficinas.

- **Interferencia Eléctrica y/o Radiación Electromagnética:** El cableado de la red de datos debe estar aislado del cableado eléctrico por canaletas. Se recomienda realizar estas instalaciones con base a la norma técnica.
- **Fallas en el Suministro de Energía:** Mantener UPS (Fuente de Suministro Eléctrico) o plantas de energía, que permitan la continuidad del suministro eléctrico y por tanto la continuidad de la funciones de la Alcaldía.

-**Robo:** Contar con alarmas de detección de intrusos, que emitan previo aviso a las autoridades. Además, contar con la vigilancia adecuada de tiempo completo (24 horas del día, todos los días).

Trabajo en Áreas Seguras

- Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.

- Evitar la ejecución de trabajos por parte de terceros sin supervisión.

- Las áreas aseguradas vacías deberían ser cerradas físicamente bajo llave y revisadas periódicamente.

Áreas de Acceso Público, Entrega y Carga

- El acceso al área de entrega y carga desde fuera de la Alcaldía se deberá restringir al personal identificado y autorizado.

- Se deberá diseñar el área de entrega y carga de manera que se pueda descargar los suministros sin que el personal de entrega tenga acceso a otras partes de la Alcaldía.

- Las puertas externas del área de entrega y carga deberán estar aseguradas cuando se abren las puertas internas.

- Se deberá inspeccionar el material que ingresa para evitar amenazas potenciales antes que el material sea trasladado del área de entrega y carga, al punto de uso.

- Se deberá registrar el material que ingresa en concordancia con los procedimientos de gestión de activos (Inventario de Activos) a su ingreso a la Alcaldía.

4.3.5.2 Seguridad de los Equipos

Sus Objetivos son:

- Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.
- Se deberá proteger el equipo de amenazas físicas y ambientales.
- La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y proteger contra pérdida o daño. Esto también debería considerar la ubicación y eliminación del equipo. Se pueden requerir controles especiales para proteger el equipo contra amenazas físicas, y salvaguardar los medios de soporte como el suministro eléctrico y la infraestructura del cableado.

Desplazamiento y Protección de Equipos

- El equipo se deberá ubicar de manera que se minimice el acceso innecesario a las áreas de trabajo.

- Los medios de procesamiento de la información que manejan datos confidenciales deberán ubicarse fuera de vista de personas no autorizadas, durante su uso.

- Se deberán adoptar controles para minimizar el riesgo de amenazas potenciales. Por ejemplo, robo, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo.

- Se deberán establecer lineamientos sobre consumir alimentos o bebidas y fumar en las áreas de trabajo o en proximidad de los medios de procesamiento de información.

- Se deberán monitorear las condiciones ambientales. Tales como temperatura y humedad, que puedan afectar los medios de procesamiento de la información, siguiendo las especificaciones del proveedor.

- Se deberá aplicar protección contra rayos a todas las líneas de ingreso de energía y comunicaciones, instalando el respectivo polo a tierra.

Servicios Públicos de Soporte

- Todos los servicios públicos de soporte (electricidad, agua, desagüe, calefacción/ventilación y aire acondicionado), deberán ser adecuados, inspeccionados regularmente y probado para asegurar su adecuado funcionamiento y para reducir cualquier riesgo por un mal funcionamiento o falla. Se deberá proveer un suministro eléctrico adecuado que esté de acuerdo a las especificaciones del fabricante del equipo.

- Se recomienda un dispositivo de suministro de energía ininterrumpido (UPS), cargado y probado regularmente, para el funcionamiento continuo de la Alcaldía, y un plan de contingencia en el caso de una falla de energía prolongada, como un generador de emergencia. Recuerde mantener el combustible necesario. El equipo UPS y los generados se deberán ser cargados y probados regularmente, para asegurar su buen funcionamiento, además de verificar que tengan la capacidad adecuada y concordancia con las recomendaciones del fabricante.

- Se deberán colocar interruptores de energía de emergencia cerca de las salidas de emergencia y proporcionar iluminación de emergencia en caso de una falla en la fuente de energía principal.
- Se recomienda evaluar e instalar, si se requiere, un sistema de alarma para detectar mal funcionamiento en los servicios públicos de soporte.

Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe estar protegido contra intercepción o daño, evitando las rutas a través de áreas públicas o mediante la distribución de sus líneas desde los medios de

procesamiento de información hasta las oficinas por vías subterráneas, canaletas o embutido en la pared. Los cables de energía deben estar separados de los cables de comunicaciones para evitar la interferencia. Se deben utilizar marcadores de cables y equipos claramente documentados e identificables para minimizar errores en la manipulación, como un empalme accidental de los cables de red equivocados.

Mantenimiento de los Equipos

El Comité de Seguridad de la información, establecerá un plan de mantenimiento preventivo para los equipos y velará por el cumplimiento del mismo.

Se realizará el mantenimiento de los equipos, para asegurar su disponibilidad e integridad permanentes, teniendo en cuenta:

- La realización de tareas de mantenimiento preventivo a los equipos, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Jefe del Área de Sistemas.

- La realización del mantenimiento y reparación de equipos, solo a personal calificado y autorizado.

- El registró de todas las fallas (supuestas y/o reales) y de todo el mantenimiento preventivo y correctivo realizado, se almacenara en una bitácora donde se describirá la fecha de realización, equipo, tipo de servicio (Mantenimiento Preventivo, Mantenimiento Correctivo o Reparación), Hora de Inicio o salida, Hora de Fin o retorno y firma del responsable del servicio (quien entrega) y del responsable del equipo (quien recibe).

República de Colombia
Departamento Del Cesar
Alcaldía Municipal
RIO DE ORO

Bitácora de Mantenimientos y Reparaciones - Área

ID	Fecha	Equipo	Servicio	Hora Inicio	Hora Fin	Entrega	Recibe
1	D/M/A			H:M am	H:M am		
2	D/M/A			H:M am	H:M am		

- El registro del retiro de equipos, para su mantenimiento de las oficinas de la Alcaldía.

- La eliminación de toda información confidencial que contenga cualquier equipo, que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

- El cumplimiento de todos los requerimientos impuestos por las pólizas de seguros de los equipos.

Seguridad de los Equipos Fuera de las Instalaciones

- El uso de equipo destinado al procesamiento de información, fuera las oficinas de la Alcaldía será autorizado por el Jefe del Área de Sistemas. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Secretario de la Dependencia.

- El equipo fuera de la Alcaldía nunca deberá ser dejado desatendido en lugares públicos. Durante un viaje, los computadores portátiles deberán ser llevadas como equipaje de mano y cuando sea posible, de manera disimulada.

- Se deberían observar en todo momento las instrucciones de los fabricantes para proteger el equipo. Por ejemplo, protección contra la exposición a fuertes campos electromagnéticos.

- El equipo de almacenamiento y procesamiento de la información incluye todas las formas de computadores personales, organizadores, celulares, tarjetas inteligentes u otras formas que se utilicen para trabajar desde la casa o se transporte fuera del área normal de trabajo.

Reutilización o Retirada Segura de Equipos

Los dispositivos que contienen información confidencial deberán ser físicamente destruidos, borrar o sobre-escribir la información utilizando técnicas que hagan imposible recuperar la información original, en lugar de simplemente utilizar la función estándar de borrar o formatear.

Cada acción realizada sobre estos dispositivos, conlleva a la actualización en el respectivo inventario de activos. Ya sea que fuese físicamente destruido o reubicado.

Retirada de Materiales Propiedad de la Empresa

- Los equipos, la información y el software no serán retirados de la Alcaldía sin autorización formal. Se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la misma.

- El retiro de los activos debe mantener un límite de tiempo de retiro y ser revisado al momento de la devolución.

- Se deberá realizar el respectivo registro de retiro y retorno del activo, que se almacenara en una bitácora donde se describirá el nombre del activo, cantidad de activos, fecha y hora de retiro, fecha y hora de retorno y la firma del responsable del retiro (quien entrega el activo) y del responsable del equipo (quien recibe el activo).

República de Colombia
Departamento Del Cesar
Alcaldía Municipal
RIO DE ORO

Bitácora de Retiro de Activos - Área

ID	Activo	Cantidad	Fecha / Hora Retiro	Fecha / Hora Retorno	Entrega	Recibe
1			D/M/A H:M am	D/M/A H:M am		
2			D/M/A H:M am	D/M/A H:M am		

4.3.6 Gestión de Comunicaciones y Operaciones

Sus objetivos son:

- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.
- Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.
- Los usuarios y funcionarios deben proteger la información utilizada en la infraestructura tecnológica de la Alcaldía. De igual forma, deberán proteger la información confidencial que por necesidades de la Alcaldía deba ser guardada, almacenada o transmitida.

4.3.6.1 Procedimientos y Responsabilidades Operacionales

Sus Objetivos son:

- Asegurar la operación correcta y segura de los medios de procesamiento de la información.
- Establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados.

Procedimientos de Operación Documentados

- Se deberá documentar y mantener actualizados los procedimientos operativos, y sus cambios serán autorizados por el Coordinador del Comité de Seguridad de la Información.

- El Jefe del Área de Sistemas, deberá documentar la configuración de los enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red.

- Todos los procedimientos de encendido y apagado de los equipos deben ser documentados; dichos procedimientos deben incluir el detalle de personal clave a ser contactado en caso de fallas no contempladas en el procedimiento regular documentado.

- Todas las tareas programadas en los sistemas para su realización periódica, deben ser documentadas. Este documento debe incluir tiempo de inicio, tiempo de duración de la tarea, procedimientos en caso de falla, entre otros.

- Los procedimientos para resolución de errores deben ser documentados, entre ellos se debe incluir: Errores en la ejecución de procesos, fallas o apagado de los sistemas, códigos de error en la ejecución de procesos y la información de los contactos que podría colaborar con la resolución de errores

- Los procesos para la realización de backup´s (copias de seguridad o respaldo), deben ser documentados detalladamente, para evitar perdida de la información por procedimientos mal ejecutados.

- Los procesos diarios llevados a cabo en cada dependencia y por cada funcionario, deberán ser documentados, para mantener la continuidad de las funciones de la Alcaldía, en caso de que el funcionario que la realiza se encuentre indispuesto, fuera del municipio o haya sido removido de su cargo por ser reemplazado o despedido.

Gestión de Cambios

- Se deben definir procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio debe ser evaluado previamente en aspectos técnicos y de seguridad. El Jefe del Área de Sistemas debe controlar que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan.

- Cada cambio realizado deberá ser comunicado al personal afectado, y se realizará la respectiva capacitación y prueba, que eliminara todo tipo de duda y evitara fallas, eventos inesperados y perdida de la información a causa de falta de información.

Segregación de los Deberes

Se debe contemplar la separación de ejecución de tareas o áreas de responsabilidad, en la medida de que la misma reduzca el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

4.3.6.2 Planificación y Aceptación del Sistema

Se deberá en todos los casos minimizar el riesgo de fallas en los sistemas.

Gestión de Capacidades

El Secretario de la respectiva Dependencia, debe efectuar el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello se debe tomar en cuenta los nuevos requerimientos de los servicios así como las tendencias actuales y proyectadas en el procesamiento de la información de la Alcaldía, para el período estipulado de vida útil de cada componente.

Aceptación del Sistema

El Comité de Seguridad de la Información debe sugerir criterios de aprobación de nuevos sistemas de información para la Alcaldía, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva.

Para la ejecución de lo anterior se deberá tener en cuenta:

- El desempeño y los requerimientos de capacidad de los equipos.
- Manuales de procedimientos, efectivos.
- Total acoplamiento del nuevo sistema con los ya existentes.
- Total convencimiento de que el nuevo sistema no afecta la seguridad de la Alcaldía.
- Capacitación para la operación o uso del nuevo sistema.
- Facilidad de uso, con el fin de no afectar el desempeño del usuario y evita el error humano.
- Certificación y acreditación formal para verificar que se hayan tratado apropiadamente los requerimientos de seguridad.

4.3.6.3 Protección Contra el Código Malicioso y Descargable

Proteger la integridad del software y la integración en la Alcaldía, tomando precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no autorizados, de los cuales el software y los medios de procesamiento son vulnerables. Por ejemplo, virus de cómputo, virus de red, caballos Troyanos y bombas lógicas; de los cuales los funcionarios de la Alcaldía deben estar al tanto.

La Administración Municipal en apoyo del Comité de Seguridad de la Información, deberán realizar capacitaciones al personal en lo referente a controles para evitar, detectar y eliminar los códigos maliciosos y controlar los códigos móviles.

Controles Contra Códigos Maliciosos

El Jefe del Área de Sistemas, debe instalar antivirus licenciado en los servidores y los equipos de la Alcaldía, configurados para actualizaciones diarias, con el fin de detectar, eliminar y prevenir la implantación de código malicioso. Se recomienda la instalación del software antivirus ESET NOD32.

Todos los archivos adjuntos recibidos a través del correo electrónico deben ser revisados por un antivirus antes de ejecutarlo.

Debe contarse con un procedimiento para la actualización periódica de los programas antivirus y el monitoreo de los virus detectados. En caso de detectarse fallas en el funcionamiento de dichos programas, éstas deben ser comunicadas al Jefe del Área de Sistemas, para una respectiva verificación.

Es obligación de la Administración Municipal que los funcionarios de la Alcaldía, usen solo programas licenciados. La instalación de software no licenciado, igualmente genera riesgos, como el ingreso de virus, instalación de software espía, hurto o divulgación no autorizada de la información. De hallarse software ilegal en alguna dependencia, será reportado como incidente de seguridad por el Coordinador de Seguridad Informática y posteriormente investigado. Se recomienda el uso del sistema operativo de Windows versión 7 (Seven) o posteriores.

La red y cada equipo de cómputo de la Alcaldía, debe contar con mínimo un cortafuego (Firewall) que prevenga el acceso de intrusos al sistema, el cual debe ser revisado continuamente para evaluar su funcionamiento.

4.3.6.4 Copias de Seguridad

Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información, realizando copias de respaldo de la información y software, las cuales deberán ser probadas regularmente.

Copias de Seguridad de la Información

Cada funcionario de la Alcaldía deberá elaborar copias de seguridad diarias a sus labores, clasificándola y resguardándola de acuerdo al protocolo establecido. Es recomendable que las copias de seguridad se almacenen en un lugar externo a la Alcaldía para prevenir pérdida de datos en el caso de incidencias o fallas. Se recomienda el uso ACRONIS BACKUP, para la elaboración de backup´s.

El Secretario de cada Dependencia, deberá revisar semanalmente las copias de seguridad, para asegurar que se puedan confiar en ellas para usarlas cuando sean necesarias en caso de emergencia, así como probar regularmente las restauraciones, para asegurar que sean efectivas, y llevará un registro de dicho procedimiento.

Para sistemas críticos, los procedimientos de respaldo deberán abarcar toda la información, aplicaciones y datos de todos los sistemas, necesarios para recuperar el sistema completo en caso de un desastre.

4.3.6.5 Gestión de seguridad de las redes

Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

Controles de Redes

El Jefe del Área de Sistemas deberá gestionar y asegurar la protección de las redes de la Alcaldía, las cuales exige permanente monitoreo del tráfico de datos, para detectar actividades inusuales en el desempeño de la misma.

La Oficina del Área de Sistemas debe contar con un servidor en paralelo, el cual permitirá la continuidad de las operaciones, en caso de falla del servidor principal.

Todo equipo de TI debe ser revisado, registrado y aprobado por el Jefe del Área de Sistemas antes de conectarse a cualquier nodo de la red de comunicaciones, así mismo, desconectará aquellos dispositivos que no estén aprobados y reportara tal conexión como un incidente de seguridad a ser investigado.

Las redes deberán ser adecuadamente manejadas y controladas para poder proteger la información en las redes, y mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.

Los dispositivos de comunicaciones (router, switch entre otros) pertenecientes a la red, deberán ser configurables y adaptables a las necesidades, por lo cual se recomienda sean remplazados los actuales.
El cable de red utilizado en las conexiones físicas deberá ser cable UTP categoría 7e. En caso de contarse con instalaciones que hagan uso de categorías inferiores a la descrita, este deberá ser inmediatamente cambiado al específico.

Seguridad de los Servicios de Red

Se deberá incluir dentro del contrato de servicio de red con el proveedor las características de seguridad, niveles de servicio y requerimientos de gestión de todos los servicios de red, asegurándose de que los proveedores del servicio de red implementen estas medidas.

Se deberá determinar y monitorear regularmente la capacidad del proveedor del servicio de red para manejar los servicios contratados de una manera segura.

4.3.6.6 Gestión de Medios

Proteger los documentos, medios de almacenamiento (CD, Disco Duro), entrada/salida de datos y documentación del sistema, de una divulgación no autorizada, modificación, eliminación y destrucción de estos activos, mediante el control físico y evitando la interrupción de las actividades laborales de la Alcaldía.

Gestión de soportes extraíbles

El Secretario de cada dependencia, con la asistencia del Jefe del Área de Sistemas, deberá implementar procedimientos para la administración de medios informáticos removibles, como USB, CD, DVD e informes impresos y la eliminación segura de los mismos, respetando la normativa vigente.

Procedimientos de Manipulación de la Información

El etiquetado y almacenamiento de los medios, deberá realizarse teniendo en cuenta su clasificación y la manipulación de estos se realizara bajo los protocolos de acceso establecido.

Estos procedimientos se aplican a la información en documentos, Sistemas de cómputo, Redes, Computación móvil, Comunicaciones móviles, Comunicaciones vía correo, uso de máquinas de fax y demás.

Seguridad de la Documentación del Sistema

La documentación del sistema puede contener información sensible, por lo que se deben considerar las precauciones necesarias para su protección, de almacenar la documentación del sistema en forma segura y restringir el acceso al personal estrictamente necesario.

4.3.6.7 Intercambio de Información

Mantener la seguridad en el intercambio de información y software dentro de la Alcaldía y con cualquier entidad externa.

Cuando se realicen intercambios de información y software se especificara el grado de sensibilidad de la información involucrada y las condiciones de seguridad sobre la misma.

Los procedimientos de transporte de medios informáticos entre diferentes puntos deben contemplar: La utilización de medios de transporte o servicios de mensajería confiables, el suficiente embalaje para envío de medios a través de servicios postales o mensajería y la adopción de controles especiales cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizada.

Políticas y Procedimientos de Intercambio de Información

La Alcaldía deberá establecer políticas, procedimientos y controles formales de intercambio con objeto de proteger la información mediante el uso de todo tipo de servicios de comunicación.

Se deberá proteger el intercambio de información en la Alcaldía, de la intercepción, copiado, modificación, routing equivocado y destrucción. Se aplicarán procedimientos para la detección y protección de contra códigos maliciosos que pueden ser transmitidos a través del uso de comunicaciones electrónicas, así como la protección de la información electrónica confidencial comunicada de forma adjunta.

Implementar procedimientos para el uso de comunicación inalámbrica, tomando en cuenta los riesgos particulares involucrados.

No dejar información confidencial o crítica en fotocopiadoras, impresoras o fax, para evitar que personas no autorizadas puedan tener acceso a ellas. Además, evitar revelar información confidencial cuando realiza una llamada telefónica para evitar ser escuchado por personas alrededor suyo, en el otro lado de la línea o por la intervención del teléfono.

Evitar dejar mensajes con información confidencial en máquinas contestadoras dado que estos pueden ser escuchados por personas no autorizadas.

Mantener total precaución al usar una máquina de fax, mientras no se esté seguro del número receptor del documento, mantenerse al pendiente el retiro de documentos recibidos, evitar la programación de envió de mensajes a números específicos y siempre recordar que las máquinas de fax y fotocopiadoras modernas tienen páginas cache y almacenan páginas en caso de una falla en la transmisión o papel, las cuales se imprimirán una vez que la falla se aclare.

Evitar enviar correos electrónicos a cuentas de correo de la cuales no se tenga seguridad, además de ser precavido al momento de revelar información en páginas web no confiables o seguras.

Evitar mantener conversaciones confidenciales en lugares públicos, u oficinas o salas de reuniones abiertas, sin paredes a prueba de ruidos.

Acuerdos de Intercambio

Cuando se realicen acuerdos de intercambio de información o software entre dependencias, se especificara el grado de sensibilidad de la información, mediante un sistema de etiquetado acordado para la información confidencial o critica, con el fin de que la información sea adecuadamente protegida y las consideraciones de seguridad sobre la misma. Este intercambio se deberá realizar por medio de mensajería interna.

El empleado encargado de la mensajería interna en la Alcaldía, deberá contar la debida de identificación como mensajero, y la debida capacitación sobre identificación de paquetes etiquetados de acuerdo a su clasificación. Además, será responsable de realizar el respectivo registro de entrega y recibo, de estos.

Soportes Físicos en Tránsito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deben utilizar los servicios de mensajería confiable (como Servientrega y Efecty), a fin de proteger la información sensible contra divulgación o modificación no autorizadas.

Antes de entregar el sobre o paquete, es necesario cerciorarse de que la persona quien lo recibe se encuentre debidamente identificado como empleado del servicio de mensajería contratado, con el fin de evitar la pérdida de la información contenida en el sobre o paquete, por suplantación de tal empleado.

Los paquetes a enviar, deberán contar con la total protección ante cualquier eventualidad ambiental (exposición al calor, humedad o campos electromagnéticos) o provocada (manipulación) durante el tránsito a su destino.

Mensajería Electrónica

Creación de cuentas de correo de uso institucional para cada uno de los funcionarios de la Alcaldía, por parte del Jefe del Área de Sistemas, el cual contara con una vigencia de acuerdo a la fecha de vencimiento de la vinculación del empleado con la Alcaldía. Finalizada su vinculación o terminada la prestación del servicio, el Jefe del Área de Sistemas eliminará las autorizaciones relacionadas con la cuenta.

El uso de correos masivos institucionales que por necesidades específicas de la Alcaldía requieran ser enviados a todas las dependencias, debe ser solicitado y autorizado al Jefe del Área de Sistemas, por medio escrito.

Se deben reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando las posibles vulnerabilidades de los mensajes al acceso o modificaciones no autorizadas, código malicioso inmerso, acceso de usuarios a las cuentas de correo, uso inadecuado por parte del personal yarchivos adjuntos; mediante la implementación de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos, definiendo del tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario y alcances del uso del correo electrónico por parte del personal de la Alcaldía, además de nunca dejar abierto el correo institucional en ninguna circunstancia.

4.3.6.8 Monitoreo

Detectar las actividades de procesamiento de información no autorizadas a la Alcaldía.

Registro de Auditoría

Se debe generar registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deben incluir la identificación del usuario, la fecha y hora de inicio y terminación, la identidad o ubicación de la terminal, un registro de intentos exitosos y fallidos de acceso a los sistemas, y un registro de intentos exitosos y fallidos de acceso a datos y otros recursos, cambios en la configuración del sistema, uso de privilegios, archivos a los cuales se tuvo acceso y los tipos de acceso, y alarmas activadas por el sistema de control de acceso.
Los registros de auditoría pueden contener datos personales confidenciales, por lo que se deberán mantener las medidas de protección de privacidad apropiadas, y en lo posible no permitir el borrado o desactivación de los registros de las actividades propias del encargado.

Supervisión del Uso del Sistema

Se deberá monitorear el uso de los medios de procesamiento de la información mediante la revisión de bitácoras de uso de estos, con el fin de asegurarse que el personal sólo esté realizando las actividades para las cuales han sido explícitamente autorizados.

- Accesos autorizados: El uso de estos archivos deberá ser registrado en una bitácora donde se describirá la fecha actual, la descripción de archivo solicitado, el motivo de su uso, hora de entrega, hora de recibo y la firma del responsable que solicita el archivo (quien usara el archivo) y del responsable de la entrega (quien entrega el archivo). Esta bitácora deberá ser revisada regularmente para cumplir con las actividades propuestas para su monitoreo, como es entender las amenazas que a las que se enfrenta y la manera en que estas ocurren.

República de Colombia
Departamento Del Cesar
Alcaldía Municipal
RIO DE ORO

Bitácora de Uso Archivos - Área

ID	Fecha	Archivo	Motivo de Uso	Hora Inicio	Hora Fin	Entrega	Recibe
1	D/M/A			H:M am	H:M am		
2	D/M/A			H:M am	H:M am		

- Accesos no autorizados: El acceso fallido o rechazado de usuarios, involucración fallida o rechazada de datos u otros recursos, la violación de políticas de acceso y alertas por detección de intrusos, deberán ser igualmente registrados.

- Alertas o fallas del sistema: Las alertas o fallas de los sistemas, también deberán ser registradas con el fin de determinar su origen e identificar las vulnerabilidades presentes

Protección del Registro de Información

Se deberá asegurar las bitácoras de registros, para evitar cambios no autorizados que alteren la información contenida en ellas, creando un falso sentido de seguridad.

Registros de administración y operación

Cada empleado asegurara el registro de las actividades realizadas en los sistemas, incluyendo según corresponda los tiempos de inicio y cierre del sistema, errores del sistema y medidas correctivas tomadas, los intentos de acceso a sistemas, recursos o información crítica, los cambios a información crítica, registrándose de manera regular, la hora en la cual ocurre el evento, la información sobre el evento y los procesos involucrados.

Registro de fallas

El Secretario de cada dependencia desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicación de su dependencia, que permita tomar medidas correctivas.
Se deberían registrar las fallas reportadas por los usuarios o por los programas del sistema relacionadas con los problemas con el procesamiento de la información o los sistemas de comunicación.
Los registros de errores y fallas determinan el desempeño de los sistemas de una forma individual mediante una evaluación del riesgo, tomando en cuenta la degradación del desempeño.

Sincronización del reloj

Los relojes de todos los equipos de la Alcaldía deberán mantenerse sincronizados a la hora exacta. Este ajuste correcto de los relojes es importante para asegurar la exactitud de los registros de auditoría, los cuales se pueden requerir para investigaciones o como evidencia en casos legales o disciplinarios. Registros de auditoría inexactos pueden entorpecer estas investigaciones y dañar la credibilidad de tales evidencias.

4.3.7 Control de Accesos

Sus objetivos son:

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos del personal por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión de red de la Alcaldía.
- Concientizar a los empleados respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utiliza equipos móviles e instalaciones de trabajo remoto.

En un sistema informático resulta de vital importancia, restringir los accesos y garantizar una adecuada utilización de los recursos.

Cada funcionario es responsable de los mecanismos de control de acceso que le sean proporcionados.

4.3.7.1 Gestión de acceso de usuario

Sus objetivos son:

Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información

Se deberían establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

Los procedimientos deberían abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta el des-registro final de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Cuando sea apropiado, se debería prestar atención especial a la necesidad de controlar la asignación de derechos de acceso privilegiados, lo que permite a los usuarios superar los controles del sistema.

Registro de usuario

Se deberá registrar cada empleado como usuario único en cuanto a su rol en la Alcaldía, definiéndose los niveles de acceso a los sistemas, la información y las áreas seguras. Para el cambio de cargo, se deberá inhabilitar los accesos del cargo anterior y habilitar los accesos del nuevo cargo, igualmente definidos. En caso de finalización del contrato se inhabilitara al empleado, de ninguna manera estos registros deberán ser eliminados, solo basta con actualizar su estado de inhabilidad. Si este antiguo empleado, retoma nuevamente labores

en la Alcaldía, se deberá realizar un nuevo registro. Es necesario realizar nuevos registros, que concuerden con la fecha de contrato, con el fin de llevar un control en caso de llevarse a cabo una auditoria.

Los permisos de acceso deberán ser llevados a cabo luego la debida autorización tras el registro del nuevo usuario y la respectiva comunicación de sus deberes en el cargo y sus responsabilidades en cuanto al manejo de los recursos y acceso otorgados.

Igualmente, se deberá llevar un registro de los accesos como respaldo a este control.

Gestión de privilegios

El uso de los sistemas de información de la Alcaldía, será limitado y controlado mediante su asignación y uso, solamente al personal capacitado y autorizado para tales fines. Con el propósito de evitar accesos no autorizados a estos, que alteren la información contenida al realizar modificaciones no autorizadas.

Gestión de contraseñas de usuario

Las contraseñas de acceso a los sistemas, serán de carácter confidencial. Deberán ser conocidas solo por el personal autorizado, con tipo de dato alfanumérico, cambiada regularmente y protegida de personas no autorizadas, evitando mencionarlas en vos alta, por teléfono o correo, registradas en documentos a la vista o almacenadas en el equipo, celular, etc. Estas no deben ser fáciles de deducir y deben estar compuestas por al menos 10 caracteres.

Las claves de acceso otorgadas por la Alcaldía a empleados que vencieron su contrato o cambiaron de cargo, deberán ser cambiadas inmediatamente ocurra el cambio en el estado del contrato del empleado. En ninguna circunstancia, se deberá retomar una clave de acceso ya usada.

Las claves otorgadas por los proveedores, deberán ser cambiadas inmediatamente, luego de la instalación.

Revisión de los derechos de acceso de usuario

Los derechos de acceso, deberán ser monitoreados a intervalos regulares de tiempo, con el fin de determinar su cumplimiento, después de cualquier cambio en la planta de empleados de la Alcaldía.

Los derechos de acceso privilegiados, deberán ser monitoreados con mayor frecuencia, para asegurar que no se hayan obtenido privilegios no autorizados.

4.3.7.2 Responsabilidades de usuario

Uso de contraseñas

Todo el personal de la Alcaldía deberá comprometerse a mantener seguras las contraseñas a su disposición al igual que su uso. Deberán mantenerse bien resguardadas evitando su registro a la vista, cambiándose cuando haya el menor indicio de un posible peligro, contar con al menos 10 caracteres de tipo alfanumérico, fácil de recordar pero nunca fácil de deducir evitando nombres, números telefónicos o fechas de nacimiento. No usar la misma contraseña que en cuentas de correo, tarjetas de crédito y demás.

Equipo de usuario desatendido

El Jefe del área de sistemas debe coordinar con el Jefe de Recursos Humanos las tareas de concienciación a todos los empleados, proveedores y contratistas de la Alcaldía, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

El personal deberá garantizar que los equipos desatendidos sean protegidos adecuadamente, cerrando sesiones activas cuando se termine o contando con un protector de pantalla asegurado mediante clave secreta. En caso de haber culminado su jornada laboral el equipo deberá ser apagado completamente.

Política de escritorio y pantalla limpios

Adoptar una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información de la Alcaldía, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Los escritorios del personal de la Alcaldía deberán en lo posible mantenerse libres de documentos o dispositivos con información, en especial cuando exista la presencia de visitantes en las instalaciones o cuando el área se encuentre vacía o desatendida.

En caso de ser necesario que un equipo de la Alcaldía permanezca temporalmente desatendido, el empleado responsable de este deberá: terminar la sesión iniciada, bloquear la sesión o apagar el equipo.

En caso de usar la impresora, fotocopiadora o fax, se deberán retirar inmediatamente los documentos, para evitar que terceras personas obtengan acceso a ellos cuando estos se encuentren desatendidos.

Antes de terminar la jornada laboral, se deberán almacenar los documentos utilizados en un lugar seguro, para evitar incidentes durante el horario no laboral.

4.3.7.3 Control de acceso a la red

Política sobre el uso de los servicios de la red

El Jefe del área de sistemas deberá elaborar, mantener y publicar los procedimientos de administración de cuentas de usuario para el uso de servicios de la red de la Alcaldía, tomando en cuenta las especificaciones del proveedor del servicio.

Se debe controlar el acceso a los servicios de red tanto internos como externos. El Jefe del área de sistemas tiene a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente a personal específicamente autorizado.

Se deberá impedir los accesos no autorizados a la red, mediante el uso de firewall. Todos los dispositivos de red, así como el cableado deben ser ubicados de manera segura.

Autenticación del usuario para las conexiones externas

El Jefe del área de sistemas en conjunto con el secretario de cada dependencia de la Alcaldía, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

Se deberían utilizar métodos de autenticación apropiados para controlar el acceso de usuarios remotos, en especial para redes inalámbricas.

Las conexiones remotas deberán realizarse por medio de un equipo de cómputo seguro.

Se deberían implementar controles de autenticación adicionales para controlar el acceso a las redes inalámbricas.

Identificación de los equipos en las redes

Se deberá contar con la identificación de cada equipo de la Alcaldía, con el fin de determinar a qué red está conectado y si tiene permiso para ello, en especial si esta cuenta con un grado de confidencialidad.

Control de la conexión a la red

El acceso a Internet debe ser utilizado con propósitos autorizados o con el destino por el cual fue provisto. El uso del correo electrónico e Internet se prohíbe para fines que no sean institucionales dentro y hacia fuera de la Alcaldía.

No está permitido el envío de mensajes anónimos, así como aquellos que consignan títulos, cargos o funciones no oficiales, además que atenten contra la dignidad humana y las garantías fundamentales.

Control de encaminamiento (routing) de red

Se deberá incorporar controles de ruteo (rutas estáticas y dinámicas, controles ARP, enrutamiento de correo electrónico), para asegurar que las conexiones y los flujos de información no violen la Política de Control de Accesos.

4.3.7.4 Control del acceso al sistema operativo

Se deberá autenticar a los usuarios autorizados para el uso de los sistemas, de acuerdo con la política de control de acceso definida, registrando los intentos exitosos y fallidos de autenticación del sistema, el uso de los privilegios especiales, emitiendo alarmas cuando se violan las políticas de seguridad del sistema, proporcionando los medios de autenticación apropiados y cuando sea conveniente, restringir el tiempo de conexión de los usuarios.

Procedimientos para un registro seguro

El acceso a los sistemas operativos debería ser controlado mediante un procedimiento de registro seguro. El procedimiento para registrarse en un sistema de operación debería ser diseñado de manera que minimice la oportunidad de un acceso no autorizado. Por lo tanto, el procedimiento para registrarse debería divulgar el mínimo de información acerca del sistema para evitar proporcionar al usuario no autorizado ninguna ayuda innecesaria. Por tal motivo, se deberá evitar mostrar identificadores del sistema o aplicación hasta que se haya completado satisfactoriamente el proceso de registro, no proporcionar mensajes de ayuda durante el procedimiento de registro que involuntariamente ayude al usuario no autorizado, validar la información del registro después de completar todas las entradas de datos. En caso de surgir errores, el sistema deberá indicar qué parte de los datos es correcta o incorrecta. Además, se deberá establecer el número de re-intentos de clave secreta, al igual que el número mínimo de caracteres necesarios para el diligenciamiento de esta y evitar transmitir claves secretas en un texto abierto a través de la red, debido a que estas pueden ser capturadas por un programa espía en la red.

Identificación y autenticación de usuario

El proceso de autenticación de usuario a los sistemas, para permitir su acceso debe ser de máximo tres intentos para una autenticación satisfactoria de usuario y contraseña, después de éste número de intentos, se deshabilitará el ingreso de usuario.

Sistema de gestión de claves secretas

- Imponer el uso de contraseñas individuales, para determinar responsabilidades; permitiendo que el personal seleccionen y cambien sus propias contraseñas (luego de

cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso. La selección de contraseñas debe cumplir con los parámetros necesarios de calidad.

- Imponer cambios en las contraseñas en aquellos casos en que el personal selecciona sus propias contraseñas; obligándolos a cambiar las contraseñas provisionales, en su primer procedimiento de identificación.

- Mantener un registro de las últimas contraseñas utilizadas por el Personal, y evitar la reutilización de las mismas, además evitar mostrar las contraseñas en pantalla, cuando son ingresadas y almacenarlas de forma cifrada. Estas deberán ser de tipo alfanumérico para evitar que sean fáciles de detectar.

Uso de los recursos del sistema

Se deberá restringir y controlar estrechamente el uso de los programas de utilidad que podrían ser capaces de superar los controles del sistema y la aplicación.

Cierre de una sesión por inactividad

Se deberá cerrar la sesión iniciada que ha permanecido inactiva por un lapso de tiempo definido (al menos cinco minutos de inactividad). Esta acción deberá tener en cuenta los riesgos de seguridad identificados en el área y la clasificación de la información que está siendo manejada. Su aplicación es importante en las áreas de alto riesgo de la Alcaldía, las cuales incluyen áreas públicas o externas a la seguridad de la infraestructura (áreas vecinas al parque principal).

Limitación del tiempo de conexión

El tiempo de conexión a las aplicaciones del sistema, deberá ser limitado en lo posible al horario de trabajo normal, para evitar accesos no autorizados.

4.3.7.5 Control de acceso a las aplicaciones y a la información

Restricción del acceso a la información

Se deberá restringir el acceso del personal a la información y funciones de los sistemas, en relación a la política de control de accesos definida.

Aislar el sistema confidencial

El proveedor de sistemas de información para la alcaldía, deberá identificar y documentar explícitamente la sensibilidad o confidencialidad del sistema de aplicación, para obtener una referencia en cuanto a que controles aplicar para su óptimo funcionamiento y

seguridad. Detallando riesgos, recursos físicos y lógicos, para su uso en un ambiente óptimo.

4.3.7.6 Computación y tele-trabajo móvil

Computación y comunicaciones móviles

Evitar comprometer la información de la Alcaldía al usar dispositivos de comunicaciones móviles, aplicando controles de protección física, acceso, técnicas criptográficas, copias de respaldo (backup's) y protección contra virus. Además de incluir reglas y consejos para su conexión a las redes y lineamientos para el uso de estos en lugares públicos evitando su pérdida o robo, procurando no dejar el dispositivo desatendido.

Tele-trabajo

Las actividades de tele-trabajo deberán ser autorizadas, solo si se cumple con los controles de seguridad necesarios para su ejecución. Se deberá contar con la protección adecuada contra el robo del equipo e información, la divulgación no autorizada de información, acceso remoto no autorizado a los sistemas internos de la Alcaldía o el mal uso de los medios. Además se deberá considerar la seguridad física existente en el lugar de la tele-trabajo, tomando en cuenta el ambiente, amenaza de acceso no autorizado a la información o al equipo por parte de otras personas (familia, amigos) que utilizan el medio y la configuración de la red.

El área destinada para el tele-trabajo deberá contar el inmobiliario necesario para su desarrollo.

4.3.8 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

4.3.8.1 Requerimientos de seguridad de los sistemas de información

Análisis y especificación de los requerimientos de seguridad

El proveedor de los sistemas de información (nuevos o actualizaciones) para la Alcaldía, deberá especificar los controles de seguridad requeridos, reflejando el valor de los activos de información, y el daño potencial que podría resultar ante una falla o ausencia de seguridad. Se deberá realizar un proceso de prueba y adquisición formal, para tratar los requerimientos de seguridad identificados antes de contratar. Si el producto ya ha sido adquirido y causa un riesgo de seguridad, este deberá ser desactivado o determinar si se puede obtener alguna ventaja de él, tras su mejoramiento.

4.3.8.2 Procesamiento correcto en las aplicaciones

Para el procesamiento correcto en las aplicaciones, el personal a cargo del uso de los sistemas de información de la Alcaldía, deberán seguir uno a uno los lineamientos especificados por el proveedor.

4.3.8.3 Controles criptográficos

Se utilizarán controles criptográficos para los siguientes casos:
- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información confidencial, fuera de las instalaciones de la Alcaldía.
- Para el resguardo de información, como resultado de una evaluación de riesgos realizada por el Comité de Seguridad de la Información.

Política sobre el uso de controles criptográficos

Se deberá realizar una evaluación de riesgos, identificando el nivel de protección requerido, e incluyendo métodos de protección a claves criptográficas y a la recuperación de la información codificada en el caso de claves pérdidas, comprometidas o dañadas, con el objetivo de mantener siempre la confidencialidad, integridad y disponibilidad de la información. El uso de este control será implementado siempre y cuando luego de un arduo análisis se decida que es el control apropiado, considerando normas que describen las condiciones para su uso aceptable y si es necesario, asesorarse de especialistas en la materia.

Gestión de claves

El comité de seguridad de la información deberá realizar la evaluación de riesgos, con el fin de identificará el nivel de protección requerido, tomando en cuenta el tipo y la calidad del algoritmo de cifrado y la longitud de las claves criptográficas a utilizar.

Para evitar comprometer las claves, se deberá definir las fechas de activación y desactivación para que las claves sólo ser utilizadas durante un período de tiempo limitado.

La técnicas criptográficas de claves secretas, permite compartir la misma clave entre dos o partes. La cual es utilizada tanto para codificar como descodificar la información, y deberá mantenerse en secreto para evitar que personas no autorizadas tengan acceso a ella y puedan decodificar toda la información codificada con esta o introducir información no autorizada haciendo uso de ella.

4.3.8.4 Seguridad de los archivos del sistema

Control del software operacional

Se deberán minimizar los riesgos operacionales manteniendo en ejecución solo software aprobado por la administración y que han sido recomendados por jefe del área de sistemas o el comité de seguridad. Estos solo deberán ser implementados en la Alcaldía luego de realizarse las respectivas pruebas de funcionamiento, vulnerabilidad, efectos sobre el sistema y facilidad de uso para el personal, con resultados satisfactorios.

Se deberá archivar el software (versiones antiguar y recientes), junto con toda la información requerida, parámetros, procedimientos y detalles de configuración, mientras se mantenga en uso. Para su funcionamiento óptimo se deberá en lo posible, mantener el software adquirido por medio de proveedores en versiones que ofrezcan soporte, para evitar no recibirlo por ser versiones antiguas del software que con el paso del tiempo podrían generar riesgos innecesarios.

Antes de adquirir una nueva versión del software en ejecución, es necesario analizar los complementos y la seguridad de esta, debido a que en algunos casos las nuevas versiones de software no cubre el mismo objetivo, es decir, cuentan con funcionalidades no aplicables a la administración o suprimen funciones requeridas, pueden ser menos seguras, menos estables y menos entendibles que la versión actual.

A los proveedores se les deberá en lo posible restringir el acceso físico o lógico solo para propósitos de soporte cuando sea necesario y con la aprobación del Comité, bajo monitoreo de sus actividades.

4.3.8.5 Gestión de la vulnerabilidad técnica

Se debería obtener oportunamente la información sobre las vulnerabilidades técnicas de los sistemas de información que se están utilizando, la exposición de la Alcaldía a dichas vulnerabilidades evaluadas, y las medidas apropiadas tomadas para tratar los riesgos asociados.

4.3.9 Gestión de Incidentes de Seguridad de la Información

Todo el personal deberá estar al pendiente de la aparición de eventos y debilidades asociados con los sistemas de información, que podrían tener un impacto en la seguridad de los activos, requiriendo que se reporten mediante procedimientos formales, lo más pronto posible al jefe del área de sistemas, con el fin de realizar las acciones correctivas de una manera oportuna.

Una adecuada gestión de incidentes le permitirá a la Alcaldía: responder a los incidentes de manera sistemática, eficiente y rápida; volver a la normalidad en poco tiempo, perder muy

poca información; realizar continuamente mejoras en la gestión y tratamiento de incidentes; generar nuevos conocimientos sobre incidentes, para evitar en lo posible que se repitan.

4.3.9.1 Notificación de eventos y debilidades de la seguridad de la información

Notificación de eventos en la seguridad de la información

El comité de seguridad de la información deberá establecer un procedimiento formal para el reporte de eventos asociados con la seguridad de la información, junto con el procedimiento de acciones a tomarse al recibir el reporte, definiéndose un punto de contacto que siempre esté disponible y sea capaz de proporcionar una respuesta adecuada y oportuna, al recibir la comunicación del evento. Además, se deberá notificar los resultados del tratamiento del evento. Para realizar un efectivo tratamiento al evento se deberá recolectar evidencias lo más pronto posible, luego de la ocurrencia. Este procedimiento deberá ser comunicado a todo el personal, para ser implementado desde el momento de su creación.

Todo el personal (empleado, proveedores o contratistas), se hará responsable de reportar cualquier evento que atente contra la seguridad de la información, lo más rápidamente posible, ejecutando de forma correcta el procedimiento de reporte.

El reporte y tratamiento del evento comunicado, deberá ser debidamente registrado en una bitácora de eventos, que detalle los eventos surgidos y el tratamiento idóneo para su efectiva solución.

Figura 110. Bitácora de Reporte de Incidentes

República de Colombia
Departamento Del Cesar
Alcaldía Municipal
RIO DE ORO

Bitácora de Reporte de Incidentes - Área

Datos del Reporte de Incidentes	
Reporte N°.	
Fecha de Reporte	
Hora de Reporte	
Descripción del Incidente	
Efectos causados	
Responsable del Activo	
Evidencias	
Tratamiento	
Fecha de Corrección	
Hora de Corrección	
Datos del Reportante	
Nombre	
Cargo	
Dependencia	

_____
Firma del Evaluador

Pueden considerarse como eventos de seguridad de la información a notificar los siguientes:

- Pérdida del servicio, equipo o medios.
- Mal funcionamiento o sobre-carga del sistema.
_ Errores humanos.
- Incumplimientos de las políticas o lineamientos.
- Violaciones de los acuerdos de seguridad física.
- Mal funcionamiento del software o hardware.
- Violaciones de acceso.

Notificación de puntos débiles de seguridad

Todo el personal deberá reportar cualquier debilidad de seguridad observada o sospechada en los sistemas o servicios, al jefe del área de sistemas para que él se haga cargo o contacte al proveedor lo más rápidamente posible, para evitar incidentes en la seguridad de la información. El mecanismo de reporte deberá ser fácil, accesible y estar disponible. Deberán estar informados de no tomar acciones ante debilidades de seguridad sospechosas, pues podría causar daños al sistema o servicio, y resultar siendo el causante de un incidente peor al inicial. De acuerdo a su gravedad podría terminar con responsabilidades legales.

4.3.9.2 Gestión de los incidentes y mejoras en la seguridad de la información

Responsabilidades y procedimientos

Se deberá realizar el monitoreo de los sistemas, alarmas y vulnerabilidades para detectar incidentes de seguridad de la información, con el fin de garantizar una respuesta rápida, eficaz y sistemática, que permita la normalidad en las funciones de la Alcaldía, mediante el reporte, recolección de evidencias, análisis e identificación de la causa del incidente y aplicación de acciones correctivas.

Se considerarán como incidentes de seguridad de la información, los siguientes:

- Fallas en los sistemas y pérdida del servicio.
- Código malicioso.
- Negación del servicio.
- Violaciones de la confidencialidad e integridad de la información.
- Mal uso de los sistemas.

Aprender de los incidentes en la seguridad de la información

Una vez verificada la incidencia, el Jefe del área de sistemas recolectará la información que le permitirá establecer el alcance del incidente, mediante la determinación de cuales redes, sistemas y aplicaciones fueron afectados, que causas generaron el incidente, como ocurrió o está ocurriendo, que tratamiento se usó, cuales vulnerabilidades fueron explotadas y el impacto negativo que pueda tener sobre la Alcaldía.

Para determinar el alcance, el Jefe de Sistema de Información, telecomunicaciones y tecnología puede hacerse las siguientes preguntas:

- ¿Qué activos que están en riesgo?
- ¿Qué impacto genera en las actividades de la Alcaldía que el equipo se encuentre comprometido en un incidente de seguridad?
- ¿Cuántos equipos fueron comprometidos?
- ¿Cuántas redes se vieron envueltas?
- ¿Hasta qué punto de la red logró penetrar el atacante?

- ¿Qué nivel de privilegio logró el atacante?
- ¿Se encuentran en riesgo aplicaciones críticas?
- ¿Cuál es el nivel de conocimiento del atacante en cuanto a la vulnerabilidades explotadas?
- ¿Existen otros equipos con la misma vulnerabilidad?

Determinado el alcance del incidente de seguridad, el Jefe del área de sistemas procederá si es el caso a incrementar o establecer controles adicionales para limitar la frecuencia, daño y costo de ocurrencias futuras, para poner en marcha las operaciones afectadas por el incidente, aplicando acciones de: contención (evita que el incidente siga produciendo daños), erradicación (elimina la causa del incidente y todo rastro de los daños) y recuperación (retorna el entorno afectado a su estado original), contando con estrategias que permitan realizar las operaciones de manera organizada, rápida y efectiva, teniendo en cuenta: el daño potencial de los activos a causa del incidente, necesidad de preservación de la evidencia, tiempo y recursos necesarios para poner en práctica la estrategia, efectividad de la estrategia (total o parcial), duración de las medidas a tomar, criticidad de los sistemas afectados, características de los posibles atacantes, si el incidente es de conocimiento público, pérdida económica, posibles implicancias legales, relación costo-beneficio de la estrategia y experiencias anteriores.

Recolección de evidencia

Una vez neutralizada la incidencia, el Jefe del área de sistemas deberá investigar las causas (contenidas en la bitácora de incidencias) que generaron dicho incidente. Corroborando que las evidencias sean válidas y que en el reporte se detallen la situación, al igual que las acciones realizadas por cada uno de los implicados, analistas y evaluadores del incidente.

Cuando ocurre una acción de seguimiento contra una persona después de un incidente en la seguridad de la información donde se involucra una acción legal (ya sea civil o criminal). Se deberá recolectar, mantener y presentar las evidencias del caso, para investigaciones más a fondo por las entidades competentes, quienes determinarán las acciones a tomar al igual que la administración de la Alcaldía.

4.3.10 Histórico de Revisiones, Actualizaciones y Aprobaciones.

Cada año la Política de Seguridad debe ser revisada y retroalimentada en los aspectos que sean necesarios mínimo cada año, y los cambios serán documentados en un Registro de Cambios de la Política de Seguridad Informática, se harán las modificaciones respectivas en el documento y posteriormente, se promulgará mediante Resolución.

El Comité de Seguridad de la Información divulgará la Política de Seguridad Informática a todos los estamentos de la comunidad universitaria.

CONCLUSIONES

Se realizó el reconocimiento de la Alcaldía Municipal de Río de Oro (Cesar), identificando la cadena de valor de sus secretarias (Hacienda, Gobierno, Planeación y Salud), modelando sus procesos a través del BMM (Business Motivation Model), creando su estructura orgánica e identificando la Tecnología de Información (TI) presente en ella.

Tomando como marcos de referencia, normas o buenas prácticas, se identificaron COBIT 4.1, ITIL v3 y ISO/IEC 27002, mostrando un cuadro comparativo entre las mismas y de acuerdo a la necesidad encontrada en la Alcaldía en cuanto a la carencia de una política de seguridad de la información, se tomó como base la norma ISO/IEC 27002, debido a que proporciona un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña y constituye un beneficio clave del aprovechamiento de un método de seguridad basado en entornos y ayuda a cumplir diferentes requerimientos de manera eficaz, repetible y escalable, en la Alcaldía del Municipio de Río de Oro, Cesar.

Seguido de la selección de la norma NTC-ISO/IEC 27002, se desarrollaron nueve dominios de la Norma (Política de Seguridad de la Información, Organización de la Seguridad de la Información, Gestión de Activos, Seguridad de los Recursos Humanos, Seguridad Física y Ambiental, Gestión de Comunicaciones y Operaciones, Control de Accesos, Adquisición-Desarrollo y Mantenimiento de Sistemas de Información y Gestión de Incidentes de la Seguridad de la Información), los cuales especifican los controles que se deberán aplicar para reducir los riesgos en materia de seguridad de la información en la Alcaldía. Para el desarrollo de la propuesta se despreciaron los dos últimos dominios de la norma: Gestión de la Continuidad del Negocio y Cumplimiento, debido a que algunas actividades diseñadas para garantizar dicha continuidad han sido contempladas en el desarrollo del presente trabajo, por su parte las estrategias serán definidas en una etapa posterior, una vez se inicie la implementación prioritaria en las diferentes áreas de la Alcaldía Municipal de Rio de Oro, de acuerdo al diagnóstico arrojado en la etapa de recolección e información, lo que así mismo justifica el desprecio del dominio de cumplimiento basado en la obligatoria aplicación de los parámetros establecidos en los dominios anteriores.

Tomando como base los resultados obtenidos de la investigación, tras la aplicación de las encuestas anteriormente definidas, se redactó un artículo donde se expuso la respectiva tabulación, enfocándose a la situación actual de la Alcaldía en cuanto a la seguridad de la información que allí se maneja. Reflejando la necesidad de aplicar políticas de seguridad de la información en todas sus secretarias, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

RECOMENDACIONES

Presentar a la administración municipal encabezada por el alcalde, esta propuesta de Políticas de Seguridad de la Información para la Alcaldía Municipal de Río de Oro (Cesar), basada en la norma ISO/IEC 27002, para su respectiva aprobación e implementación.

Crear un acuerdo de confidencialidad de la información confidencial y privada, para los empleados de la Alcaldía, que les informe de sus responsabilidades y posibles sanciones, en caso de una violación a la seguridad de la información a su cargo. Esto con el objetivo de asegurar que los empleados, proveedores y contratitas entiendan sus responsabilidades, y sean idóneos para los roles en los que fueron contratados, reduciendo el riesgo de robo, fraude y mal uso de los medios. Es necesario definir claramente los roles y responsabilidades de cada empleado en materia de seguridad de la información. Todo esto no debe ser simplemente mediante acuerdos verbales, sino que se debe plasmar en el contrato de trabajo. También deben existir capacitaciones periódicas para concientizar y proporcionar formación y procesos disciplinarios relacionados a la seguridad y responsabilidad de los recursos humanos en este ámbito.

Se debe tener en cuenta mantener los contactos apropiados con las autoridades relevantes, como policía y bomberos; para el desarrollo de foros o capacitaciones al personal de la Alcaldía, en materia de seguridad. En caso de presentarse un incidente de seguridad, se deberá llevar a cabo la respectiva investigación con el fin de ajustar aquellos controles de seguridad que están siendo quebrantados.

Se deben asignar responsabilidades por cada uno de los activos de la Alcaldía, así como poseer un inventario actualizado de todos los activos (Hardware y software, bienes muebles e inmuebles, equipo de oficina y comunicaciones, archivos y backup's) con los que se cuenta, y la respectiva clasificación de estos, con fin de medir su nivel de exigencia en materia de resguardo.

Se debe también contar con controles físicos de entrada, tales como puertas de hierro con llave, para las oficinas que se comunican con el parque principal y en especial para la entrada anterior y posterior de la Alcaldía, y barrotes en las ventanas. Además de eso, es necesario considerar la seguridad física con respecto a amenazas externas y de origen ambiental, como incendios (para los cuales debe haber extintores adecuados para uso en salas de cómputo y ubicados en los lugares convenientes), terremotos, inundaciones, atentados terroristas, etc. Deben también haber áreas de acceso público de carga y descarga, parqueos, áreas de visita, entre otros. Las gradas, deben ser seguras y con las medidas respectivas como antideslizantes y barras de apoyo sobre la pared para sujetarse. Se debe contar con rapas para el acceso de personas discapacitadas y en caso de no ser posible se debe optar por reubicar ciertas oficinas donde el acceso al público es más continuo. Se debe incluir dentro de las obras de planeación, los requerimientos de mejoramiento de la infraestructura física de la Alcaldía, en algunas de sus áreas donde se presenta humedad, incluyendo la creación de puestos de trabajo limitados en cubículos, dentro de estas áreas.

En cuanto a la seguridad ambiental, se debe controlar la temperatura adecuada para los equipos, seguridad del cableado, mantenimiento de equipos, etc. La ubicación de los equipos también debe ser adecuada y de tal manera que evite riesgos innecesarios.

Se debe igualmente verificar y controlar el tiempo de vida útil de los equipos para que trabajen en condiciones óptimas.

Es necesario que los procedimientos de operación estén bien documentados, pues no basta con tener las ideas en la mente, sino que se deben plasmar en documentos que por supuesto estén autorizados por la administración. Todo con el fin de ser usados por un nuevo personal en caso de que el responsable de las funciones se encuentre indispuesto o haya sido retirado de su cargo por finalización de su contrato o por ser promovido a un nuevo cargo.

Se debe tener cuidado que nadie pueda tener acceso, modificar o utilizar de los activos sin autorización o detección. Para ello debe haber una bitácora de accesos, con las respectivas horas y tiempos de acceso, entre otros.

Se deben también tener controles de detección, prevención y recuperación de la información para protegerla contra códigos maliciosos, mediante el uso de antivirus actualizados y copias de respaldos de la información. De hecho, las copias de respaldo de la información son vitales y deben realizarse con una frecuencia preferiblemente diaria, pues de lo contrario, pueden existir pérdidas de información con gran impacto negativo.

En cuanto a las redes, es necesario asegurar la protección de la información que se transmite y la protección de la infraestructura de soporte. Los servicios de red tienen que ser igualmente seguros, especialmente considerando cómo la tendencia de los últimos años se encamina cada vez más a basar todas las tecnologías de la información a ambientes en red para transmitir y compartir la información efectivamente. Los sistemas tienen que estar muy bien documentados, detalle a detalle, incluyendo por supuesto la arquitectura de red con la que se cuenta.

Además de las medidas directas para proteger el adecuado intercambio de información, se le debe recordar al personal el tomar las precauciones adecuadas, como no revelar información confidencial al realizar una llamada telefónica para evitar ser escuchado o interceptado por personas alrededor suyo, intervención de teléfonos, personas en el otro lado de la línea (del lado del receptor), entre otras.

Igualmente para los mensajes electrónicos se deben tomar medidas adecuadas, para evitar así cualquier tipo de problema que afecte la seguridad de la información, como estar seguro del correo del remitente, para evitar que destinatarios no autorizados la adquieran.

Las fallas deben ser inmediatamente corregidas, pero también registradas y analizadas para que sirvan en la toma de decisiones y para realizar acciones necesarias.

Todo acceso no autorizado debe ser evitado y se deben minimizar al máximo las probabilidades de que eso suceda. Todo esto se controla mediante registro de personal, gestión de privilegios a roles, autenticación mediante usuarios y contraseñas, las cuales deben ser cambiadas con regularidad si el equipo resguarda información de clasificación confidencial o privada.

El personal debe asegurarse de que el equipo desatendido tenga la protección apropiada, como la activación automática de un protector de pantalla después de cierto tiempo de inactividad, el cual permanezca impidiendo el acceso hasta que se introduzca la contraseña correcta, conocida por el funcionario autorizado para utilizar el equipo. Además se debe tener en cuenta, que un equipo desatendido es un área de trabajo desatendida, por lo que se debe mantener una política de escritorios limpios, donde el área de trabajo debe permanecer libre de documentos a los cuales una persona no autorizada podría tener acceso.

Son necesarios controles de acceso a la red, al sistema operativo, a las aplicaciones y a la información. Para todo esto deben existir registros y bitácoras de acceso.

BIBLIOGRAFÍA

ALCALDIA MAYOR DE BOGOTA D.C. Direccionamiento Estratégico. Gestión Estratégica y Planes Institucionales. Bogotá. Colombia. 2013. 7h. [en línea]. http://www.patrimoniocultural.gov.co/descargas/nosotros/mapa-de-procesos/DE-P01%20GESTION%20ESTRATEGICA%20Y%20PLANES%20INST.pdf

ALCALDÍA MUNICIPAL DE BUCARAMANGA. Política de Seguridad de la Información para la Alcaldía de Bucaramanga. Bucaramanga. Colombia. 2012. 3h. [en línea]. http://www.bucaramanga.gov.co/documents/Politica_de_Seguridad_de_la_Informacion.pdf

ALCALDÍA MUNICIPAL DE DURANIA. Política de Actualización de Contenidos del Portal Web www.durania-nortedesantander.gov.co, como una iniciativa por parte de la Estrategia de Gobierno en Línea. Durania, Durania. Colombia. 2009. 18h. [en línea]. http://durania-nortedesantander.gov.co/apc-aa-files/33666536313963356239323539346563/Politica_Editorial_Sitio_Web.pdf

ALCALDÍA MUNICIPAL DE FLORIDABLANCA. Políticas de Seguridad de la Información para la Alcaldía de Floridablanca. Floridablanca. Colombia. 2013. 3h. [en línea]. http://floridablanca.gov.co/wp-content/uploads/2013/06/POLITICA-DE-LA-SEGURIDAD-DE-LA-INFORMACION-1.pdf

ALCALDÍA MUNICIPAL DE MUTISCUA. Políticas de Seguridad de la Información para el Sitio Web de la Alcaldía Municipal de Mutiscua, Mutiscua. Colombia. 2009. 6h. [en línea]. http://mutiscua-nortedesantander.gov.co/apc-aa-files/63366536346631323039323934613532/DECRETO_N__28_DE_09_NOVIEMBRE_DE_2009.pdf

ALCALDÍA MUNICIPAL DE OCAÑA. Plan de Acción Municipio de Ocaña. Ocaña. Colombia. 2010. 17h. [en línea]. http://ocana-nortedesantander.gov.co/apc-aa-files/61643230666336653165633566373234/Plan_de_Accion_GEL___si_Oca_a__.pdf

ALCALDÍA MUNICIPAL DE SOTAQUIRÁ. Modelo Política de Seguridad de la Información del Municipio de Sotaquirá. Sotaquirá, Colombia. 2009. 3h. [en línea]. http://sotaquira-boyaca.gov.co/apc-aa-files/32383063636332366139383566353635/politica-de-seguridad-de-la-informacin-sotaquir.pdf

ERB, Markus. Gestión de Riesgo en la Seguridad Informática. Amenazas y Vulnerabilidades. España. 3h. [en línea]. http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

GOVERNANCE INSTITUTE, OFICINA GUBERNAMENTAL DE COMERCIO y THE STATIONERY OFFICE. Alineando COBIT 4.1, ITIL V3 e, ISO/IEC 27002 en beneficio del negocio. Estados Unidos e Inglaterra. 2010. 130h. [en línea]. http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf.

MINISTERIO DE LA INFORMATICA Y LAS COMUNICACIONES. Reglamento sobre Seguridad Informática. La Habana. Cuba. 2012. 15h. [en línea]. http://fcmfajardo.sld.cu/seguridad_informatica/resol_y_dispos_del_mic/reglamento_seguridad_informatica.pdf

MINISTERIO DEL INTERIOR Y DE JUSTICIA DE COLOMBIA. Dirección Nacional del Derecho de Autor. Unidad Administrativa Especial. [en línea]. http://www.propiedadintelectualcolombia.com/Site/LinkClick.aspx?fileticket=yDsveWsCdGE%3D&tabid=

PACHECO SOLANO, Andrés Alfonso y TORO RUEDA, Mileidy. Políticas de Seguridad de la Información para la Unidad de Almacén de la Universidad Francisco de Paula Santander Ocaña. Ocaña, Colombia. 2013. 232h. Trabajo de grado (Profesional en Ingeniería de Sistemas). Universidad Francisco de Paula Santander Ocaña. Facultad de Ingenierías.

PRESIDENCIA DEL CONSEJO DE MINISTROS DE PERU. Políticas de Seguridad Informática a través de la Oficina de Gobierno Electrónico e Informático. Lima. Perú. 2013. 15h. [en línea]. http://www.enterese.net/entidades-del-estado-se-modernizan-con-politicas-de-seguridad-informatica/

SUPERINTENDENCIAS DE SOCIEDADES. Manual Manejo y Control Administrativo de los Bienes de Propiedad. Bogotá D.C., Colombia, 2009. 29h. [en línea]. http://www.supersociedades.gov.co/web/Ntrabajo/SISTEMA_INTEGRADO/Documentos%20Infraestructura/DOCUMENTOS/GINF-M-001%20MANUAL%20ADMINISTRATIVO.pdf

FRANCISCO DE PAULA SANTANDER OCAÑA. Modulo Evaluación de la Seguridad de la Información. Ocaña. Colombia. 2012. 65h.

UNIVERSIDAD LIBRE. Acuerdo No. 05 (Noviembre 17 de 2009). Colombia. 2009. 85h. [en línea]. http://www.unilibre.edu.co/images/pdf/acd_05-09.pdf

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Gerencia de Innovación y Desarrollo Tecnológico. Última actualización el Lunes, 22 de Abril de 2013 09:05. [en línea]. http://www.unad.edu.co/gidt/index.php/leyesinformaticas

ANEXOS

ANEXO A: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA ENCUESTA DE SEGURIDAD DE LA INFORMACION DIRIGIDA A LA SECRETARIA DEL ALCALDE DEL MUNICIPIO DE RIO DE ORO (CESAR)

Objetivo: Conocer la existencia de políticas de seguridad en la Alcaldía de Río de Oro.

Funcionario: *Nerys Amparo Martínez Mier* **Dependencia:** *Despacho Municipal*

(*Marque con una X su repuesta*)

1. La Alcaldía de Rio de Oro, cuenta con:

Planes de Contingencia, ante cualquier tipo de eventualidad natural (sismos, inundaciones, incendios)	Sí __ No X
Planes de Contingencia, ante cualquier tipo de eventualidad criminal (vandalismo, robo, sabotaje)	Sí __ No X
Políticas de privacidad y confidencialidad de la información por parte de cada uno de sus empleados	Sí __ No X
Inventario de Hardware y Software	Sí __ No X
Inventario de Bienes Muebles e Inmuebles	Sí X No__
Inventario de Activos (Decretos, Contratos, Resoluciones e Informes)	Sí __ No X
Control de Acceso a sus instalaciones del personal, visitantes y demás	Sí __ No X
La respectiva identificación de sus Áreas	Sí __ No__ Algunas X
Manual de funciones y competencias del personal de planta	Sí X No__
Manual de funciones y competencias del personal contratado	Sí X No__
Filosofía institucional (Misión, Visión, Objetivos, funciones, etc.)	Sí X No__
Manual de procedimientos a usuarios	Sí __ No__ Algunos X
Planes de mantenimiento de equipos	Sí __ No X
Vigilancia en sus instalaciones (vigilante, cámaras de seguridad) todo el tiempo	Sí __ No X
Planes de copias de respaldo de la información	Sí __ No X

Sistemas de refrigeración para los equipos de computo Sí __ No X

2. En su estructura orgánica, ¿cuenta con personal encargado del área de sistemas (mantenimiento de equipos)? Sí __ No X

GRACIAS POR SU COLABORACIÓN

ANEXO B: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
ENCUESTA DE SEGURIDAD DE LA INFORMACION DIRIGIDA AL PERSONAL DE LAS DIFERENTES ÁREAS DE LA ALCALDÍA DEL MUNICIPIO DE RÍO DE ORO, CESAR

Objetivo: Conocer la existencia de políticas de seguridad en la Alcaldía de Río de Oro.

Funcionario: _____ Dependencia: _____

(*Marque con una X su repuesta*)

1. ¿Cuentan con un acuerdo de confidencialidad de la información? Sí__ No__

2. ¿Tiene usted conocimiento de sus responsabilidades y sanciones, frente a la seguridad de la información? Sí __ No__

Si su respuesta es negativa, continuar con la pregunta Nº 4.

3. Estas sanciones se encuentra estipuladas en:
- ☐ Decretos o resoluciones institucionales
- ☐ Decretos de ley de la nación

Otros _____

4. ¿El área en la cual labora, se encuentra debidamente identificada? Sí__ No__

5. ¿Su área cuenta con controles de ingreso del personal? Sí__ No__

6. ¿Se controla el trabajo, fuera del horario laboral definido? Sí __ No__

7. El área cuenta con:

Vigilancia	Sí __ No__
Recepcionista	Sí __ No__
Infraestructura sólida y segura	Sí __ No__
Ruta de Evacuación	Sí __ No__
Cámaras de Vigilancia	Sí __ No__
Detectores de Humo	Sí __ No__
Alarmas	Sí __ No__
Extintores	Sí __ No__
Instalaciones eléctricas ideales	Sí __ No__
UPS (Fuente de Suministro Eléctrico)	Sí __ No__
Aire Acondicionado	Sí __ No__
Prohibición de consumo de alimentos y bebidas	Sí __ No__
Prohibición de Fumar en las instalaciones	Sí __ No__

8. Sabe usted si la Alcaldía cuenta con registros de:

Acceso al Personal	Sí __ No__
Acceso a Visitantes	Sí __ No__
Uso de los Sistemas	Sí __ No__
Uso de Documentos Institucionales	Sí __ No__
Servicios de Red	Sí __ No__

9. El equipo de cómputo a su disposición, cuenta con:

Contraseña, para permitir el acceso a los sistemas	Sí__ No__
Antivirus, actualizado	Sí__ No__
Software, con licencia	Sí __ No__ Algunos__
Restricción de accesos a páginas web (redes sociales, etc.)	Sí __ No__ Algunos__
Acceso restringido a aplicaciones, luego de varios intentos	Sí __ No__ Algunos__
Requerimientos necesarios para la realización de sus labores	Sí __ No__ Algunos__
Conexión de polo a tierra	Sí __ No__

10. El equipo de cómputo que actualmente está a su disposición, ¿Es utilizado por otro funcionario? Sí__ No__

11. ¿Cuenta con manuales de procedimientos para la operación de cada uno de los sistemas de cómputo del área? Sí __ No__ Algunos__

12. ¿Con que frecuencia el equipo de cómputo a su disposición recibe mantenimiento?

- ☐ Mensualmente
- ☐ Trimestralmente
- ☐ Semestralmente
- ☐ Anualmente
- ☐ Cuando lo requiere

13. Su escritorio personal, Permanece libre de:

Archivos o documentos institucionales	Sí __ No__
Alimentos	Sí __ No__
Polvo	Sí __ No__

14. ¿Realiza backup's (Copias de Seguridad de la Información) de la información a su disposición? Sí __ No__

Si su respuesta es negativa, continuar con la pregunta Nº 22.

15. ¿En qué medio almacena esta información?

- ☐ CD
- ☐ DVD
- ☐ Memorias USB
- ☐ Impresiones

☐ Disco Duro
Otras _____

16. ¿Con que periodicidad se realizan?
☐ Diariamente
☐ Semanalmente
☐ Mensualmente
☐ Bimestralmente
☐ Anualmente
Otras _____

17. Las copias de respaldo de la información es almacenada en:
☐ Caja Fuerte o Bóveda
☐ Estantes o Gavetas
☐ Muebles con cerradura o Archivador
☐ Fuera de la Alcaldía (para prevenir pérdida de datos en el caso de incidencias)
Otras _____

18. ¿El acceso a estas copias de respaldo o documentos institucionales es restringido, según su rol en la institución? Sí __ No__

19. ¿Cómo se permite el acceso a estas?
☐ Mediante solicitud verbal
☐ Mediante solicitud escrita
Otras _____

20. ¿El acceso a estas copias de respaldo o documentos institucionales es restringido, a usuarios externos a la institución? Sí __ No__

Sí su respuesta es positiva, continuar con la pregunta 22.

21. ¿Cómo se permite el acceso a estas?
☐ Mediante solicitud verbal
☐ Mediante solicitud escrita
Otras _____

22. ¿Cuenta con mensajería electrónica interna para sus labores diarias? Sí __ No__

Si su respuesta es negativa, continuar con la pregunta Nº 24.

23. ¿Este tipo de mensajería se podría considerar segura? Sí __ No__

24. ¿Cuentan con programas para la encriptación (camuflar información a destinatarios no deseados) de datos? Sí __ No__

25. ¿La Alcaldía cuenta con un procedimiento formal para reportes de incidentes (robos de información, pérdida de datos, accesos no permitidos, etc.)? Sí __ No__

26. ¿Al presentarse un incidente de seguridad en la Alcaldía, se cuenta con un plan de contingencia? Sí __ No__

27. ¿Se investiga y recolectan evidencias sobre el incidente de seguridad de la información? Sí __ No__

28. ¿Acostumbra utilizar programas de descarga de archivos de usuario (música, películas, programas...)? Sí __ No__

GRACIAS POR SU COLABORACIÓN

ANEXO C: CÓDIGO DE ÉTICA DE LA ALCALDÍA DEL MUNICIPIO DE RÍO DE ORO, CESAR

CODIGO DE ETICA

INTRODUCCIÓN

El código de Ética es la concreción de los principios y valores de la Entidad y sus funcionarios en el diario quehacer. Compila la reflexión, la experiencia y la práctica de una organización en la que el tema de la ética pública ha sido una preocupación constante.

El objeto del presente Código es servir de guía ética, para que los trabajadores de la administración Municipal de Río de Oro actuemos con propiedad en el desempeño de nuestras funciones.

Pretende éste Código de Ética promover un activo compromiso con la puesta en práctica de los principios y valores, en procura del cumplimiento de nuestra misión constitucional, propendiendo por el buen uso de los recursos, y alcanzar la visión de ser la mejor Administración Municipal, con la utilización de nuestros talentos y sistemas de información y modelos estratégicos y participación para afianzar la credibilidad de la comunidad y facilitar el control político.

Todo ello dentro del contexto de la responsabilidad social que nos es exigible, misma que en los últimos años ha adquirido una nueva dimensión, y que obliga a cumplir de manera excelente los cometidos para continuar siendo una organización comprometida y asegurar la supervivencia, en la cual la ética ha de impregnar todas nuestras funciones, las decisiones de los directivos y formar parte consustancial de la cultura de la Entidad.

Debe este Código ser una guía de actuación por excelencia para nuestra Entidad y servidores públicos. Para los clientes constituye el marco ético de su relación con nosotros. Para la comunidad debe ser la norma contra la cual evalúe nuestro comportamiento en el ejercicio de la función pública.

De ahí que corresponde a cada uno de nosotros conocerlo, interiorizarlo, divulgarlo y observarlo, para alcanzar el propósito de desarrollar y perpetuar una organización orientada al servicio, inspirada en la calidad y proyectada con gran responsabilidad hacia la comunidad.

ÁMBITO DE LA APLICACIÓN

Este Código de Ética tiene por objeto ser el referente que oriente la gestión pública de los servidores públicos de la Administración Municipal de Río de Oro. En consecuencia, nuestros servidores públicos aplicarán en todas sus actuaciones y decisiones lo establecido en este documento.

Todos los servidores públicos de la Entidad, sin perjuicio de las normas consagradas en el ámbito jurídico, asumirán y cumplirán de manera consciente y responsable, los principios, valores y directrices éticas establecidas a continuación.

PRINCIPIOS ÉTICOS

Los principios éticos son las normas internas y creencias básicas sobre las formas correctas como debemos relacionarnos con los otros y con el mundo, desde las cuales se rige el sistema de valores que profesan las personas y los grupos.

- La generación de confianza de la ciudadanía frente al Estado, es el propósito fundamental del servidor público.
- El interés general prevalece sobre el particular.
- El buen uso y administración de los recursos públicos garantizan la calidad de vida de la comunidad.
- Es imperativo ético del servidor público rendir cuentas a la ciudadanía sobre la utilización de los recursos públicos encomendados y los resultados de su gestión.
- En la Democracia Participativa, el Control Social es complemento fundamental en la vigilancia de la gestión fiscal.
- La sostenibilidad ambiental es uno de los criterios orientadores del gato público.
- Los bienes públicos están destinados exclusivamente al servicio de la comunidad.

VALORES ÉTICOS

Por Valores se entiende aquellas formas de ser y de actuar de las personas que son altamente deseables como atributos o cualidades nuestras y de los demás, por cuanto posibilitan la construcción de una convivencia gratificante en el marco de la dignidad humana.

Respeto	**Lealtad**
Justicia	**Servicio**
Responsabilidad	**Participación**
Transparencia	**Eficiencia**

RESPETO. Consideración y reconocimiento del derecho de los demás a ser, sentir, pensar y actuar diferente.

El respeto en la Administración Municipal de Río de Oro está presente en el reconocimiento de los derechos de la comunidad, de sus funcionarios y de sus clientes.

JUSTICIA. Dar a cada cual lo suyo. La Administración Municipal de Río de Oro obra con imparcialidad y equidad en el ejercicio de sus funciones constitucionales y legales.

Los servidores públicos desarrollamos nuestras actuaciones dentro de la legalidad y la rectitud dando a todos un trato igualitario.

RESPONSABILIDAD. Capacidad para asumir las obligaciones contraídas y las consecuencias de nuestros actos.

La Administración Municipal de Río de Oro responde ante la comunidad por lo que hace, cómo lo hace y lo que deja de hacer.

Los servidores públicos asumimos los deberes que impone el servicio público, nos hacemos cargo de las consecuencias de nuestras acciones para el logro de la misión de la entidad, y somos cuidadosos en el uso de la información y de los recursos asignados.

TRANSPARENCIA. Es actuar con claridad haciendo evidentes las decisiones y acciones.

La Administración Municipal de Río de Oro es una Entidad transparente que da cuenta a la comunidad de su gestión y está abierta al ejercicio del control social.

Los Servidores Públicos producimos y entregamos información veraz y oportuna para la entidad y nuestros clientes.

LEALTAD. Fidelidad en el trato y el desempeño, la Administración Municipal de Río de Oro es fiel a los compromisos que se derivan de sus funciones y sus propósitos constitucionales y legales.

Los servidores públicos somos fieles a la misión de nuestra entidad y al servicio público.

SERVICIO. Disposición permanente para el cumplimiento de una función, atendiendo las necesidades de los clientes.

En la Administración Municipal de Río de Oro el servicio se refleja en la permanente disposición para satisfacer las demandas y necesidades de nuestros clientes.

Los servidores públicos atendemos cálida, oportuna y eficientemente a nuestros clientes.

PARTICIPACIÓN. Compartir, abrir espacios para que otros hagan parte de una actividad o movilizarse para intervenir en ella.

La Administración Municipal de Río de Oro facilita y promueve la intervención de la comunidad en el ejercicio del control social.

Los servidores públicos estamos dispuestos a emprender actividades y generar espacios que conduzcan al mejoramiento de nuestra entidad y somos proactivos en el cumplimiento de nuestras funciones.

EFICIENCIA. Optimización de los recursos y talentos para maximizar nuestros resultados.

La Administración Municipal de Río de Oro utiliza de manera óptima sus recursos para el cumplimiento de su misión.

Los servidores públicos optimizamos nuestros talentos y recursos para el logro de la misión de la Entidad.

DIRECTRICES ÉTICAS

Las Directrices son orientaciones acerca de cómo debe relacionarse la entidad y los servidores públicos con un sistema o grupo de interés específico para la puesta en práctica del respectivo valor al que hace referencia la directriz.

CON LOS SERVIDORES PÚBLICOS. La Administración Municipal de Río de Oro reconoce los derechos y particularidades de sus servidores e identifica sus capacidades, habilidades y competencias para aplicarlos en el desarrollo de sus labores, asegurando el cumplimiento de la misión institucional.

Igualmente reconoce los logros personales y laborales de sus servidores y aplica criterios de igualdad e imparcialidad en la promoción, capacitación y desarrollo del talento humano.

CON OTRAS CORPORACIONES PÚBLICAS. La Administración Municipal de Río de Oro rinde cuenta de su gestión a las Corporaciones Públicas, a través de informes oportunos y veraces que reflejen nuestra situación real, posibilitando el ejercicio del control político.

CON ORGANOS DE CONTROL Y JUDICIALES. La Administración Municipal de Río de Oro interactúa con los órganos de control y los organismos judiciales de manera armónica y diligente, suministrando información oportuna y veraz debidamente soportada, para facilitar el ejercicio de sus respectivas competencias.

CON CONTRATISTAS Y PROVEEDORES. La Administración Municipal de Río de Oro contrata la adquisición de bienes y servicios en el marco del estatuto contractual, mediante la selección objetiva e imparcial, haciendo públicas las razones que motivaron la escogencia del contratista.

CON LA COMUNIDAD EN GENERAL. La Administración Municipal de Río de Oro abre espacios a los ciudadanos y a la comunidad organizada para el ejercicio del control social promoviendo los mecanismos de participación ciudadana, y rinde cuentas de su gestión de manera amplia y detallada.

CON EL MEDIO AMBIENTE. La Administración Municipal de Río de Oro trabaja integralmente con todos los organismos de Control y autoridades ambientales para promover el respeto de las normas ambientales, a través de campañas educativas para la protección y conservación de los recursos naturales.

Al interior de nuestra Entidad propiciamos una cultura ecológica, desarrollando acciones para el manejo y disposición adecuada de residuos sólidos.

CON LOS MEDIOS DE COMUNICACIÓN. La Administración Municipal de Río de Oro se relaciona con los medios de comunicación sin discriminaciones de ninguna índole y entrega de información clara, veraz y oportuna sobre los resultados de su gestión.

La formulación del Código de Ética de la Administración Municipal de Río de Oro fue posible gracias al compromiso decidido de todos los servidores públicos, quienes con su espíritu participativo y proactivo establecieron los criterios básicos para normar el comportamiento ético de todas las personas que laboran en la Entidad.

ANEXO D: MANUAL DE FUNCIONES Y DE COMPETENCIAS DE LOS CARGOS DE LA PLANTA DE PERSONAL DE LA ALCALDÍA DEL MUNICIPIO DE RÍO DE ORO, CESAR

DECRETO No. – 045A

(Octubre 12 de 2005)

POR MEDIO DEL CUAL SE ADOPTA EL MANUAL DE FUNCIONES Y DE COMPETENCIAS DE LOS CARGOS DE LA PLANTA DE PERSONAL DE LA ALCALDÍA DEL MUNICIPIO DE RÍO DE ORO, CESAR.

El Alcalde Municipal de Río de Oro, Cesar, en ejercicio de las facultades que le confiere el numeral 7 del artículo 315 de la Constitución política, el numeral 4 literal D, del artículo 91 de la ley 136 de 1994 y los artículo 13 y 28 del decreto ley 775 de 2005.

CONSIDERANDO:

Qué, mediante el decreto 735 de marzo 17 de 2005, el Departamento administrativo de la Función Pública estableció el sistema de nomenclatura, clasificación, funciones y requisitos generales para los empleos de las entidades territoriales, e igualmente en el artículo 33 estableció un plazo de 12 meses para que las autoridades territoriales realicen los ajustes pertinentes.

Que, es deber del Alcalde Municipal dar cabal cumplimiento o adecuarse a los parámetros del decreto prenombrado.

En mérito de lo expuesto,

DECRETA:

ARTÍCULO 1. Adóptese como Manual especifico de funciones y de competencias laborales, para los cargos que conforman la planta de personal de la Alcaldía Municipal de Río de Oro, Cesar, fijada por el decreto No. 031 de junio 20 de 2005, cuyas funciones deberán ser cumplidas por los funcionarios con criterios de eficiencia y eficacia, para así lograr la misión, objetivos, y funciones que la ley y los reglamentos señalan a la Alcaldía Municipal de Río de Oro, Cesar, así:

DESPACHO DEL ALCALDE

ALCALDE MUNCIPAL

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	ALCALDE
CÓDIGO:	005
GRADO:	02
No. De Cargos:	1
DEPENDENCÍA:	DESPACHO ALCALDE

II. PROPÓSITO GENERAL

Dirigir, coordinar, programar y controlar la prestación de los servicios públicos, la construcción de obras, el mejoramiento socio cultural de la comunidad, y las demás funciones delegadas de acuerdos con los planes, políticas y programas adoptados de conformidad con las leyes, las ordenanzas y los acuerdos.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Dirigir y coordinar los servicios a cargo del Municipio y vigilar el cumplimiento de los planes, políticas y programas.

2. Dirigir y coordinar el desarrollo municipal, urbano, rural, económico y social de acuerdo con los planes generales de desarrollo del nivel nacional, departamental y local.

3. Dirigir y coordinar el desarrollo y el mejoramiento socio cultural de la comunidad de Río de Oro.

4. Coordinar, dirigir y cumplir las funciones delegadas que le sean otorgadas por ley y decretos nacionales.

5. Dirigir y coordinar los programas y políticas a cargo de la secretaria del despacho a su cargo.

6. Dirigir y coordinar la gestión municipal.

7. Las demás funciones que conforme a la Constitución Política, la ley, los decretos, ordenanzas y acuerdos le asignen.

IV. CONTRIBUCIONES INDIVIDUALES

1. Plantear, organizar, dirigir, coordinar, controlar y supervisar los recursos humanos, financieros y materiales del municipio, buscando cumplir con unos objetivos previamente establecidos.

2. Dictar los actos necesarios para el cabal funcionamiento de la administración Municipal.

3. Presentar al concejo los proyectos de acuerdos que juzguen conveniente para la buena marcha del Municipio.

4. Dictar las medidas para la preservación del orden público conforme a los lineamientos del orden nacional.

5. Coordinar y supervisar los servicios que presten en el Municipio las entidades nacionales o departamentales.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Legislación Municipal.

2. Gerencia Municipal.

3. Participación Comunitaria.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

Los de ley.

2. SECRETARIO DE DESPACHO

SECRETARÍA DE GOBIERNO

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	SECRETARIO DE DESPACHO
CÓDIGO:	020
GRADO:	01
No. De Cargos:	1
DEPENDENCÍA:	SECRETARÍA DE GOBIERNO
CARGO DE JEFE INMEDIATO	ALCALDE

II. PROPÓSITO GENERAL

Cooperar con las autoridades competentes para prevenir conjurar calamidades públicas a fin de dar protección a la vida, honrar y bienes de la comunidad.

Integrar activamente a la comunidad en el proceso general de desarrollo del municipio.

Desarrollar programas de asistencia y protección a la población vulnerable del Municipio.

Promover y organizar la participación comunitaria para el desarrollo social.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Ejercer las funciones que sean de su competencia y vigilar en cumplimiento de las atribuciones asignadas por la ley, las normas y las normas y la autoridad competente.

2. Coordinar, administrar y supervisar los programas y acciones del gobierno en materia de policía, orden público, desarrollo y bienestar de la comunidad.

3. Asesorar al Alcalde en la elaboración y adopción de planes y programas de seguridad ciudadana, culturales, educativos, recreacionales y de desarrollo y bienestar comunitarios, en coordinación con la oficina de Planeación Municipal.

4. La demás funciones que le sean asignadas por la autoridad competente y que estén acorde con la naturaleza del despacho.

IV. CONTRIBUCIONES INDIVIDUALES

1. Promover y organizar la participación comunitaria.

2. Coordinar oportunamente las actividades institucionales relativas al mantenimiento de orden público.

3. Interactuar con la comunidad para adoptar políticas que generen convivencia ciudadana.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Legislación Municipal.

2. Participación Comunitaria.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Título de tecnólogo o de Profesional en Administración Pública, Derechos, Economía, Comunicador Social, o en áreas administrativas y financieras.

EXPERIENCIA: Seis (6) meses de experiencia profesional relacionada.

SECRETARÍA DE PLANEACIÓN

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	SECRETARIO DE DESPACHO
CÓDIGO:	020
GRADO:	01
No. De Cargos:	1
DEPENDENCÍA:	SECRETARÍA DE PLANEACIÓN
CARGO DE JEFE INMEDIATO	ALCALDE

II. PROPÓSITO GENERAL

Realizar estudios necesarios para la elaboración de planes, programas y proyectos específicos de desarrollo.

Producir referencias de conveniencia técnica y económica de proyectos para el municipio.

Preparar y proponer sistemas sobre organización y métodos para mejorar y hacer más eficiente el funcionamiento de la gestión administrativa.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Ejercer bajo su propia responsabilidad las funciones que competen a la oficina de planeación municipal y vigilar el cumplimiento de las atribuciones, asignar a los funcionarios de sus dependencias.

2. Asesorar al Alcalde Municipal en la elaboración y adopción de los planes de desarrollo urbano, económico y social, los programas de inversiones públicas municipal y asesorar a los Secretarios en la elaboración de los proyectos respectivos.

3. Preparar, con la colaboración de la Secretaría de Hacienda Municipal, los programas de inversiones públicas, con sujeción a las prioridades identificadas en el plan, definiendo los recursos financieros y las entidades que participen en la ejecución.

4. Adelantar estudios o evaluar estudios específicos de factibilidad técnica, urbana, cultural de servicios públicos. Obras públicas, tendientes a promover el desarrollo municipal.

5. Velar por el mantenimiento, la interventoría y el seguimiento de las obras públicas que se adelanten en el Municipio.

6. Elaborar los prepliegos, pliegos de condiciones, los estudios y cuadros comparativos necesarios para adelantar los procesos de contratación municipal.

7. Inspeccionar y regular el desarrollo urbanístico del municipio, mediante la aplicación de las normas establecidas en la ley o en el EOT y los acuerdos municipales.

8. Definir, diseñar y asesorar los procedimientos relacionados con prevención y atención de emergencias y desastres en el municipio, mediante la participación activa de la comunidad y el compromiso interinstitucional.

9. Coordinar y administrar el SISBEN y su base de datos, así como el programa de sistemas de selección de beneficiarios APRA programas sociales SISBEN del municipio de Río de Oro.

10. Las demás funciones que le sean asignadas por la autoridad competente y que estén acorde con la naturaleza del despacho.

VI. CONTRIBUCIONES INDIVIDUALES

1. Realizar estudios técnicos para evaluar y proponer ajustes o modificaciones a los planes generales y sectoriales de desarrollo del municipio.

2. Aplicar medidas que contribuyan al mantenimiento del orden físico del municipio.

3. Preparar los planes de desarrollo de orden municipal bajo los criterios que determine el Alcalde Municipal y en coordinación con la Secretaría de Despacho.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Legislación Municipal.

2. Legislación específica que tenga que ver con proyectos para causar inversión.

3. Legislación sobre urbanismo, planeación y presupuesto.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Título de tecnólogo o de Profesional en: Obras civiles, Ingeniería civil, arquitectura.

EXPERIENCIA: Seis (6) meses de experiencia profesional relacionada.

SECRETARÍA DE HACIENDA

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	SECRETARIO DE DESPACHO
CÓDIGO:	020
GRADO:	01
No. De Cargos:	1
DEPENDENCÍA:	SECRETARÍA DE HACIENDA
CARGO DE JEFE INMEDIATO	ALCALDE

II. PROPÓSITO GENERAL

Asesorar al Alcalde en la formulación de la política financiera del municipio y ejecutarla.

Programar las actividades tendientes a prevenir el fraude de las rentas y el no pago de las mismas.

Administrar la política de la hacienda política municipal.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Asesorar al Alcalde en la política y la gestión fiscal del municipio de conformidad con la ley.

2. Elaborar el proyecto de presupuesto general del municipio en coordinación con la oficina de Planeación Municipal.

3. Elaborar el proyecto de decreto de liquidación, del presupuesto aprobado para la vigencia siguiente, para la firma del Alcalde.

4. Adoptar las políticas necesarias para la prevención y represión del fraude, evasión y alusión a las rentas municipales de conformidad con la ley.

5. Aprobar el plan general en materia de gestión tributaria del municipio.

6. Evaluar la realidad socioeconómica del municipio, el comportamiento de los ingresos y su ejecución, para diseñar y proponer el plan financiero que deba adoptar la Administración Municipal.

7. Coordinar la política financiera del municipio de acuerdo con las directrices impartidas por el Alcalde.

8. Coordinar la ejecución de la política financiera decretada a nivel nacional.

9. Evaluar periódicamente el desarrollo de los planes programas y proyectos de su sector y definir los caminos a seguir.

10. Promover la asesoría a la comunidad en la captación, administración y destinación de su recurso financiero.

11. Efectuar análisis y proyecciones de ingresos y egresos, establecer estrategias financieras y elaborar el plan financiero municipal como soporte para la ejecución del plan de desarrollo. Además de ejercerle seguimiento y control administrativo a la ejecución y proponer los ajustes necesarios.

12. Adelantar estudios sobre impuestos, temas, contribuciones y gravámenes a favor del municipio con miras a optimizar los mecanismos de liquidación y recaudo, para garantizar la exacta recaudación de las rentas municipales, de los entes descentralizados y las que serán objeto de transferencia por parte de la Nación.

13. Efectuar estudios para la construcción, administración y control de fondos, cuentas o la constitución de fiducias para administrar recursos con destinación específica o que contribuyan a optimar el manejo de los mismos para el logro de muy precisos fines.

14. Proferir los actos administrativos, requerimientos, pliegos de cargos y actos de trámite relacionados con la actuación fiscalizadora e impositiva de acuerdo con el Estatuto de Rentas del Municipio.

15. Dirigir y controlar las operaciones del presupuesto, tesorería y contabilidad para garantizar que éstas se efectúen con sujeción a los principios de oportunidad, seguridad, rentabilidad y liquidez.

16. Preparar los proyectos de acuerdo, relativos a su sector y los proyectos de decreto que deban dictarse en ejercicio de las actividades propias de la Hacienda Municipal.

17. Recaudar los ingresos por todo concepto, incluyendo las transferencias de los ingresos corrientes de la nación.

18. Efectuar diariamente las consignaciones por el valor de los dineros recaudados en Tesorería.

19. Programar y efectuar el pago de las obligaciones a cargo de la entidad.

20. Programar y efectuar el pago de las obligaciones parafiscales.

21. Elaborar comprobantes de ingreso y egreso cada vez que se haga una operación.

22. Llevar control estricto sobre los movimientos de las cuentas bancarias.

23. Remitir oportunamente los documentos y la información requerida por las diferentes oficinas del área financiera.

24. Preparar y elaborar los informes financieros y contables requeridos por las entidades del orden nacional, departamental y municipal.

25. Coordinar y elaborar el plan anual de caja.

IV. CONOCIMIENTOS BASICOS O ESENCIALES

1. Legislación Municipal.

2. Legislación específica que tenga que ver con tesorería y finanzas públicas.

3. Legislación sobre planeación y presupuesto.

V. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Título de tecnólogo o de Profesional en: Administración Pública o área contable, economía, contaduría, administración de empresas.

EXPERIENCIA: Seis (6) meses de experiencia profesional relacionada.

SECRETARÍA DE SALUD

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	SECRETARIO DE DESPACHO
CÓDIGO:	020
GRADO:	01
No. De Cargos:	1
DEPENDENCÍA:	SECRETARÍA DE SALUD
CARGO DE JEFE INMEDIATO	ALCALDE

II. PROPÓSITO GENERAL

Dirigir, coordinar, controlar y supervisar la prestación del servicio de salud en el municipio a través de programas de prevención en salud y seguridad social.

Contribuir a la formulación de planes, programas y proyectos del sector salud del municipio, en coordinación con las autoridades de salud.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Dirigir el funcionamiento de la Secretaría de Salud Municipal en responsabilidad por el personal, los equipos, la información, las promotoras de salud y proyectos del PAB, en coordinación con la Alcaldía Municipal.

2. Integrar los comités y juntas directivas en pro del desarrollo de programas que beneficien a la comunidad de Río de Oro, Cesar.

3. Representar a la Secretaría de Salud municipal como organismo vocero de la comunidad urbana y rural, promoviendo permanentemente el desarrollo general y el mejoramiento de la calidad de vida de los habitantes del municipio.

4. Organizar capacitaciones, talleres, seminarios y conferencias sobre temas de salud en convenio con instituciones como el Magisterio, Hospital Local y ARS, que sean de interés y beneficio para la comunidad.

5. Rendir informes a la Superintendencia Nacional de Salud y a la Secretaría de Salud Departamental con relación al cumplimiento de programas.

6. Elaborar, ejecutar e implementar programas en salud, por intermedio del plan de atención básica PAB.

7. Vigilar y controlar el desempeño de las ARS promotoras de salud, técnico en saneamiento ambiental y Hospital Local de Río de Oro.

8. Suministrar las herramientas necesarias para que las promotoras de salud puedan desarrollar su trabajo.

9. Las demás que por la naturaleza de sus funciones le sean asignadas por la autoridad competente o por la Ley.

VI. CONTRIBUCIONES INDIVIDUALES

1. Interactuar con la comunidad, para facilitar la llegada de programas o proyectos de salud sin ningún tipo de resistencia.

2. Coordinar con otras dependencias o instituciones públicas o privadas programas de prevención de salud.

3. Garantizar la afiliación de la población a los diferentes regímenes del sistema de seguridad social en salud y vigilar el acceso de ésta a los servicios contemplados en el plan de los servicios de salud POS, de conformidad con los lineamientos establecidos por el Consejo de Seguridad Social en Salud.

4. Coordinar y administrar los programas de salud.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Legislación en salud.

2. Legislación específica que tenga que ver con régimen subsidiado y contributivo.

3. Legislación sobre planeación y proyectos de salud.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Título de tecnólogo o de Profesional en: Carreras de la salud, o en áreas de conocimiento de sistemas coadyuvantes en el cumplimiento de las responsabilidades de salud

EXPERIENCIA: Seis (6) meses de experiencia profesional relacionada.

COMISARÍA DE FAMILIA

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	SECRETARIO DE DESPACHO
CÓDIGO:	020
GRADO:	01
No. De Cargos:	1
DEPENDENCÍA:	COMISARÍA DE FAMILIA
CARGO DE JEFE INMEDIATO	ALCALDE

II. PROPÓSITO GENERAL

Colaborar con el Instituto Colombiano de Bienestar Familiar y las demás autoridades competentes con la misión de proteger a los menores que se hallen en situación irregular y en los casos de conflictos familiares.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Las contempladas en el Decreto 2737 de 1989 y que se discriminan a continuación:

Recibir a prevención denuncias sobre hechos que puedan configurarse como delito o contravención, en los que aparezca involucrado un menor como ofendido o sindicado, tomar las medidas de emergencia correspondientes y darles un trámite correspondiente de acuerdo a las disposiciones del presente código y de los procedimientos penal, Nacional, Departamental, municipal o Distrital y de policía y de las normas pertinentes, el primer día hábil siguiente al recibo de la denuncia.

Aplicar las sanciones policías de acuerdo de acuerdo con las facultades previstas en este código y las que le otorgue el respectivo Concejo Municipal o distrital.

Efectuar las comisiones, peticiones, practica de pruebas y demás actuaciones que le solicite el Instituto de Bienestar Familiar y los funcionarios encargados de la jurisdicción de la familia, en todos los aspectos relacionados con la protección del menor y la familia .

Practicar allanamientos para conjurar las situaciones de peligro en las que pueda encontrarse un menor, cuando la urgencia del caso lo demande, de oficio o a solicitud de un juez o del defensor de la familia, de acuerdo con el procedimiento señalado para ello en esté código.

Recibir a prevención las quejas o informes sobre todos aquellos aspectos relacionados con conflictos familiares, atender las demandas relativas a la protección del menor, especialmente en los casos de maltrato y explotación y atender los casos de violencia familiar, tomando las medidas de urgencia que sean necesarias mientras se remiten a la autoridad competente.

Las demás que le asigne el Concejo Municipal o autoridad competente y que sean compatibles con la naturaleza policiva de sus responsabilidades.

IV. CONTRIBUCIONES INDIVIDUALES

1. Interactuar con la comunidad y de ahí recomendar al alcalde la adopción de políticas favorables para la familia y los menores de edad.

2. Ser vigilante en el cumplimiento de la normatividad vigente del menor.

3. Vincularse a los programas sociales de interés de la familia y el menor.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Legislación de familia y del menor.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Título de Abogado inscrito, con especialización en derecho de familia o de menores o con experiencia no inferior a un año.

COORDINADOR DE GESTIÓN Y BANCO DE PROYECTOS

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	COORDINADOR DE GESTIÓN Y BANCO DE PROYECTOS
CÓDIGO:	303
GRADO:	03
No. De Cargos:	1
DEPENDENCÍA:	SECRETARIA DE PLANEACIÓN MUNICIPAL
CARGO DE JEFE INMEDIATO	ALCALDE

II. PROPÓSITO GENERAL

Apoyar el proceso de planeación y programación de la inversión y evaluación de la gestión pública.

Contribuir a que la asignación de recursos se realice con criterios de eficiencia y rentabilidad social.

Generar todo tipo de información sobre programas y proyectos de cada sector que sirvan de apoyo al municipio en el proceso de gestión, planeación, elaboración del presupuesto y programación de la inversión.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Dar aplicación al funcionamiento al manual operativo del Banco de programas y proyectos del Municipio.

2. Coordinar y dirigir el riesgo de programas y proyectos viables técnica, económica, social y ambientalmente susceptibles de ser financiados con recursos del estado.

3. Registrar la información de los proyectos a lo largo de todo su ciclo de vida, permitiendo hacer seguimiento a la ejecución de la inversión y monitoreo durante la operación.

4. Facilitar información para formular los planes de acción en cada vigencia.

5. Realizar seguimiento y evaluación de los objetivos y metas de planes, programas y proyectos.

6. Y las demás que le asigne el jefe Superior.

IV. CONTRIBUCIONES INDIVIDUALES

1. Hacer que todos los proyectos de inversión, antes de su ejecución estén previamente registrados en el banco de proyectos.

2. Generar insumos necesarios de orden técnico para facilitar la gestión municipal ante otras entidades del orden departamental y nacional.

3. Producir referencia de gestión pública.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Legislación Municipal.

2. Legislación específica que tenga que ver con gestión y proyectos.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Título de tecnólogo o Profesional en: Administración Publica, obras civiles, ingeniería civil, arquitectura o áreas de sistemas.

EXPERIENCIA: Seis (6) meses de experiencia profesional relacionada.

INSPECTOR DE POLICÍA

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	INSPECTOR DE POLICÍA
CÓDIGO:	303
GRADO:	03
No. De Cargos:	1
DEPENDENCÍA:	INSPECCIÓN DE POLICÍA
CARGO DE JEFE INMEDIATO	ALCALDE

II. PROPÓSITO GENERAL

Coadyuvar en el mantenimiento del orden público y en la protección de los derechos e intereses de la comunidad.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Recibir declaraciones extrajuicio.

2. Efectuar lanzamiento por ocupación de hecho.

3. Llevar procesos de policías por perturbación a la posesión, propiedad privada y servidumbres.

4. Atender asuntos de contravenciones, daño en bien ajeno en accidentes de tránsito.

5. Expedir Certificados de supervivencias.

6. Diligenciar las denuncias de conciliación.

7. Ejecutar las cauciones impuestas por conciliación por violación de las mismas.

8. Efectuar las comisiones emanadas de los juzgados.

9. Recibir demandas por contravenciones especiales y delitos y compulsarlas al juzgado en virtud de lo dispuesto en la ley 228, competencia de la justicia ordinaria.

10. Dar aplicación a los artículos en la ley 103, 104 y concordantes de la ley 338 de 1997 y capítulo V del decreto 1052 de 1998.

IV. CONTRIBUCIONES INDIVIDUALES

1. Hacer cumplir el código nacional y el Departamental de policía.

2. Interactuar con la comunidad, para recomendar al Alcalde la adopción de medidas convenientes para la convivencia de la comunidad.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Legislación Municipal (Código nacional de policía y departamental).

2. Legislación específica que tenga que ver con orden policivo.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Tecnólogo en Administración pública, o haber terminado como mínimo cuatro (4) años de educación básica secundaria y curso específico mínimo de sesenta (60) horas relacionado con las funciones del cargo, o abogado.

CORREGIDOR

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	CORREGIDOR
CÓDIGO:	227
GRADO:	01
No. De Cargos:	11
DEPENDENCÍA:	ALCALDÍA MUNICIPAL
CARGO DE JEFE INMEDIATO	ALCALDE

II. PROPÓSITO GENERAL

Administrar el Corregimiento y velar por el buen funcionamiento de los servicios públicos.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Cumplir y hacer que se cumplan en el territorio de su jurisdicción las normas de la constitución, de las leyes y de los derechos y decisiones de las autoridades competentes.

2. Administrar el Corregimiento de acuerdo con las instrucciones de la Alcaldía.

3. Coordinar y desempeñar las labores de la Inspección de Policía detalladas en las funciones de la Inspección de Policía dentro del Corregimiento.

4. Coordinar con la Inspección de Policía, los Juzgados de turno, la Comisaría de Familia y la Secretaría de Gobierno Municipal, todo lo relacionado con el desempeño de las funciones propias y la relación con los habitantes del corregimiento.

IV. CONTRIBUCIONES INDIVIDUALES

1. Velar porque los servicios públicos esenciales se presenten en el corregimiento.

2. Informar oportunamente a la Secretaría de Gobierno Municipal toda situación que amenace la tranquilidad de la población del corregimiento.

3. Interactuar con la comunidad, y así recomendar al Alcalde Municipal la adopción de medidas que contribuyan al progreso y desarrollo del corregimiento.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Legislación de Policía.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Haber terminado como mínimo la educación básica primaria.

SUPERVISOR DE OBRAS

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	SUPERVISOR DE OBRAS
CÓDIGO:	501
GRADO:	02
No. De Cargos:	1
DEPENDENCÍA:	SECRETARÍA DE PLANEACIÓN MUNICIPAL
CARGO DE JEFE INMEDIATO	ALCALDE

II. PROPÓSITO GENERAL

Comprobar, constatar el cumplimiento de las obras en ejecución, teniendo en cuanta las normas, especificas técnicas, contenidos, calidades y demás detalles consignados en los documentos contractuales.

Informar de inmediato al superior de las novedades que se presenten durante la ejecución de las obras.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Prever los requerimientos urbanísticos, servicios públicos, obras públicas y servicios comunitarios para atender la expansión de los recursos urbanos.

2. Coordinar y controlar las acciones del municipio con el sector privado y demás participantes en el desarrollo, para la ejecución de obras, el recibo de áreas de sesión.

3. Coordinar y controlar las intervenciones de los sectores públicos y privados para la conformación, protección y uso adecuado del espacio público.

4. Llevar el registro de las personas naturales y jurídicas que se dediquen a las actividades contempladas en la ley 66/1968 y el decreto 2610/1979.

5. Coordinar y controlar la reglamentación de la construcción y el desarrollo de programas habitacionales conforme a la normatividad vigente.

6. Y las demás que le asigne el jefe superior.

IV. CONTRIBUCIONES INDIVIDUALES

1. Vigilar el desarrollo de los contratos de obra.

2. Ejecutar el control en la ejecución de obras públicas.

3. Hacer cumplir estrictamente las normas técnicas de ejecución de las obras.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Legislación Técnica sobre ejecución de obras civiles.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Título de tecnólogo, técnico o Profesional en: Obras civiles, ingeniería civil, arquitectura o áreas de construcción.

EXPERIENCIA: Seis (6) meses de experiencia profesional relacionada.

COORDINADOR DE RENTAS E IMPUESTOS

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	COORDIANDOR DE RENTAS E IMPUESTOS
CÓDIGO:	501
GRADO:	02
No. De Cargos:	1
DEPENDENCÍA:	SECRETARÍA DE HACIENDA MUNICIPAL
CARGO DE JEFE INMEDIATO	ALCALDE

II. PROPÓSITO GENERAL

Coordinar y velar porque todas las rentas del municipio tengan aplicación.

Desarrollar actividad tendiente a que los sujetos pasivos de los tributos municipales cumplan oportunamente con tales obligaciones.

Llevar registro y control de todo lo que implique bienes del municipio.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Acometer las acciones para el recaudo, cobro y registro de los impuestos, renta, tazas, participaciones, servicios, de acuerdo con las normas legales vigentes.

2. Coordinar con el Secretario de Hacienda Municipal las visitas e inspecciones a los establecimientos de comercio que existen en el municipio con el fin de controlar y para que se adecuen en el cumplimiento de sus atribuciones tributarias.

3. Llevar las estadísticas financieras con el fin de actualizar y llevar las cuentas municipales.

4. Ejercer el control sobre las rifas, espectáculos y sorteos que se celebren en el municipio a fin de asegurar el pago de los gravámenes correspondientes.

5. Manejar y llevar el control de los inventarios y seguros de los bienes municipales.

6. Administrar los bienes muebles, en lo que tiene que ver con almacén para proveer a las distintas dependencias de la administración central y en fin llevar el registro de las entradas y salidas de los elementos de consumo y devolución.

7. Y las demás que le asigne el jefe superior.

IV. CONTRIBUCIONES INDIVIDUALES

1. Organizar y ordenar la manualización de los bienes del municipio, desde el concepto de almacén, para así concecuenciar una verdadera rentabilización de los mismos.

2. Implementar mecanismos a efectos de fortalecer las rentas municipales.

3. Propulsar actividades que consoliden cultura de pago de impuestos.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Estatuto de Rentas del Municipio y normas tributarias.

2. Acuerdo de manualización de los bienes del municipio.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Título de tecnólogo, técnico o Profesional en: Obras civiles, ingeniería civil, arquitectura o áreas de construcción.

EXPERIENCIA: Seis (6) meses de experiencia profesional relacionada.

COORDINADOR DEL SISBÉN

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	COORDINADOR DEL SISBEN
CÓDIGO:	501
GRADO:	02
No. De Cargos:	1
DEPENDENCÍA:	SECRETARÍA DE PLANEACIÓN MUNICIPAL
CARGO DE JEFE INMEDIATO	ALCALDE

I. PROPÓSITO GENERAL

Establecer un sistema de información oportuno y actualizado de la población vulnerable para acceder a los programas de beneficio social de orden nacional, departamental y municipal.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Es el responsable de la conformación, actualización y uso de la información de la base de datos. Por lo tanto las funciones deben estar orientadas a lograr y mantener una estrecha coordinación interinstitucional y una adecuada administración del sistema.

2. Es el responsable del funcionamiento del sistema de información Sisbén en sus aspectos administrativos y operativos.

3. Y las demás que le asigne el jefe superior.

IV. CONTRIBUCIONES INDIVIDUALES

1. Que el Municipio cuente con un sistema de información actualizado y permanente de la población vulnerable, para ser beneficiados con programas sociales.

2. Consolidar un Sisbén traducidos en reglas, normas y procedimientos que permitan obtener información socio-económica confiable y así identificar el grado de pobreza de la población en sus diferentes niveles.

3. Dar cumplimiento a la ley de la seguridad social en cuanto a la administración de los recursos del régimen subsidiado a través de la identificación y selección de beneficiarios derivados del Sisbén.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Legislación sobre seguridad social.

2. Conocimientos sobre Sisbén y régimen subsidiado.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Título de tecnólogo, técnico o Profesional en: Administración Pública o de empresas, o en áreas de sistemas y afines.

EXPERIENCIA: Seis (6) meses de experiencia profesional relacionada.

SECRETARIO EJECUTIVO

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	SECRETARIO EJECUTIVO
CÓDIGO:	425
GRADO:	02
No. De Cargos:	2
DEPENDENCÍA:	ALCALDÍA
CARGO DE JEFE INMEDIATO	ALCALDE

II. PROPÓSITO GENERAL

Apoyar en la sustanciación y tramitación de actos propios de la Alcaldía.

Servir de puente de comunicación entre la administración municipal y la comunidad.

Generar actitudes de calidez en las funciones del funcionariado.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Realizar tareas tales como la realización de informes, liquidación de prestaciones sociales, liquidación de seguridad social, elaboración de nómina y el diligenciamiento oportuno de los pagos parafiscales que incumben al Municipio.

2. Velar por el oportuno envío de la correspondencia, el debido registro de la misma, el correcto archivo de los documentos emanados en el despacho donde se le asigne, la elaboración correcta de los oficios y cartas que emita el despacho, así como el control en el uso de los mismos por parte del personal ajeno a la administración.

3. Tener conocimiento y manejo de programas software.

4. Atender eficazmente a la población y comunidad en general brindando adecuada información, y colaboración requerida.

5. Mantener excelentes relaciones personales y utilización adecuada de la comunicación, especialmente el Vocabulario y la telefonía.

6. Prudencia y reserva a la hora de tratarse de temas propios de la administración.

7. Hacer sabe al jefe inmediato los comentarios de inconformismo o que revistan peligrosidad para él o para la administración.

8. Responder y velar por la preservación e integridad de los bienes de orden técnico y logístico que para el desarrollo de sus funciones se le asigne en la dependencia donde labore.

9. Y las demás que le asigne el jefe superior.

IV. CONTRIBUCIONES INDIVIDUALES

1. Manifestar relaciones de respeto y de atención oportuna a todos los que requieran servicio de la administración municipal.

2. Adoptar actitudes que den buena imagen a la administración.

3. Responsabilidad frente a los bienes de orden técnico y logístico de la administración municipal.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Conocimientos de Secretariado y de relaciones públicas.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Acreditación diploma de bachiller en cualquier modalidad.

EXPERIENCIA: Seis (6) meses de experiencia profesional relacionada.

AUXILIAR ADMINISTRATIVO

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	AUXILIAR ADMINISTRATIVO
CÓDIGO:	407
GRADO:	01
No. De Cargos:	1
DEPENDENCÍA:	SECRETARÍA DE HACIENDA MUNICIPAL
CARGO DE JEFE INMEDIATO	ALCALDE

II. PROPÓSITO GENERAL

Desarrollar actividades de apoyo y complementarias de las tareas propias de los niveles superiores o de labores que se caracterizan por el predominio de acciones manuales o tareas de simple ejecución.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Realizar mantenimiento adecuado de la correspondencia utilizando mecanismos y normas en archivística.

2. Realizar las tareas propias del secretariado auxiliar en lo concerniente a la elaboración correcta de documentos, el envió de la correspondencia, el registro de la misma, y el proceso correcto para el archivo y registro de esta.

3. Mantener excelentes relaciones personales y utilización adecuada de la comunicación, especialmente Vocabulario y telefonía.

4. Responder por el manejo y cuidado de los equipos de oficina y otros que le sean asignados.

5. Exigir y entregar los equipos debidamente inventariados mediante oficio o acta de la cual una copia será para él y otra para el jefe de recursos humanos y físicos o el encargado de almacén.

6. Hacer entrega oportuna de los documentos que su oficina genere dentro o fuera de la administración.

7. Atender al trabajo mecanográfico y de digitación de documentos, el envío por correo de los mismos, el correcto archivo de los comprobantes y los recibidos de acuerdo con las instrucciones recibidas.

8. Redactar y transcribir oficios a tiempo de acuerdo con instrucciones dadas.

9. No hacer comentarios mal intencionados o imprudentes ni ser fuente de murmuraciones que afecten el buen desempeño de la administración, si existe inconformidad por alguna situación, buscar el mecanismo para hacerlo saber a sus jefes inmediatos.

10. Y las demás que le asigne el jefe superior.

IV. CONTRIBUCIONES INDIVIDUALES

1. Facilitar la ejecución de funciones de los niveles superiores, en cuanto a su complementariedad.

2. Colaborar en labores auxiliares para llevar a delante las responsabilidades de la dependencia donde este asignado tal cargo.

3. Establecer en coordinación con el secretario de despacho políticas que contribuyan a cumplir con las funciones del nivel directivo de la dependencia.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Conocimientos de Secretariado y de apoyo relacionado con la actividad de la administración municipal.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Acreditación diploma de bachiller en cualquier modalidad.

EXPERIENCIA: Seis (6) meses de experiencia profesional relacionada.

SECRETARIO BIBLIOTECA Y ARCHIVO MUNICIPAL

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	SECRETARIO BIBLIOTECA Y ARCHIVO MUNICIPAL
CÓDIGO:	482
GRADO:	01
No. De Cargos:	1
DEPENDENCÍA:	ALCALDÍA
CARGO DE JEFE INMEDIATO	ALCALDE

II. PROPÓSITO GENERAL

Organizar, coordinar y dirigir poner la documentación e información de la Alcaldía Municipal y llevar el respectivo archivo, conforme a las disposiciones legales.

Operar apoyo para el funcionamiento de la biblioteca y archivo del municipio.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Atender y proporcionar la información solicitada acerca de contenidos existentes en el archivo municipal o en la biblioteca.

2. Organizar, manejar y mantener actualizado el archivo del municipio.

3. Colaborar y apoyar las actividades que se desarrollen en la biblioteca del municipio.

4. Cumplir con los requerimientos de orden legal o reglamentario que se derive de la actividad del archivo o de la operatividad de la biblioteca pública.

5. Y las demás que le asigne el jefe superior.

IV. CONTRIBUCIONES INDIVIDUALES

1. Velar por el buen orden de los libros y documentos existentes en el archivo y la biblioteca.

2. Crear un ambiente de motivación para que la comunidad se interese en la información y literatura existente en el archivo y la biblioteca.

3. Organizar el control de salida y entrada de los usuarios del archivo y la biblioteca.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Legislación sobre archivo y biblioteca.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Acreditación diploma de bachiller en cualquier modalidad.

EXPERIENCIA: Seis (6) meses de experiencia profesional relacionada.

CHOFER MECÁNICO

I. IDENTIFICACIÓN

NIVEL:	CENTRAL
DENOMINACIÓN DEL EMPLEO:	CHOFER MACÁNICO
CÓDIGO:	482
GRADO:	01
No. De Cargos:	1
DEPENDENCÍA:	ALCALDÍA
CARGO DE JEFE INMEDIATO	ALCALDE

II. PROPÓSITO GENERAL

Contribuir en actividades de la administración de orden manual y mecánico.

Complementar con su apoyo celeridad y seguridad en la actividad locomotriz del municipio.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Estar disponible para conducir el vehículo que le sea asignado.

2. Velar por el cuidado y mantenimiento del vehículo.

3. Propender por la refacción oportuna y de alta calidad del vehículo asignado.

4. Responder por todos los elementos propios del vehículo tales como equipos de sonido, batería, llantas de repuestos y otros.

5. Estar en el sitio de trabajo con el vehículo disponible a tiempo.

6. Cuando por algún motivo el vehículo que normalmente conduce no esté disponible el conductor deberá permanecer en el Palacio municipal o la dependencia donde haya sido asignado en cumplimiento del horario establecido para los funcionarios de la Administración Municipal y dispuesto para cualquier actividad que por la naturaleza de sus funciones el superior inmediato le asigne.

7. El cambio de aceite periódico para los vehículos, el combustible, el periódico engrase, la rotación de las llantas, los aditamentos especiales para maniobrar el vehículo en condiciones extremas, la vigencia de los documentos, la renovación oportuna de la licencia de conducción son responsabilidad del conductor asignado a cada vehículo y cualquier percance sufrido por la carencia o mal estado de estas tareas son responsabilidad del conductor.

8. Las asignaciones del vehículo a conducir, y los cambios en ellos deben ser autorizados por el superior inmediato, el conductor no puede dejar el vehículo bajo su responsabilidad para ser conducido por personal ajeno a la administración, o por un conductor asignado para otro vehículo sin el permiso o autorización de autoridad competente.

9. Guardar discreción en cuanto a los temas que por razón de su trabajo se platiquen en presencia suya.

10. Y las demás que le asigne el Jefe Superior.

IV. CONTRIBUCIONES INDIVIDUALES

1. Asegurar el correcto funcionamiento del vehículo municipal.

2. Informar las necesidades de orden técnico necesario para el vehículo.

3. Estar a disposición cuando sea requerido por la Alcaldía en los aspectos de conducción y mantenimiento del vehículo.

V. CONOCIMIENTOS BASICOS O ESENCIALES

1. Conocimiento en conducción y mantenimiento de vehículo.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS: Acreditación diploma de bachiller en cualquier modalidad o mínimo tercer año de educación básica primaria y además contar con la licencia de conducción.

EXPERIENCIA: Seis (6) meses de experiencia profesional relacionada.

ARTÍCULO 2.

Competencias común a los servidores públicos: Las competencias comunes de los servidores públicos a que se refiere el presente manual específico de funciones y competencias serán las siguientes:

COMPETENCIA	DEFINICIÓN DE LA COMPETENCIA	CONDUCTAS ASOCIADAS
Orientación a resultados	Realizar las funciones y cumplir los compromisos organizacionales con eficacia y calidad.	-Cumple con oportunidad en función de estándares, objetivos y metas establecidas por la entidad, las funciones que le son asignadas. -Asume la responsabilidad por sus resultados. -Compromete recursos y tiempos para mejorar la productividad tomando las medidas necesarias para minimizar los riesgos. -Realiza todas las acciones necesarias para alcanzar los objetivos propuestos enfrentando los obstáculos que se presentan.
Orientación al usuario y al ciudadano.	Dirigir las decisiones y acciones a la satisfacción de las necesidades e intereses de los usuarios internos y externos, de conformidad con las responsabilidades públicas asignadas a la entidad.	-Atiende y valora las necesidades y peticiones de los usuarios y ciudadanos en general. -Considera las necesidades de los usuarios al diseñar proyectos o servicios. -Da respuesta oportuna a las necesidades de los usuarios de conformidad con el servicio que ofrece la entidad. -Establece diferentes canales de comunicación con el usuario para conocer sus necesidades y propuestas y responde a las mismas. -Reconoce la interdependencia entre su trabajo y el de otros.
	Hacer uso responsable y claro de los	-Proporciona información veraz, objetiva y basada en

Transparencia.	recursos públicos, eliminando cualquier discrecionalidad indebida en su utilización y garantizar el acceso a la información gubernamental.	hechos. -Facilita el acceso a la información relacionada con sus responsabilidades y con el servicio a cargo de la entidad en que labora. -Demuestra imparcialidad en sus decisiones. -Ejecuta sus funciones con base en las normas y criterios aplicables. -Utiliza los recursos de la entidad para el desarrollo de las labores y la prestación del servicio.
Compromiso con la Organización.	Alinear el propio comportamiento a las necesidades, prioridades y metas organizacionales.	-Promueve las metas de la organización y respeta sus normas. -Antepone las necesidades de la organización a sus propias necesidades. -Apoya a la organización en situaciones difíciles. -Demuestra sentido de pertenencia en todas sus actuaciones.

ARTÍCULO 3. COMPETENCIAS COMPORTAMENTALES POR NIVEL JERÁRQUICO DE EMPLEO.

Las competencias comportamentales por nivel jerárquico de empleos que como mínimo, se requieren para desempeñar los empleos a que se refieren el presente manual específico de funciones y de competencias laborales, serán las siguientes:

3.1. NIVEL DIRECTIVO

COMPETENCIA	DEFINICIÓN DE LA COMPETENCIA	CONDUCTAS ASOCIADAS
	Guiar y dirigir grupos y establecer y mantener la cohesión de grupos necesaria	-Mantiene a sus colaboradores motivados. -Fomenta la comunicación clara, directa y concreta.

LIDERAZGO	para alcanzar los objetivos organizacionales.	-Constituye y mantiene grupos de trabajo con un desempeño conforme a los estándares. -Promueve la eficacia del equipo. -Genera un clima positivo y de seguridad en sus colaboradores. -Fomenta la participación de todos en los procesos de reflexión y de toma de decisiones. -Unifica esfuerzos, hacia objetivos y metas institucionales.
PLANEACIÓN	Determinar eficazmente las metas y prioridades institucionales, identificando las acciones, los responsables, los plazos y los recursos requeridos para alcanzarlas.	-Anticipa situaciones y escenarios futuros con acierto. -Establece objetivos claros y concisos, estructurados y coherentes con las metas organizacionales. -Traduce los objetivos estratégicos en planes prácticos y factibles. -Busca soluciones a los problemas. -Distribuye el tiempo con eficiencia. -Establece planes alternativos de acción.
TOMA DE DESICIONES	Elegir entre una o varias alternativas para solucionar un problema o atender una situación. Comprometiéndose con acciones concretas y consecuentes con la decisión.	-Elegir con oportunidad entre muchas alternativas los proyectos a realizar. -Efectúa cambios complejos y comprometidos en sus actividades o en las funciones que tiene asignadas cuando detecta problemas o dificultades para su realización. -Decide bajo presión. -Decide en situaciones de alta complejidad e incertidumbre.
	Favorece el aprendizaje y desarrollo de sus colaboradores, articulando las	-Identifica las necesidades de formación y capacitación y propone acciones para satisfacerlas.

DIRECCIÓN Y DESARROLLO DE PERSONAL	potencialidades y necesidades individuales con las de la organización para optimizar la calidad de las contribuciones de los quipos de trabajo y de las personas, en el cumplimiento de los objetivos y metas organizacionales presentes y futuras.	-Permite niveles de autonomía con el fin de estimular el desarrollo integral del empleado. -Delega de manera efectiva sabiendo cuando intervenir y cuando no hacerlo. -Hace uso de las habilidades y recurso de su grupo de trabajo para alcanzar las metas y los estándares de productividad. -Establece espacios regulares de retroalimentación y reconocimiento del desempeño y sabe manejar hábilmente el bajo desempeño. -Tiene en cuenta las opiniones de sus colaboradores. -Mantiene con sus colaboradores relaciones de respeto.
CONOCIMIENTO DEL ENTORNO	Estar al tanto de las circunstancias y las relaciones de poder que influyen en el entorno organizacional.	-Es consciente de las condiciones específicas del entorno organizacional. -Está al día en los acontecimientos claves del sector y del estado. -Conoce y hace seguimiento a las políticas a las políticas gubernamentales. Identifica las fuerzas políticas que afectan la organización y las posibles alianzas para cumplir con los propósitos.

3.2. NIVEL PROFESIONAL

COMPETENCIA	DEFINICIÓN DE LA COMPETENCIA	CONDUCTAS ASOCIADAS
	Adquirir y desarrollar permanentemente conocimientos, destrezas y habilidades, con	-Aprende de la experiencia de otros y de la propia. -Se adapta y aplica nuevas tecnologías que se

Aprendizaje Continuo	el fin de mantener altos estándares de eficacia organizacional.	implanten en la organización. -Aplica los conocimientos adquiridos a los desafíos que se presentan en el desarrollo del trabajo. -Investiga, indaga y profundiza en los temas de su entorno o área de desempeño. -Reconoce las propias limitaciones y las necesidades de mejorar su preparación. -Asimilar nueva información y la aplica correctamente.
Experticia Profesional	Aplicar el conocimiento profesional en la resolución de problemas y transferirlo a su entorno laboral.	-Analiza de un modo sistemático y racional los aspectos del trabajo, basándose en la información relevante. -Aplica reglas básicas y conceptos complejos aprendidos. -Identifica y reconoce con facilidad las causas de los problemas y sus posibles soluciones. -Clarifica datos o situaciones complejas. -Planea, organiza y ejecuta múltiples tareas tendientes a alcanzar resultados institucionales.
Trabajo en Equipo y Colaboración **Trabajo en Equipo y Colaboración**	Trabaja con otros de forma conjunta y de manera participativa, integrando esfuerzos para la consecución de metas institucionales comunes.	-Coopera en distintas situaciones y comparte información. -Aporta sugerencias, ideas y opiniones. -Expresa expectativas positivas del equipo o de los miembros del mismo. -Planificas las propias acciones teniendo en cuenta la repercusión de las mismas para la consecución de los objetivos grupales. -Establece diálogo directo con los miembros del equipo que permita compartir información e ideas en

		condiciones de respeto y cordialidad. -Respeta criterios dispares y distintas opiniones del equipo.
Creatividad e Innovación	Generar y desarrollar muevas ideas, conceptos, métodos y soluciones.	-Ofrece respuestas alternativas. -Aprovecha las oportunidades y problemas para dar soluciones novedosas. -Desarrolla nuevas formas de hacer y tecnologías. -Busca nuevas alternativas de solución y se arriesga a romper esquemas tradicionales. -Inicia acciones para superar los obstáculos y alcanzar metas específicas.

3.3. NIVEL TÉCNICO

COMPETENCIA	DEFINICIÓN DE LA COMPETENCIA	CONDUCTAS ASOCIADAS
Experiencia Técnica	Entender y aplicar los conocimientos técnicos del área de desempeño y mantenerlos actualizados.	-Capta y asimila con facilidad conceptos e información. -Aplica el conocimiento técnico a las actividades cotidianas. -Analiza la información de acuerdo con las necesidades de la organización. -Comprende los aspectos técnicos y los aplica al desarrollo de procesos y procedimientos en los que esta involucrado. -Resuelve problemas utilizando sus conocimientos técnicos de su especialidad y garantizando indicadores y estándares establecidos.
	Trabajar con otros para conseguir metas	-Identificar claramente los objetivos del grupo y

Trabajo en Equipo	comunes.	orienta su trabajo a la consecución de los mismos. -Colabora con otros para la realización de actividades y metas grupales.
Creatividad e Innovación	Presenta ideas y métodos novedosos y concretados en acciones.	-Propone y encuentra formas nuevas y eficaces de hacer las cosas. -Es recursivo. -Es práctico. Busca nuevas alternativas de solución. -Revisa permanentemente los procesos y procedimientos para optimizar los resultados.

3.4. NIVEL ASISTENCIAL

COMPETENCIA	DEFINICIÓN DE LA COMPETENCIA	CONDUCTAS ASOCIADAS
Manejo de la Información	Manejar con respeto las informaciones personales e institucionales de que dispone.	-Evade temas que indagan sobre información confidencial. -Recoge sólo información imprescindible para el desarrollo de la tarea. -Organiza y guarda de forma adecuada la información a su cuidado, teniendo en cuenta las normas legales y de la organización. -No hace pública información laboral o de las personas que pueda afectar la organización o las personas. -Es capaz de discernir que se puede hacer pública o no. -Transmite información oportuna y objetiva.
	Enfrentarse con flexibilidad y versatilidad a	-Acepta y se adapta fácilmente a los cambios.

Adaptación al Cambio	situaciones nuevas para aceptar los cambios positiva y constructivamente.	-Responde al cambio con flexibilidad. -Promueve el cambio.
Disciplina	Adaptarse a las políticas institucionales y buscar información de los cambios en la autoridad competente.	-Acepta instrucciones aunque se difiera de ellas. -Realiza los cometidos y tareas del puesto de trabajo. -Acepta la supervisión constante. -Realiza funciones orientadas a apoyar la acción de otros miembros de la organización.
Relaciones Interpersonales	Establecer y mantener relaciones de trabajo amistosas y positivas, basadas en la comunicación abierta y fluida y en el respeto por los demás.	-Escuchar con interés a las personas y capta las preocupaciones, interés y necesidades de los demás. -Trasmite eficazmente las ideas, sentimientos e información impidiendo con ello malos entendidos o situaciones confusas que puedan generar conflictos.
Colaboración	Cooperar con los demás con el fin de alcanzar los objetivos institucionales.	-Ayuda al logro de los objetivos articulando sus actuaciones con los demás. -Cumple con los compromisos que adquiere. -Facilita la labor de sus superiores u compañeros de trabajo.

ARTÍCULO 4.

El Secretario de Gobierno entregará a cada funcionario copia de las funciones y competencias determinadas en el presente manual para el respectivo empleo en el momento de la posesión, cuando sea ubicado en otra dependencia que implique cambio de funciones o cuando mediante la adopción o modificación del manual se afecten las establecidas para los empleos. Los Jefes inmediatos responderán por la orientación del empleado en cumplimiento de las mismas.

ARTÍCULO 5.

Cuando para el desempeño de un empleo se exija una profesión, arte u oficio debidamente reglamentado, los grados, títulos, licencias, matriculas o autorizaciones previstas en las leyes o reglamentos, no podrán ser compensados por experiencia u otras calidades, salvo cuando las mismas leyes así lo establezcan.

ARTÍCULO 6.

El presente decreto rige a partir de la fecha de su expedición.

COMUNIQUESE Y CUMPLASE

Dado en Río de Oro, Cesar, a los (12) días del mes de octubre de 2005.

Original Fdo.

_____

MANUEL OTILIO SALAZAR RIZO
Alcalde Municipal

ANEXO E: MANUAL DE FUNCIONES DE LAS DEPENDENCDIAS DE LA ALCALDÍA DEL MUNICIPIO DE RÍO DE ORO, CESAR

MANUAL DE LAS FUNCIONES DE LAS DEPENDENCIAS DE LA ALCALDÍA DEL MUNICIPIO DE RÍO DE ORO, CESAR

BIBLIOTECA Y ARCHIVO MUNICIPAL

Objetivos

1. Organizar, coordinar y dirigir la documentación e información de la Alcaldía Municipal y llevar el respectivo archivo, conforme a las disposiciones legales.

2. Operar apoyo para el funcionamiento de la biblioteca y el archivo del municipio.

Funciones

Atender y proporcionar la información solicitada acerca de contenidos existentes en el archivo municipal o en la biblioteca.

COMISARÍA DE FAMILIA

Misión. La Comisaría de Familia tiene como misión prevenir, garantizar, restablecer y reparar los derechos de los miembros de la familia, conculcados por situaciones de violencia intrafamiliar y las demás establecidas por la ley.

Objetivos. La Comisaría de familia como dependencia de la Administración Municipal ha sido creada y puesta en funcionamiento con el objetivo de brindar ayuda y orientación psicológica y jurídica a las familias del Municipio en aras de mantener la unidad y bienestar de los miembros de cada una de éstas. Además de esto con el apoyo de la Comisaría de Familia se busca garantizar a los niños, niñas y adolescentes su pleno y armonioso desarrollo para que crezcan en el seno de la familia y de la comunidad en un ambiente de felicidad, amor y comprensión.

Funciones

Funciones y Competencias De La Comisaria De Familia

1. Atender al usuario

2. Brindar la asesoría jurídica en todos los temas de familia

3. Realización de audiencias de conciliación en casos de:

- **a)** Medida de protección
- **b)** Audiencia de conciliación de alimentos
- **c)** Audiencias de conciliación de separación de bienes y de cuerpos.
- **d)** Audiencia de conciliación de suspensión de la vida en común.
- **e)** Audiencia de conciliación de incumplimiento de medida de protección
- **f)** Audiencia de exoneración de cuota alimentaria
- **g)** Audiencia pública de reducción de la cuota alimentaria
- **h)** Audiencia de conciliación de custodia de los menores
- **i)** Audiencia de conciliación de la existencia de la unión marital de hecho
  - **1)** Operativos: cuando lo requiera el superior.
  - **2)** Allanamientos: cuando haya menores o miembros del núcleo
  - **3)** familiar en inminente peligro.

4. Las demás funciones que surjan en el transcurso de la realización de las labores

Metas. La Comisaría de Familia del Municipio deberá ser reconocida como la entidad encargada de proteger y velar el cumplimiento de los derechos y deberes no sólo de los niños, niñas y adolescentes, sino de la familia en general.

COORDINACIÓN DE BANCO DE PROYECTOS

Misión. Registrar, evaluar y viabilizar los proyectos y programas del Municipio.

Objetivos

Apoyar el proceso de planeación y programación de la inversión y evaluación de la gestión pública.

Contribuir a que la asignación de recursos se realice con criterios de eficiencia y rentabilidad social.

Generar todo tipo de información sobre programas y proyectos de cada sector que sirvan de apoyo al municipio en el proceso de gestión, planeación, elaboración del presupuesto y programación de la inversión.

Funciones

1. Dar aplicación al funcionamiento del manual operativo del Banco de Proyectos del Municipio.

2. Coordinar y dirigir el registro de programas y proyectos viables técnica, económica, social y ambientalmente sostenibles de ser financiados con recursos del estado.

3. Registrar la información de los proyectos a lo largo de todo su ciclo de vida, permitiendo hacer seguimiento a la ejecución de la inversión y monitoreo durante la operación.

4. Facilitar la información para formular los planes de acción en cada vigencia.

5. Realizar seguimiento y evaluación de los objetivos y metas de planes, programas y proyectos.

6. Las demás que le asigne el jefe supervisor.

COORDINACIÓN DE CULTURA Y TURISMO

Misión. Promover difundir y formular políticas y directrices en el campo de la diversidad cultural, formación artística y el turismo, implementando procesos de investigación, participación, coordinación, comunicación, reconocimiento del patrimonio y el desarrollo artístico, turístico y cultural que conlleven al respeto, la tolerancia y reconocimiento del otro.

Objetivos

Objetivo General. Promover las artes, las letras, el folclor, las artesanías y el desarrollo turístico en el Departamento. Igualmente, impulsar todas las formas de expresión y creación artística, la defensa del patrimonio cultural del pueblo riodorense y propiciar la investigación de la cultura abierta a los procesos socio-culturales propios.

Objetivos Específicos

1. Propiciar el cambio de actitud en procura de un riodorenses tolerante, solidario, respetuoso de su patrimonio natural y cultural, productivo y creador, centrado en la formación educativa.

2. Promover y mantener la organización Cultural, en el marco del Sistema Nacional de Cultura, para garantizar la participación de la población en los procesos de investigación, formación y difusión artística y cultural.

3. Planificar el desarrollo turístico del municipio, en cumplimiento de los principios generales de la Ley de Turismo.

4. Promover la investigación, el reconocimiento, valoración, apropiación, difusión y aprovechamiento turístico del patrimonio natural y cultural tangible e intangible de Río de Oro.

5. Coordinar las relaciones interinstitucionales con los sectores público y privado a nivel departamental, nacional e internacional, en procura de establecer mecanismos tendientes a la dinamización, crecimiento, desarrollo y sostenibilidad del turismo e implementar acciones de promoción y divulgación del entorno turístico.

6. Facilitar la divulgación de expresiones artísticas, folclóricas y artesanales del Municipio en eventos de intercambio cultural a nivel regional, nacional e internacional.

Funciones

1. Formular y desarrollar la política municipal de formación cultural y coordinar su ejecución.

2. Formular políticas para la promoción turística y velar por su ejecución.

3. Elaborar y ejecutar planes y programas de los sectores de cultura y turismo, de acuerdo con el Plan de Desarrollo Municipal, buscando la cooperación y coordinación de los organismos regionales, municipales y nacionales del ramo.

4. Prestar asesoría y asistencia técnica a las entidades culturales, turísticas y a los municipios.

5. Difundir información turística y cultural del Municipio.

6. Promover, organizar y coordinar actividades de difusión y promoción del arte, el folclor, la cultura y el turismo.

7. Propiciar procesos de investigación y apropiación social del patrimonio natural y cultural del Municipio.

8. Planear, organizar, dirigir, ejecutar y controlar la realización del Desfile de la Leyenda del Tigre y Reinado Municipal de carnaval.

9. Coordinar la operación de los componentes que a nivel regional constituyen el Sistema Nacional de Cultura.

10. Elaborar estudios e indicadores sobre el comportamiento de los sectores cultural y turístico.

11. Adelantar la gestión para mejorar la infraestructura y los servicios en el municipio de las Áreas de interés turístico y cultural.

12. Participar y fortalecer el Consejo Municipal de Cultura.

COORDINACIÓN DE DEPORTE Y RECREACIÓN

Misión. La coordinación de deporte y recreación fomenta el espíritu deportivo y la recreación de los riodorenses para su desarrollo integral como seres humanos mediante la formación deportiva, la organización de eventos deportivos y la recreación, atendiendo todos los principios que rigen la actuación administrativa del municipio.

Objetivos

1. Fomento al deporte.

2. Fomento a la recreación.

3. Mantenimiento de los escenarios deportivos y recreativos del municipio.

4. Apoyo y Gestión para la construcción de escenarios deportivos y recreativos.

Funciones

1. Formula mecanismos para lograr la participación de los ciudadanos y ciudadanas en programas recreativos y deportivos en desarrollo del derecho constitucional que le asiste a todas las personas para la práctica del deporte y el aprovechamiento del tiempo libre.

2. Formula estrategias para garantizar la formación y apoyo integral a los deportistas.

3. Coordinar la creación de Escuelas de Formación Deportiva en cumplimiento de Plan de Desarrollo Municipal.

COORDINACIÓN DE DESARROLLO RURAL

Misión. Prestar de manera eficaz y eficiente el servicio de asistencia técnica rural a los pequeños productores, transferencia de tecnología, asesoría en la implementación de proyectos productivos y en la organización de grupos de trabajo asociado, con el fin de mejorar los sistemas de producción, el nivel de ingresos y las condiciones de vida, sin que esta labor conlleve al deterioro de los recursos naturales.

Objetivos. Prestar de manera eficaz y eficiente el servicio de asistencia técnica rural a los pequeños productores, transferencia de tecnología, asesoría en la implementación de proyectos productivos y en la organización de grupos de trabajo asociado, con el fin de mejorar los sistemas de producción, el nivel de ingresos y las condiciones de vida, sin que esta labor conlleve al deterioro de los recursos naturales.

Funciones

1. Formular y adoptar políticas, planes y programas que fomenten o estimulen el desarrollo de proyectos productivos, empresariales y agroempresariales en beneficio de la población campesina del Municipio.

2. Formular y adoptar políticas, planes, programas y proyectos encaminados a la producción de empleo en el sector rural.

3. Formular, coordinar, y ejecutar planes, programas y acciones en materia de asistencia técnica agropecuaria.

Metas

1. Fortalecimiento de Asistencia Técnica Agropecuaria en el Municipio de Río de Oro.

2. implementación de un programa de mejoramiento de las condiciones agropecuarias mediante brigadas de asistencia técnica.

3. Implementación de un programa de capacitación para la adopción de nuevos procesos productivos.

4. Apoyo de proyectos productivos.

5. Promoción y apoyo a los cultivo orgánicos.

6. Puesta en marcha de los programas encaminados a mejorar las condiciones de vida de los campesinos riodorenses.

COORDINACIÓN DE MEDIO AMBIENTE

Misión. La Coordinación de Medio Ambiente promueve, orienta y regula la sustentabilidad ambiental del Municipio, como garantía presente y futura del bienestar de la población; y como requisito indispensable para la conservación y uso de bienes y servicios ecosistémicos y valores de biodiversidad.

Objetivos. Corresponde a la Coordinación Municipal de Medio Ambiente y liderar la formulación de políticas ambientales y de aprovechamiento sostenible de los recursos ambientales y del suelo, tendientes a preservar la diversidad e integridad del ambiente, el manejo y aprovechamiento sostenible de los recursos naturales y la conservación del sistema de áreas protegidas, para garantizar una relación adecuada entre la población y el entorno ambiental y crear las condiciones que garanticen los derechos fundamentales y colectivos relacionados con el medio ambiente.

Funciones

1. Formular participativamente la política ambiental del Municipio.

2. Liderar y Coordinar el proceso de preparación de los planes, programas y proyectos que tengan que ver con el Medio Ambiente.

3. Liderar y coordinar el Sistema Ambiental del Municipio.

4. Ejercer la autoridad ambiental, en cumplimiento de las funciones asignadas por el ordenamiento jurídico vigente, a las autoridades competentes en la materia.

5. Formular, ajustar y revisar periódicamente el Plan de Gestión Ambiental l y coordinar su ejecución a través de las instancias de coordinación establecidas.

6. Formular y orientar las políticas, planes y programas tendientes a la investigación, conservación, mejoramiento, promoción, valoración y uso sostenible de los recursos naturales y servicios ambientales y sus territorios socio ambientales reconocidos.

7. Promover planes, programas y proyectos tendientes a la conservación, consolidación, enriquecimiento y mantenimiento de la Estructura Ecológica Principal y del recurso hídrico de Río de Oro.

8. Formular, implementar y coordinar, con visión integral, la política de conservación, aprovechamiento y desarrollo sostenible de las áreas protegidas.

9. Definir los lineamientos ambientales que regirán las acciones de la administración pública municipal.

10. Definir y articular con las entidades competentes, la política de gestión estratégica del ciclo del agua como recurso natural, bien público y elemento de efectividad del derecho a la vida.

11. Formular, ejecutar y supervisar, en coordinación con las entidades competentes, la implementación de la política de educación ambiental de conformidad con la normativa y políticas nacionales en la materia.

12. Ejercer el control y vigilancia del cumplimiento de las normas de protección ambiental y manejo de recursos naturales, emprender las acciones de policía que sean pertinentes al efecto, y en particular adelantar las investigaciones e imponer las sanciones que correspondan a quienes infrinjan dichas normas.

13. Dirigir el diseño, implementación y seguimiento de planes, programas y proyectos ambientales.

14. Coordinar las instancias ambientales de los procesos de integración regional.

15. Diseñar y coordinar las estrategias de mejoramiento de la calidad del aire y la prevención y corrección de la contaminación auditiva, visual y electro magnética, así como establecer las redes de monitoreo respectivos.

16. Fortalecer los procesos territoriales y las organizaciones ambientales urbanas y rurales.

17. Realizar el control de vertimientos y emisiones contaminantes, disposición de desechos sólidos y desechos o residuos peligrosos y de residuos tóxicos, dictar las medidas de corrección o mitigación de daños ambientales y complementar la acción de las Empresa de Acueducto y Alcantarillado para desarrollar proyectos de saneamiento y descontaminación.

18. Promover y desarrollar programas educativos, recreativos e investigativos en materia ecológica, botánica, de fauna, medio ambiente y conservación de los recursos naturales.

19. Trazar los lineamientos ambientales de conformidad con el plan de desarrollo, el plan de ordenamiento territorial y el plan de gestión ambiental.

DESPACHO DEL ALCALDE

Misión. Administrar con eficiencia y eficacia los recursos de la entidad territorial, con el fin de lograr una óptima calidad de la prestación de los servicios, teniendo en cuenta el marco legal, en concordancia con el plan de gobierno, las políticas del plan de desarrollo Municipal, Departamental y Nacional, con el ánimo de alcanzar el bienestar de la población en general y mejorar su calidad de vida.

Objetivos

El Despacho del Alcalde tiene como objetivo dirigir, coordinar con las demás dependencias y, entidades descentralizadas, el cumplimiento de la misión institucional del Municipio, del Plan de Desarrollo, del Plan de Ordenamiento Territorial, de los planes, programas y proyectos a ser ejecutados, y en general de la prestación de los servicios a cargo del Municipio.

El Despacho será dirigido por el Alcalde Municipal, teniendo como apoyo administrativo directo, a un grupo de funcionarios y asesores especializados en áreas específicas, cuando así se requiera.

Funciones

Son funciones del Despacho del Alcalde, además de las dispuestas por la Constitución y la Ley, las siguientes:

1. Atender los servicios que demande el ejercicio de las funciones y atribuciones constitucionales, legales, las ordenanzas y los acuerdos Municipales que corresponda cumplir al Alcalde del Municipio de conformidad con el Artículo 315 de la Constitución Política de Colombia.

2. Conservar el orden público en el Municipio, de conformidad con la Ley, las instrucciones y las órdenes que impartidas por el Presidente de la República y el Gobernador del Departamento de Cundinamarca, dictando las medidas y reglamentos pertinentes, rendir los respectivos informes ante las instancias competentes.

3. Fijar políticas, dirigir, orientar, proponer los Acuerdos ante el Concejo Municipal en cuanto a la formulación de los planes, programas, presupuesto y demás iniciativas ejecutivas necesarias para la buena marcha del Municipio, sancionar, promulgar y reglamentar los actos administrativos que de éstos se deriven y sean considerados convenientes, con sujeción a las normas, reglamentos y actos de delegación que le sean atribuidos expresamente.

4. Dirigir, presidir, articular y controlar la acción administrativa del Municipio, apoyando y velando por el cumplimiento de la misión, objetivos, planes, programas y proyectos de cada una de las dependencias que conforman la Administración central, asegurando el cumplimiento de las funciones y la prestación de los servicios Municipales.

5. Fortalecer la organización administrativa, adecuándola oportunamente a las necesidades del servicio y a sus realidades socioeconómicas y tecnológicas, reglamentar áreas funcionales de gestión o grupos de trabajo para la atención de asuntos propios de las dependencias, conformar, reglamentar y asignar funciones a los órganos de asesoría y coordinación, crear, suprimir o fusionar dependencias Municipales con sujeción a las normas, reglamentos y actos de delegación que le sean atribuidos expresamente por las instancias y autoridades competentes.

6. Dirigir, ordenar y controlar los recursos humanos, financieros, ambientales y físicos del Municipio de acuerdo con la normatividad y disposiciones vigentes y con los principios de organización y delegación de funciones establecidos en el presente Decreto, buscando cumplir

con los objetivos, planes, programas y proyectos fijados, aplicando clara y cabalmente los principios gerenciales y administrativos que orientan la función pública moderna.

7. Gestionar, promover, concertar, articular y focalizar dentro del marco de los servicios, objetivos y funciones del Municipio y las atribuciones del Alcalde, los recursos económicos, técnicos, tecnológicos, humanos y otros, que requieran de la coordinación, concurrencia, subsidiaridad, complementariedad y apoyo en general, del orden internacional, nacional, departamental, regional, local, interinstitucional y del sector privado vinculados al desarrollo de la comunidad.

8. Dirigir, asesorar y coordinar la formulación, adopción y ejecución de procesos comunicativos y de información, orientados a consolidar una imagen institucional coherente con la misión de la Administración, coordinar con los medios de comunicación la divulgación de las actividades y eventos asociados con la gestión de Gobierno.

9. Formular, dirigir y coordinar de acuerdo con las entidades de vigilancia y control del Estado las políticas generales sobre régimen disciplinario, fijar los procedimientos operativos disciplinarios para que los procesos se desarrollen dentro de los principios legales de economía, celeridad, eficacia, imparcialidad y publicidad, buscando salvaguardar el derecho de defensa y el debido proceso.

10. Conocer en segunda instancia los procesos disciplinarios preliminares e investigaciones disciplinarias que deban adelantarse contra los empleados del nivel central de la Administración.

11. Ejercer vigilancia de la conducta oficial de los servidores de la Alcaldía garantizando los medios administrativos y logísticos necesarios para la implementación de control disciplinario interno de conformidad con las Leyes y normatividad vigentes, y resolviendo en primera instancia los procesos disciplinarios que así se determinen.

12. Establecer, mantener y perfeccionar los Sistemas funcionales previstos en el Estatuto Básico de la Administración Municipal, los cuales deben ser permanentemente adecuados a la naturaleza, estructura y misión de la organización.

13. Crear y promover un ambiente de Servicio y Atención al Usuario interno y externo de la Administración Municipal, implementando el respectivo Sistema, concertando con las organizaciones sociales el diseño de indicadores de calidad y contenido de la oferta de los productos y servicios a su cargo, ofreciendo información segura y confiable y

asegurando las acciones necesarias para resolver en los términos que establece la Ley y demás disposiciones vigentes las Quejas y Reclamos que formulen los usuarios.

14. Suscribir y ejecutar conforme con las facultades expresamente atribuidas y delegadas la Contratación administrativa de los servicios y/o actividades necesarias para el normal funcionamiento de la Administración y disponer las acciones necesarias para ejercer su vigilancia y control en los términos previstos en las normas Constitucionales, legales y en los demás actos administrativos vigentes que la regulan.

15. Ejercer las acciones de vigilancia y control sobre el cumplimiento de las normas urbanísticas y del Esquema de Ordenamiento territorial, en aplicación de la Ley 388 de 1997 y demás normas y actos administrativos que lo modifiquen o complementen.

16. Colaborar con el Concejo Municipal y demás autoridades e instancias competentes para el buen desempeño de sus funciones, presentar los informes debidamente soportados que le sean solicitados. Las demás que surjan de la naturaleza de la dependencia o le sean asignadas por autoridad competente.

Metas

Administrar los recursos económicos de manera eficaz y eficiente dando prioridad a la inversión social, buscando mejorar la calidad de vida de los habitantes del Municipio.

Lograr las metas de desarrollo económico y social propuestas que demostrarán la eficiencia de la administración municipal.

Gestionar con el Departamento, La nación y Organizaciones Públicas Nacionales, Privadas o Internacionales los recursos económicos necesarios para la ejecución de los programas y proyectos.

Cumplir con el Plan de Gobierno que responde eficientemente a la política pública y de elección de la comunidad.

Concertar y socializar con la comunidad el Plan de Desarrollo Municipal.

INSPECCIÓN DE POLICÍA

Misión. Velar por el respeto de los derechos civiles y garantías sociales, vida, honra y bienes de los ciudadanos, apoyar permanentemente a las autoridades de policía a fin de conservar el orden público, aplicar la correspondiente normatividad a los problemas que se presentan en jurisdicción del municipio de Río de Oro y que sean de la incumbencia de este Despacho.

Objetivos

Coadyuvar en el mantenimiento del orden público y en la protección de los derechos e intereses de la comunidad.

Hacer cumplir el código nacional y el departamental de policía.

Interactuar con la comunidad para recomendar al alcalde la adopción de medidas convenientes para la convivencia de la comunidad.

Funciones

1. Recibir declaraciones extrajuicio.

2. Efectuar lanzamiento por ocupación de hecho.

3. Llevar procesos de policías por perturbación a la posesión, propiedad privada y servidumbres.

4. Atender asuntos de contravenciones, daño en bien ajeno en accidentes de tránsito.

5. Expedir certificados de supervivencias.

6. Diligenciar las denuncias de conciliación.

7. Ejecutar las cauciones por conciliación por violación de las mismas.

8. Efectuar las comisiones emanadas de los juzgados.

9. Recibir demandas por contravenciones especiales y delitos y compulsarlas al juzgado en virtud de lo dispuesto en la ley 228, competencia de la justicia ordinaria.

10. Dar aplicación a los artículos 103, 104 y concordantes de la ley 388 de 1997 y capítulo V del decreto 1052 de 1998.

Metas. Propiciar la tranquilidad ciudadana en forma integral con las autoridades de policía a nivel de jurisdicción, con el apoyo de autoridades de orden nacional y departamental para que se cumplan las normas establecidas en el Código de Policía Nacional y Departamental, con el objeto de fomentar la sana convivencia de la comunidad en el municipio, obteniendo de esa forma ciudadanos satisfechos.

OFICINA DE "MÁS FAMILIAS EN ACCIÓN"

Misión. La oficina de Más Familias en Acción tiene como misión el cumplimiento de éste programa: Que Consiste en la entrega, condicionada y periódica de una transferencia monetaria directa para complementar el ingreso y mejorar la salud y, educación de los menores de 18 años de las familias que se encuentran en condición de pobreza, y vulnerabilidad.

Objetivos. Contribuir a la superación y prevención de la pobreza y la formación de capital humano, mediante el apoyo monetario directo a la familia beneficiaria.

Funciones. Entregar de manera eficiente y eficaz, un apoyo monetario directo a las familias del nivel 1 del SISBEN o a las familias desplazadas para mejorar la salud y la educación de los menores de 18 años, a cambio del cumplimiento de compromisos.

Funciones del Enlace Municipal.

Las principales funciones del EM son:

1. Participar en los procesos de inscripción de beneficiarios y apoyar toda la logística requerida.

2. Coordinar la convocatoria de madres titulares para la elección de las madres líderes y capacitar a las madres líderes en el diligenciamiento del Informe de Seguimiento Comunitario.

3. Capacitar a las madres líderes entre el primer y segundo pago en cuestiones como los compromisos adquiridos con el Programa, el diligenciamiento y entrega de formularios, la obtención de los pagos, los diversos mecanismos para la remisión de quejas y la atención a las charlas educativas (Esta actividad deben hacerse durante la misma reunión de elección de madre líder).

4. Disposición permanente para responder a las inquietudes tanto operativas como conceptuales que tenga la comunidad en general acerca del Programa.

5. Capacitar y dar asesoría permanente a las instituciones educativas y de salud del municipio sobre sus funciones en el Programa y velar porque las mismas cumplan con las funciones requeridas.

6. Actuar como intermediario en la recolección y envío de los formularios involucrados en los diferentes procesos.

7. Atender y dar trámite a reclamos y quejas presentadas por las madres titulares.

8. Promocionar el funcionamiento de las veedurías ciudadanas y/o otras instancias de participación ciudadana, para que éstas se involucren en el control social del Programa.

9. Atender cambios o novedades que presente la madre titular sobre la estructura familiar en el formulario NOV.

10. Hacer seguimiento a las propuestas de solución relacionadas al Programa y planteadas en el CMPS.

11. Diligenciar con la periodicidad establecida los informes de indicadores de seguimiento y monitoreo, diseñados por la Coordinación de Planeación y Seguimiento, y enviarlos a la UCR.

OFICINA DE CONTROL INTERNO

Misión. "Definir y evaluar en forma independiente y coordinada el Sistema de Control Interno, en las áreas Misionales y de apoyo, constatando que cada una de las Actividades cumplan Con los parámetros de Eficiencia, eficacia y economía, encaminando Sus esfuerzos hacia el logro de la calidad total en la gestión de la administración y teniendo como instrumento básico, la creación y el Fortalecimiento del AUTOCONTROL".

Objetivos

El Sistema de Control Interno es un instrumento que busca facilitar que la gestión administrativa de la entidades y organismos del Estado, en este orden de ideas a la Oficina de Control Interno como elemento asesor, evaluador y dinamizador del Sistema de Control Interno propende por el logro en el cumplimiento de la misión y los objetivos propuestos de acuerdo con la normatividad y políticas del Estado.

a) Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten.

b) Garantizar la eficacia, la eficiencia y economía en todas las operaciones, promoviendo y facilitando la correcta ejecución de las funciones y actividades definidas para el logro de la misión institucional.

c) Velar porque todas las actividades y recursos de la organización estén dirigidos al cumplimiento de los objetivos de la entidad.

d) Garantizar la correcta evaluación y seguimiento de la gestión organizacional.

e) Asegurar la oportunidad y confiabilidad de la información y de sus registros.

f) Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos.

g) Garantizar que el sistema de control Interno disponga de sus propios mecanismos de verificación y evaluación.

h) Velar porque la entidad disponga de procesos de planeación y mecanismos adecuados para el diseño y desarrollo organizacional, de acuerdo con su naturaleza y características.

Fundamentos Del Control Interno

Constituyen las condiciones imprescindibles y básicas que garantizan la efectividad del Control Interno de acuerdo con la naturaleza de las funciones y competencias asignadas por la Constitución y la ley a cada entidad pública y a las características que le son propias. La Autorregulación, el Autocontrol y la Autogestión son los pilares esenciales que garantizan el funcionamiento del Control Interno.

AUTORREGULACIÓN: Es la capacidad institucional de la Entidad Pública para reglamentar, con base en la Constitución y en la ley, los asuntos propios de su función y definir aquellas normas, políticas y procedimientos que permitan la coordinación efectiva y transparente de sus acciones. Mediante la Autorregulación la entidad adopta los principios, normas y procedimientos necesarios para la operación del Sistema de Control Interno. Favorece el Autocontrol al normalizar los patrones de comportamiento requeridos para el cumplimiento de los objetivos, y hace efectivo y transparente el ejercicio de su función constitucional ante la comunidad y los diferentes grupos de interés.

Se lleva a cabo, entre otras formas, a través de:

1. La promulgación de valores, principios y conductas éticas propias del servicio público.

2. La generación de Códigos de Buen Gobierno, que establece las normas que así mismas se imponen las entidades públicas para garantizar el cumplimiento de una función administrativa proba, eficiente y transparente.

3. La definición de un modelo de operación que armonice las leyes y las normas pertinentes a su fin, con los sistemas, los procesos, las actividades y las acciones necesarias para el cumplimiento de los propósitos institucionales.

4. El establecimiento de políticas, normas y controles tendientes a evitar o minimizar las causas y los efectos de los riesgos capaces de afectar el logro de los objetivos.

5. La reglamentación del Control Interno a través de los mecanismos proporcionados por la Constitución y la ley.

Metas

Proponer los lineamientos y directrices para el diseño y organización de un sistema de evaluación y control integral de gestión y resultados de la entidad.

Verificar y evaluar permanentemente el Sistema de Control Interno y recomendar las medidas de mejoramiento necesarias para el adecuado desarrollo de los objetivos, planes, programas y proyectos.

Diseñar y proponer los instrumentos de control asociados a cada una de las actividades de la entidad y propiciar su optimización permanente.

Velar por el cumplimiento de las leyes, planes, programas, proyectos de la entidad y recomendar los ajustes correspondientes.

Promover la formación de una cultura de autocontrol con el fin de contribuir al mejoramiento continuo de la gestión de la entidad.

Realizar las evaluaciones periódicas a la gestión del Municipio y elaborar los informes correspondientes a los entes de control.

Evaluar y verificar los mecanismos de participación ciudadana en los procesos de la entidad, de conformidad con la constitución y la ley.

Velar por que los controles identificados para el seguimiento de los procesos y actividades administrativas y técnicas de la entidad, sean aplicados por los responsables de cada área.

Verificar que el sistema de control interno sea intrínseco a desarrollo de las funciones de las dependencias y cargos de la entidad.

Asesorar en el proceso de análisis de las debilidades administrativas y técnicas planteadas por los órganos de control y en el diseño y concertación de las metas que deban incorporarse en los planes de mejoramiento respectivos.

OFICINA DEL ADULTO MAYOR

Misión. El Programa de Protección Social al Adulto Mayor es una iniciativa de asistencia social que consiste en un subsidio económico que es entregado en efectivo y en servicios sociales complementarios, en la modalidad directa, y en servicios sociales básicos y efectivos, en la modalidad indirecta.

Objetivos. Proteger al adulto mayor, que se encuentra en estado de indigencia o de extrema pobreza, contra el riesgo económico de la imposibilidad de generar ingresos y contra el riesgo derivado de la exclusión social.

Funciones

1. Coordinar la operación del programa.

2. Apoyar y prestar asesoría técnica para la adecuada implementación del programa.

3. Conocer y dar a conocer avances en atención a esta población en todo el municipio.

4. Participar y fortalecer el comité del adulto mayor.

5. Coordinar actividades que propendan por la inclusión social del Adulto Mayor.

OFICINA DEL SISBEN

Misión. El Sisbén comprende un conjunto de reglas, normas y procedimientos, que permiten obtener información socioeconómica confiable y actualizada de grupos específicos en los distritos y municipios del país.

Es una herramienta básica que facilita el diagnóstico socioeconómico preciso de determinados grupos de la población, se aplica a hogares no colectivos, y es muy útil para la elaboración del plan de desarrollo social de los municipios y la selección técnica, objetiva, uniforme y equitativa de beneficiarios para programas sociales, de acuerdo con su condición socioeconómica particular, representada mediante un indicador resumen de calidad de vida - índice Sisbén.

El índice refleja un puntaje de O a 100 para cada una de las familias. Una familia es más pobre cuanto más se acerca su puntaje a O y menos cuanto más se aproxima a 100.

Objetivos

Establecer un sistema de información oportuno y actualizado de la población vulnerable para acceder a los programas de beneficio social de orden nacional, departamental y municipal.

Permitir la elaboración de diagnósticos socioeconómicos precisos de la población pobre para apoyar los planes de desarrollo municipal, y el diseño y elaboración de programas concretos, orientados a los sectores de menores recursos o población vulnerable.

Contribuir al fortalecimiento institucional del municipio, mediante la puesta en marcha de un sistema moderno de información social confiable.

Facilitar la clasificación de los potenciales beneficiarios para programas sociales de manera rápida, objetiva, uniforme y equitativa.

Apoyar la coordinación interinstitucional municipal para mejorar el impacto del gasto social, eliminar duplicidades y facilitar el control tanto municipal, como de la sociedad y entidades que ejecutan programas sociales, posibilitando la asignación de recursos a los más pobres.

Facilitar la evaluación de las metas de focalización de los departamentos, distritos y municipios, y lucha contra la pobreza en el territorio colombiano

Funciones

Principales Funciones:

1. Actualizar, operar y administrar la base de datos del Sisbén.

2. Colaborar en la creación del comité técnico del Sisbén.

3. Cumplir con los procedimientos determinados por el comité técnico del Sisbén

4. Convocar el comité técnico del Sisbén cuando sea necesario.

5. Propiciar la participación de los organismos de control y vigilancia y de la comunidad.

6. Controlar el uso de la base en los programas sociales que involucran subsidios del orden municipal.

7. Instalación y configuración del software.

8. Entregar las bases de datos en las fechas establecidas bien sea al departamento o al DNP.

9. Realizar los procesos requeridos para la fase de demanda.

10. Hacer la labor administrativa que demanda el Sisbén.

SECRETARÍA DE GOBIERNO

Misión. Proporcionar las condiciones necesarias en procura del mejoramiento del bienestar y la calidad de vida de los habitantes del Municipio de Río de Oro, mediante la prestación oportuna, equitativa y eficiente de bienes, servicios y la elaboración y adopción de planes, programas y proyectos de desarrollo, al trabajo de los funcionarios de esta entidad del Estado.

Objetivos

1. Garantizar que las actividades desarrolladas por los funcionarios de la Administración Municipal, se realicen dentro del marco de la legalidad existente, atender los asuntos jurídicos y técnicos relacionados con la administración de personal, y velar por el cumplimiento de las normas legales, contractuales, o convencionales que regulan las relaciones del trabajo del municipio con sus servidores.

2. Coadyuvar en el logro de los objetivos a través de la presentación de apoyo logístico necesario como: La administración de bienes muebles, elementos de consumo y la información.

3. Dar recomendaciones a la Administración Municipal sobre el cumplimiento y puesta en marcha de las normas legales y acuerdos del Concejo Municipal.

4. Presentar iniciativas en materia de seguridad y administración de justicia, tendencias a prevenir, conservar y establecer el orden público, así como coordinar con los diferentes organismos municipales, departamentales y nacionales, todo lo relacionado con la materia.

5. Definir las directrices de los programas a desarrollar por las distintas dependencias que integran la secretaría, enmarcadas dentro del plan de desarrollo (programa de gobierno).

6. Determinar medidas que permitan ejercer un control a establecimientos públicos, así como a los precios, pesas y medidas.

7. Tramitar oportunamente los procesos, diligenciar los exhortos y demás asuntos que sean de su competencia.

8. Proteger los recursos del municipio, buscando su adecuada administración ante posibles riesgos que le afecten.

9. Garantizar la eficiencia, la eficacia y economía en todas las operaciones y actividades definidas para el logro de la misión institucional.

10. Velar porque todas las actividades y recursos de la organización estén dirigidos al cumplimiento de los objetivos del municipio.

11. Garantizar la correcta evaluación y seguimiento de la gestión organizacional.

12. Asegurar la oportunidad y confiabilidad de la información y sus registros.

13. Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos.

14. Garantizar que el sistema de control interno disponga de sus propios mecanismos de verificación y evaluación.

15. Velar porque la entidad disponga de procesos de planeación y mecanismos adecuados para el diseño y desarrollo organizacional, de acuerdo con su naturaleza y características.

16. Realizar los planes mensuales de compra de elementos devolutivos y de consumo que se requieran para el normal funcionamiento de la administración, todo esto de conformidad con la reglamentación que se expida sobre los procesos y procedimientos a seguir.

17. Velar por el cumplimiento del sistema de contratación establecido en la ley 80 de 1993 y sus decretos reglamentarios.

Funciones

1. Determinar las políticas hacer adoptadas por la administración municipal, tendientes a la conservación y restablecimiento al orden- público y ` control a establecimientos públicos, como también para precios, pesas y medidas.

2. Asesorar a la administración municipal en el aspecto jurídico y, tramitar de acuerdo con los reglamentos y disposiciones legales vigentes, los procesos que le sean requeridos. Como también orientar a la comunidad en las consultas realizadas por ellas.

3. Ejercer en el municipio las funciones de control interno en las diferentes dependencias a fin de garantizar la adecuada aplicación de los procesos y procedimientos previamente establecidos.

4. Evaluar la eficiencia, eficacia y economía de los demás controles, asesorando

al Alcalde Municipal en la continuidad del proceso administrativo, la reevaluación de los planes establecidos y en la introducción de los correctivos necesarios para el cumplimiento en las metas u objetivos previstos.

Metas

Garantizar que los servicios prestados por la Secretaria de Gobierno se realicen de manera objetiva, equitativa y transparente.

Implementar y garantizar canales de comunicación efectivos para desarrollar un trabajo en equipo con la comunidad.

Desarrollar una cultura de mejora continua que garantice el sostenimiento y desarrollo del sistema de gestión de la calidad.

Ejecutar eficientemente el Plan de Desarrollo en lo que respecta a Convivencia ciudadana, movilidad, seguridad, orden público, espacio público, y violencia familiar.

Establecer las políticas necesarias para cumplir los fines misionales. Acatamiento de los procedimientos para el sistema de evaluación de desempeño y el cumplimiento efectivo de la rendición de cuentas a la sociedad sobre la gestión de la Secretaría de Gobierno y sus resultados.

Mantenerse informado del desarrollo de los actos delegados, impartir orientaciones generales sobre el ejercicio de las funciones entregadas y establecer sistema de control y evaluación periódica de las mismas.

SECRETARÍA DE HACIENDA

Misión. La misión de la Secretaría de Hacienda, es desarrollar una política fiscal responsable del Municipio, para asegurar la financiación de los programas y proyectos de inversión pública contenidos en el Plan de Desarrollo y los gastos autorizados para el normal funcionamiento de la Administración y el cumplimiento oportuno de las obligaciones contraídas por el Municipio y la rendición de informes a los entes de Control.

Objetivos

Objetivo General. Garantizar la óptima gestión de los recursos y el registro ordenado, sistemático y claro de las operaciones de gasto público.

Funciones

Funciones Generales. Son funciones de la Secretaría de Hacienda, las siguientes:

1. Planificar y determinar las políticas de liquidación y fiscalización de las rentas municipales.

2. Gestionar la obtención de los recursos de crédito interno y externo que requiera el municipio.

3. Dirigir la elaboración del presupuesto y plan anual de inversión del Municipio en coordinación con el Departamento Administrativo de Planeación Municipal y demás Secretarías de Despacho.

4. Liderar los procesos de recaudo y administración de los recursos financieros.

5. Dirigir y controlar la aplicación de las normas y procedimientos contables, fiscales, presupuéstales y de tesorería.

6. Programar y dirigir en coordinación con el Departamento Administrativo de Planeación Municipal y demás dependencias, la formulación de los proyectos del Presupuesto General del Municipio de acuerdo con lo estipulado en las normas vigentes.

7. Responder por el control de la deuda pública contraída por el Municipio.

8. Establecer los mecanismos de cobro coactivo a los contribuyentes de acuerdo con la normatividad legal establecida para ello.

9. Dirigir la elaboración oportuna de los estados financieros del Municipio de Neiva.

10. Presentar y realizar seguimiento a los proyectos de Acuerdo, Decretos y demás actos administrativos que modifiquen el presupuesto municipal.

11. Realizar Gestión de seguimiento y control al Presupuesto Municipal.

12. Coordinar y controlar la elaboración del plan financiero y someterlo a consideración de las instancias correspondientes.

13. Trazar las directrices para la adecuada conservación y protección de los títulos valores y demás bienes monetarios de propiedad del municipio.

Metas. Garantizar la eficiente y oportuna gestión de recaudo de los ingresos, la custodia y cancelación del gasto público; la política de financiación de los programas y proyectos que componen el Plan de Desarrollo “MOMENTO PARA LA PROSPERIDAD 2012-2015”, y el registro, consolidación, buen manejo y rendición de informes de la hacienda pública municipal.

SECRETARÍA DE PLANEACIÓN

Misión. Planear el desarrollo integral del municipio de Río de Oro, mediante la aplicación del conocimiento técnico, científico y tecnológico en la formulación, evaluación, seguimiento y retroalimentación de planes, programas y proyectos, fundamentados en la participación social, el respeto, la equidad, la transparencia y la efectividad.

Objetivos

Realizar estudios necesarios para la elaboración de planes, programas y proyectos específicos de desarrollo.

Producir referencias de conveniencia técnica y económica de proyectos para el municipio.

Preparar y proponer sistemas sobre organización y métodos para mejorar y hacer más eficiente el funcionamiento de la gestión administrativa.

Funciones

Descripción De Las Funciones Esenciales

1. Ejercer bajo su propia responsabilidad las funciones que competen a la oficina de planeación municipal y vigilar el cumplimiento de las atribuciones, asignar a los funcionarios de sus dependencias.

2. Asesorar al Alcalde Municipal en la elaboración y adopción de los planes de desarrollo urbano, económico y social, los programas de inversiones públicas municipal y asesorar a los Secretarios en la elaboración de los proyectos respectivos.

3. Preparar, con la colaboración de la Secretaría de Hacienda Municipal, los programas de inversiones públicas, con sujeción a las prioridades identificadas en el plan, definiendo los recursos financieros y las entidades que participen en la ejecución.

4. Adelantar estudios o evaluar estudios específicos de factibilidad técnica, urbana, cultural de servicios públicos. Obras públicas, tendientes a promover el desarrollo municipal.

5. Velar por el mantenimiento, la interventoría y el seguimiento de las obras públicas que se adelanten en el Municipio.

6. Elaborar los prepliegos, pliegos de condiciones, los estudios y cuadros comparativos necesarios para adelantar los procesos de contratación municipal.

7. Inspeccionar y regular el desarrollo urbanístico del municipio, mediante la aplicación de las normas establecidas en la ley o en el EOT y los acuerdos municipales.

8. Definir, diseñar y asesorar los procedimientos relacionados con prevención y atención de emergencias y desastres en el municipio, mediante la participación activa de la comunidad y el compromiso interinstitucional.

9. Coordinar y administrar el SISBEN y su base de datos, así como el programa de sistemas de selección de beneficiarios APRA programas sociales SISBEN del municipio de Río de Oro.

10. Las demás funciones que le sean asignadas por la autoridad competente y que estén acorde con la naturaleza del despacho.

Metas. Lograr que el municipio de Río de oro avance permanente y coordinadamente por un camino claramente planeado y establecido con visión prospectiva del desarrollo y el progreso, que lo conduzca a unas condiciones de vida, socio-económicas y ambientales, cada vez mejores, enmarcadas dentro de un proceso de desarrollo humano sostenible.

Programas y proyectos

Proyectos

"Mantenimiento De La Cancha De Futbol Municipal Del Municipio De Río De Oro, Cesar Año 2012".

SECRETARÍA DE SALUD

Misión. Garantizar la Dirección, coordinación, vigilancia del sector salud y el cumplimiento del servicio público en salud según la normatividad vigente ,adoptando la Estrategia de Atención Primaria en Salud para la coordinación intersectorial que permita la atención integral e integrada, desde la salud pública, la promoción de la salud, la prevención de la enfermedad, el diagnóstico, el tratamiento, la rehabilitación del paciente sangileño a fin de garantizar el mejoramiento de la salud en los sectores más vulnerables y marginados

Objetivos. Garantizar el acceso de la población del Municipio al Sistema General de Seguridad Social en Salud y a la Salud Pública.

Funciones. Son funciones de la Secretaría de Salud, las siguientes:

1. Formular, ejecutar y evaluar, programas y proyectos en salud, en armonía con las políticas y disposiciones del orden nacional y departamental.

2. Gestionar el recaudo, flujo y ejecución de los recursos con destinación específica para salud del municipio, y administrar los recursos del Fondo Local de Salud.

3. Gestionar y supervisar el acceso a la prestación de los servicios de salud para la población de la jurisdicción.

4. Impulsar mecanismos para la adecuada participación social y el ejercicio pleno de los deberes y derechos de los ciudadanos en materia de salud y de seguridad social en salud.

5. Adoptar, administrar e implementar el sistema integral de información en salud, así como generar y reportar la información requerida por el Sistema.

6. Promover planes, programas, estrategias y proyectos en salud y seguridad social en salud, para su inclusión en los planes y programas departamentales y nacionales.

7. Financiar y cofinanciar la afiliación al Régimen Subsidiado de la población pobre y vulnerable y ejecutar eficientemente los recursos destinados a tal fin.

8. Identificar a la población pobre y vulnerable en la jurisdicción y seleccionar a los beneficiarios del Régimen Subsidiado, atendiendo las disposiciones que regulan la materia.

9. Celebrar contratos para el aseguramiento en el Régimen Subsidiado de la población pobre y vulnerable, y realizar el seguimiento y control directamente o por medio de interventorías.

10. Promover en la jurisdicción la afiliación al Régimen Contributivo del Sistema General de Seguridad Social en Salud de las personas con capacidad de pago y evitar la evasión y elusión de aportes.

11. Adoptar, implementar y adaptar las políticas y planes en salud pública de conformidad con las disposiciones del orden nacional y departamental, así como formular, ejecutar y evaluar el Plan Municipal de Salud de Acciones Colectivas.

12. Monitorear, evaluar, y analizar la situación de salud en el municipio y propender por el mejoramiento de las condiciones determinantes de dicha situación. De igual forma, promover la coordinación, cooperación e integración funcional de los diferentes sectores para la formulación y ejecución de los planes, programas y proyectos en salud pública en su ámbito territorial.

Metas

Mejorar la salud infantil.

Mejorar la salud sexual y reproductiva.

Mejorar la salud mental y las lesiones violentas evitables .

Disminuir las enfermedades transmisibles y la zoonosis.

Mejorar la situación nutricional.

Mejorar la seguridad sanitaria y ambiental.

SUPERVISIÓN DE OBRAS

Objetivos

Comprobar, constatar el cumplimiento de las obras en ejecución, teniendo en cuenta las normas, específicamente técnicas, contenidos, cualidades y demás detalles consignados en los documentos contractuales.

Informar de inmediato al superior de las novedades que se presenten durante la ejecución de las obras.

Funciones

1. Prever los requerimientos urbanísticos, servicios públicos, obras públicas y servicios comunitarios para atender la expansión de los recursos urbanos.

2. Coordinar y contralor las acciones del municipio con el sector privado y demás participantes en el desarrollo, para la ejecución de obras, el recibo de áreas de sesión.

3. Coordinar y controlar las intervenciones de los sectores públicos y privados para la conformación, protección y uso del espacio público.

4. Llevar el registro de las personas naturales y jurídicas que se dediquen a las actividades contempladas en la ley 66/1968 y el decreto 2610/1979.

5. Coordinar y controlar la reglamentación de la construcción y el desarrollo de programas habitacionales conforme a la normatividad vigente.

6. Y las demás que le asigne el jefe superior.

ANEXO F: INVENTARIO DE EQUIPOS DE CÓMPUTO DE LA ALCALDÍA DEL MUNICIPIO DE RÍO DE ORO, CESAR

- Equipos de Cómputo (de Escritorio) de la Alcaldía Municipal y sus Características:

EQUIPO	CARACTERISTICAS	
PC DE ESCRITORIO Inspector (Secretaría De Planeación)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	LG
	Fecha Adquisición	Noviembre de 2013
	Pantalla	19 Pulgadas
	CPU	
	Color	Negro
	Procesador	Core 7
	RAM	4 GB
	Disco Duro	1 Tera
	SOFTWARE	
	Sistema Operativo	Windows 8 (con licencia)
	"SW Especifico"	**Ninguno**
PC DE ESCRITORIO Arquitecto (Secretaría De Planeación)	**HARDWARE**	
	Modelo	Presario CQ1
	Fabricante	COMPAQ
	Fecha Adquisición	**Indefinida**
	Pantalla	19 Pulgadas
	CPU	
	Color	Negro
	Procesador	2 en 1
	RAM	2 GB
	Disco Duro	500 MB
	SOFTWARE	
	Sistema Operativo	Windows 7 (con licencia)
	"SW Especifico"	**Ninguno**
PC DE ESCRITORIO Coordinador De Gestión Del Banco De Proyectos (Secretaría De Planeación)	**HARDWARE**	
	Modelo	Presario CQ1
	Fabricante	COMPAQ
	Fecha Adquisición	**Indefinida**
	Pantalla	19 Pulgadas
	CPU	
	Color	Negro
	Procesador	2 en 1
	RAM	2 GB
	Disco Duro	500 MB
	SOFTWARE	
	Sistema Operativo	Windows 7 (con licencia)
	"SW Especifico"	**Ninguno**

PC DE ESCRITORIO **Inspector De Obras** (Secretaría De Planeación)	**HARDWARE**	
	Modelo	**indefinido**
	Fabricante	LG
	Fecha Adquisición	Noviembre de 2013
	Pantalla	19 Pulgadas
	CPU	
	Color	Negro
	Procesador	Core 7
	RAM	4 GB
	Disco Duro	1 Tera
	SOFTWARE	
	Sistema Operativo	Windows 8 (con licencia)
	“SW Especifico”	Ninguno
PC DE ESCRITORIO **Secretaria** (Secretaría De Planeación)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	AOC
	Fecha Adquisición	**indefinida**
	Pantalla	Monitor AUC, 18 Pulgadas
	CPU	Camex
	Color	Negro
	Procesador	MD Centro 1800
	RAM	1024 MB
	Disco Duro	250 MB
	SOFTWARE	
	Sistema Operativo	Windows 7
	“SW Especifico”	**Ninguno**
PC DE ESCRITORIO **Secretaria De Apoyo** (Secretaría De Salud)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	Hacer
	Fecha Adquisición	**Indefinida**
	Pantalla	Monitor Acer, 19 Pulgadas
	CPU	Delux
	Color	Negro
	Procesador	AMD Admin
	RAM	2 GB
	Disco Duro	80 MB
	SOFTWARE	
	Sistema Operativo	Windows XP
	“SW Especifico”	**Ninguno**
PC DE ESCRITORIO **Coordinador SAC**	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	LG
	Fecha Adquisición	**Indefinida**
	Pantalla	19 Pulgadas
	CPU	**Indefinida**
	Color	Negro
	Procesador	Intel Celeron 2.6 GHZ

(Secretaría De Salud)	**RAM**	4 GB
	Disco Duro	350 GB
	SOFTWARE	
	Sistema Operativo	Windows 7 (con Licencia)
	"SW Especifico"	**Ninguno**
PC DE ESCRITORIO **Secretaria Ejecutiva** (Secretaría De Hacienda)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	LENOVO
	Fecha Adquisición	**Indefinida**
	Pantalla	21 Pulgadas
	CPU	
	Color	Negro
	Procesador	Core 3
	RAM	4 GB
	Disco Duro	1 Tera
	SOFTWARE	
	Sistema Operativo	Windows 7 (con Licencia)
	"SW Especifico"	Visual TNS
PC DE ESCRITORIO **Coordinador De Rentas** (Secretaría De Hacienda)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	SAMSUNG
	Fecha Adquisición	**Indefinida**
	Pantalla	18 Pulgadas
	CPU	
	Color	Negro
	Procesador	Core 7 340 GHZ
	RAM	6 GB
	Disco Duro	1 Tera
	SOFTWARE	
	Sistema Operativo	Windows 7 (con Licencia)
	"SW Especifico"	Neptuno
PC DE ESCRITORIO **Auxiliar De Tesorería** (Secretaría De Hacienda)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	COMPAQ
	Fecha Adquisición	**Indefinida**
	Pantalla	14 Pulgadas, Convencional
	CPU	
	Color	Negro y Gris
	Procesador	Intel
	RAM	2 GB
	Disco Duro	80
	SOFTWARE	
	Sistema Operativo	Windows XP
	"SW Especifico"	**Ninguno**
	HARDWARE	
	Modelo	AMD FX (TM) 8120
	Fabricante	AOC

PC DE ESCRITORIO Contador (Secretaría De Hacienda)	**Fecha Adquisición**	**Indefinida**
	Pantalla	19 Pulgadas
	CPU	
	Color	Negro
	Procesador	Core 7, con 8 nucleos
	RAM	4 GB
	Disco Duro	1 Tera
	SOFTWARE	
	Sistema Operativo	Windows 8 (con Licencia)
	"SW Especifico"	Visual TNS
PC DE ESCRITORIO PASIBOCOL (Secretaría De Hacienda)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	SAMSUNG
	Fecha Adquisición	**Indefinida**
	Pantalla	19 Pulgadas
	CPU	DELUX
	Color	Negro
	Procesador	AMD Admin
	RAM	2 GB
	Disco Duro	80
	SOFTWARE	
	Sistema Operativo	Windows 7
	"SW Especifico"	**Ninguno**
PC DE ESCRITORIO Tesorero (Secretaría De Hacienda)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	SAMSUNG
	Fecha Adquisición	**Indefinida**
	Pantalla	18 Pulgadas
	CPU	
	Color	Negro
	Procesador	AMD Dual Core
	RAM	2 GB
	Disco Duro	250
	SOFTWARE	
	Sistema Operativo	Windows 7
	"SW Especifico"	Visual TNS
PC DE ESCRITORIO (Todo En Uno) Secretaria Ejecutiva (Despacho Del Alcalde)	**HARDWARE**	
	Modelo	Presario CQ1
	Fabricante	COMPAQ
	Fecha Adquisición	**Indefinida**
	Pantalla	18,5 Pulgadas
	CPU	
	Color	Negro
	Procesador	Intel Atom 1,66 GHZ, 2 en 1
	RAM	2 GB
	Disco Duro	500
	SOFTWARE	

	Sistema Operativo	Windows 7 (con Licencia)
	"SW Especifico"	**Ninguno**
PC DE ESCRITORIO **Secretario De Gobierno** (Secretaría De Gobierno)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	ACER
	Fecha Adquisición	**Indefinida**
	Pantalla	18 Pulgadas
	CPU	LG
	Color	Negro
	Procesador	AMD 2,01
	RAM	1 GB
	Disco Duro	240
	SOFTWARE	
	Sistema Operativo	Windows XP
	"SW Especifico"	**Ninguno**
PC DE ESCRITORIO **Coordinador Del SISBEN** (Oficina Del SISBEN)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	JANUS
	Fecha Adquisición	**Indefinida**
	Pantalla	21 Pulgadas
	CPU	JANUS
	Color	Negro
	Procesador	Pentium Dual Core
	RAM	4 GB
	Disco Duro	1 Tera
	SOFTWARE	
	Sistema Operativo	Windows 7
	"SW Especifico"	**Ninguno**
PC DE ESCRITORIO **(Todo En Uno)** **Coordinador Adulto Mayor - Victimas** (Oficina Del SISBEN – Adulto Mayor)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	LENOVO
	Fecha Adquisición	**Indefinida**
	Pantalla	21 Pulgadas
	CPU	
	Color	Negro
	Procesador	Intel Atom 1,8 GHZ
	RAM	6 GB
	Disco Duro	500
	SOFTWARE	
	Sistema Operativo	Windows 7 (con Licencia)
	"SW Especifico"	**Ninguno**
	HARDWARE	
	Modelo	**Indefinido**
	Fabricante	LENOVO
	Fecha Adquisición	**Indefinida**
	Pantalla	21 Pulgadas

PC DE ESCRITORIO Secretario Adulto Mayor (Oficina Del SISBEN – Adulto Mayor)	**CPU**	**Indefinido**
	Color	Negro
	Procesador	Core 3, 3,1 GHZ
	RAM	4 GB
	Disco Duro	1 Tera
	SOFTWARE	
	Sistema Operativo	Windows 7 (con Licencia)
	"SW Especifico"	**Ninguno**
PC DE ESCRITORIO Aux. Administrativo Más Familias En Acción (Oficina Enlace Municipal)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	JANUS
	Fecha Adquisición	**Indefinida**
	Pantalla	19 Pulgadas
	CPU	JANUS
	Color	Negro
	Procesador	Dual Core
	RAM	3 GB
	Disco Duro	1 Tera
	SOFTWARE	
	Sistema Operativo	Windows XP
	"SW Especifico"	**Ninguno**
PC DE ESCRITORIO Secretaria Más Familias En Acción (Oficina Enlace Municipal)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	JANUS
	Fecha Adquisición	**Indefinida**
	Pantalla	19 Pulgadas
	CPU	JANUS
	Color	Negro
	Procesador	Dual Core
	RAM	3 GB
	Disco Duro	1 Tera
	SOFTWARE	
	Sistema Operativo	Windows XP
	"SW Especifico"	**Ninguno**
PC DE ESCRITORIO Inspectora (Inspección De Policía)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	COMPAQ
	Fecha Adquisición	**Indefinida**
	Pantalla	14 Pulgadas, Convencional
	CPU	**Indefinida**
	Color	Negro y Gris
	Procesador	Pentium 4, 2,8 GHZ
	RAM	240

	Disco Duro	80
	SOFTWARE	
	Sistema Operativo	Windows XP
	"SW Especifico"	**Ninguno**
PC DE ESCRITORIO Comisaria De Familia (Comisaría De Familia)	**HARDWARE**	
	Modelo	**Indefinido**
	Fabricante	SAMSUNG
	Fecha Adquisición	**Indefinida**
	Pantalla	18 Pulgadas
	CPU	SAMSUNG
	Color	Negro
	Procesador	Intel Celron 1,66 GHZ
	RAM	1 GB
	Disco Duro	240
	SOFTWARE	
	Sistema Operativo	Windows 7
	"SW Especifico"	**Ninguno**

- Equipos de Cómputo (Portátil) de la Alcaldía Municipal y sus Características.

EQUIPO	CARACTERISTICAS	
PORTÁTIL Secretaria De Salud (Secretaría De Salud)	**HARDWARE**	
	Fabricante	ACER
	Pantalla	14 Pulgadas
	Color	Negro
	Procesador	Core 5
	RAM	4 GB
	Disco Duro	750 MB
	SOFTWARE	
	Sistema Operativo	Windows 8
PORTÁTIL Coordinador De Discapacidad (Secretaría De Salud)	**HARDWARE**	
	Fabricante	ACER
	Pantalla	14 Pulgadas
	Color	Negro
	Procesador	Core 5
	RAM	4 GB
	Disco Duro	700
	SOFTWARE	
	Sistema Operativo	Windows 8
PORTÁTIL Coordinador De Salud	**HARDWARE**	
	Fabricante	LENOVO
	Pantalla	14 Pulgadas
	Color	Negro

Pública (Secretaría De Salud)	**Procesador**	Core 5
	RAM	4 GB
	Disco Duro	500
	SOFTWARE	
	Sistema Operativo	Windows 8
PORTÁTIL Secretaria SISBEN (Oficina SISBEN)	**HARDWARE**	
	Fabricante	COMPAQ
	Pantalla	14 Pulgadas
	Color	Negro
	Procesador	Intel 2,0 GHZ
	RAM	1 GB
	Disco Duro	120
	SOFTWARE	
	Sistema Operativo	Windows 7

ANEXO G: INVENTARIO DE EQUIPOS DE OFICINA DE LA ALCALDÍA DEL MUNICIPIO DE RÍO DE ORO, CESAR

EQUIPO	CARACTERISTICAS	
IMPRESORA Coordinador De Gestión Del Banco De Proyectos (Secretaría De Planeación)	**GENERALES**	
	Modelo	Multifuncional f4-180
	Fabricante	HP
	Fecha Adquisición	Noviembre de 2013
	Color	Negro
IMPRESORA Secretaria (Secretaría De Planeación)	**GENERALES**	
	Modelo	Multifuncional L210
	Fabricante	Epson
	Fecha Adquisición	Noviembre de 2013
	Color	Negro
IMPRESORA (Secretaría De Salud)	**GENERALES**	
	Modelo	Multifuncional L210
	Fabricante	Epson
	Fecha Adquisición	**Indefinida**
	Color	Negro
IMPRESORA Secretaria Ejecutiva (Secretaría De Hacienda)	**GENERALES**	
	Modelo	Multifuncional L210
	Fabricante	Epson
	Fecha Adquisición	**Indefinida**
	Color	Negro
IMPRESORA Coordinador De Rentas (Secretaría De Hacienda)	**GENERALES**	
	Modelo	Laser 1102
	Fabricante	HP
	Fecha Adquisición	**Indefinida**

	Color	Negro
IMPRESORA Auxiliar De Tesorería (Secretaría De Hacienda)	**GENERALES**	
	Modelo	Cinta LX-300X
	Fabricante	Epson
	Fecha Adquisición	**Indefinida**
	Color	Blanco
IMPRESORA Secretaria Ejecutiva (Despacho Del Alcalde)	**GENERALES**	
	Modelo	Laser 1120
	Fabricante	HP
	Fecha Adquisición	**Indefinida**
	Color	Negro
IMPRESORA Secretario De Gobierno (Secretaría De Gobierno)	**GENERALES**	
	Modelo	Laser 1102
	Fabricante	HP
	Fecha Adquisición	**Indefinida**
	Color	Negro
IMPRESORA Coordinador Del Adulto Mayor (Oficina Del SISBEN – Adulto Mayor)	**GENERALES**	
	Modelo	Multifuncional L210
	Fabricante	Epson
	Fecha Adquisición	**Indefinida**
	Color	Negro
IMPRESORA (Enlace Municipal)	**GENERALES**	
	Modelo	Multifuncional L210
	Fabricante	Epson
	Fecha Adquisición	**Indefinida**
	Color	Negro
IMPRESORA Inspectora De Policía (Inspección De Policía)	**GENERALES**	
	Modelo	Laser ML-2240
	Fabricante	Samsung
	Fecha Adquisición	**Indefinida**
	Color	Gris
IMPRESORA Comisaria De Familia (Comisaría De Familia)	**GENERALES**	
	Modelo	Laser 1010
	Fabricante	HP
	Fecha Adquisición	**Indefinida**
	Color	Negro y Gris
FAX Inspector De Obras (Secretaría De Planeación)	**GENERALES**	
	Modelo	KX-FT937
	Fabricante	Panasonic
	Fecha Adquisición	**Indefinida**
	Color	Negro
FAX	**GENERALES**	
	Modelo	KX-FT77

Secretaria Ejecutiva (Secretaría De Hacienda)	**Fabricante**	Panasonic
	Fecha Adquisición	**Indefinida**
	Color	Negro
FAX Secretaria Ejecutiva (Despacho Del Alcalde)	**GENERALES**	
	Modelo	KX-FT981
	Fabricante	Panasonic
	Fecha Adquisición	**Indefinida**
	Color	Negro
TELEFONO Tesorero (Secretaría De Hacienda)	**GENERALES**	
	Modelo	**Indefinido**
	Fabricante	Panasonic
	Fecha Adquisición	**Indefinida**
	Color	Negro
PLOTER Secretario De Planeación Y Arquitecto (Secretaría De Planeación)	**GENERALES**	
	Modelo	DesingYeg T120
	Fabricante	HP
	Fecha Adquisición	Noviembre de 2013
	Color	Negro
	Serial	cn2cq1m04x
ESCANER Inspector De Obras (Secretaría De Planeación)	**GENERALES**	
	Modelo	Automático 5590
	Fabricante	HP
	Fecha Adquisición	**Indefinida**
	Color	Negro
ESCANER Secretaria Ejecutiva (Despacho Del Alcalde)	**GENERALES**	
	Modelo	ScanJet G2410
	Fabricante	HP
	Fecha Adquisición	**Indefinida**
	Color	Blanco y Gris

ANEXO H: INVENTARIO DE DISPOSITIVOS DE COMUNICACIONES DE LA ALCALDÍA DEL MUNICIPIO DE RÍO DE ORO, CESAR

DISPOSITIVO	CARACTERISTICAS	
SERVIDOR Secretaría de Hacienda	**Especificas**	x3100 M4, Xeon 4C E3-1220 80W 3.1GHz/1333MHz/8MB, 1x2GB, O/Bay SS 3.5in SATA, SR C100, DVD-ROM, 350W p/s, Tower + 1 DD 500G SATA 39M4514 - 1 año de garantía
	Licencia	WINSOWS SERVER 2008

SWITCH Secretaría de Hacienda	**GENERALES**	
	Fabricante	Encore
	Puertos	8 puertos 10/100/1000 Mbps
	Protocolo de Gestión Remota	
	Voltaje Necesario	12V DC - 1.0 Amperios
	Consumo Eléctrico	
SWITCH Secretaría de Planeación	**GENERALES**	
	Fabricante	Encore
	Puertos	16 puertos 10/100/1000 Mbsps
	Protocolo de Gestión Remota	IEEE 802.3 10Base-T; IEEE 802.3u 100Base-TX IEEE 802.3ab 1000Base-T; IEEE 802.3x control de flujo Total Dúplex
	Voltaje Necesario	100~240V 50/60Hz
	Consumo Eléctrico	19 W
ROUTER Secretaría de Salud y Hacienda, oficina de Asesores, Inspección de Policía y Despacho del Alcalde.	**GENERALES**	
	Modelo	WR 740 N
	Fabricante	Tepelink
	TECNICAS	
	Puertos	5 puertos
	Interfaces WAN	1 puerto 10/100 Mbps
	Interfaces LAN	4 puertos 10/100 Mbsps
ROUTER Oficina del SISBEN y Victimas	**GENERALES**	
	Modelo	**WR 840 N**
	Fabricante	**Tepelink**
	TECNICAS	
	Puertos	**5 puertos**
	Interfaces WAN	**1 puerto 10/100 Mbps**
	Interfaces LAN	**4 puertos 10/100 Mbsps**

ANEXO I: INVENTARIO DE SISTEMAS OPERATIVOS DE LA ALCALDÍA DEL MUNICIPIO DE RÍO DE ORO, CESAR

SISTEMA OPERATIVO	CARACTERISTICAS	
WINDOWS	**GENERALES**	
	Versión	7
	Fabricante	MICROSOFT
	N° de Licencias	
WINDOWS	**GENERALES**	
	Versión	8
	Fabricante	MICROSOFT

	N° de Licencias	
WINDOWS	**GENERALES**	
	Versión	XP
	Fabricante	MICROSOFT
	N° de Licencias	

ANEXO J: INVENTARIO DE SOFTWARE EMPRESARIAL DE LA ALCALDÍA DEL MUNICIPIO DE RÍO DE ORO, CESAR

SOFTWARE EMPRESARIAL	CARACTERISTICAS	
Visual TNS	**GENERALES**	
	Fabricante	TNS S.A.S.
	Descripción	Sistema contable y administrativo integrado Visual TNS - Oficial
	Módulos	Contabilidad, Presupuesto y Tesorería
	Fecha Adquisición	Enero 30 de 2014
	Licencia	Sí
	N° de Licencias	3
	Dependencia	Secretaría de Hacienda
	Responsable	Secretaria Ejecutiva, Contador y Tesorero.
NEPTUNO PREDIAL	**GENERALES**	
	Fabricante	MICROSHIF S.A.S.
	Descripción	Software para la facturación y gestión del impuesto predial incluyendo el módulo de cobro coactivo.
	Módulos	Facturación, Gestión del Impuesto Predial y Cobro Coactivo.
	Fecha Adquisición	Diciembre de 2013
	Licencia	Sí
	N° de Licencias	1
	Dependencia	Secretaría de Hacienda
	Responsable	Coordinador de Rentas

ANEXO K: INVENTARIO DE BIENES MUEBLES E INMUEBLES DE LA ALCALDÍA DEL MUNICIPIO DE RÍO DE ORO, CESAR

ID	NOMBRE	DETALLE	DEPENDENCIA	PERSONA A CARGO	SERIAL
1	Mueble	Mueble Marrón	Despacho Del Alcalde	Nerys Amparo Martínez	000
2	Mueble	Mueble Marrón	Despacho Del Alcalde	Nerys Amparo Martínez	000
3	Mueble	Mueble Azul	Despacho Del Alcalde	Nerys Amparo Martínez	000
4	Mueble	Mueble Marrón 2	Despacho Del Alcalde	Nerys Amparo Martínez	000
5	Árbol	Árbol De Navidad	Despacho Del Alcalde	Nerys Amparo Martínez	000
6	Meza	Meza Pequeña 2 Puestos	Despacho Del Alcalde	Nerys Amparo Martínez	000
7	Mueble	Mueble Verde 1	Despacho Del Alcalde	Nerys Amparo Martínez	000
8	Mueble	Mueble Verde 2	Despacho Del Alcalde	Nerys Amparo Martínez	000
9	Escritorio	Escritorio	Despacho Del Alcalde	Nerys Amparo Martínez	000
10	Computador	Todo En Uno	Despacho Del Alcalde	Nerys Amparo Martínez	00194898278133
11	Impresora	Impresora Hp	Despacho Del Alcalde	Nerys Amparo Martínez	Vnb3q88291
12	Teléfono	Telefax	Despacho Del Alcalde	Nerys Amparo Martínez	8j0cwa024826
13	Grapadora	Grapadora Azul Con Gris	Despacho Del Alcalde	Nerys Amparo Martínez	000
14	Perforadora	Perforadora Negra	Despacho Del Alcalde	Nerys Amparo Martínez	000
15	Almohadilla	Almohadilla Del Sello	Despacho Del Alcalde	Nerys Amparo Martínez	000
16	Fechador	Fechador Gris Con Rojo	Despacho Del Alcalde	Nerys Amparo Martínez	000
17	Planta	Planta Panasonic	Despacho Del Alcalde	Nerys Amparo Martínez	3javd016932
18	Modem	Modem De Internet Blanco	Despacho Del Alcalde	Nerys Amparo Martínez	F8d1112ccd60
19	Silla	Silla De Oficina Azul	Despacho Del Alcalde	Nerys Amparo Martínez	000
20	Caneca	Caneca De La Basura	Despacho Del Alcalde	Nerys Amparo Martínez	000
21	Escritorio	Escritorio Dos	Despacho Del Alcalde	Nerys Amparo Martínez	000
22	Escritorio	Escritorio Del Gobierno	Secretaria De Gobierno	Nerys Amparo Martínez	000
22	Archivador	Archivador Marrón	Despacho Del Alcalde	Nerys Amparo Martínez	000

23	Silla	Silla De Oficina Negra	Secretaria De Gobierno	Nerys Amparo Martínez	000
24	Silla	Silla De Oficina Beis	Secretaria De Gobierno	Nerys Amparo Martínez	000
25	Silla	Silla De Oficina Beis	Secretaria De Gobierno	Nerys Amparo Martínez	000
26	Computador	Computador ACER Negro	Secretaria De Gobierno	Nerys Amparo Martínez	81090100240
27	Impresora	Impresora Negra Hp	Secretaria De Gobierno	Nerys Amparo Martínez	Vnb3x21650
28	CPU	CPU LG	Secretaria De Gobierno	Nerys Amparo Martínez	027070001805
29	Teléfono	Teléfono Fijo	Secretaria De Gobierno	Nerys Amparo Martínez	Ex29252ge2a
30	Estabilizador	Estabilizador Negro	Secretaria De Gobierno	Nerys Amparo Martínez	000
31	Cuadro	Cuadro	Secretaria De Gobierno	Nerys Amparo Martínez	000
32	Cuadro	Cuadro	Secretaria De Gobierno	Nerys Amparo Martínez	000
33	Silla	Silla RIMAX	Secretaria De Gobierno	Nerys Amparo Martínez	000
34	Estante	Estante Gris	Secretaria De Gobierno	Nerys Amparo Martínez	000
35	Estante	Estante	Secretaria De Gobierno	Nerys Amparo Martínez	000
36	Archivador	Archivador De Madera	Secretaria De Gobierno	Nerys Amparo Martínez	000
37	Archivador	Archivador Gris	Secretaria De Gobierno	Nerys Amparo Martínez	000
38	Estante	Estante	Asesores	Javier Sánchez	000
39	Meza	Meza De Nevera	Asesores	Javier Sánchez	000
40	Escritorio	Escritorio	Asesores	Javier Sánchez	000
41	Silla	Silla De Oficina	Asesores	Javier Sánchez	000
42	Impresora	Impresora Epson Negra	Asesores	Javier Sánchez	S3yk068637
43	Meza	Meza Pequeña	Asesores	Javier Sánchez	000
44	Escritorio	Escritorio	Asesores	Javier Sánchez	000
45	Silla	Silla De Oficina Negra	Asesores	Javier Sánchez	000
46	Estabilizador	Estabilizador	Asesores	Javier Sánchez	000
47	Escritorio	Escritorio	Asesores	Javier Sánchez	000
48	Silla	Silla De Oficina Azul	Asesores	Javier Sánchez	000

49	Escritorio	Escritorio	Asesores	Javier Sánchez	000
50	Escritorio	Escritorio	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
51	Sumadora	Sumadora	Secretaria De Hacienda	Elisa María Suarez Ramírez	Q5039703
52	Silla	Silla De Oficina	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
53	Teléfono	Telefax	Secretaria De Hacienda	Elisa María Suarez Ramírez	2lbwb050081
54	Computador	Computador Lenovo	Secretaria De Hacienda	Elisa María Suarez Ramírez	Omo4711b1650229
55	Estabilizador	Estabilizador	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
56	CPU	CPU	Secretaria De Hacienda	Elisa María Suarez Ramírez	Es07620496
57	Escritorio	Escritorio	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
58	Impresora	Impresora Epson	Secretaria De Hacienda	Elisa María Suarez Ramírez	S26k013251
59	Escritorio	Escritorio	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
60	Impresora	Impresora Epson	Secretaria De Hacienda	Elisa María Suarez Ramírez	Fcty039353
61	Computador	Computador Samsung	Secretaria De Hacienda	Elisa María Suarez Ramírez	Ha17h9nyb03310h
62	CPU	CPU LG	Secretaria De Hacienda	Elisa María Suarez Ramírez	Ha17h9nyb03310h
63	Estabilizador	Estabilizador	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
64	Sumadora	Sumadora CASIO	Secretaria De Hacienda	Elisa María Suarez Ramírez	Q5039704
65	Escritorio	Escritorio	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
66	Silla	Silla De Oficina	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
67	Meza	Meza Pequeña	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
68	Silla	Silla De Oficina	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
69	Escritorio	Escritorio	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
70	Impresora	Impresora Epson	Secretaria De Hacienda	Elisa María Suarez Ramírez	Etuy281974
71	Computador	Monitor Compaq	Secretaria De Hacienda	Elisa María Suarez Ramírez	Cnc4250nz2
72	CPU	CPU LG	Secretaria De Hacienda	Elisa María Suarez Ramírez	Cnc425onz2
73	Sumadora	Sumadora CASIO	Secretaria De Hacienda	Elisa María Suarez Ramírez	6506255
74	Grapadora	Grapadora Negra	Secretaria De Hacienda	Elisa María Suarez Ramírez	000

75	Escritorio	Escritorio Pequeño	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
76	Archivador	Archivador	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
77	Archivador	Archivador	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
78	Archivador	Archivador	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
79	Archivador	Archivador	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
80	Archivador	Archivador	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
81	Archivador	Archivador	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
82	Archivador	Archivador	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
83	Estante	Estante	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
84	Estante	Estante	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
85	Estante	Estante	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
86	Abanico	Dañado	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
87	Impresora	Impresora Hp Dañada	Secretaria De Hacienda	Elisa María Suarez Ramírez	Us88r1v04e
88	Escritorio	Escritorio	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
89	Silla	Silla De Oficina	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
90	Computador	Monitor Samsung	Secretaria De Hacienda	Elisa María Suarez Ramírez	Lb15hchy900292n
91	CPU	CPU DELUX	Secretaria De Hacienda	Elisa María Suarez Ramírez	Lb15hchy900292n
92	Parlantes	Parlantes	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
93	Escritorio	Escritorio	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
94	Computador	Monitor Samsung	Secretaria De Hacienda	Elisa María Suarez Ramírez	Zugthtjc504403r
95	CPU	CPU INTEL	Secretaria De Hacienda	Elisa Amaría Suarez Ramírez	2582ac1kq2c3no
96	Estabilizador	Estabilizador	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
97	Archivador	Archivador	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
98	Estante	Estante	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
99	Estante	Estante	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
100	Silla	Silla Dañada	Secretaria De Hacienda	Elisa María Suarez Ramírez	000

101	Silla	Silla Dañada	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
102	Escritorio	Escritorio Dañado	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
103	Escritorio	Escritorio	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
104	Silla	Silla De Oficina	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
105	Computador	Monitor Samsung	Secretaria De Hacienda	Elisa María Suarez Ramírez	My17hvlq105561v
106	CPU	CPU ASUS	Secretaria De Salud	Secretaria De Salud	My17hvlq105561v
107	Impresora	Impresora Hp Dañada	Secretaria De Hacienda	Elisa María Suarez Ramírez	Cnb2677247
108	Estabilizador	Estabilizador Dañado	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
109	Escritorio	Escritorio	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
110	Teléfono	Teléfono Fijo Dañado	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
111	Meza	Meza De Madera	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
112	Meza	Meza De Madera	Secretaria De Hacienda	Elisa María Suarez Ramírez	000
113	Escritorio	Escritorio	Secretaria De Salud	Amparo Chacón	000
114	Computador	Monitor LG	Secretaria De Salud	Amparo Chacón	303ndcr35995
115	Estabilizador	Estabilizador	Secretaria De Salud	Amparo Chacón	Hd21e627686075507
116	Cpu	Cpu Intel	Secretaria De Salud	Amparo Chacón	Hsi18073013122
117	Impresora	Impresora Epson	Secretaria De Salud	Amparo Chacón	S25k168379
118	Silla	Silla Rimax	Secretaria De Salud	Amparo Chacón	000
119	Estante	Estante	Secretaria De Salud	Amparo Chacón	000
120	Estante	Estante	Secretaria De Salud	Amparo Chacón	000
121	Escritorio	Escritorio	Secretaria De Salud	Amparo Chacón	000
122	Silla	Silla Rimax	Secretaria De Salud	Amparo Chacón	000
123	Escritorio	Escritorio	Secretaria De Salud	Amparo Chacon	000
124	Computador	Monitor Samsung Dañado	Secretaria De Salud	Amparo Chacon	Lb15hcgya00318j
125	Impresora	Impresora Hp Dañada	Secretaria De Salud	Amparo Chacon	Cnb0328686
126	Cpu	Cpu Lg Dañada	Secretaria De Salud	Amparo Chacon	Lb15hcgya0018j

127	Parlantes	Parlantes De Pc Dañados	Secretaria De Salud	Amparo Chacon	000
128	Televisor	Televisor Sharp	Secretaria De Salud	Amparo Chacon	C409866419
129	Archivador	Archivador	Secretaria De Salud	Amparo Chacon	000
130	Archivador	Archivador	Secretaria De Salud	Amparo Chacon	000
131	Escritorio	Escritorio	Secretaria De Salud	Amparo Chacon	000
132	Silla	Silla De Oficina	Secretaria De Salud	Amparo Chacon	000
133	Computador	Monitor Acer	Secretaria De Salud	Amparo Chacon	9980236335
134	Cpu	Cpu Lg	Secretaria De Salud	Amparo Chacon	9980236335
135	Estabilizador	Estabilizador	Secretaria De Salud	Amparo Chacon	000
136	Impresora	Impresora Hp Dañada	Secretaria De Salud	Amparo Chacon	Cnfb017008
137	Escritorio	Escritorio	Secretaria De Salud	Amparo Chacon	000
138	Silla	Silla De Oficina	Secretaria De Salud	Amparo Chacon	000
139	Escritorio	Escritorio	Planeacion	Camilo Gelvis	000
140	Computador	Monitor Compaq	Planeacion	Camilo Gelvis	3cr0270c3t
141	Estabilizador	Estabilizador	Planeacion	Camilo Gerlvis	000
142	Impresora	Impresora Hp	Planeacion	Camilo Gelvis	Cb58460014
143	Silla	Silla De Oficina	Planeacion	Camilo Gelvis	000
144	Escritorio	Escritorio	Planeacion	Camilo Gelvis	000
145	Computador	Monitor Aoc	Planeacion	Camilo Gelvis	E1779ja006343
146	Parlantes	Parlantes De Pc	Planeacion	Camilo Gelvis	000
147	Impresora	Impresora Epson	Planeacion	Camilo Gelvis	S25k085394
148	Cpu	Cpu Lg	Planeacion	Camilo Gelvis	2060300002179
149	Silla	Silla De Oficina	Planeacion	Camilo Gelvis	000
150	Escritorio	Escritorio	Planeacion	Camilo Gelvis	000
151	Computador	Monitor Lg	Planeacion	Camilo Gelvis	209ndfv1y347
152	Telefono	Telefax	Planeacion	Camilo Gelvis	000

153	Estabilizador	Estabilizador	Planeacion	Camilo Gelvis	000
154	Impresora	Impresora Hp	Planeacion	Camilo Gelvis	Cn2d9vh079
155	Silla	Silla De Oficina	Planeacion	Camilo Gelvis	000
156	Cpu	Cpu Power	Planeacion	Camilo Gelvis	209ndfv1y347
157	Archivador	Archivador	Planeacion	Camilo Gelvis	000
158	Meza	Meza De Madera	Planeacion	Camilo Gelvis	000
159	Silla	Silla De Oficina Azul	Planeacion	Camilo Gelvis	000
160	Escritorio	Escritorio	Planeacion	Camilo Gelvis	000
161	Computador	Monitor Lg	Planeacion	Camilo Gelvis	209ndwe1y345
162	Cpu	Cpu Power	Planeacion	Camilo Gelvis	209ndwe1345
163	Silla	Silla De Oficina	Planeacion	Camilo Gelvis	000
164	Estabilizador	Estabilizador	Planeacion	Camilo Gelvis	000
165	Estante	Estante	Planeacion	Camilo Gelvis	000
166	Meza	Meza De Madera	Planeacion	Camilo Gelvis	000
167	Ploter	Ploter Negro	Planeacion	Camilo Gelvis	Cn2cq1m04x
168	Escritorio	Escritorio	Planeacion	Camilo Gelvis	000
169	Computador	Monitor Lg	Planeacion	Camilo Gelvis	210ndez42532
170	Cpu	Cpu Power	Planeacion	Camilo Gelvis	210ndez42532
171	Silla	Silla De Oficina	Planeacion	Camilo Gelvis	000
172	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
173	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
174	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
175	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
176	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
177	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
178	Estante	Estante	Centro De Historia	Diosa Chscon Mejia	000

179	Archivador	Archivador	Centro De Historia	Diosa Chacon Mejia	000
180	Meza	Meza De Madera	Centro De Historia	Diosa Chacon Mejia	000
181	Archivador	Archivador De Madera	Centro De Historia	Diosa Chacon Mejia	000
182	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
183	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
184	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
185	Escritorio	Escritorio	Centro De Historia	Diosa Chacon Mejia	000
186	Impresora	Impresora	Centro De Historia	Diosa Chacon Mejia	1467bkaq900040n
187	Computador	Monitor Samsung	Centro De Historia	Diosa Chacon Mejia	V88bh9nz212904e
188	Estabilizador	Estabilizador	Centro De Historia	Diosa Chacon Mejia	000
189	Cpu	Cpu	Centro De Historia	Diosa Chacon Mejia	B88bh9nz212904e
190	Archivador	Archivador	Centro De Historia	Diosa Chacon Mejia	000
191	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
192	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
193	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
194	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
195	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
196	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
198	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
199	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
200	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
201	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
202	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
203	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
204	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
205	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000

206	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
207	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
208	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
209	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
210	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
211	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
212	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
213	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
214	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
215	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
216	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
217	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
218	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
219	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
220	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
221	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
222	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
223	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
224	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
225	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
226	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
227	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
228	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
229	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	Ooo
230	Estante	Estante	Centro De Historia	Diosa Chacon Mejia	000
231	Meza	Meza De Madera	Centro De Historia	Diosa Chacon Mejia	000

232	Meza	Meza De Madera Dañada	Centro De Historia	Diosa Chacon Mejia	000
233	Silla	Silla De Oficina	Centro De Historia	Diosa Chacon Mejia	000
234	Archivador	Archivador	Adultos Mayor	Lorena Villamizar	000
235	Archivador	Archivador	Adultos Mayor	Lorena Villamizar	000
236	Escritorio	Escritorio	Adultos Mayor	Lorena Villamizar	000
237	Silla	Silla De Oficina Dañada	Adultos Mayor	Lorena Villamizar	000
238	Computador	Portatil Toshiba	Adultos Mayor	Lorena Villamizar	2a2696638q
239	Estante	Estante	Sisben	Lorena Villamizar	000
240	Estante	Estante	Sisben	Lorena Villamizar	000
241	Estante	Estante	Sisben	Lorena Villamizar	000
242	Escritorio	Escritorio	Sisben	Lorena Villamizar	000
243	Silla	Silla De Oficina Dañada	Sisben	Lorena Villamizar	000
244	Computador	Monitor Janus	Sisben	Lorena Villamizar	J2013li11091500599
245	Computador	Portatil Compaq	Sisben	Lorena Villamizar	2ce8460hv2
246	Impresora	Impresora Samsung	Sisben	Lorena Villamizar	1467bkbqc01189e
247	Escritorio	Escritorio	Sisben	Lorena Villamizar	000
248	Estabilizador	Estabilizador	Sisben	Lorena Villamizar	000
249	Silla	Silla De Oficina Dañada	Sisben	Lorena Villamizar	000
250	Meza	Meza De Madera Pequeña	Sisben	Lorena Villamizar	000
251	Escritorio	Escritorio	Sisben	Lorena Villamizar	000
252	Silla	Silla Mueble Dañada	Sisben	Lorena Villamizar	000
253	Mueble	Mueble De Madera	Familias En Accion	Torcoroma Osorio	000
254	Archivador	Archivador Dañado	Familias En Accion	Torcoroma Osorio	Ooo
255	Estante	Estante	Familias En Accion	Torcoroma Osorio	000
256	Estante	Estante	Familias En Accion	Torcoroma Osorio	000
257	Escritorio	Escritorio Dañado	Familias En Accion	Torcoroma Osorio	000

258	Escritorio	Escritorio	Familias En Accion	Torcoroma Osorio	000
259	Computador	Monitor Janus	Familias En Accion	Torcoroma Osorio	J2013le11091500089
260	Cpu	Cpu Janus	Familias En Accion	Torcoroma Osorio	12021569566
261	Silla	Silla Mueble Dañada	Familias En Accion	Torcoroma Osorio	000
262	Silla	Silla Rimax	Familias En Accion	Torcoroma Osorio	000
263	Escritorio	Escritorio Dañado	Familias En Accion	Torcoroma Osorio	000
264	Escritorio	Escritorio	Familias En Accion	Torcoroma Osorio	000
265	Impresora	Impresora Epson	Familias En Accion	Torcoroma Osorio	C25k124724
266	Computador	Monitor Janus	Familias En Accion	Torcoroma Osorio	J2013li11091500586
267	Cpu	Cpu Janus	Familias En Accion	Torcoroma Osorio	12021569560
268	Sillas	Sillas Verdes	Familias En Accion	Torcoroma Osorio	000
269	Mueble	Mueble Verde	Comisaria De Familia	Antonia Ramirez	000
270	Estante	Estante	Comisaria De Familia	Antonia Ramirez	000
271	Archivador	Archivador	Comisaria De Familia	Antonia Ramirez	000
272	Archivador	Archivador	Comisaria De Familia	Antonia Ramirez	000
273	Escritorio	Escritorio	Comisaria De Familia	Antonia Ramirez	000
274	Impresora	Impresora Hp	Comisaria De Familia	Antonia Ramirez	Cnfb083542
275	Computador	Monitor Samsung	Comisaria De Familia	Antonia Ramirez	P17h9npb13556v
276	Cpu	Cpu Avant	Comisaria De Familia	Antonia Ramirez	Zf030714200
277	Silla	Silla De Oficina	Comisaria De Familia	Antonia Ramirez	000
278	Estabilizador	Estabilizador	Comisaria De Familia	Antonia Ramirez	000
279	Silla	Silla De Oficina	Comisaria De Familia	Antonia Ramirez	000
280	Silla	Silla De Oficina	Comisaria De Familia	Antonia Ramirez	000
281	Estante	Estante	Inspeccion De Policia	Liliana Sanchez	000
282	Escritorio	Escritorio	Inspeccion De Policia	Liliana Sanchez	000
283	Silla	Silla De Oficina	Inspeccion De Policia	Liliana Sanchez	000

284	Impresora	Impresora Samsung	Inspeccion De Policia	Liliana Sanchez	1467bkdq901019a
285	Estabilizador	Estabilizador	Inspeccion De Policia	Liliana Sanchez	000
286	Máquina De Escribir	Máquina De Escribir Blanca	Inspeccion De Policia	Liliana Sanchez	000
287	Mueble	Mueble De Computador	Inspeccion De Policia	Liliana Sanchez	000
288	Silla	Sillas De Colores	Inspeccion De Policia	Liliana Sanchez	000
289	Silla	Sillas Muebles	Inspeccion De Policia	Liliana Sanchez	000
290	Archivador	Archivador	Nucleo Educativo	Nelly Chincilla	000
290	Computador	Monitor Compaq	Inspeccion De Policia	Liliana Sanchez	146bm28hc524
291	Archivador	Archivador	Nucleo Educativo	Nelly Chinchilla	000
292	Estante	Estante Dañado	Nucleo Educativo	Nelly Chinchilla	000
293	Estante	Estante	Nucleo Educativo	Nelly Cinchilla	000
294	Archivador	Archivador	Nucleo Educativo	Nelly Chinchilla	000
295	Archivador	Archivador	Nucleo Educativo	Nelly Chinchilla	000
296	Archivador	Archivador	Nucleo Educativo	Nelly Chinchilla	000
297	Archivador	Archivador	Nucleo Educativo	Nelly Chinchilla	000
298	Archivador	Archivador	Nucleo Educativo	Nelly Chinchilla	000
299	Mueble	Mueble De Madera	Nucleo Educativo	Nelly Chinchilla	000
300	Archivador	Archivador	Nucleo Educativo	Nelly Chinchilla	000
301	Archivador	Archivador	Nucleo Educativo	Nelly Chinchilla	000
302	Escritorio	Escritorio	Nucleo Educativo	Nelly Chinchilla	000
303	Escritorio	Escritorio	Nucleo Educativo	Nelly Chinchilla	000
304	Archivador	Archivador	Nucleo Educativo	Nelly Chinchilla	000
305	Impresora	Impresora Samsung	Nucleo Educativo	Nelly Chinchilla	144mbkaz200393n
306	Escritorio	Escritorio	Nucleo Educativo	Nelly Chinchilla	000
307	Silla	Silla De Oficina	Nucleo Educativo	Nelly Chinchilla	000
308	Archivador	Archivador	Nucleo Educativo	Nelly Chinchilla	000

309	Silla	Silla De Oficina	Nucleo Educativo	Nelly Chinchilla	000
310	Escritorio	Escritorio	Nucleo Educativo	Nelly Chinchilla	000
311	Silla	Silla De Oficina	Nucleo Educativo	Nelly Chinchilla	000
340	Silla	Silla De Escritorio Ejecutiva	Asesores Juridicos	Jair Hernandes Quintero	0000
341	Silla	Silla Vaniplas Blancas	Secretaria De Gobierno	Jair Hernandes Quintero	Oooo
342	Silla	Silla Vaniplas Blancas	Secretaria De Gobierno	Jair Hernandes Quintero	0000
343	Silla	Silla Vaniplas Blacas	Secretaria De Gobierno	Jair Hernandes Quintero	0000
344	Sillla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
345	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
346	Sillla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
347	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
348	Silla	Silla Vaniplas Blanca	Secretaria De Salud	Jair Hernandes Quintero	0000
349	Silla	Silla Vaniplas	Secretaria De Gobierno	Jair Hernandes Quintero	0000
350	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
351	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
352	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
353	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
354	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
355	Silla	Silla Vaniplas Blanca	Secretaria De Salud	Jair Hernandes Quintero	0000
356	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
357	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
358	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
359	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
360	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
361	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
362	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000

363	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
364	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
365	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
366	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
367	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
368	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
369	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
370	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
371	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
372	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
373	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernades Quintero	0000
374	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernades Quintero	0000
375	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
376	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
377	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
378	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
379	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
380	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
381	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
382	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
383	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
384	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
385	Silla	Silla Vaniplas Blanco	Secretaria De Gobierno	Jair Hernandes Quintero	0000
386	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
387	Silla	Silla Vaniplas Blanco	Secretaria De Gobierno	Jair Hernandes Quintero	0000
388	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000

389	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
390	Silla	Silla Vaniplas Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
391	Carpa	Carpa De Plastica Blanca	Secretaria De Gobierno	Jair Hernades Quintero	0000
392	Carpa	Carpa Plastica Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
393	Carpa	Carpa Plastica Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
394	Carpa	Carpa Plastica Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
395	Carpa	Carpa Plastica Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	Oooo
396	Carpa	Carpa Plastica Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	0000
397	Carpa	Carpa Plastica Blanca	Secretaria De Gobierno	Jair Hernandes Quintero	Oooo
398	Portatil	Portil Acer Negro	Secretaria De Gobierno	Jair Hernades Quintero	Nxmfqal004310545b7600
399	Computador	Computador Hp Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	00186-753-640-947
400	Computador	Computador	Biblioteca Publica	Diosa Lorena Chacon Mejia	00186-753-640-235
401	Computador	Computador Hp Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	00186-753-490-104
402	Computador	Computador Hp Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	00186-753-640-986
403	Computador	Computador Hp Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	00186-753-640-733
404	Computador	Computador Hp Gris	Biblioteca Publica	Diosa Chacon Mejia	00186-753-640-205
405	Computador	Computador Hp Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	00186-753489-202
406	Computador	Computador	Biblioteca Publica	Diosa Lorena Chacon Mejia	00186-753-490-100
407	Computador	Computador Hp Gris	Biblioteca Publica	Diosa Lorena Chacon Mejis	00186-753-640-194
408	Computador	Computador Hp Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	00186-753-640-201
409	Computador	Computador Hp Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	00186-753-640-870
410	Computador	Computador Hp Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	00186-753-665
412	Vitrina	Vitrina De Metal Color Azul	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
413	Unidad Externa	Lector De Dvd Color Negro	Biblioteca Publica	Diosa Lorena Chacon Mejia	6f8227400509-3734208339
414	Silla	Silla Ejecutiva Negra	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
415	Silla	Silla Ejecutiva Negra	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000

416	Silla	Silla Ejecutiva Negra	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
417	Silla	Silla Ejecutiva Negra	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
418	Silla	Silla Ejecutiva Negra	Bibliotca Publica	Diosa Lorena Chacon Mejia	0000
419	Estante	Estante Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
420	Estante	Estante De Libros Color Rojo	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
421	Dvd	Dvd Lg Color Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	408sh01378
422	Televisor	Televisor Sankey Pequeño	Biblioteca Publica	Diosa Lorena Chacon Mejia	60409209
423	Televisor	Televisor Sankey Pequeño	Biblioteca Publica	Diosa Lorena Chacon Mejia	0512j140233
424	Vhs	Vhs Color Negro	Biblioteca Publica	Diosa Lorena Chacon Mejia	Slv-X533mx
425	Vhs	Vhs Color Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	Lg-Gc47m
426	Cuadro	Cuadro De Vidrio Color Rojo	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
427	Cuadro	Cuadro De Vidrio Color Negro	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
428	Cuadro	Cuadro De Vidrio	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
430	Computador	Computador Hp	Biblioteca Publica	Diosa Lorena Chacon Mejia	00186-753-665-242
431	Mesa	Mesa Marrón	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
432	Silla	Silla Ejecutiva	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
433	Estante	Estante Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
434	Mesa	Mesa Marrón	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
435	Silla	Silla De Pasta Blanca	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
436	Estante	Estante Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
437	Estante	Estante Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
438	Estante	Estante Gris	Biblioteca Publica	Diosa Lorena Cahcon Mejia	0000
439	Estante	Estante Gris	Biblioteca Publica	Dios Lorena Chacon Mejia	0000
440	Estante	Estante Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000

441	Estante	Estante Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
442	Estante	Estante Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
443	Estante	Estante Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
444	Estante	Estante Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
445	Estante	Estante Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
446	Pupitres	Pupitres Universitarios	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
447	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
448	Estante	Estante	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
449	Estante	Estante Gris	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
450	Estante	Estante De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
451	Mesa	Mesa De Pasta Blanca	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
452	Mesa	Mesa De Pasta Roja	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
453	Mesa	Mesa De Pasta Blanca	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
454	Mesa	Mesa De Pata Roja	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
455	Mesa	Mesa De Pasta Blanca	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
456	Mesa	Mesa De Pasta Blanca	Biblioteca `Publica	Diosa Lorena Chacon Mejia	0000
457	Mesa	Mesa De Pasta Blanca	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
458	Escritorio	Escritorio Negro	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
459	Escritorio	Escritorio Negro	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
460	Escritorio	Escritorio Negro	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
461	Escritorio	Escritorio De Madera Marrón	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
462	Escritorio	Escritorio Negro	Biblioteca	Diosa Lorena Chacon Mejia	0000
463	Escritorio	Escritorio Negro	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
464	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
465	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
466	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000

467	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejiia	0000
468	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
469	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
470	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
471	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
472	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
473	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
474	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
475	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
476	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
477	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
478	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
479	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
480	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
481	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
482	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
483	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
484	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
485	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
486	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
487	Pupitre	Pupitre Universitario	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
488	Mesa	Mesa De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
489	Mesa	Mesa De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
490	Silla	Silla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
491	Silla	Silla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
492	Silla	Silla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000

493	Silla	Silla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
494	Silla	Sillla De Madera	Biblioteca	Diosa Lorena Cahcon Mejia	0000
495	Silla	Silla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
496	Silla	Silla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	00000
497	Silla	Silla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
498	Silla	Silla	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
499	Sillla	Silla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
500	Silla	Silla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
501	Silla	Silla De Madera	Biblioteca	Diosa Lorena Chacon Mejia	0000
502	Televisor	Televisor Panasonic 24 Pulgadas En Mal Estado	Ceac	Yesid Ramirez	0000
503	Grabadora	Grabadora Sony En Mal Estado	Ceac	Yesid Ramirez	Cdf-C6100s
504	Nevera	Nevera Abba Blanca Pequeña	Ceac	Yesid Ramirez	0000
504	Nevera	Nevera			
505	Escritorio	Escritorio De Madera De 6 Gabetas	Ceac	Yesid Ramirez	0000
506	Silla	Silla De Oficina Color Negro	Ceac	Yesid Ramirez	0000
507	Escritorio	Escritorio De Madera Vinotinto	Ceac	Yesid Ramirez	0000
508	Silla	Silla De Madera Elaborada En Tela De Color Rojo	Ceac	Yesid Ramirez	0000
509	Estante	Estante Biblioteca De Madra	Ceac	Yesid Ramirez	0000
510	Maquina	Maquina De Escribir Color Negra	Ceac	Yesid Ramirez	16-83-Archivo
511	Archivador	Archivador De Madera	Ceac	Yesid Ramirez	0000
512	Archivador	Archivador Metalico	Ceac	Yesid Ramirez	0000

513	Silla	Silla Doble De Madera	Ceac	Yesid Ramirez	0000
514	Archivador	Archivador Metalico Marron	Ceac	Yesid Ramirez	0000
515	Estante	Estante Metalico Gris	Ceac	Yesid Ramirez	000'
516	Estante	Estante De Nmadera	Ceac	Yesid Ramirez	0000
517	Nevera	Nevera Philips Blanca	Ceac	Yesid Ramirez	0000
518	Escritorio	Escritorio De Madera	Ceac	Yesid Ramirez	0000
519	Tablero	Tablero Aclirico	Ceac	Yesid Ramirez	0000
520	Mesa	Mesa De Mdera	Ceac	Yesid Ramirez	0000
521	Escritorio	Escritorio Metalico	Ceac	Yesid Ramirez	0000
522	Tablero	Tablero Aclirico	Ceac	Yesid Ramirez	0000
523	Cuadro	Cuadro De Vidrio	Ceac	Yesid Ramirez	0000
524	Cuadro	Cuadro De Vidrio	Ceac	Yesid Ramirez	0000
525	Cuadro	Cuadro De Vidrio	Ceac	Yesid Ramirez	0000
526	Cuadro Ç	Cuadro De Vidrio	Ceac	Yesid Ramirez	0000
527	Cuadro	Cuadro De Vidrio	Ceac	Yesid Ramirez	0000
528	Cuadro	Cuadro De Vidrio	Ceac	Yesid Ramirez	0000
529	Tablero	Tablero Acrilico	Ceac	Yesid Ramirez	0000
530	Tablero	Tablero Acrilico	Ceac	Yesid Ramirez	0000
531	Mesa	Mesa De Madera Marron	Ceac	Yesid Ramirez	0000
532	Tanque	Tanque De Agua De Eternit	Ceac	Yesia Ramirez	0000
533	Mesa	Mesa De Madera	Ceac	Yesid Ramirez	0000
534	Mesa	Mesa De Madera	Ceac	Yesid Ramirez	0000
535	Mesa	Mesa De Madera	Ceac	Yesid Ramirez	0000
536	Tablero	Tablero Acrilico	Ceac	Yesid Ramirez	0000
537	Escultura	Escultura En Fibra De Vidrio	Ceac	Yesid Ramirez	0000

541	Pupitre	Pupitre Universitario De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
542	Silla	Silla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
543	Silla	Sillla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
544	Silla	Silla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
545	Mesa	Mesa De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
546	Mesa	Mesa De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
547	Mesa	Mesa De Madera	Biblioteca	Diosa Lorena Chacon Mejia	0000
548	Mesa	Mesa De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
549	Silla	Silla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
550	Mesa	Mesa De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
551	Mesa	Mesa De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
552	Silla	Silla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
553	Silla	Silla De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
554	Silla	Silla De ,Adera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
555	Mesa	Mesa De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
556	Televisor	Televisor Panasonic	Biblioteca		Ct-G2974j
557	Cuadro	Cuadro De Vidrio	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
558	Cuadro	Cuadro De Vidrio	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
559	Cuadro	Cuadro De Vidrio	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
560	Cuadro	Cuadro De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
561	Cuadro	Cuadro De Madera	Biblioteca Publica	Diosa Lorena Chacon Mejia	0000
562	Caja	Caja Vallenata	Ceac	Yesid Ramirez	0000
563	Caja	Caja Vallenata	Ceac	Yesid Ramirez	0000
564	Caja	Caja Vallenata	Ceac	Yesid Ramirez	0000
565	Caja	Caja Vallenata	Ceac	Yesid Ramirez	0000
566	Base	Base Tibal De Metal	Ceac	Yesid Ramirez	0000

567	Cencerro	Cencerro Del Tinbal	Ceac	Yesid Ramirez	0000
568	Tinbal	Tinbal De Metal	Ceac	Yesid Ramirez	0000
569	Tinbal	Tinbal De Metal	Ceac	Yesid Ramirez	0000
570	Platillos	Platillos Del Tinbal	Ceac	Yesid Ramirez	0000
571	Base	Base De Los Paltillos	Ceac	Yesid Ramirez	0000
572	Bombo	Bombo Grande	Ceac	Yesit Ramirez	0000
573	Estante	Estante De Metal	Ceac	Yesith Ramirez	0000
574	Planta	Planta Electrica	Ceac	Yesith Ramirez	0000
575	Trompeta	Trompeta Conductor Dorada	Ceac	Yesith Ramirez	0000
576	Trompeta	Trompeta Dorada	Ceac	Yesith Ramirez	0000
577	Trompeta	Trompeta Plateada	Ceac	Yesith Ramirez	0000
578	Trompeta	Trompeta Dorada	Ceac	Yesith Ramirez	0000
579	Trompeta	Trompeta Dorada	Ceac	Yesith Ramirez	0000
580	Trompeta	Trompeta Dorada	Ceac	Yesith Ramirez	0000
581	Trompeta	Trompeta Plateada	Ceac	Yesith Ramirez	0000
582	Clarinete	Clarinete Conducto Negro	Ceac	Yesith Ramirez	0000
583	Clarinete	Clarinete Conducto Negro	Ceac	Yesith Ramirez	0000
584	Clarinete	Clarinete Conducto Negro	Ceac	Yesith Ramirez	0000
585	Clarinete	Clarinete Conducto Negro	Ceac	Yesith Ramirez	0000
586	Clarinete	Clarinete Conducto Negro	Ceac	Yesith Ramirez	0000
587	Clerinete	Clerinete Cinducto Negro	Ceac	Yesith Ramirez	0000
588	Clerinete	Clerite Conducta Negra	Ceac	Yesith Ramirez	0000
589	Caja	Caja Ballenata	Ceac	Yesith Ramirez	0000
590	Bombardino	Bombardino Dorado	Ceac	Yesith Ramirez	0000
591	Bombardino	Bombardino Dorado	Ceac	Yesith Ramirez	0000
592	Bombardino	Bombardino Dorado	Ceac	Yesith Ramirez	0000

593	Trombon	Trombon De Bara Dorado	Ceac	Yesith Ramirez	0000
594	Platillos	Platillos Dorado	Ceac	Yesith Ramirez	0000
595	Platillo	Platillo Dorado	Ceac	Yesith Ramirez	0000
596	Saxo Tenor	Saxo Tenor Dorado	Ceac	Yesith Ramirez	0000
597	Saxo Alto	Saxo Alto Dorado	Ceac	Yesith Ramirez	0000
598	Atriles	Atriles Con Partituras Negro	Ceac	Yesith Ramirez	0000
599	Atriles	Atriles Con Partituras Negro	Ceac	Yesith Ramirez	0000
600	Atriles	Atriles Con Partiduras Negras	Ceac	Yesith Ramirez	0000
601	Atriles	Atriles Con Partiduras	Ceac	Yesith Ramirez	0000
602	Atriles	Atriles Con Partidura Negra	Ceac	Yesith Ramirez	0000
603	Atriles	Atriles Con Partidura Plateado	Ceac	Yesith Ramirez	0000
604	Atriles	Atriles Con Partidura Plateada	Ceac	Yesith Ramirez	0000
605	Atriles	Atriles Con Partidura Pateada	Ceac	Yesith Ramirez	0000
606	Atriles	Atriles Con Partidura Dorada	Ceac	Yesith Ramirez	0000
607	Atriles	Atriles Con Partiduras Plateadas	Ceac	Yesith Ramires	0000
608	Atriles	Atriles Con Partidura Plateada	Ceac	Yesith Ramirez	0000
609	Atriles	Atriles Con Partidura Plateada	Ceac	Yesith Ramirez	0000
610	Atriles	Atriles Con Partidura Plateada	Ceac	Yesith Ramirez	0000
611	Atriles	Atriles Con Partidura Negra	Ceac	Yesith Ramirez	0000
612	Atriles	Atriles Con Partidura Negra	Ceac	Yesith Ramirez	0000

613	Atriles	Atriles Con Pertidura Negra	Ceac	Yesith Ramirez	0000
614	Atriles	Atriles Con Partidura Negra	Ceac	Yesith Ramirez	0000
615	Atriales	Atriales Con Partidura Negra	Ceac	Yesith Ramirez	0000
616	Atriles	Atriles Con Partidura Negra	Ceac	Yesith Ramirez	0000
617	Maracas	Maracas De Cuero	Ceac	Yesith Ramirez	0000
618	Maracas	Maracas De Cuero	Ceac	Yesith Ramirez	0000
619	Parlantes	Parlantes Audio Kinc Negro	Ceac	Yesith Ramireez	Akpj-12
620	Planta	Planta Audio Kinc Negro	Ceac	Yesith Ramirez	Akpj-12
621	Guache	Guache Plateado	Ceac	Yesith Ramirez	0000
622	Guache	Guache Plateado	Ceac	Yesith Ramirez	0000
623	Planta Electrica	Planta Electica 3 Salidas	Ceac	Yesith Ramirez	Shinvco Av- 727
624	Bases	Bases Para Parlantes Thunder	Ceac	Yesith Ramirez	0000
625	Base	Base Thunder	Ceac	Yesid Ramirez	0000
626	Tambora	Tambora Grande De Madera	Ceac	Yesid Ramirez	0000
627	Alegre	Alegre Grande	Ceac	Yesid Ramirez	0000
628	Llamador	Lllamador Grande	Ceac	Yesid Ramires	0000
629	Llamador	Llamador Grande	Ceac	Yesid Ramirez	0000
630	Llamador	Llamador Garnde	Ceac	Yesid Ramirez	0000
631	Alegre	Alegre Grande	Ceac	Yesid Ramirez	0000
632	Alegre	Alegre Grande	Ceac	Yesid Ramirez	0000
633	Tambora	Tambora Grande	Ceac	Yesid Ramirez	0000
634	Tambora	Tambora Grande	Ceac	Yesid Ramirez	0000
635	Atril	Atril Para Tamnbora Mayor	Ceac	Yesid Ramirez	0000
636	Bajo	Bajo Electrico	Ceac	Yesid Ramirez	0000

637	Bajo	Bajo Electrico Yamaha Color Madera	Ceac	Yesid Ramirez	0000
638	Guitarrra	Guitarra Con Estuche	Ceac	Yesid Ramirez	0000
639	Guitarrav	Guitarra Con Estuche	Ceac	Yesid Ramirez	0000
640	Piano	Piano Yamaha	Ceac	Yesid Ramirez	0000
641	Piano	Piano Yamaha	Ceac	Yesid Ramirez	0000
642	Piano	Piano Yamaha	Ceac	Yesid Ramirez	0000
643	Piano	Piano Yamaha	Ceac	Yesid Ramirez	0000
644	Base	Base De Piano Hamilton Stants	Ceac	Yesid Ramirez	0000
645	Base	Base De Piano Hamliton Atants	Ceac	Yesid Ramirez	0000
646	Base	Base De Piano	Ceac	Yesid Ramirez	0000
647	Base	Base De Piano	Ceac	Yesid Ramirez	0000
648	Acordeon	Acordeon Amarillo Hohner	Ceac	Yesid Ramirez	0000
649	Acordeon	Acordeon Verde Hohner	Ceac	Yesid Ramirez	0000
650	Acordeon	Acordeon Roja Hohner	Ceac	Yesid Ramirez	0000
651	Acordeon	Acordeon Roja Hohner	Ceac	Yesid Ramirez	0000
652	Acordeon	Acordeon Verde	Ceac	Yesid Ramirez	0000
653	Acordeon	Acordeon Roja Hohner	Ceac	Yesid Ramirez	0000
654	Acordeon	Acordeon Azul Hohner	Ceac	Yesid Ramirez	0000
655	Acordeon	Acordeon Roja Hohner	Ceac	Yesid Ramirez	0000
656	Estante	Estante De Metal	Ceac	Yesid Ramirez	0000
657	Estante	Estante De Metal	Ceac	Yesid Ramirez	0000
658	Estante	Estante De Metal	Ceac	Yesid Ramirez	0000
659	Estante	Estante De Metal	Ceac	Yesid Ramirez	0000
660	Guacharaca	Guacharaca De Metal	Ceac	Yesid Ramirez	0000

661	Guacharaca	Guacharaca De Madera	Ceac	Yesid Ramirez	00000
662	Guacharaca	Guacharaca De Madera	Ceac	Yesid Ramirez	0000
663	Planta	Planta Electrica	Ceac	Yesid Ramirez	0000
664	Estante	Estante De Metal	Ceac	Yesid Ramirez	0000
665	Estante	Estante De Metal	Ceac	Yesid Ramirrez	0000
666	Estante	Estante De Metal	Ceac	Yesid Ramirez	0000
667	Estante	Estante De Metal	Ceac	Yesid Ramirez	0000
668	Estante	Estante De Metal	Ceac	Yesid Ramirez	0000
669	Estante	Estante Metal	Ceac	Yesid Ramirez	0000

ANEXO L: ARTÍCULO INVESTIGATIVO

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN ALCALDÍA DE RÍO DE ORO, CESAR.

Kathedrin Sánchez Arias
Esp. Yesenia Areníz Arévalo
Facultad de Ingenierías
Plan de Estudios de Ingeniería de Sistemas
Universidad Francisco de Paula
Santander Ocaña
ksancheza@ufpso.edu.co

RESUMEN

Las Alcaldías son entidades del estado, del orden territorial y al servicio de la comunidad y cuyo objetivo es brindar programas de educación, salud, bienestar, servicios públicos y protección; de los cuales se maneja gran cantidad de información confidencial, que de no estar segura, generaría una mala imagen institucional, inconsistencias y pérdidas.

Para definir el nivel de seguridad en la Alcaldía, se realizó una investigación, mediante la aplicación de encuestas dirigidas a su personal de planta y OPS, con el fin determinar el nivel de efectividad de los controles que actualmente aseguran la información manejada por esta.

Como se demuestra en la investigación realizada, la vigilancia se mantiene solo en las horas de la noche, no se realiza controles en los horarios laborales, accesos del personal y visitantes, no se registra el uso de los sistemas, documentos institucionales y servicios, ni se investigan las incidencias ocurridas. Además algunas áreas carecen de identificación, alarmas, cámaras, detectores de humo o extintores y de la prohibición del consumo de alimento y bebidas, o el fumar, entre otras.

Tras el análisis de las necesidades presentes, se recomienda aplicar las Políticas de Seguridad de la Información ajustadas a la Alcaldía, fomentando el compromiso de uso.

Palabras Claves

Alcaldía, Análisis de riesgos, ISO/IEC 27002 y Seguridad de la información.

Abstract.

The mayors are entities of state, territorial order and serving the community which aims to provide education, health, welfare, public services and protection; of which large amount of confidential information that you are not sure, generate a poor corporate image, inconsistencies and losses are handled.

To define the level of security at City Hall, an investigation was carried out by applying its surveys of plant personnel and OPS, to determine the level of effectiveness of controls to ensure the information currently managed by this.

As demonstrated in the investigation, surveillance is maintained only in the evening hours, no controls on working hours, access for staff and visitors is performed, the use of systems, institutional documents and services is not recorded, nor investigated the incident occurred. In addition, some areas lack identification, alarms, cameras, smoke detectors, fire extinguishers and the prohibition of the consumption of food and beverages, or smoking, among others.

After analyzing the present needs, it is recommended to apply the Policy Information Security tight for mayor, fostering commitment of Use.

Key Words.

Governorship, Analysis of risks, ISO/IEC 27002and Security of the information.

INTRODUCCIÓN

La seguridad informática siempre ha sido importante, desde los inicios de los computadores, pero ahora se ha agudizado más la importancia de contar con buenos mecanismos de seguridad debido a que los riesgos y amenazas no solamente consisten en que personas que se encuentren en el área donde están los equipos, roben información, sino que ahora también existen riesgos de robo o accesos no autorizados a información mediante las diferentes redes que interconectan a los computadores o a cualquier equipo tecnológico utilizado para transmitir información digital.

Aunque muchas entidades públicas y privadas le restan valor o importancia al aspecto de seguridad, no se puede dudar que las pérdidas por la falta de seguridad pueden ser realmente caras, tanto en materia económica como en prestigio o problemas legales, entre otros.

En vista de la importancia que tiene la seguridad en las tecnologías de la información, es suficiente estudiar buenas prácticas y consejos sabios de personas que llevan una gran trayectoria en el área de la informática, sino que más aún, Normas Internacionales certificables, son un beneficio de grandes magnitudes para cualquier organización. Por esto, la adopción de la Norma Internacional ISO/IEC 27002 es totalmente beneficioso para cualquier entidad que tenga que ver de alguna forma con la seguridad de las tecnologías de la información, mediante la implementación de acciones y procedimientos necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información.

La Organización Internacional de Normalización (ISO) y La Comisión Electrotécnica Internacional (IEC), se unieron para crear lo que actualmente son lineamientos de seguridad que se ajustan a los objetivos de las organizaciones, los cuales se encuentran consagrados en un documento titulado “Política de Seguridad de la Información” referenciado como la norma internacional de buenas práctica ISO/IEC 27002, compuesta por 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Esta política cuenta con una serie de lineamiento de implementación, que definen el tema, sus objetivos, alcances e importancia, estructuras de evaluación y gestión de riesgos, entre otros.

Se debe saber que ningún conjunto de controles puede lograr la seguridad completa, pero sí puede reducir al máximo los riesgos que amenacen con afectar la seguridad en una organización. Por lo que las políticas de seguridad de la información deben ser continuamente revisadas y actualizadas para que se mantengan en condiciones favorables y en concordancia con los cambios tecnológicos y demás, que se den a través del tiempo.

El documento de la política de seguridad de la información, debe ser creado de forma particular por cada organización, aprobado por la administración y luego publicado y comunicado a todo el personal y las partes externas relevantes. Pero no antes de realizar un análisis de riesgos y controles actualmente aplicados, que definan los lineamientos a implementar, para minimizar los riesgos a los cuales se encuentra expuesta la información en la actualidad.

Para el caso, la Alcaldía Municipal de Río de Oro (Cesar), está conformada por cuatro (4) Secretarías, las cuales brindan apoyo al alcalde en los diferentes programas, estas son: La Secretaría de Gobierno, Planeación, Hacienda y Salud, de las cuales dependen oficinas, como: La Comisaría de Familia, La Inspección de Policía, La Coordinación de Cultura, Deporte y Recreación, La Coordinación Ambiental, de Salud Pública, de Promoción Social, La Coordinación del SISBEN y de Gestión de Banco de Proyectos. Además existen oficinas destinadas al apoyo de Los Programas de Más Familias en acción, Adulto Mayor y Victimas.

Materiales y Métodos.

Con el fin de determinar, ¿En qué medida, es necesaria la aplicación de Políticas de Seguridad de la Información en la Alcaldía de Río de Oro, Cesar?, se realizó una investigación que buscaba calcular el nivel de aplicación y de efectividad de los controles de seguridad de la información en esta; usando como técnica, una encuesta dirigida a 21 de los 31 empleados que componen el organigrama, distribuidos en 13 empleados de planta y 8 OPS, con el propósito de lograr un paralelo entre ellos.

Se empleó el tipo de investigación descriptiva, ya que se refirieron las características de la situación actual en la Alcaldía, mediante representaciones gráficas, asociadas a los cuestionarios realizados.

RESULTADOS

A continuación se reflejan y detallan los resultados de la investigación anteriormente descrita.

Por parte de los Empleados de Planta:

Figura 1. Acuerdo de Confidencialidad

Se observa que el 85% de los encuestados, no cuenta con un acuerdo de confidencialidad de la información, de los cuales poco más de la mitad, no conoce

sus responsabilidades y sanciones, frente a la seguridad de la información, mientras que el 15% restante, cuenta con pleno conocimiento de estas, de decretos o resoluciones Institucionales.

Figura 2. Áreas Identificadas

El 54% de los empleados afirma que el área en la cual labora se encuentra debidamente identificada, mientras que el 46% afirma que no lo está, lo que provoca que los visitantes no encuentren el área de la cual requieren el servicio, creando retrasos y una mala imagen institucional.

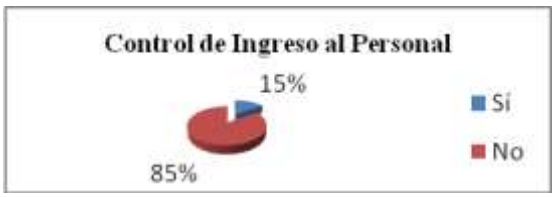


Figura 3. Control de Ingreso al Personal

El ingreso del personal no es controlado en un 85%, así con el trabajo fuera del horario laboral definido, por la administración.

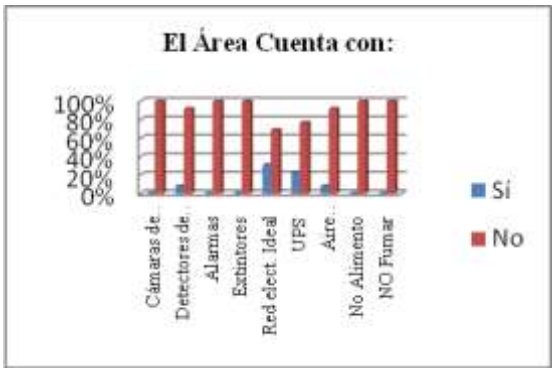


Figura 4. El Área Cuenta con

En la figura 4. Se observa que ninguna de las áreas cuenta con cámaras de vigilancia, Alarmas o Extintores, y sólo el 8% cuenta con detectores de humo, lo que implica un riesgo importante en la Alcaldía.

Figura 5. Cuenta con Registros de.

La Alcaldía no cuenta con el registro de acceso a sus instalaciones del personal y los visitantes, ni del uso de los sistemas por alguien distinto al empleado en específico. Además, el uso de los documentos institucionales sólo se registra en un 15% y el uso de los servicios de red en un 38%.

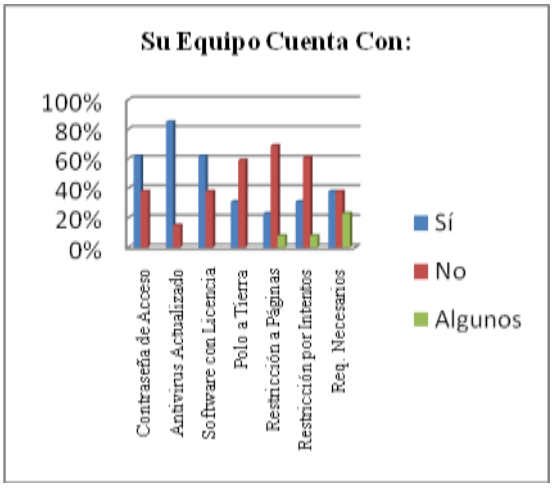


Figura 6. Su Equipo Cuenta con

El 62% de los equipos cuenta con una contraseña (para permitir el acceso de usuarios a los sistemas), por su parte el

85% de estos, mantiene el antivirus actualizado, el 62% cuenta con su software licenciado e indistintamente el 59%, carece de polo a tierra.
Las restricciones de acceso a páginas web (redes sociales, etc.) en los equipos de los empleados encuestados, es del 23% para todas, del 69% para ninguna y el 8% para algunas de estas.

Por otra parte el acceso restringido a las aplicaciones después de varios intentos es usado en el 23% de los equipos, nulo en el 61% y parcial en el 8%.Además, el 38% de los encuestados consideran que su equipo cuenta con los requerimientos necesarios para la realización óptima de sus labores, al igual que una misma fracción de estos considera que no, pero indistintamente un 8%, considera que cuenta con solo algunos de estos requerimientos.

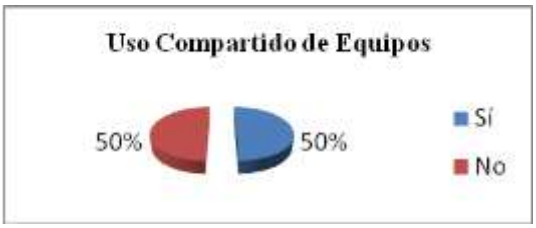


Figura 7. Uso compartido de Equipos

La figura 7. Muestra que el 50% de los equipos es usado por alguien además del encuestado, una situación que contrasta con la seguridad de la información.

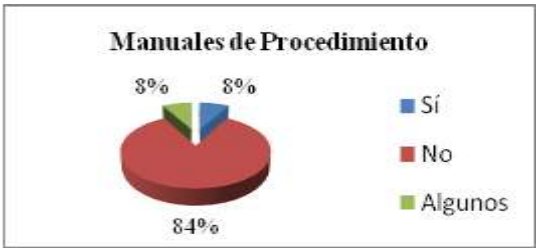


Figura 8. Manuales de procedimiento

Se evidencia en la figura anterior, el gran porcentaje que afirma no disponer de un manual de procedimiento, limitando en gran medida las actividades del área.

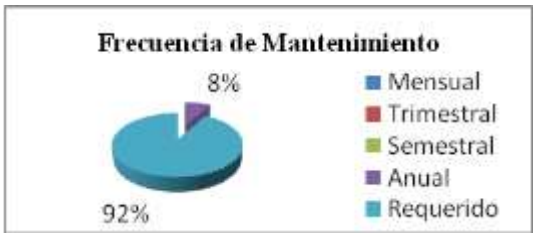


Figura 9. Frecuencia de Mantenimiento.

En cuanto a la frecuencia con la que los equipos a disposición de los encuestados, recibe mantenimiento, es del 92% cuando este lo requiere y el 8% Anualmente. Es indudable la falta de mantenimiento preventivo que reciben estos equipos, poniendo en riesgo la información en las áreas.

Figura 10. Escritorio Libre de.

En lo referente a la política de escritorios limpios, el 58% de los empleados afirma que su escritorio no permanece libre de archivos o documentos institucionales.

El 83% de ellos mantiene su escritorio libre de alimentos y el 75%, libre de polvo.

Se puede percibir que hay un nivel de cultura entre los funcionarios a cerca de la importancia de cuidar los equipos ante los inminentes riesgos de la cotidianidad, pero se debe mejorar aún más.

Figura 11. Realización de Backup's.

La figura 11, muestra que el 33% de los encuestados no realiza Backup's (Copias de Seguridad) de la información a su disposición, mientras que el otro 67% prefieren almacenar sus backup's en memorias USB, Discos Duros o imprimirlas, las cuales son realizadas con una periodicidad diaria, semanal y hasta mensual.

En cuanto al almacenamiento de Backup's, los encuestados prefiere resguardar su información en estantes o gavetas, muebles con cerradura o archivadores, y en algunos casos un sitio fuera de las instalaciones de la Alcaldía, para prevenir la pérdida de datos en caso de incidencias.

En ese sentido y debido a que la información debe mantenerse segura, gran parte de los encuestados opina que el acceso a las copias de respaldo o documentos institucionales es restringido, según el rol del funcionario dentro de la Alcaldía y su solicitud puede realizarse de forma verbal o escrita.

Aunque la Alcaldía es un establecimiento público, que debe brindar la disponibilidad de la información ante la solicitud del interesado, existe cierta información que debe ser confidencial para evitar episodios que pongan en peligro su integridad. Por tal razón, los encuestados concuerdan en que cierta información no debe ser divulgada y que su solicitud en la mayoría de los casos debe realizarse de forma escrita.

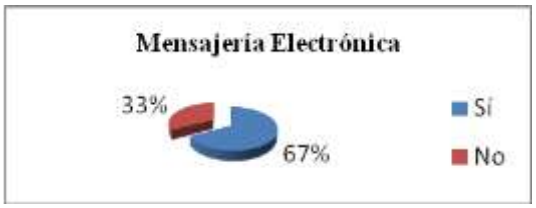


Figura 12. Mensajería Electrónica

Los empleados no cuentan con ningún tipo de aplicación que les permita encriptar su información de destinatarios no deseados, confiando en los controles de seguridad que practican los proveedores de correo electrónico, sin embargo el uso de mensajería electrónica es del 67%. Así mismo no cuentan con un procedimiento formal para reporte de incidentes (robos de información, pérdida de datos, accesos no permitidos, etc.), de los que hasta el momento no se realizan investigaciones, ni recolección de evidencias.

Figura 13. Descargas

El 42% de los encuestados realiza descargas de música, películas, programas entre otros, lo que pone en riesgo la seguridad de la información a su cargo, debido a los virus al realizala.

Por parte de los Empleados OPS:

Figura 14. Acuerdo de Confidencialidad

Se observa que el 62% no cuenta con un acuerdo de confidencialidad de la información, la mitad de ellos no tiene conocimiento de sus responsabilidades y sanciones, frente a la seguridad de la información, mientras que los demás, cuentan con pleno conocimiento de dicha normatividad.

Figura 15. Control de Ingreso al Personal

Al personal no se le controla el acceso al igual que su trabajo fuera del horario laboral definido, por la administración.

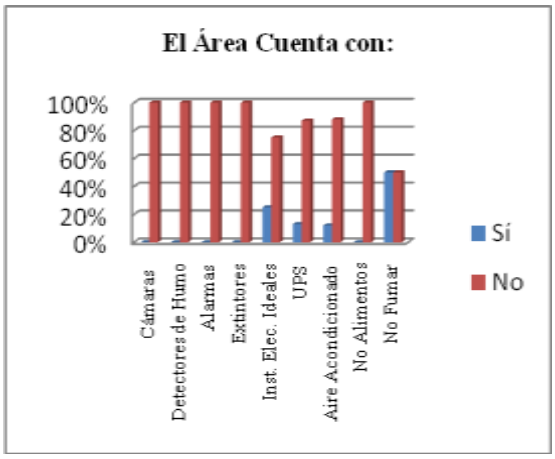


Figura 16. El Área Cuenta con

En la figura 16. Se observa Que ninguna de las áreas de trabajo de los empleados OPS, cuenta con cámaras de vigilancia, detectores de humo, alarmas o Extintores.

Figura 17. Cuenta con Registros de

En la figura anterior, se aprecia que la Alcaldía Municipal no cuenta en un 100% con el registro de acceso a sus instalaciones del personal y los visitantes, ni del uso de los sistemas por alguien distinto al empleado en específico.

Además, el uso de los documentos institucionales sólo se registra en un 38% el uso de los servicios de red en un 0%.

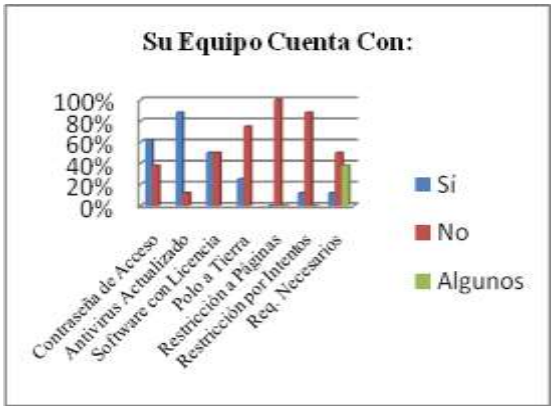


Figura 18. Su Equipo Cuenta con

En lo relacionado con los controles de seguridad de la información aplicados en cada equipo, cabe mencionar que el 62% de los equipos de los empleados encuestados cuenta con una contraseña (para permitir el acceso de usuarios a los sistemas), mientras que el 88% de estos, mantiene el antivirus actualizado, el 50% cuenta con su Software licenciado e

indistintamente el 25%, carece de polo a tierra.

Las restricciones de acceso a páginas web (redes sociales, etc.) en los equipos de los empleados encuestados son del 0% para todas, del 100% para ninguna y el 0% para algunas de estas.

Por otra parte el acceso restringido a las aplicaciones después de varios intentos es de total uso en el 12% de los equipos, nulo en el 88% y parcial el 0%.

Además, el 12% de los encuestados consideran que su equipo cuenta con los requerimientos necesarios para la realización óptima de sus labores, pero el 50% de estos considera que no, indistintamente un 38%, considera que cuenta con sólo algunos de estos requerimientos.

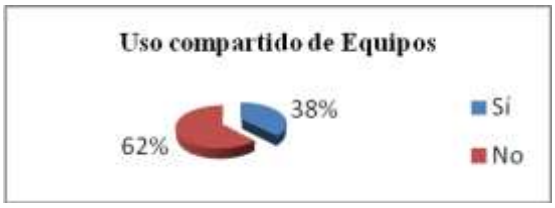


Figura 19. Uso compartido de Equipos

A diferencia de los empleados de planta, en los OPS el número se incrementa a un 67% de aquellos quienes el uso de su computador es exclusivo.

Figura 20. Frecuencia de Mantenimiento.

En cuanto a la frecuencia con la que los equipos a disposición de los encuestados, recibe mantenimiento, es del 63% cuando este lo requiere, el 25% Anualmente y el 12% Trimestralmente. En los OPS existe al menos un pequeño porcentaje de mantenimientos que se hacen de forma preventiva, aunque el número si debería ser mayor.

Figura 21. Escritorio Libre de

En lo referente a la política de escritorios limpios, el 38% de los empleados afirma que su escritorio no permanece libre de archivos o documentos institucionales.

El 88% de ellos mantiene su escritorio libre de alimentos y el 50%, libre de polvo.

Frente a los de planta hay una mayor cultura de los elementos que pueden afectar los equipos, pero es necesario se siga trabajando en este aspecto.

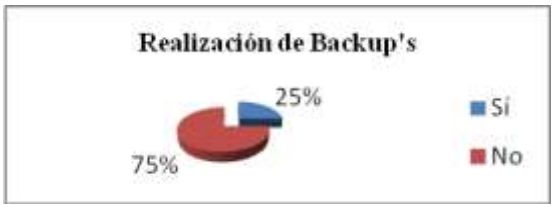


Figura 22. Realización de Backup's

La figura 22. Muestra que el 75% de los encuestados no realiza Backup's (Copias de Seguridad) de la información a su disposición, mientras que el otro 25% prefieren almacenar sus backup's en memorias USB, Discos Duros o imprimirlas.

Figura 23. Periodicidad de Backup's

En la figura 23. Se observa que los empleados encuestados realizan sus backup's con una periodicidad diaria en un 50%, mientras que semanalmente se realizan en el 50% restante, convirtiéndose en un ejercicio apropiado para la seguridad de la información.

En cuanto al almacenamiento de Backup's, los encuestados prefieren resguardar su información en estantes o gavetas.
Debido a que la información debe mantenerse segura, el 100% de los encuestados opina que el acceso a las copias de respaldo o documentos institucionales es restringido, según el rol del funcionario dentro de la Alcaldía y su respectiva solicitud de acceso debe realizarse de forma verbal o escrita, depende el caso.

Los encuestados concuerdan en opinar que la información confidencial no sea divulgada.

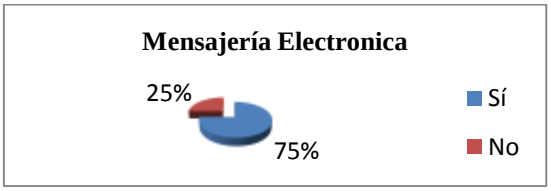


Figura 24. Mensajería Electrónica

Como se evidencia en la figura anterior, un gran porcentaje (75%), hacen uso de la mensajería electrónica, pero no cuentan con ningún control adicional al que suministra el proveedor.

Figura 25. Descargas.

El 62% de los encuestados realiza descargas de música, películas, programas entre otros, lo que pone en riesgo la seguridad de la información a su cargo, debido a virus al descargar.

RECOMENDACIONES

Tras el análisis de los resultados obtenidos en esta investigación, se recomienda:

- Realizar el respectivo control de los horarios laborales de los empleados.
- Realizar el registro de accesos del personal y los visitantes a las instalaciones.
- Realizar el registro de uso de los sistemas, documentos institucionales y servicios.
- Implementar planes de contingencia y realizar la respectiva investigación de incides ocurridos.
- Contar con vigilantes las 24 horas del día.
- Realizar la respectiva y correcta identificación de la totalidad de las áreas pertenecientes a la Alcaldía.
- Contar con una recepcionista para las áreas con mayor flujo de personas.
- Instalar alarmas, cámaras de vigilancia, aire acondicionado, detectores de humo y extintores en áreas estratégicas, además de contar y mantener cargadas las UPS´s necesarias.
- Prohibir el consumo de alimentos y bebidas, así como fumaren el área de trabajo o cerca a los equipos.

- Contar con acuerdos de confidencialidad físicos, que describan sus responsabilidades y sanciones, en caso de provocar la violación a la seguridad de la información a su disposición.
- Contar con manuales de procedimiento necesarios para la operación de los sistemas de su área.
- Realizar copias de respaldo de la información a su cargo, para evitar la pedida de esta.
- Permitir el acceso a los documentos institucionales solo a personas autorizadas.
- Realizar comunicaciones electrónicas, solo por medios seguros.
- Evitar al máximo la descarga de archivo, a menos que sea de una página considerablemente segura.
- Mantener una contraseña de acceso, de tipo alfanumérico, con mínimo 10 caracteres, no deducible y cambiada regularmente.
- Mantener el software (sistema operativo, antivirus, programas, etc.) licenciado y actualizado (preferiblemente últimas versiones o al menos que aun mantengan soporte del proveedor).
- Restringir el acceso a páginas web, que comprometan la seguridad de la información.
- Establecer restricciones de acceso por contraseña luego al menos tres (3) intentos erróneos.
- Contar con los requerimientos necesarios para la realización optima de las labores diarias de los empleados.
- Evitar al máximo que los equipos sean usados por más de una (1) persona.
- Contar con polo a tierra, evitar accidentes.
- Establecer planes de mantenimiento continuo.

CONCLUSIONES

A través de la investigación realizada, sobre los controles de seguridad de la información que actualmente se lleva a cabo, en la Alcaldía Municipal de Río de Oro (Cesar), se puede concluir que: su información es propiedad del municipio y requiere una protección especial que garantice su preservación así como su integridad, confidencialidad y disponibilidad.

A modo de consideraciones, se recomienda: Aplicar las Políticas de Seguridad de la Información ajustadas a la Alcaldía, además de fomentar el compromiso en los empleados con la aplicación de los controles allí consagrados.

REFERENCIAS

ERB, Markus. Gestión de Riesgo en la Seguridad Informática. Amenazas y Vulnerabilidades. España. 3h. [en línea]. http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

GOVERNANCE INSTITUTE, OFICINA GUBERNAMENTAL DE COMERCIO y THE STATIONERY OFFICE. Alineando COBIT 4.1, ITIL V3 e, ISO/IEC 27002 en beneficio del negocio. Estados Unidos e Inglaterra. 2010. 130h. [en línea]. http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf.

MINISTERIO DE LA INFORMATICA Y LAS COMUNICACIONES. Reglamento sobre Seguridad Informática. La Habana. Cuba. 2012. 15h. [en línea]. http://fcmfajardo.sld.cu/seguridad_informatica/resol_y_dispos_del_mic/reglamento_seguridad_informatica.pdf

MINISTERIO DEL INTERIOR Y DE JUSTICIA DE COLOMBIA. Dirección Nacional del Derecho de Autor. Unidad Administrativa Especial. [en línea]. http://www.propiedadintelectualcolombia.com/Site/LinkClick.aspx?fileticket=yDsveWsCdGE%3D&tabid=

PRESIDENCIA DEL CONSEJO DE MINISTROS DE PERU. Políticas de Seguridad Informática a través de la Oficina de Gobierno Electrónico e Informático. Lima. Perú. 2013. 15h. [en línea]. http://www.enterese.net/entidades-del-estado-se-modernizan-con-politicas-de-seguridad-informatica/

SUPERINTENDENCIAS DE SOCIEDADES. Manual Manejo y Control Administrativo de los Bienes de Propiedad. Bogotá D.C., Colombia, 2009. 29h. [en línea]. http://www.supersociedades.gov.co/web/Ntrabajo/SISTEMA_INTEGRADO/Documentos%20Infraestructura/DOCUMENTOS/GINF-M-001%20MANUAL%20ADMINISTRATIVO.pdf

FRANCISCO DE PAULA SANTANDER OCAÑA. Modulo Evaluación de la Seguridad de la Información. Ocaña. Colombia. 2012. 65h.

UNIVERSIDAD LIBRE. Acuerdo No. 05 (Noviembre 17 de 2009). Colombia. 2009. 85h. [en línea]. http://www.unilibre.edu.co/images/pdf/acd_05-09.pdf

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Gerencia de Innovación y Desarrollo Tecnológico. Última actualización el Lunes, 22 de Abril de 2013 09:05. [en línea]. http://www.unad.edu.co/gidt/index.php/leyesinformaticas