RESUMEN - TESIS DE GRADO

AUTORES	**MAIRE LISNETH SERNA VEGA** **ALEIDA DURAN PEÑARANDA** **ROSY SANCHEZ ACOSTA**
FACULTAD	**DE INGENIERÍAS**
PLAN DE ESTUDIOS	**ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS**
DIRECTOR	**ANDRÉS MAURICIO PUENTES VELÁSQUEZ**
TÍTULO DE LA TESIS	**DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA SECRETARIA DE HACIENDA DE RIO DE ORO-CESAR, BASADO EN LA NORMA ISO/IEC 27001:2013**

RESUMEN
(70 palabras aproximadamente)

EL DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA NORMA ISO/IEC 27001:2013, Y EN LA NORMA ISO/IEC 27005:2011; LE PROVEERÁ A LA SECRETARIA DE HACIENDA DE RIO DE ORO CESAR, LOS ELEMENTOS NECESARIOS PARA PODER GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN Y MINIMIZAR LOS RIESGOS REALES Y POTENCIALES DE LOS ACTIVOS DE LA INFORMACIÓN, DE UNA FORMA ORGANIZADA Y EFICIENTE

CARACTERÍSTICAS

PÁGINAS: 184	PLANOS:	ILUSTRACIONES: 2	CD-ROM: 1

DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA SECRETARIA DE HACIENDA DE RIO DE ORO-CESAR, BASADO EN LA NORMA ISO/IEC 27001:2013

AUTORES:

MAIRE LISNETH SERNA VEGA

ALEIDA DURAN PEÑARANDA

ROSY SANCHEZ ACOSTA

Trabajo de grado presentado para optar el título de especialistas en Auditoria de Sistemas

Director

Ing. ANDRÉS MAURICIO PUENTES VELÁSQUEZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER

FACULTAD DE INGENIERIAS

ESPECIALIZACION EN AUDITORIA DE SISTEMAS

Ocaña, Colombia Octubre, 2017

Índice

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Resumen

Para la Secretaria de Hacienda de Rio de Oro-Cesar es de vital importancia garantizar la protección de la información y de toda la infraestructura que soporta el sistema de información de la dependencia. Por lo tanto el presente trabajo de grado se sustentó en el Diseño de un Sistema de Gestión de la Seguridad de la Información, basado en el estándar internacional ISO/IEC27001:2013.

Para llevar a cabo el Diseño del SGSI, se hizo necesario inicialmente realizar un diagnóstico de la situación actual de la gestión de la seguridad de la información en la Secretaria de Hacienda de Rio de Oro-Cesar. Seguidamente se determinó el estado de madurez desde la óptica de los procesos misionales de la dependencia, frente a los requerimientos metodológicos y de acuerdo a los dominios y controles establecidos en el anexo A de la norma ISO IEC-27001:2013. Posteriormente se aplicó la metodología para la Gestión del Riesgo, propuesta en la norma ISO/IEC 27005, logrando identificar las principales vulnerabilidades y amenazas, a las que se encuentran expuestos los principales activos ligados al sistema de información de la Secretaria de Hacienda, con el fin de llevar a cabo el plan para el tratamiento de riesgos de la seguridad de la información, de acuerdo a los hallazgos encontrados y por último se definieron las políticas de seguridad de la información que proveen a la dependencia de los lineamientos necesarios para proteger sus activos.

Introducción

La información en los últimos tiempos se ha convertido en uno de los activos más valiosos con los que cuenta cualquier tipo de organización (MONTOYA, 2016).

Por lo anterior, es preciso que los responsables del uso y manejo de la información dentro de las organizaciones, tengan conciencia de los riesgos que pueden afectar la seguridad de la información, con el fin de establecer controles, orientados a salvaguardar tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas.

En el caso particular de la Secretaria de Hacienda del municipio de Rio de Oro Cesar, no se cuenta con una adecuada Gestión de Seguridad de la Información, lo que dificulta visualizar el estado real y la efectividad de los sistemas de información existentes .

Los responsables de la Secretaria de Hacienda, son conscientes de que la seguridad de la información establecida por la dependencia no es suficiente; de ahí surgió la necesidad diseñar un SGSI basado en la norma ISO/IEC 27001:2013 que se enmarcó en la fase planear del ciclo de Deming PHVA que corresponde al diseño, el mismo no abarca la fase de implementación, mantenimiento y revisión del Sistema de Gestión de Seguridad de la Información, que se relaciona con las fases Hacer, Actuar y Verificar. El diseño de un SGSI, le permitirá a la Secretaria de Hacienda de Rio de Oro-Cesar, establecer un modelo adecuado de seguridad de la información, basado en las buenas practicas del manejo y uso de la misma, promoviendo y extendiendo una cultura de seguridad en todos los niveles de la dependencia y fortaleciendo en la

mente de sus colaboradores los principios fundamentales de la información en cuanto integridad, confidencialidad y disponibilidad.

Para llevar a cabo el Diseño SGSI, para la Secretaria de Hacienda de Rio de Oro-Cesar, se utilizó el tipo de investigación descriptiva cualitativa, con aporte de herramientas cuantitativas. En esta etapa se elaboraron los instrumentos de recolección de la información que permitieron el desarrollo y posterior cumplimiento de los objetivos.

Capítulo 1. Diseño de un sistema de gestión de la seguridad de la información para la Secretaria de Hacienda de Rio de Oro-Cesar, basado en la norma ISO/IEC 27001:2013.

1.1 Planteamiento del problema

La información en los últimos tiempos se ha convertido en uno de los activos más valiosos con los que cuenta cualquier tipo de organización (MONTOYA, 2016). Sin embargo la seguridad de la información se ha limitado a la simple percepción de adquisición de nuevas tecnologías y solamente se relaciona con el área de sistemas.

Lo anterior se confirma en los ataques informáticos a los que han estado expuestas la empresas y los diferentes municipios del país y que han afectado directamente los activos de información y sus recursos financieros, ejemplo de ello es el robo por banca virtual ocurrido en el año 2016 en el Municipio de Timbío – Cauca, en donde fueron hurtados 146 millones de pesos luego de haber suplantado las cuentas del alcalde y el secretario de hacienda el año anterior. (RCN radio, 2016). Entre otros muchos casos que se dan a diario a nivel nacional.

Por tal razón, es preciso que los responsables del uso y manejo de la información dentro de las organizaciones, tengan conciencia de los riesgos que pueden afectar la seguridad de la información, con el fin de establecer controles, orientados a salvaguardar tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas.

En el caso particular de La Secretaria de Hacienda de Rio de Oro Cesar, por ser una entidad de carácter público y estar vigilada por los entes de control del Estado, está en la obligación de cumplir con la normatividad vigente, orientada a garantizar la seguridad, protección y privacidad de la información financiera y personal de los usuarios de sus bases de datos. Lo anterior implica que la entidad debe contar con estándares de seguridad que le permitan asegurar los sistemas de recolección, almacenamiento, tratamiento, uso y manejo de la información.

Actualmente La Secretaria de Hacienda de Rio de Oro Cesar, no cuenta con una adecuada Gestión del Sistema de Seguridad de la Información, lo que se evidencia en un insipiente sistema de gestión de riesgos, en una escasa gestión de la seguridad de la información de las áreas involucradas y en la poca conciencia en el tratamiento de la seguridad de la información por parte de los funcionarios de la dependencia.

La situación anterior dificulta visualizar el estado real y la efectividad de los sistemas de información. Lo que puede generar una imagen negativa para la dependencia y un desgaste innecesario de recursos técnicos, humanos y económicos.

Con la Gestión de la seguridad de la información en la Secretaria de Hacienda de Rio de Oro-Cesar, la entidad podrá contar con una serie de elementos que le permitirán a sus directivos tomar decisiones convenientes a las falencias presentadas en el sistema que soporta los procesos operativos y toda la infraestructura ligada a los mismos. De igual forma le facilitara optimizar la administración de la información por parte de los usuarios a través de la inclusión de procesos,

procedimientos y políticas que promuevan una cultura de buenas prácticas de seguridad de la información al interior de la dependencia.

1.2 Formulación del problema

¿Un sistema de Gestión de la Seguridad de la Información, le proporcionara a la Secretaria de Hacienda del Municipio de Rio De Oro-Cesar, contar con los elementos necesarios e idóneos para mejorar la seguridad de la información de la dependencia y la gestión y el tratamiento de los riesgos asociados al uso de la información?

1.3 Objetivos

1.3.1 Objetivo general. Diseñar un sistema de gestión de la seguridad de la información para la Secretaría de Hacienda de Rio de Oro-Cesar, basado en la norma ISO/IEC 27001:2013.

1.3.2 Objetivo específicos. Realizar un diagnóstico de la Secretaria de Hacienda de Rio de Oro-Cesar, con relación a la gestión de la seguridad de la información.

Determinar el nivel de madurez de la Secretaria de Hacienda con respecto al modelo de seguridad de la información que plantea la norma ISO/IEC 27001:2013.

Efectuar un diagnóstico de los riesgos de la seguridad de la información en la Secretaria de Hacienda de Rio de Oro-Cesar.

Documentar las buenas prácticas de Seguridad de la información de la Secretaria de Hacienda de Rio de Oro-Cesar tomando como base la norma ISO 27001:2013.

1.4 Justificación

Partiendo de la base que "la información es la herramienta que hace fuerte a las empresas" (CONSULTORES, s.f.) y tomando en cuenta que las mismas, debido al avance de las tecnologías de la información, están expuestas a una serie de amenazas informáticas que cada día son más complejas y especializadas. Se hace necesario que las organizaciones se concienticen y le den prioridad al tema relacionado con la seguridad de la información, estableciendo políticas, planes y controles orientados a garantizar la confidencialidad, integridad y disponibilidad de la información que procesa.

En el caso particular de La Secretaria de Hacienda de Rio de Oro-Cesar, la información que maneja es de suma importancia, por cuanto la dependencia es la encargada de llevar a cabo todos los procesos relacionados con la Gestión Fiscal, Gestión de Impuestos, Gestión Financiera y Gestión Contable. Y gran parte de la información institucional, se encuentra depositada en los equipos, en los sistemas de información, en la base de datos y en formatos físicos que usan y operan el personal administrativo de la dependencia.

Los responsables de la Secretaría son conscientes de que la seguridad de la información establecida por la dependencia no es suficiente. Por lo tanto es preciso que la dependencia, cuente con los elementos necesarios y adecuados para gestionar de manera eficiente la

seguridad de la información y de esta forma le garantizarle un servicio confiable a todos sus usuarios.

Es por lo anterior que este proyecto se sustenta en el diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013, para la Secretaria de Hacienda de Rio de Oro-Cesar, el cual le facilitará a la entidad, las condiciones de gobernabilidad, oportunidad y viabilidad necesarias para que la seguridad de la información apoye y se extienda a los objetivos estratégicos de la misma, mediante la protección y aseguramiento de su información y con ello asegurar el cumplimiento de su misión. Además la dependencia podrá medir y cuantificar el nivel de madurez de los indicadores basados en la norma ISO/IEC 27001:2013, con el fin de establecer el estado actual de la seguridad de la información y a partir de este punto, definir los controles, procedimientos y estándares para el tratamiento de la información, adaptados a los cambios que se produzcan el entorno y las tecnologías.

El diseño de un Sistema de Gestión de Seguridad de la información, también le permitirá a la Secretaria de Hacienda, establecer un adecuado modelo de seguridad de la información, basado en las buenas practicas del manejo y uso de la misma, promoviendo y extendiendo una cultura de seguridad en todos los niveles de la dependencia y fortaleciendo en la mente de sus colaboradores los principios fundamentales de la información en cuanto integridad, confidencialidad y disponibilidad.

Por último a través del Sistema de Gestión de la Seguridad de la Información, la Secretaria de Hacienda inicialmente tendrá la oportunidad de identificar las amenazas que

pueden llegar a comprometer los activos que conforma su sistema de información, y seguidamente podrá gestionar de manera efectiva los riesgos asociados a la seguridad de la información con el fin de establecer los mecanismos necesarios tendientes a minimizar el impacto en caso de presentarse la materialización de una vulnerabilidad y por ende mitigar, asumir, aceptar o transferir el riesgo.

1.5 Hipótesis

El Sistema de Gestión de Seguridad de la información para la Secretaria de Hacienda de Rio de Oro-Cesar, permitirá detectar las falencias y las amenazas a las que se encuentra expuesta la dependencia con el fin de mitigar los riegos existentes y salvaguardar la información.

1.6 Delimitaciones

1.6.1 Delimitación conceptual. Para el diseño de un Sistema de Gestión de la Seguridad de la Información para la Secretaria de Hacienda del Municipio de Rio de Oro – Cesar, se tendrán en cuenta conceptos relacionados con: gestión, tecnología auditoria, políticas, seguridad de la información, riesgos, controles, normas entre otros.

1.6.2 Delimitación geográfica. La investigación objeto de este estudio se llevará a cabo en las instalaciones de Secretaria de Hacienda del Municipio de Río de Oro – Cesar

1.6.3 Delimitación temporal. La propuesta se ejecutará durante tres (3) meses. Las actividades correspondientes al cumplimiento de los objetivos se programarán de acuerdo al tiempo y necesidades de los responsables de la investigación.

Capítulo 2. Marco Referencial

2.1 Marco histórico

El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial.

Esta ofrece muchas áreas de profundización, incluidos la auditoría de sistemas de información, Planificación de la continuidad del negocio, Ciencia Forense Digital y los Sistemas de Gestión de Seguridad de la información por nombrar algunos.

Los procedimientos de seguridad de la información surgen como una herramienta organizacional para concienciar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información que favorecen el desarrollo y el buen funcionamiento de la organización (Alexander, Alexander, & Buitrago, 2007).

La seguridad de la información ha sido una preocupación que les surgió a las empresas desde muchos años atrás, las alusiones en la historia a la protección de la información son muy numerosos. Como casos más conocidos están la 'máquina enigma' de la II Guerra mundial o la defensa de archivos estatales en cualquier país (20minutos, 2011), pero en sí, la historia de la seguridad de la información puede ser tan antigua como la humanidad misma, pero la historia de la seguridad de la información contenida en archivos digitales o sistemas computacionales data de ciertas fechas que se mencionan a continuación (Argüello, 2014) y que son referentes mundiales:

En Junio de 1942, un problema criptográfico japonés tuvo como consecuencia la destrucción de sus 4 mayores portaaviones y supuso el fin del dominio japonés del Pacífico.

En 1983 nace la Internet, aunque el concepto original se remonta los años 60 cuando el Ministerio de Defensa de Estados Unidos estableció una red interestatal, de modo que toda la defensa del país dependiera de la misma red y compartiera los recursos de ésta. Así nació ARPANet (Advanced Projects Agency Net, llamada también DARPANet, por Defensa), con tres requisitos fundamentales:

A ARPANet se le unen, todavía en Estados Unidos, otras instituciones, como Universidades, centros gubernamentales, organizaciones privadas, etc. A principios de los 80 se unen otros países.

Así en 1983 nace lo que hoy conocemos como Internet o la red de redes, ya con un gran número de usuarios y ordenadores enlazados o con la capacidad de enlazarse.

El 2 de Noviembre de 1988 un joven llamado Robert Morris escribió un pequeño programa capaz de, usando algunas vulnerabilidades de UNIX, transmitirse de unos sistemas a otros a gran velocidad infectándolos a su paso. En unas horas miles de equipos tenían sus CPUs al 100% sin solución de continuidad. Se trataba del primer Gusano (Worm) de la historia.

En Junio de 2005 un hacker logró un listado de 40 millones de tarjetas de crédito. Servired, Visa y 4B tuvieron que localizar y avisar urgentemente a más de 50.000 clientes en España del riesgo que corrían.

El 17 de junio de 2010, *VirusBlokAda* emitió una alerta por todo el mundo que desató una carrera internacional para rastrear lo que se conoce como Stuxnet: el más sofisticado *malware* de ordenadores que se haya encontrado y que deja entrever una nueva generación de amenazas cibernéticas.

2017. El secuestro de datos es la tendencia cibercriminal de 2017, Esta modalidad consiste en que los ciberdelincuentes acceden a los dispositivos donde se guarda información confidencial, habitualmente de carácter financiero, para extorsionar a sus víctimas. Los ladrones informáticos usualmente infectan y bloquean los computadores y le exigen a los vulnerados un pago en Bitcoins, una transacción que se puede llevar a cabo fácilmente y sin dejar rastro en tanto no está regulada por ningún gobierno. Incluso, en algunos casos, les han solicitado a los dueños de la información realizar una encuesta como 'forma de pago'. Aún si el usuario accede a alguno de estas intimidaciones, no hay garantía de que pueda volver a utilizar su equipo o recuperar su información.

Luego de hacer un recuento de las fechas más importantes de eventos de seguridad informática se exponen los Sistemas de Gestión de Seguridad de la Información (SGSI) que surgieron para garantizar la confiabilidad, disponibilidad e integridad de la información.

En línea con estos propósitos, uno de los estándares más reconocidos mundialmente para la gestión de la seguridad de la información es la serie ISO/IEC 27000 que proviene de la norma BS 7799 de la British Standars Institution. Esta familia de normas se compone de siete estándares, de los cuales el ISO/IEC 27001 contiene los requisitos del sistema de gestión de seguridad de la información, el estándar ISO/IEC 17799 se ha convertido en una referencia para la comunidad internacional con respecto a la gestión de la seguridad de la información.

ISO/IEC 17799 es de alto nivel, amplia en su alcance, y conceptual en su naturaleza. Este enfoque le permite ser aplicada a múltiples tipos de empresas y aplicaciones. También se ha hecho polémica entre aquéllos que creen que las normas deben ser lo más precisas posibles. A pesar de esta controversia, ISO 17799 es el único "Standard" consagrado a la Gestión de Seguridad de Información en un campo generalmente gobernado por las "Pautas, las Guías" y "las Mejores Prácticas."

En Colombia, por parte del Ministerio de las Tecnologías de la Información y la Comunicación, dentro de sus objetivos de desarrollo 2011- 2014 ha planteado el impulso a la masificación y uso eficiente de las TIC para el cumplimiento de los objetivos del Gobierno Nacional de: disminuir pobreza, aumentar seguridad y aumentar empleo. Bajo esa concepción se ha hecho necesario también la capacitación en temas relacionados con la seguridad de la información de acuerdo a lo planteado en el documento CONPES 3701 por la Información y las Comunicaciones realizar las gestiones necesarias con el Ministerio de Educación Nacional y el SENA, para la generación de un plan de capacitación para el sector 12 privado en temas de ciberseguridad y de seguridad de la información." (Mintic, 2012)

El documento CONPES tiene como objetivo central fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio (Mintic, 2012).

2.1.1 Antecedentes. Con el fin de dar cumplimiento a los objetivos a continuación se describe una serie antecedentes que servirán de apoyo para tener una mejor comprensión en cada uno de estos temas y alcances significativos evidenciados en otro u otros proyectos similares. Los sistemas de Gestión de la Seguridad de la información surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información que favorecen el desarrollo y el buen funcionamiento de la empresa, con miras a obtener la certificación en normas como la ISO/IEC 27001.

A continuación se presentan trabajos que se han realizado en esta área:

Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013. De acuerdo con la tesis realizada en la Universidad católica del Perú (Salinas & Isabel, 2015), en la actualidad los sistemas que se utilizan para almacenar, procesar y transmitir información se encuentran en toda clase de instituciones de diferentes rubros y funciones. Los sistemas de información se han vuelto más complejos debido a la globalización que tiene por consecuencia que las distancias geográficas ya

no supongan un obstáculo. De esta forma se tiene que existe una cantidad cada vez mayor de personas que tienen acceso a información que podría ser crítica para las diferentes empresas e instituciones en las que trabajan. Adicionalmente a este riesgo interno, siempre se tiene presente el riesgo que supone la fuga de información sensible ya sea por medio de personas que cuentan con acceso a dicha información, como por terceros que han accedido a ella mediante algún mecanismo de ataque. En respuesta a este nuevo escenario, las instituciones públicas han sido llamadas a realizar la implementación de diversos controles a través de un Sistema de Gestión de Seguridad de la Información – a través de diferentes normas, entre ellas la Norma Técnica NTP ISO/IEC 27001 – con la finalidad de asegurar el buen uso y protección de la información crítica que manejen, ya sea de clientes o información estratégica interna. El presente trabajo de fin de carrera desarrolla el Análisis y Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad pública del sector Salud – el Instituto Nacional Materno Perinatal – sujeta al cumplimiento de la normativa vigente relativa a Seguridad de la Información.

Manual de seguridad de la información para un organismo del estado colombiano.

Según lo expuesto por (Ramírez, 2014), El manual de seguridad de la información permite determinar las fortalezas y debilidades que tiene la organización frente a los activos de información, conocer el estado actual ante seguridad de información y sus controles, con el fin de crear estrategias que minimicen las amenazas que impactan la vulnerabilidad organizacional. Basado en una investigación de campo y documental se pudo establecer el nivel de madurez actual en que se encuentra la organización por medio de encuestas, revisión de documentos e igualmente, se realizaron visitas a las instalaciones y se revisaron aspectos de seguridad física haciendo una valoración inicial a los controles establecidos por la Norma ISO 27001:2013. La

creación de políticas pertinentes y aplicables, basadas en el análisis y evaluación de riesgo de las informaciones obtenidas de los activos que son permitidas valorar, es el resultado de la investigación realizada a la organización. Para conseguir la efectividad esperada del Sistema de Gestion de seguridad de la información, fue necesario quemar etapas específicas y en un orden determinado, calculado entre 6 y 12 meses, dependiendo del grado de madurez actual de seguridad de la información y el alcance. El hecho de que la organización quiera vivir actualizada y de haber tomado la decisión de transformar desarrollar y estar siempre en un nivel competitivo, hace parte de la estrategia de la organización que quiere la mejora continua, siempre bajo el marco legal y normativo. Con un Sistema de Gestión de Información la organización conoce los riesgos a los que está sometida su información y los asume, los sistematiza, documenta, da a conocer, revisa y mantiene actualizados.

Modelo de gestión de seguridad de la información ICETEX. De acuerdo con El (Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior [ICETEX], s.f.): La información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades actuales, ICETEX 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, regulatorios y de negocio vigentes. El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en ICETEX; este proceso será liderado de manera permanente por el Oficial de Seguridad de la Información.

Política de la seguridad de la información en la Alcaldía de Río de Oro, Cesar. Según lo expuesto por (Areniz &Sánchez, 2014) para definir el nivel de seguridad en la Alcaldía del municipio de Río de Oro, departamento del Cesar, se realizó una investigación mediante la aplicación de encuestas dirigida al personal de planta y OPS con el fin de determinar el nivel de efectividad de los controles que actualmente aseguran la información manejada por esta.

Este estudio fue desarrollado en el año 2014 y finalmente, se recomendó aplicar las Políticas de Seguridad de la Información ajustadas a la Alcaldía, para fomentar el compromiso de uso.

2.2 Marco conceptual

A continuación se relacionan algunos conceptos pertinentes al desarrollo del proyecto: Gestión de la seguridad de la información para la Secretaria de Hacienda del Municipio De Rio De Oro Cesar:

2.2.1 Información. Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. La información, ya sea impresa, almacenada digitalmente o hablada, actualmente es considerada como un activo dentro de las compañías y que se debe proteger, ya que es de gran importancia.

2.2.2 Seguridad de la información. La ISO la define como la preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

2.2.3 Características principales de la información. Los siguientes términos son definidos según (ICONTEC, 2013):

Confidencialidad: o que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

Integridad: o mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Disponibilidad: o disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

2.2.4 Sistema de información. Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

2.2.5 Sistema de Gestión de Seguridad de la Información (SGSI). SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. (CNB - INDECOPI, 2008) (ISACA, 2012).

2.2.6 Control. Según (ISO, 2005) los controles son: "Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. El control también se utiliza como sinónimo de salvaguarda o contramedida."

2.2.7 Amenaza. Es la probabilidad de ocurrencia de un suceso potencialmente desastroso durante cierto periodo de tiempo, en un sitio dado.

En general el concepto de amenaza se refiere a un peligro latente o factor de riesgo externo, de un sistema o de un sujeto expuesto, expresada matemáticamente como la

probabilidad de exceder un nivel de ocurrencia de un suceso con una cierta intensidad, en un sitio específico y durante un tiempo de exposición determinado (UNAD, s.f)

Una amenaza informática es un posible peligro del sistema. Puede ser una persona (cracker), un programa (virus, caballo de Troya, etc.), o un suceso natural o de otra índole (fuego, inundación, etc.). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema.

2.2.8 Política de seguridad. Declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.

2.2.9 Riesgo. Se refiere a la incertidumbre o probabilidad de que una amenaza se materialice utilizando la vulnerabilidad existente de un activo o grupo de activos, generándole pérdidas o daños.

2.2.10 Gestión del riesgo. Actividades coordinadas para dirigir y controlar los aspectos asociados al Riesgo dentro de una organización.

2.2.11 Vulnerabilidad. Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

2.2.12 Auditoría de sistemas. Está dirigida a evaluar los sistemas y procedimientos de uso en una empresa, con el propósito de determinar si su diseño y aplicación son correctos; y comprobar el sistema de procesamiento de información como parte de la evaluación de control interno; así como para identificar aspectos susceptibles de mejorarse o eliminarse. (Prezi.com, 2014)

2.2.13 Análisis GAP. Se define al análisis Gap como una palabra proveniente del idioma inglés, que en español hace referencia a una Brecha que mide cómo una organización está llevando a cabo su desempeño con respecto a una serie de criterios establecidos en base a normas o procedimientos internos, controles seleccionados, las mejores prácticas de competencia, etc.

El resultado de este análisis establece la diferencia entre el desempeño actual y el esperado, con un informe presentado con indicaciones sobre dónde están las deficiencias y "qué" falta para cumplir con cada requisito de la norma.

2.3 Marco contextual

La Gestión de la Seguridad de la Información, se llevara a cabo en la Secretaria de Hacienda de Rio de Oro-Cesar. La cual es una entidad de carácter público que tiene como finalidad garantizar la óptima gestión de los recursos y el registro ordenado, sistemático y claro de las operaciones de gasto público.

2.4 Marco teórico

Las bases teóricas para el desarrollo del presente proyecto se sustentaran en buenas prácticas de seguridad de la información, Para lograr una adecuada gestión de la información es indispensable que las organizaciones establezcan una metodología estructurada, clara y rigurosa para la valoración y tratamiento de los riesgos de seguridad, es por ello que se tiene como referente teórico la familia de normas ISO/IEC 27000

Familia de Normas ISO/IEC 27000: La familia de las normas ISO/IEC 27000, son un marco de referencia de seguridad a nivel mundial desarrollado por la International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, que proporcionan un marco, lineamientos y mejores prácticas para la debida gestión de seguridad de la información en cualquier tipo de organización. Estas normas especifican los requerimientos que deben cumplir las organizaciones para establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.

En Colombia, el Instituto Colombiano de Norma Técnicas y Certificaciones, ICONTEC, es el organismo encargado de normalizar este tipo de normas.

Las siguientes son algunas de las normas que componen la familia ISO/IEC 27000, las cuales serán el marco teórico que se tendrá en cuenta para efectos del presente trabajo:

Norma ISO/IEC 27000. Según (INCONTEC, sf) esta norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización.

La norma ISO/IEC 27000 es más precisamente un conjunto de normas las cuales cada una trata un aspecto determinado dentro del área de estudio, a continuación se describe brevemente las normas más reconocidas de la familia 27000

ISO 27001: Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la única norma de la familia que es certificable.

Ciclo PDCA: Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

- Plan (planificar): establecer el SGSI.
- Do (hacer): implementar y utilizar el SGSI.
- Check (verificar): monitorizar y revisar el SGSI.
- Act

ISO/IEC 27001:2013. Tiene como prioridad proteger

a) La confidencialidad de la información

b) La integridad de la información

c) La Disponibilidad de la información

ISO/IEC 27001 se divide en 11 secciones las cuales se describen a continuación:

Sección 0 – Introducción – explica el objetivo de ISO/IEC 27001:2013 y su compatibilidad con otras normas de gestión.

Sección 1 – ***Alcance*** – explica que esta norma es aplicable a cualquier tipo de organización.

Sección 2 – ***Referencias normativas*** – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.

Sección 3 – ***Términos y definiciones*** – de nuevo, hacen referencia a la norma ISO/IEC 27000.

Sección 4 – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). 21

Sección 5 – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

Sección 6 – ***Planificación*** – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

Sección 7 – ***Apoyo*** – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8 – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.

Sección 9 – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

Sección 10 – Mejora – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua. (Actuar): mantener y mejorar el SGSI.

ISO 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. En la más reciente versión ISO/IEC 27002:2013 presenta 14 dominios, 35 objetivos de control Y 114 controles.

ISO 27003: Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.

ISO 27004: Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.

ISO 27005: Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

ISO 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

ISO 27007: Es una guía para la aplicación de auditorías a un SGSI como complemento especificado en ISO 19011.

2.5 Marco legal

2.5.1 Ley 1266 del 31 de diciembre de 2008. El Congreso de Colombia decretó: "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." (Congreso de Colombia, 2015)

2.5.2 Artículo 71 de la Constitución Política de Colombia. Este artículo otorga al Estado la responsabilidad de promover el desarrollo tecnológico e incentivar a quienes se dediquen a trabajar en este ámbito "… El Estado creará incentivos para personas e instituciones que desarrollen y fomenten la ciencia y la tecnología y las demás manifestaciones culturales y

ofrecerá estímulos especiales a personas e instituciones que ejerzan estas actividades." (República de Colombia, 2012)

2.5.3 Ley 1341 de 2009. 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 (MinTic, 2009).

2.5.4 Ley 1273 del 5 de enero de 2009. 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, y las siguientes disposiciones:

De los atentados contra la confidencialidad Acceso abusivo a un sistema informático, Obstaculización ilegítima de sistema informático o red de telecomunicación, Interceptación de datos informáticos, Daño Informático, Uso de software malicioso, Violación de datos personales, Suplantación de sitios web para capturar datos personales.

La integridad y la disponibilidad de los datos y de los sistemas informáticos hurto por medios informáticos y semejantes, Transferencia no consentida de activos. (DIARIO OFICIAL, 2009).

Capítulo 3. Diseño metodológico

3.1 Tipo de Investigación

De acuerdo a las características del proyecto, se empleó el tipo de investigación descriptiva-cualitativa, con aportes de herramientas cuantitativas. La investigación descriptiva brinda una metodología apropiada para recolectar información básica para llevar a cabo el proyecto, ya que la misma describe de modo sistemático las características de una población, situación o área de interés.

En esta etapa se elaboraron los instrumentos de recolección de la información que permitió llevar a cabo el Diseño del Sistema de Gestión de la Seguridad de la Información para la Secretaria de Hacienda de Rio de Oro-Cesar, con el fin de analizarla, detallarla e interpretarla, para el desarrollo y cumplimiento de los objetivos.

La línea de investigación para la elaboración del proyecto, se enmarcó en el Gobierno de TI, y los conceptos utilizados se relacionaron con temas como: tecnología de la información, seguridad de la información, gestión de la seguridad, gestión de riesgos y sistema de gestión de seguridad de la información.

El diseño del Sistema de Gestión de Seguridad de la Información, se llevó a cabo en (4) fases:

Primera Fase: Diagnostico de la Gestión de la Seguridad de la Información, de la Secretaría de Hacienda de Rio de Oro-Cesar. Tomando como base la norma ISO/IEC 27001:2013.

- Investigación documental de manuales, políticas, decretos, normas.
- Investigación de campo a través encuestas, auto evaluación, y visitas a las instalaciones con el personal vinculados a los procesos.
- Procesamiento, análisis y evaluación de los hallazgos encontrados.
- Dictamen de la evaluación.

Segunda Fase: Determinación del nivel de madurez de la Secretaria de Hacienda con respecto al modelo de seguridad de la información que plantea la norma ISO/IEC 27001:2013.

- Nivel de madurez en cuanto al Anexo A de la Norma ISO-IEC 27001:2013.
- Nivel de madurez de los requerimientos de la Norma ISO-IEC 27001: 2013.

Tercera Fase: Diagnóstico de los riesgos de seguridad de la información en la Secretaria de Hacienda de Rio de Oro-Cesar.

- Análisis de riesgos.
- Identificación de Amenazas
- Identificación de las Vulnerabilidades.
- Identificación y Valoración del Riesgo.

- Análisis y Evaluación del Riesgo.
- Tratamiento del Riesgo.
- Cuarta Fase: Documentación de buenas prácticas.
- Guía de buenas prácticas de la Seguridad de la Información.

3.2 Población

En cuanto a la población objeto de estudio se tomaron en cuenta todos los funcionarios que laboran en la dependencia, y tienen directa relación con la información que se maneja al interior de la Secretaria de Hacienda de Rio de Oro-Cesar.

3.3 Muestra

Debido a que la población es limitada, se trabajó como muestra toda la población que conforma la Secretaria de Hacienda de Rio de Oro-Cesar.

3.4 Técnicas de recolección de la información

Para el desarrollo del proyecto se utilizó la encuesta como técnica de recolección de la información, aplicando cuestionarios y realizando entrevistas directas a los funcionarios de la Secretaria de Hacienda de Rio de Oro-Cesar. Se solicitó a la entidad la documentación existente del sistema de gestión de la seguridad, y se utilizó la técnica de observación y evaluación de acuerdo a la experiencia de las autoras del proyecto.

3.4.1 Fuentes primarias

Entrevistas: Al llevar a cabo las entrevistas a los funcionarios de la Secretaria de Hacienda de Rio de Oro-Cesar, se buscó inicialmente identificar la seguridad que se maneja en la dependencia, como contraseñas y usuarios autorizados en el manejo de equipos y acceso a archivos. Por otro lado se intentó conocer y documentar las políticas de gestión de la seguridad que actualmente manejan al interior de la dependencia.

Observación: A través de la observación se reconoció y registró, los controles que se tienen actualmente para el uso y manejo de la información en la entidad, con la finalidad de revisar los resultados junto con el personal de la Secretaria de Hacienda de Rio de Oro-Cesar, que intervienen en el proceso.

Documentales. Para el desarrollo del proyecto, se tuvo en cuenta los la documentación que ha sido gestada y elaborada en la Secretaria de Hacienda de Rio de Oro-Cesar, como son manuales de funciones y procedimientos, resultados de auditorías anteriores, políticas y normas de seguridad de la información, entre otros.

3.4.2 Fuentes secundarias. Apoyo en leyes, estándares y normas relacionadas con la seguridad de la información, artículos científicos relacionados con la seguridad de la información y auditorias basadas en riesgos y administración de riesgos.

Capítulo 4. Presentación de resultados

Para dar cumplimiento a los objetivos propuestos para el diseño del Sistema de Gestión de la Seguridad de la información para la Secretaria de Hacienda de Rio de Oro-Cesar se ejecutaron varias actividades que permitieron llevar a cabo el proyecto y que se detallan a continuación: Ver tabla 1.

Tabla 1
Actividades por objetivo

Objetivo	Actividades	Producto
Diagnóstico de la Secretaria de Hacienda de Rio de Oro-Cesar, con relación a la Gestión de la Seguridad de la Información. Norma ISO-IEC/27001:2013	1. Definir Alcance SGSI. 2. Definir procesos de misión crítica. 3. Investigación documental de información relacionada con el SGSI. 4. Elaboración de instrumentos alineados a la Norma ISO-IEC/27001:2013. 5. Investigación de campo. 6. Procesamiento y análisis GAP, de la información recabada. 7. Evaluación de los hallazgos.	Modelado del negocio. Diagnóstico de la seguridad de la información, respecto al criterio escogido. (Niveles de Cumplimiento)
Nivel de Madurez de La Secretaria de Hacienda de Rio de Oro-Cesar, respecto al modelo de Seguridad de la Información que plantea la Norma ISO-IEC/27001:2013	1. Identificación de controles que aplican en la Secretaria de Hacienda de Rio de Oro-Cesar, de acuerdo a la Norma ISO-IEC 27001:2013. 2. Ponderación de los criterios identificados. 3. Análisis GAP, referente Anexo A, Norma NTC ISO 27001: 2013.	Evaluación del Estado de Madurez de la Secretaria de Hacienda de Rio de Oro-Cesar.
Diagnóstico de los riesgos de la Seguridad de la Información en la Secretaria de Hacienda de Rio de Oro-Cesar.	1. Clasificación de Activos. 2. Tasación de Activos. 3. Selección de Metodología de análisis y evaluación del riesgo. 4. Identificación de vulnerabilidades, amenazas e impacto. 5. Análisis y evaluación del Riesgo.	Matriz del Riesgo de la Secretaria de Hacienda de Rio de Oro-Cesar.
Documentar las buenas prácticas de Seguridad de la información, tomando como base la Norma ISO-IEC/27001:2013.	1. Documentación de la Auditoria del estado del Sistema de Gestión de la Información de la Secretaria de Hacienda de Rio de Oro-Cesar. 2. Documentación del Estado de Madurez de la Secretaria de Hacienda de Rio de Oro-Cesar. 3. Documentación de la Evaluación del Riesgo. 4. Recomendaciones y Controles.	Guía de buenas prácticas para el manejo de la Seguridad de la información, para la Secretaria de Hacienda de Rio de Oro-Cesar.

Fuente. Autores del proyecto

4.1 Diagnóstico de la Secretaria de Hacienda de Rio de Oro-Cesar, con relación a la Gestión de la Seguridad de la Información.

4.1.1 Alcance del SGSI. El desarrollo de este proyecto, abarca el Diseño de un Sistema de Gestión de Seguridad de la Información para la Secretaria de Hacienda de la Alcaldía de Rio de Oro-Cesar. Se enmarco en la fase del planear del ciclo de Deming PHVA (Planificar, Hacer, Verificar y Actuar); Los Sistemas de Gestión de Seguridad de la Información según la norma ISO/IEC 27001:2013 deben ser mejorados de forma continua siguiendo la filosofía del ciclo PHVA.

Este trabajo no abarca la fase de implementación, mantenimiento y revisión del Sistema de Gestión de Seguridad de la Información, que corresponden a las fases Hacer, Actuar y Verificar, sin embargo es importante resaltar que de la fase hacer se llevara a cabo la definición del plan de tratamiento del riesgo.

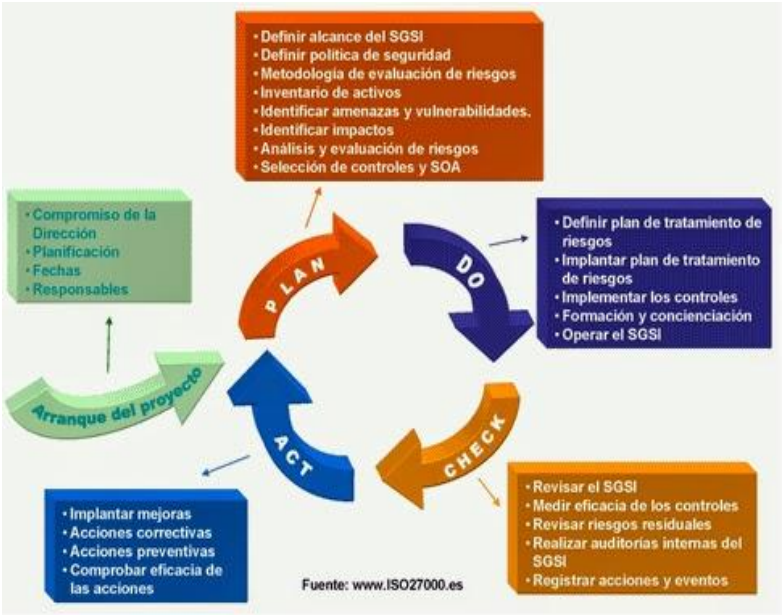

Figura 1. Ciclo PHVA
Fuente: www.ISO 27001

El alcance del SGSI abarca todos los sistemas de información que dan soporte a los procesos del negocio, como son los procesos misionales críticos de la dependencia que involucran la Gestión de Tesorería, Gestión Presupuestal, Gestión de Rentas, Gestión de Contabilidad y todas las actividades que soportan dichos procesos en la secretaría de hacienda del Municipio de Río de Oro. De igual forma se tomaran en cuenta las áreas de la dependencia, especialmente aquellas que hacen uso y manejo de información sensible, como son: Contabilidad, Rentas, Presupuestos y Tesorería y todo el soporte Técnico que está estrechamente relacionado con el manejo de TIC.

De acuerdo al estándar internacional ISO-IEC/27001:2013, inicialmente se realizó un diagnóstico de la situación actual de la seguridad de la información, seguidamente se estableció el estado de madurez de la dependencia de acuerdo a los criterios de la norma establecida y posteriormente se identificaron, las amenazas, riesgos e impacto, permitiendo así un análisis y evaluación del riesgo.

La norma ISO/IEC 27001:2013 señala que se debe conocer la entidad por fuera y por dentro, y como pude afectar positiva o negativamente la implementación de las políticas de seguridad de la información. Con el fin de emitir un juicio objetivo en relación a la Gestión de la Seguridad de la Información en la Secretaria de Hacienda de Rio de Oro-Cesar re realizaron las siguientes actividades:

4.1.2 Reconocimiento de la empresa. Alcaldía de Rio de Oro-Cesar.

Misión Alcaldía Río de Oro – Cesar. Consolidar el desarrollo Municipal mediante la eficaz y eficiente utilización de todos nuestros recursos; con ejecutorias que dinamicen la vida social, económica, ambiental e institucional a todos los sectores de la población, implementadas desde el núcleo familiar y dentro del marco de las competencias que deben cumplirse para mejorar las condiciones de vida, propendiendo por un municipio equitativo, sin pobreza y encaminado en la construcción de la paz.

Visión Alcaldía Río de Oro – Cesar. En el 2032 Río de Oro, será un municipio constructor de paz; polo de desarrollo turístico de la región; próspero, incluyente, equitativo y participativo; comprometido y garante de la protección integral de los niños, niñas y adolescentes.

Con altos estándares de calidad en la prestación de servicios de salud, educación y domiciliarios; que le permitirán a sus habitantes gozar de un buen nivel de vida, plenas garantías de sus derechos y cumplidores de sus deberes; con un alto grado desarrollo social y protección ambiental.

Estructura Organizacional

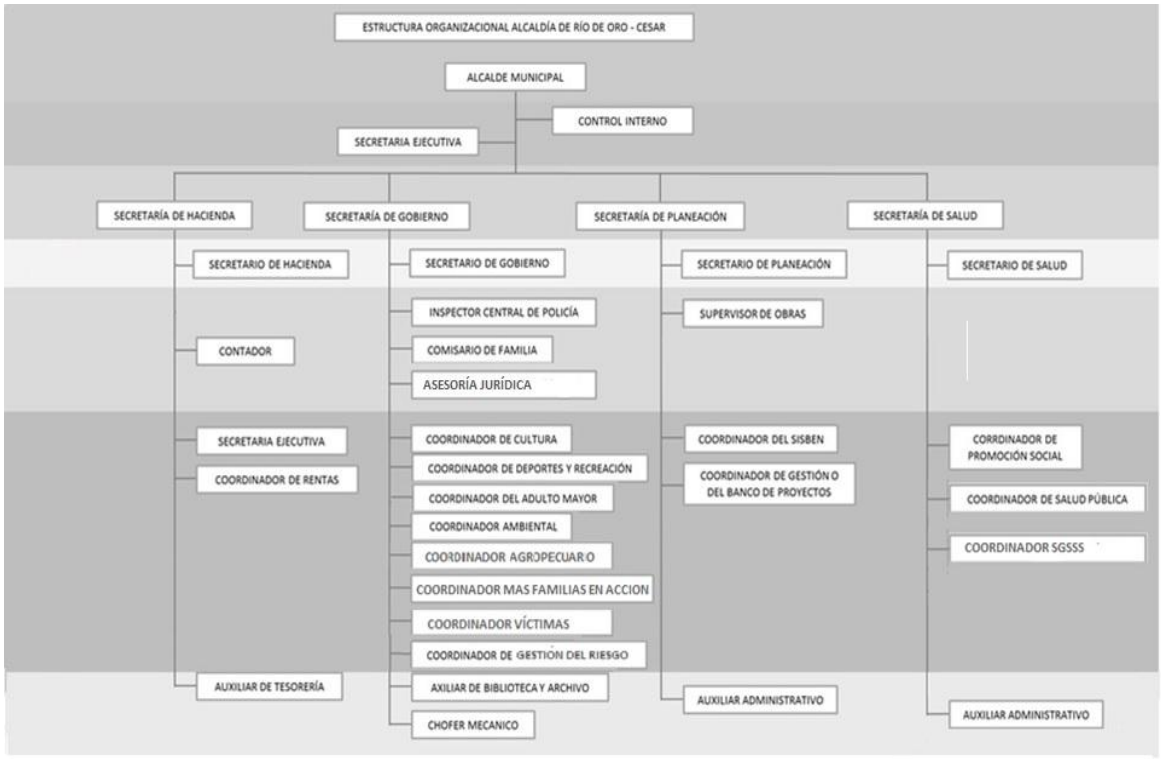

Figura 2. Estructura organizacional Alcaldía de Río de Oro - Cesar
Fuente. Alcaldía de Rio de Oro - Cesar

4.1.3 Modelado del negocio de la Secretaria de Hacienda de Rio de Oro-Cesar.

Misión Secretaría de Hacienda. 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.

Estructura Organizacional. La Secretaria de Hacienda del municipio de Rio de Oro-Cesar, está conformada por una estructura de jerarquía vertical en cabeza del alcalde, seguidamente coordinada por la Secretaria de Hacienda, quien tiene a su cargo el área de Contabilidad, La Coordinación de Rentas, La Secretaria Ejecutiva y al Auxiliar de Tesorería, como se observa en la figura 2.

Objetivo general de la secretaria de hacienda. Garantizar la óptima gestión de los recursos y el registro ordenado, sistemático y claro de las operaciones de gasto público.

Funciones generales. Son funciones de la Secretaría de Hacienda, las siguientes:

- Planificar y determinar las políticas de liquidación y fiscalización de las rentas Municipales;
- Gestionar la obtención de los recursos de crédito interno y externo que requiera el municipio;
- 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;
- Liderar los procesos de recaudo y administración de los recursos financieros.
- Dirigir y controlar la aplicación de las normas y procedimientos contables, fiscales, presupuéstales y de tesorería;
- 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;
- Responder por el control de la deuda pública contraída por el Municipio;

- Establecer los mecanismos de cobro coactivo a los contribuyentes de acuerdo con la normatividad legal establecida para ello;
- Dirigir la elaboración oportuna de los estados financieros del Municipio de Neiva;
- Presentar y realizar seguimiento a los proyectos de Acuerdo, Decretos y demás actos administrativos que modifiquen el presupuesto municipal;
- Realizar Gestión de seguimiento y control al Presupuesto Municipal;
- Coordinar y controlar la elaboración del plan financiero y someterlo a consideración de las instancias correspondientes;
- Trazar las directrices para la adecuada conservación y protección de los títulos valores y demás bienes monetarios de propiedad del municipio.

4.1.4 Modelado de procesos de la Secretaria de Hacienda de Rio de Oro-Cesar. La cadena de valor describe los procesos que se llevan a cabo al interior de la dependencia y la forma como se realizan las actividades. Ver figura 3.

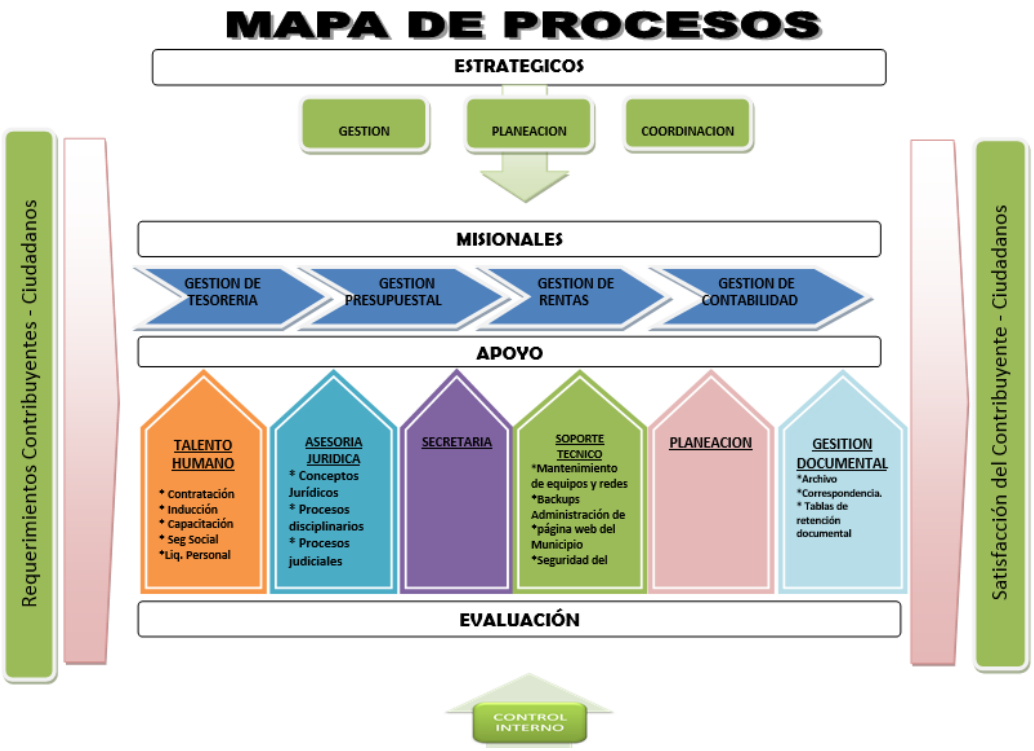

Figura 3. Mapa de procesos de la secretaría de Hacienda
Fuente Alcaldía Municipal

Descripción de los procesos.

Procesos Estratégicos:

Gestión: Garantizar la óptima gestión de los recursos y el registro ordenado, sistemático y claro de las operaciones de gasto público.

Planeación: Determinar las políticas de liquidación y fiscalización de las rentas municipales y asesorar al alcalde en la formulación de políticas financieras, fiscales y

económicas, así como encargarse del recaudo de los ingresos y pagos de las obligaciones a cargo del municipio y los asuntos relacionados con la Contabilidad, el Presupuesto y la Tesorería.

Coordinación: Formular, coordinar, dirigir y ejecutar las políticas de gobierno en materia fiscal, de hacienda, de crédito público, presupuestal y financiera en concordancia con las formuladas en el Plan de Desarrollo Municipal y teniendo en cuenta las normas legales, estatutarias.

Procesos Misionales: Estos procesos relacionados con los servicios que brinda la Administración Municipal a la comunidad; entre estos se encuentran las siguientes: Gestión de Tesorería, Gestión de Presupuesto, Gestión de Rentas y Gestión de Contabilidad.

Diagrama de procesos: a continuación se muestra el diagrama de procesos de la secretaría de hacienda del Municipio de Río de Oro – Cesar:

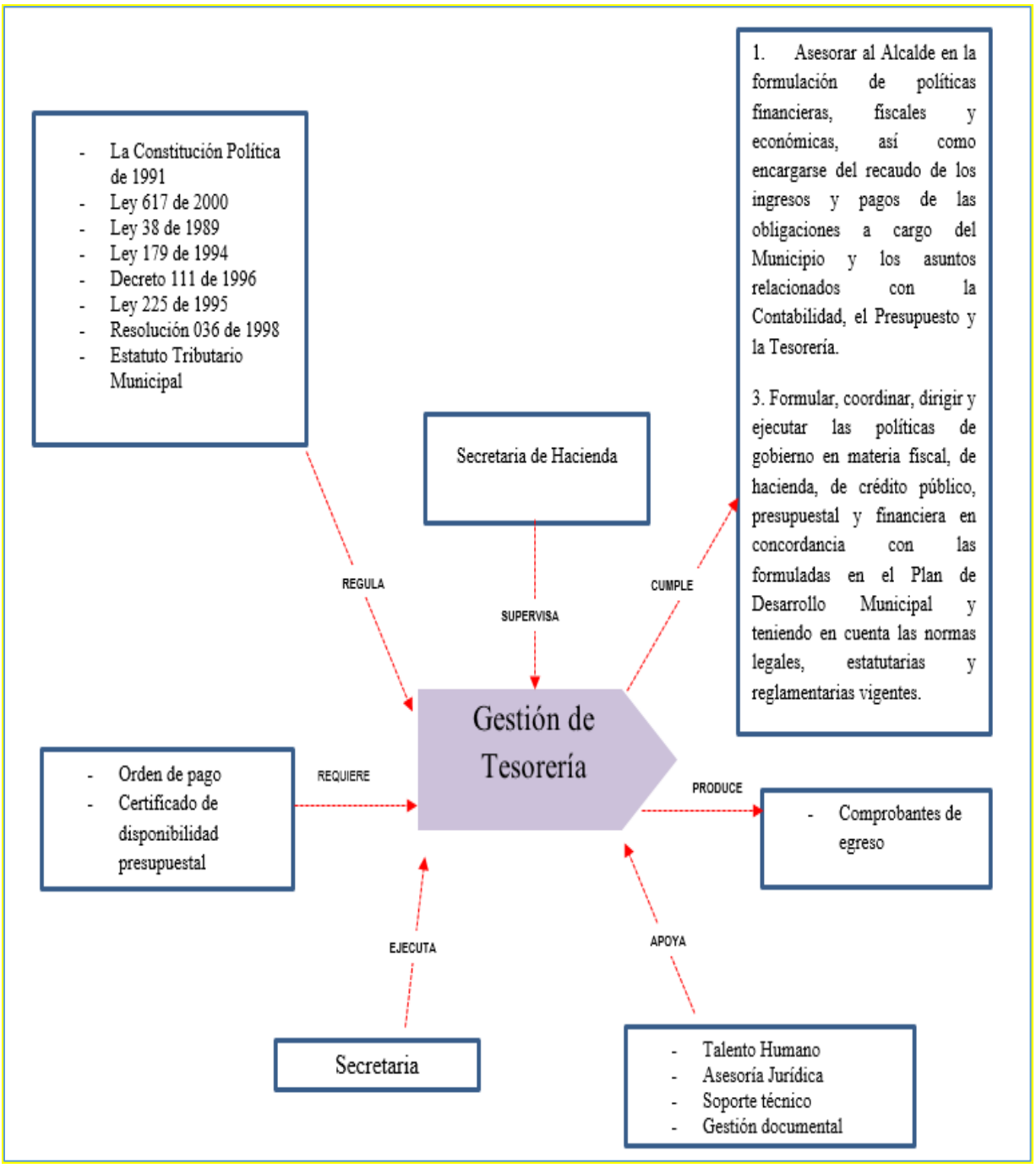

Figura 4. Proceso gestión de tesorería.
Fuente autoras del proyecto.

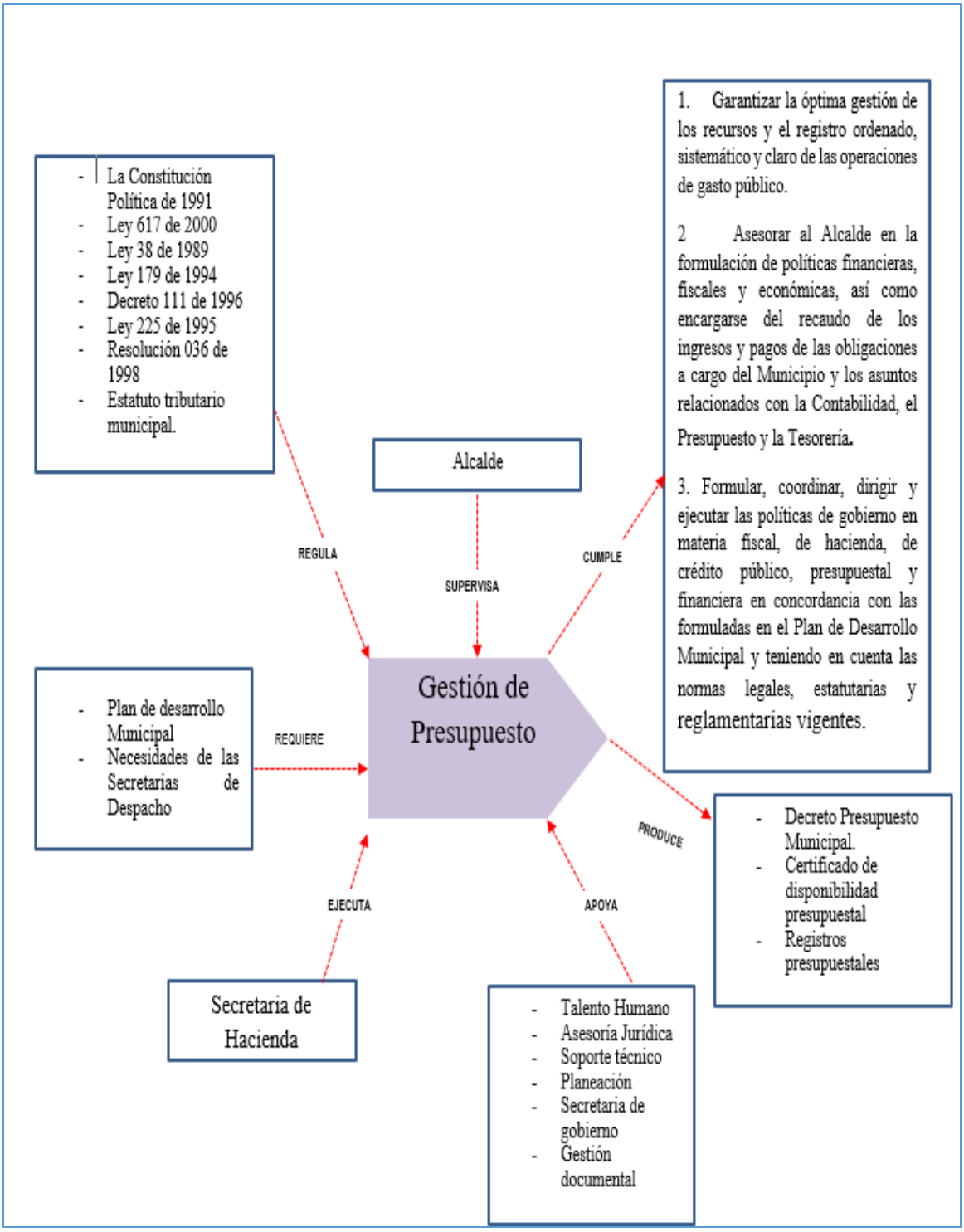

Figura 5. Proceso gestión presupuestal.
Fuentes autora del proyecto.

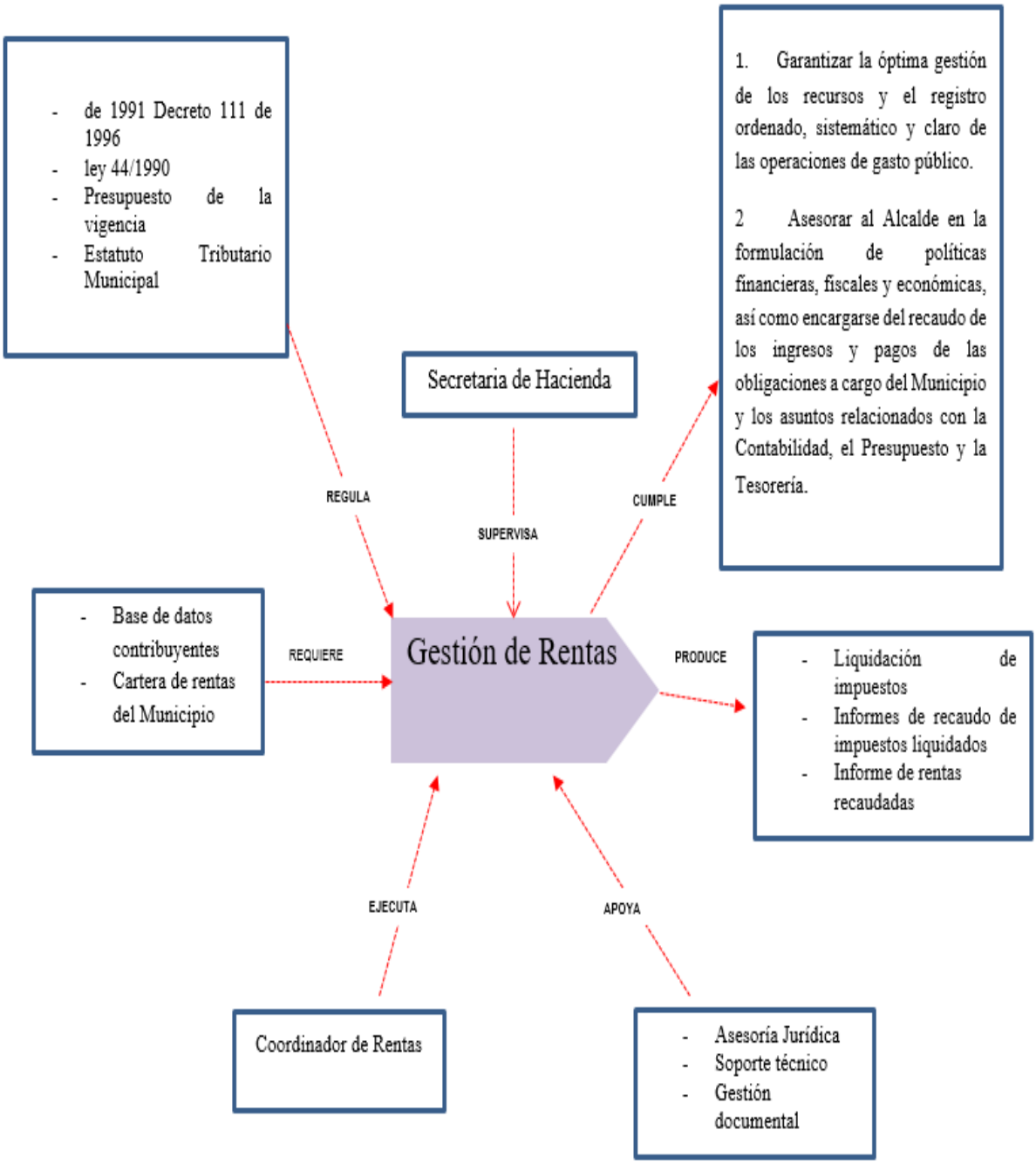

Figura 6. Proceso gestión de rentas.
Fuentes autora del proyecto.

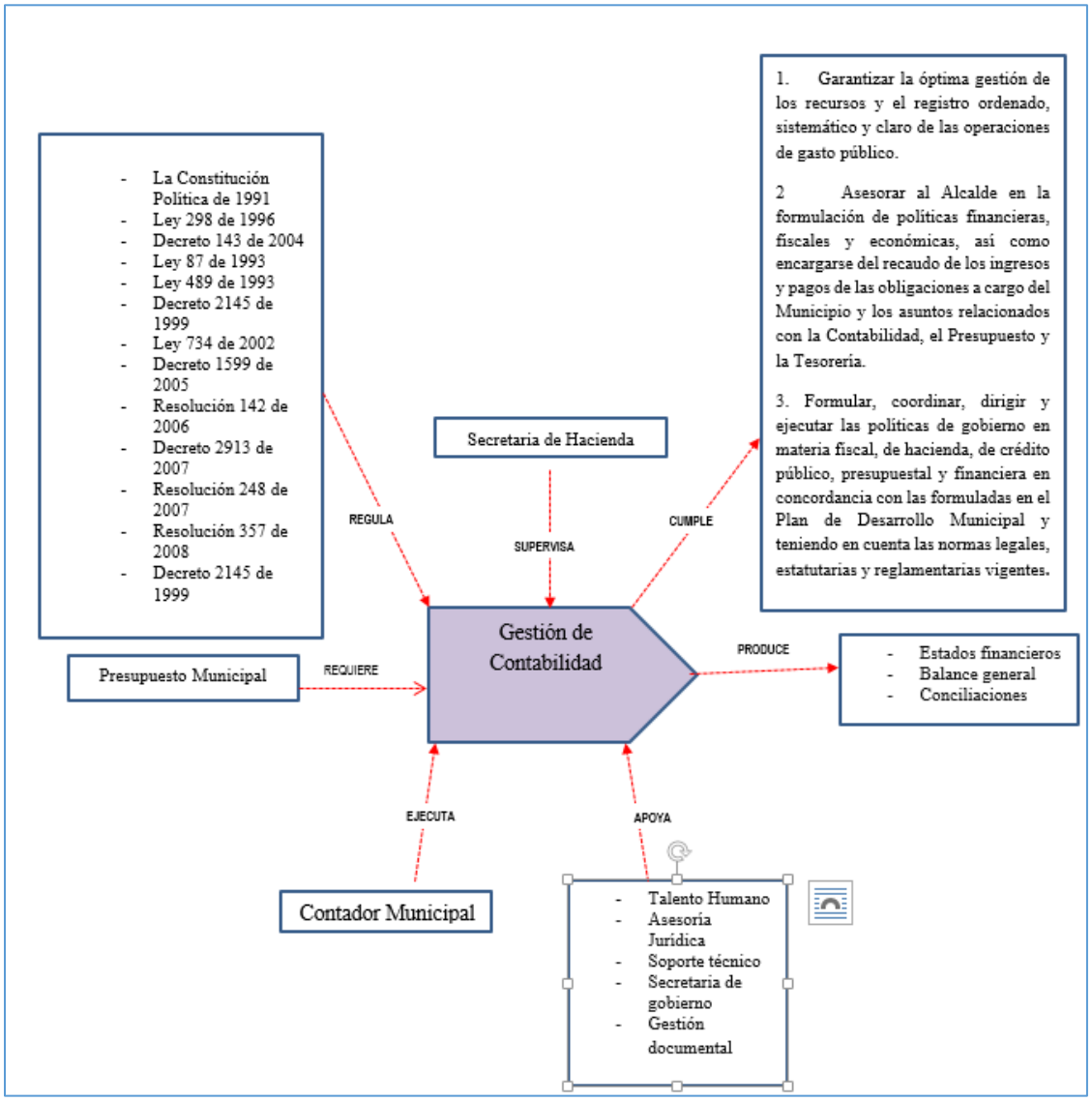

Figura 7. Proceso gestión contabilidad
Fuente autoras del proyecto.

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 Planeación, Gestión de Talento Humano, Gestión Jurídica, Gestión de Documental y Secretaría.

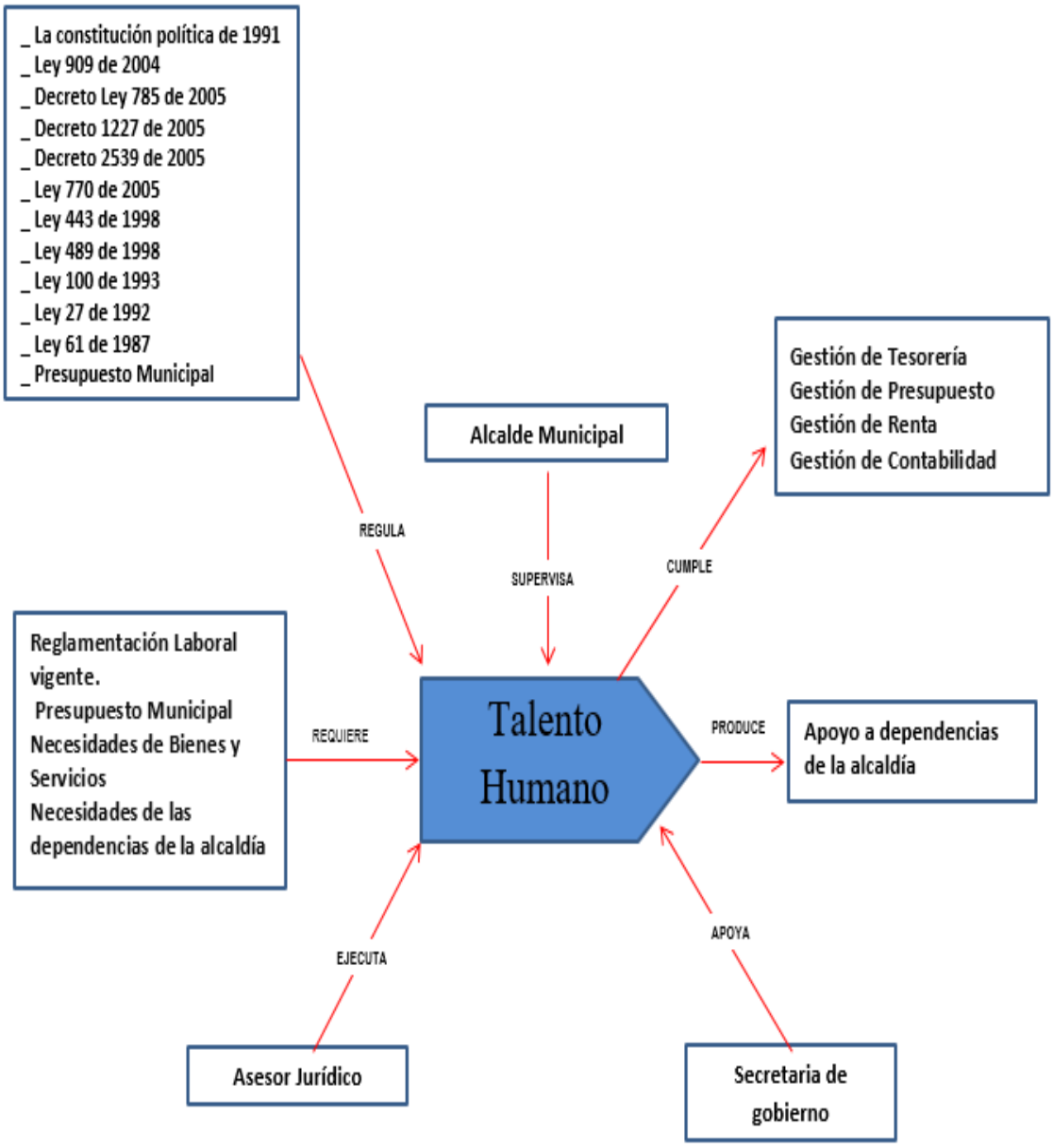

Figura 8. Talento Humano.
Fuente autoras del proyecto

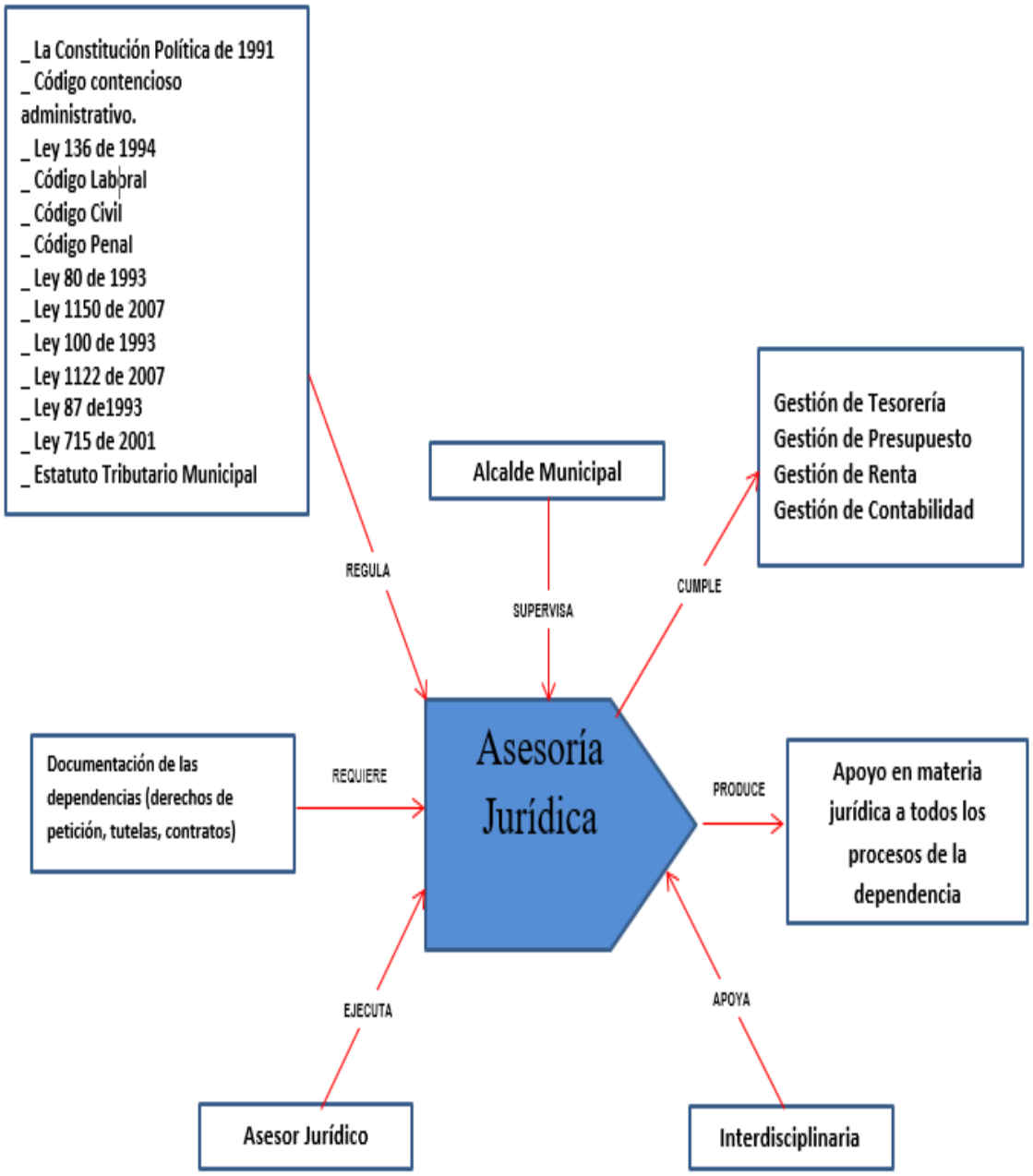

Figura 9. Asesoría Jurídica
Fuente autoras del proyecto

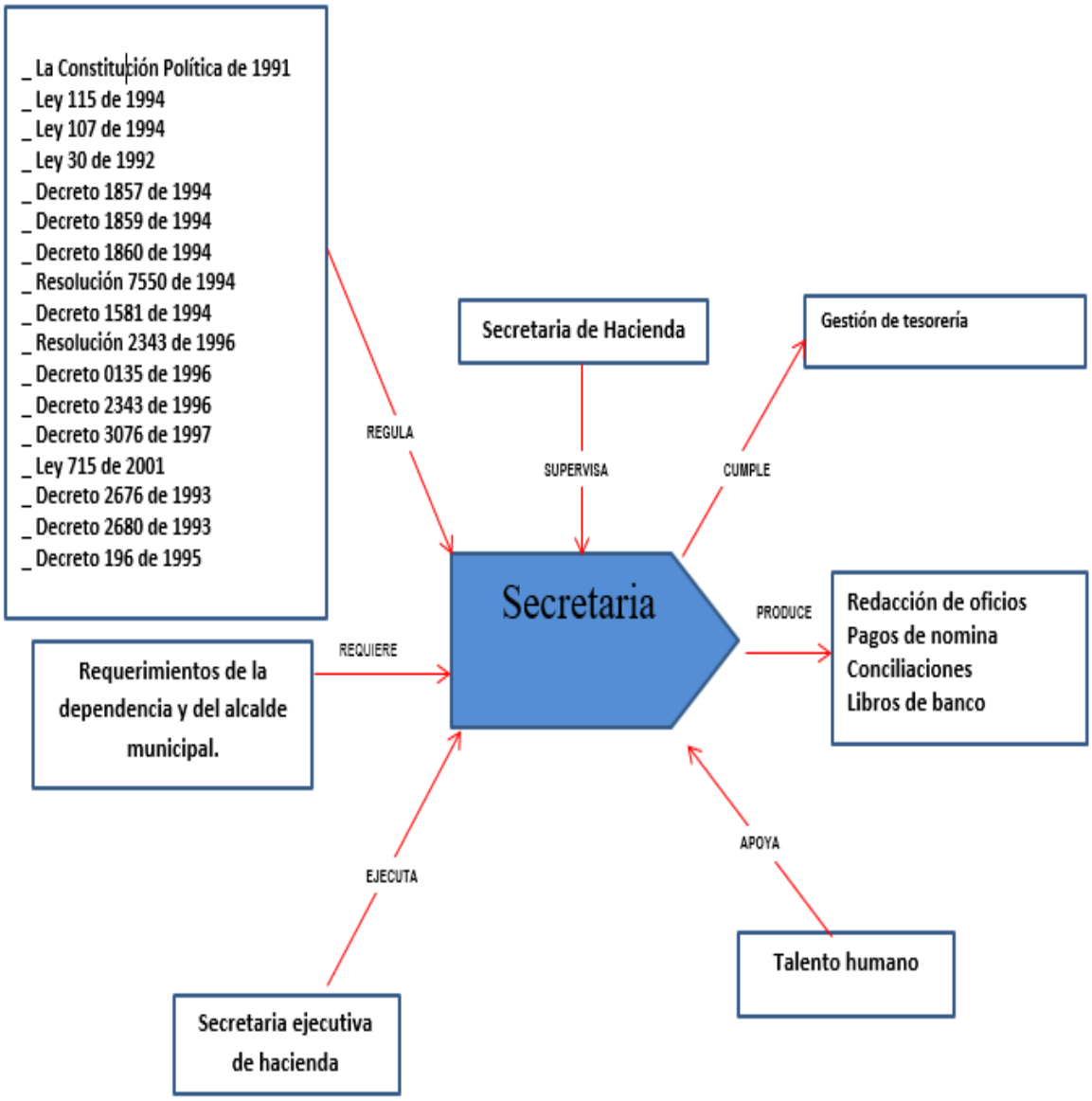

Figura 10. Secretaria
Fuente autoras del proyecto.

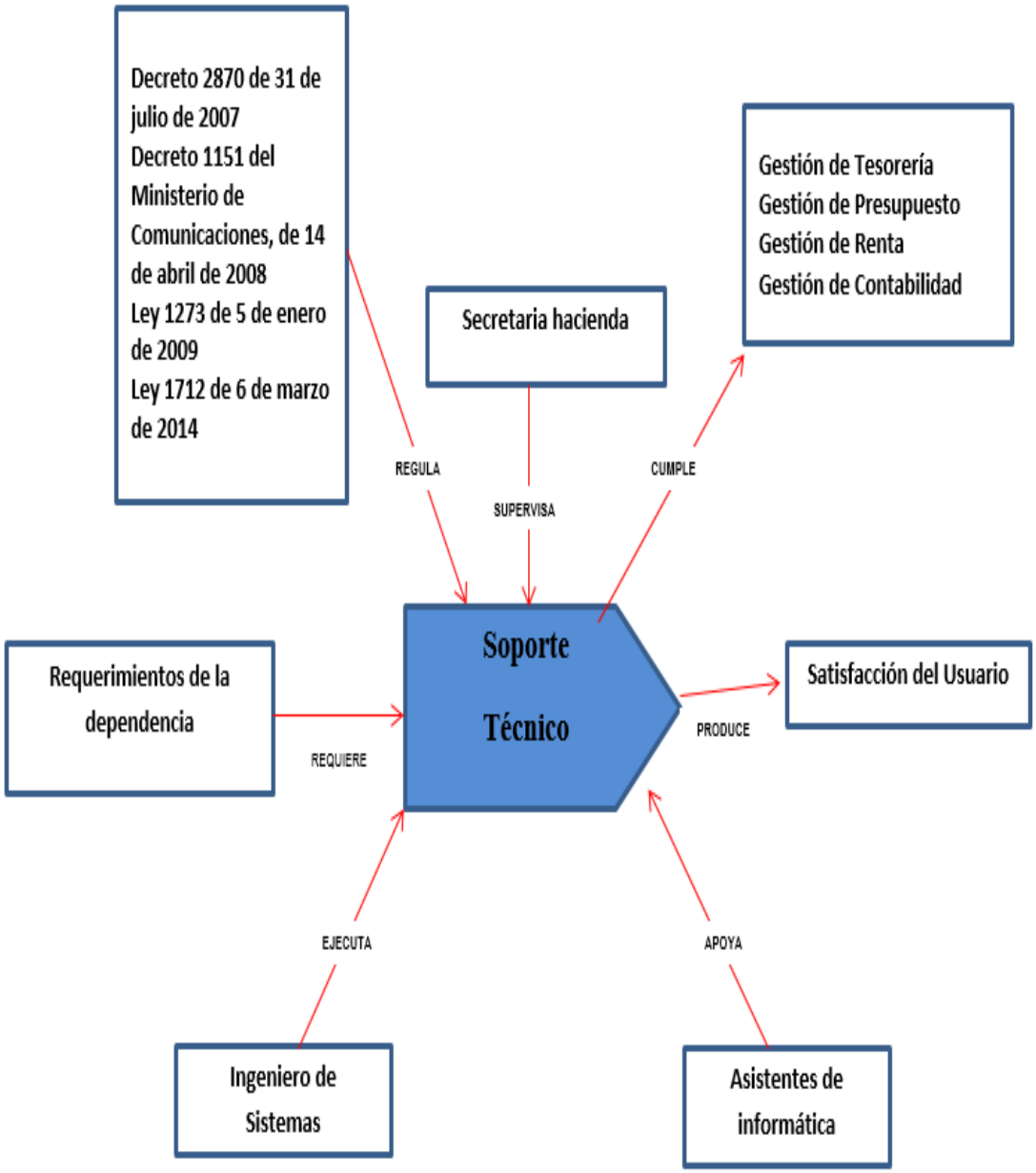

Figura 11. Soporte Técnico.
Fuente: Autoras del proyecto

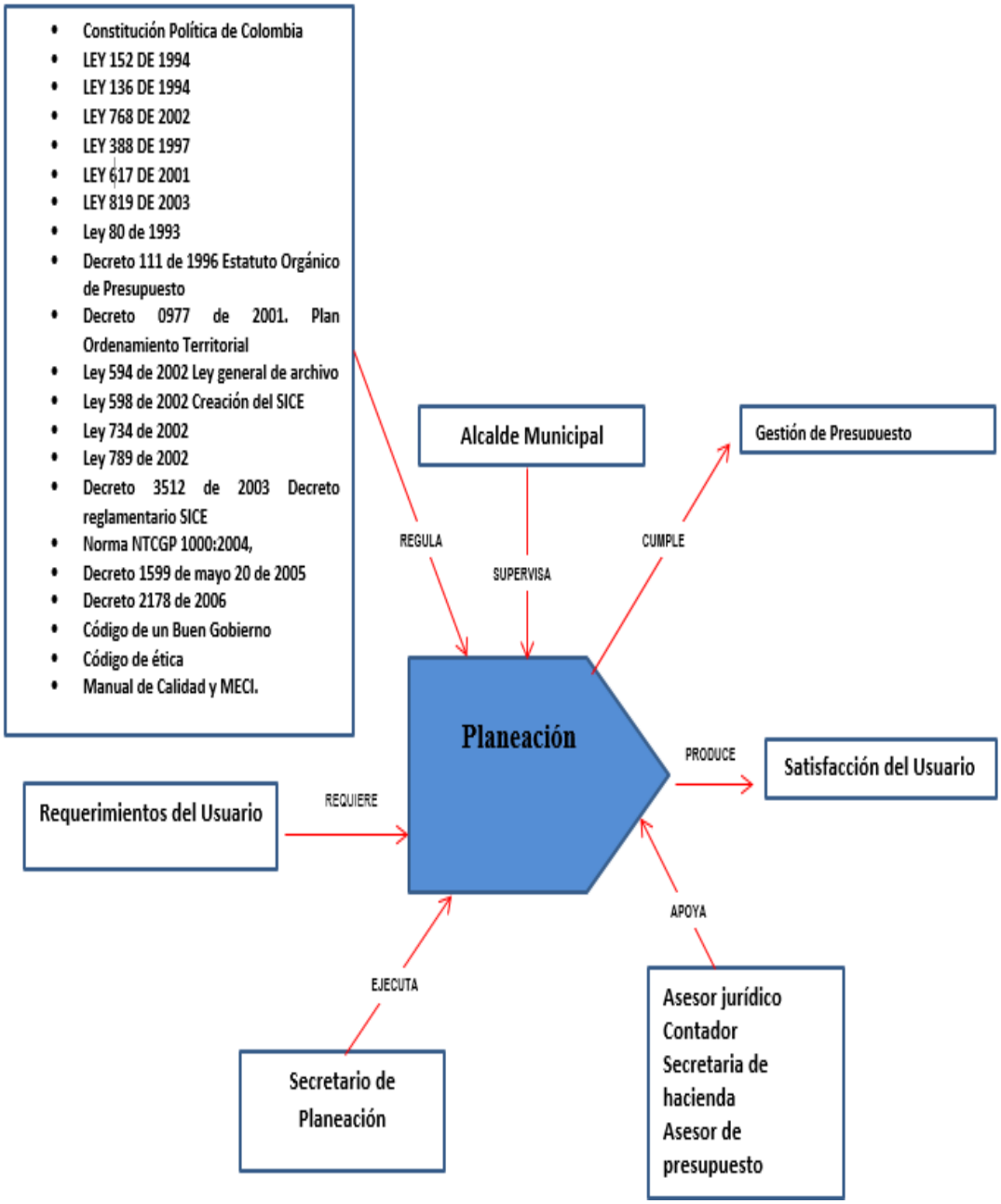

Figura 12. Planeación.
Fuente: Autoras del proyecto

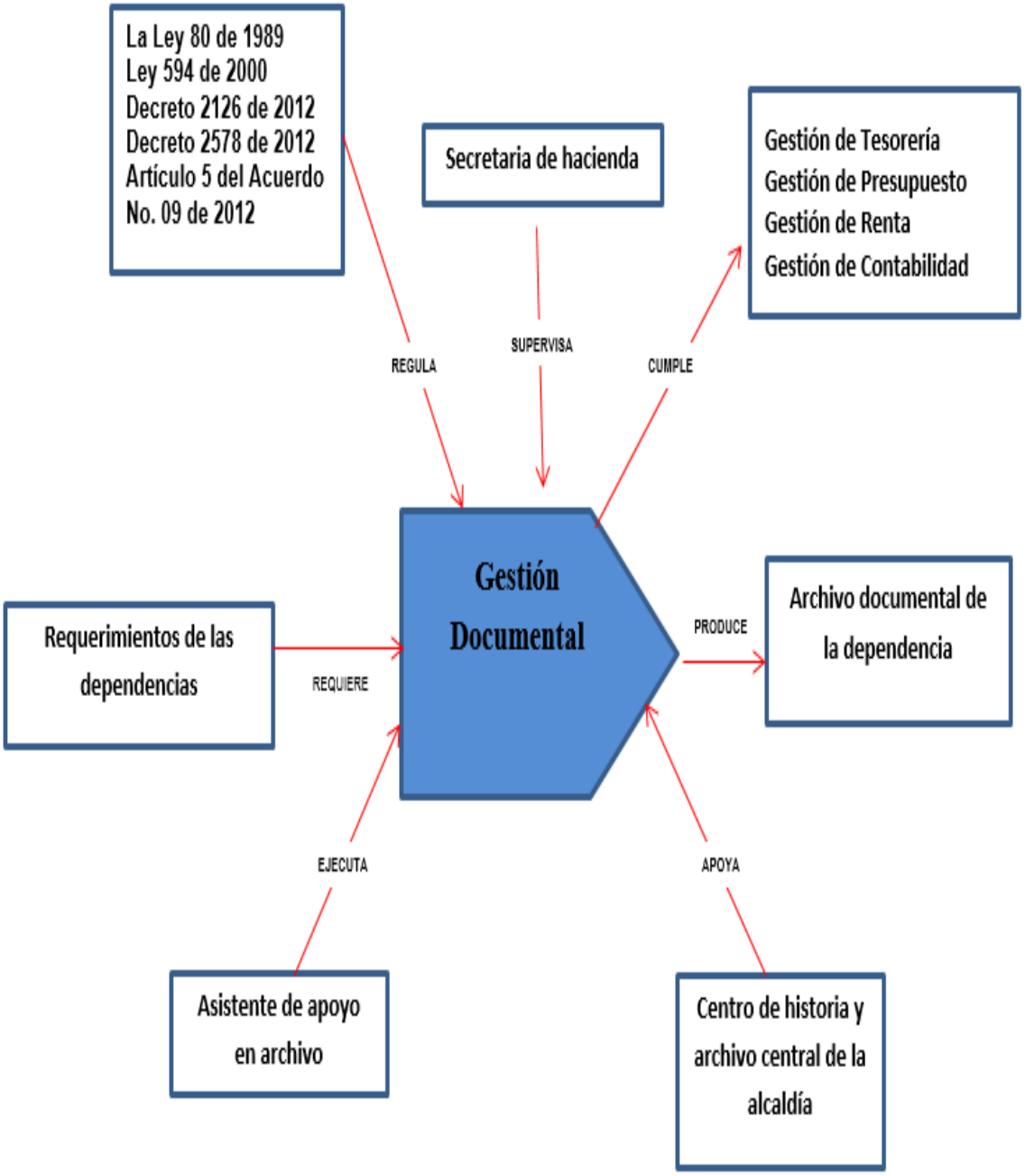

Figura 13. Gestión Documental.
Fuente: Autoras del proyecto

4.1.5 Infraestructura tecnológica de la Secretaría de Hacienda de Rio de Oro- Cesar.

La dependencia cuenta con una red local LAN que intercomunica a los dispositivos finales (computadores de los funcionarios) con el servidor donde se encuentran instaladas las bases de datos de los sistemas de información que son utilizados en la Secretaria.

Es importante mencionar que no existe una red LAN que comunique a todas las dependencias de la alcaldía, existen redes LAN por dependencia y con una infraestructura pobre en cuanto a equipos de redes. La topología de red de la dependencia Secretaría de Hacienda es una red LAN en estrella.

Equipos de comunicación. En la Secretaría de Hacienda de Rio de Oro- Cesar, se cuenta con los siguientes equipos que se detallan en la tabla 2.

Tabla 2.
Inventario de equipos secretaría de hacienda

DESCRIPCIÓN	RESPONSABLE	ESPECIFICACIONES
1. PC de Escritorio	Secretaria Ejecutiva	Modelo Indefinido Fabricante LENOVO Fecha Adquisición Indefinida Pantalla 21 Pulgadas CPU Color Negro Procesador Core 3 RAM 4 GB Disco Duro 1 Tera Sistema Operativo Windows 7 (con Licencia) "SW Especifico" Visual TNS
2. PC de Escritorio	Coordinador de Rentas	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 Sistema Operativo Windows 7 (con Licencia)

		"SW Especifico" Neptuno impuestos
3. PC de Escritorio	Auxiliar de Tesorería	Modelo Indefinido Fabricante COMPAQ Fecha Adquisición Indefinida Pantalla 14 Pulgadas, Convencional CPU Color Negro y Gris Procesador Intel RAM 2 GB Disco Duro 80 Sistema Operativo Windows XP "SW Especifico" Ninguno
4. PC de Escritorio	Contador	Modelo AMD FX (TM) 8120 Fabricante AOC Modelo Indefinido Fabricante LENOVO Pantalla 19 Pulgadas CPU Color Negro Procesador Core 7, con 8 núcleos RAM 4 GB Disco Duro 1 Tera Sistema Operativo Windows 8 (con Licencia) "SW Especifico" Visual TNS
5. PC de Escritorio	PASIVOCOL	Modelo Indefinido Fabricante SAMSUNG Fecha Adquisición Indefinida Pantalla 19 Pulgadas CPU DELUX Color Negro Procesador AMD Admin RAM 2 GB Disco Duro 80 Sistema Operativo Windows 7 "SW Especifico" Ninguno
6. PC de Escritorio	Secretaria de Hacienda	Modelo Indefinido Fabricante SAMSUNG Fecha Adquisición Indefinida Pantalla 18 Pulgadas CPU Color Negro Procesador AMD Dual Core RAM 2 GB Disco Duro 250 Sistema Operativo Windows 7 "SW Especifico" Visual TNS CPU Color Negro Procesador Intel Atom 1,66 GHZ, 2 en 1 RAM 2 GB Disco Duro 500
7. Router	Secretaria de Hacienda	Modelo WR 740 N Fabricante Tepelink TECNICAS Puertos 5 puertos

8.	**Servidor**	Secretaria de Hacienda	Interfaces WAN 1 puerto 10/100 Mbps Interfaces LAN 4 puertos 10/100 Mbsps Licencia Winsows Server 2008 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 -

Fuente. Alcaldía Municipal

Aplicativos de apoyo (SGBD).Firebird: Es un sistema de gestión de base de datos (SGBD) para bases de datos relacionales que ofrece muchas características estándar ANSI SQL que se ejecuta en Linux, Windows y una variedad de plataformas Unix. Firebird ofrece una excelente concurrencia, alto rendimiento, y potente soporte de idiomas para los procedimientos almacenados. Buena Seguridad Basada en usuarios/roles. Soporte de transacciones ACID y claves foráneas. Alta compatibilidad con ANSI SQL.

Si alguna conexión de red o programa cliente tiene un problema, puede dañar el archivo de datos, ya que lo está abriendo directamente.

Los requerimientos mínimos para la utilización de Firebird son de 64MB de RAM y 20MB de Disco Duro

.

Sistemas de información. En la secretaría de hacienda se manejan dos sistemas de información: VISUAL TNS OFICIAL, con licencia actualizada. Neptuno Impuestos versión 2.5.1.0, con licencia actualizada.

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.

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.

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.

Software Neptuno Impuestos: este Software está compuesto por los siguientes módulos que se detallan a continuación:

Módulo impuesto predial unificado.

- Se crea políticas de financiación para los acuerdos de pago
- Se diseña el recibo de pago en fastreport y permite poner hasta cuatro códigos de barras en la impresión con 4 fechas de vencimiento.
- Se crea el manejo de exentos y excluidos.
- Permite parametrizar la liquidación de interés por trimestres según cuadro de la DIAN, o liquidación de interés por la última tasa.
- Permite proyectar el valor de loa interés en acuerdos de pagos según la liquidación bancaria.
- Creación de número de cuenta o ID de predio para el manejo más sencillo del código de único nacional de 30 dígitos.
- Aplicación masiva de novedades de exclusiones y exenciones de los predios.
- Procesar el plano Asobancaria 98 o Asobancaria 2001 en el recaudo de archivos planos con código Permite registrar anotaciones especiales a los predios.

- Nueva Opción de Procesar o reprocesar mediante un archivo plano o formato Excel los pagos registrados en la plataforma de pagos ONLINE que se realizan a través del portal WEB.
- Nueva opción de pagos por lotes que permite reprocesar los planos de los bancos en el formato que se desee
- Nueva opción de Generar el aviso de Cobro desde la ventana de liquidación de predial.
- Consulta del plano de Novedades del IGAC cuando se realice el cargue de resoluciones del IGAC.
- Nueva opción de parametrizarla funcionalidad de crear saldos a favor del contribuyente automáticos al momento de re liquidar deuda por menor avalúo.

Módulo de industria y comercio

- Permite la creación de políticas de financiación para los acuerdos de pago.
- Actualización del módulo de Novedades ajustando algunos criterios para facilitar la aplicación de novedades.
- Encriptación de la Clave en MD5 para mejorar la seguridad y evitar que las claves sean descifradas.
- Nueva opción de parametrización que permite en una sola ventana accedes a la creación de la vigencia inicial cuando hay cambio de vigencia, allí se pueden crear los intereses, descuentos, tarifas, entre otras opciones del sistema. Simplifica el manejo de estas tablas básicas y el inicio de la Vigencia.
- Impresión del Formato de Declaración una vez digitada la declaración editable en ejecución (FastReport).

- Impresión del Formato de Novedades una vez Creada la novedad editable en ejecución (FastReport).
- Impresión del Formato de Inscripción de Establecimiento editable en ejecución (FastReport).
- Opción de Facturación Masiva de Establecimientos que tiene cartera pendiente.
- Opción de Generación de plano e integración en línea con el módulo de Fiscalización WEB.
- Opción de liquidación de pagos de fechas anteriores
- Opción de Modificar datos básicos del establecimiento en una solo novedad en la cual se registrar los datos anteriores y actuales de cada campo.
- Opción de Crear datos adicionales de Revisor Fiscal, con sus respectivos datos.
- Permite registrar sedes del mismo contribuyente para evitar dobles registros de placas del mismo NIT de contribuyente.
- Opción de generar Recibo al Contribuyente por vigencias específicas.
- Parametrización de liquidación de interés por trimestres según cuadro de la DIAN, o liquidación de interés por la última tasa.
- Proyección de interés en acuerdos de pagos según la liquidación bancaria.

Módulo De Impuestos Menores

- Permite consultar la base de datos de predial con el fin que en la factura de paz y salvo en el campo notas muestre el código predial y el número de cuenta
- Permite ingresar un valor alterno para el cálculo de fórmulas que solicita ingresar más de dos valores
- Diseño de la factura de impuestos menores en mostrar datos completos del tercero

4.1.6 Auditoria del estado actual de la gestión de la seguridad de la Secretaria de Hacienda de Rio de Oro-Cesar.

Objetivo. Evaluar la existencia y eficiencia de los controles de seguridad de la información en La Secretaria de Hacienda de Rio de Oro-Cesar, de acuerdo con los dominios contemplados en el estándar ISO/IEC 27001:2013.

Alcance. Esta auditoría comprende un análisis bajo tres perspectivas procedimental, tecnológica y de talento humano y de todos los elementos existentes, para garantizar la gestión de la seguridad de la información en la Secretaría de Hacienda del Municipio de Rio de Oro – Cesar. La evaluación cubrió trece de los catorce dominios del estándar internacional ISO/IEC 27002:2013.

Plan de auditoría. Se elaboró un plan diseñado por etapas, y a su vez, fraccionado por actividades. Ver Tabla 3.

En ocasión a que en la Secretaria de Hacienda de Rio de Oro-Cesar no existe un sistema de gestión de seguridad de la información, se desarrollaron las fases que se enuncian a continuación enmarcadas dentro de la norma ISO/IEC 2001:2013 ubicado dentro de la fase de planeación del ciclo PHVA:

Tabla 3.
Plan de auditoria Secretaria de Hacienda de Rio de Oro-Cesar.

	Equipo de auditoría	**Fecha auditoría**	**Lugar**	**Firma auditor líder**
Secretaría de Hacienda	Maire Lisneth Serna Vega Aleida Duran Peñaranda Rosy Sánchez Acosta	04/07/2017 al 28/07/2017		
Objetivo	Evaluar la existencia y eficiencia de controles de seguridad de la información en La Secretaria de Hacienda de Rio de Oro-Cesar, de acuerdo con los dominios contemplados en el estándar ISO/IEC 27001:2013.			
Alcance	Esta auditoría comprende un examen a los elementos existentes para garantizar la gestión de la seguridad de la información en la Secretaría de Hacienda del Municipio de Rio de Oro - Cesar, durante el periodo que va del 04 de julio de 2017 al 28 de julio de 2017			
Criterio	Se regirá por los dominios de la norma ISO/IEC 27001: 2013, exceptuando el dominio de adquisición, desarrollo y mantenimiento de sistemas de información que fue considerado por el equipo auditor como no aplicable a la organización.			
Etapa	Actividad			Auditor
Contacto Inicial	Reunión con la secretaria de Hacienda, Mayra Alejandra Vanegas Picón			
Inicio de la Auditoría	Reunión de apertura de la auditoría con los funcionarios en la Secretaría de Hacienda del Municipio de Rio de Oro - Cesar			
Recolección de información	Solicitar los siguientes documentos: manual de funciones, reglamento interno, código de ética de los funcionarios de la administración, documentación corporativa: estructura orgánica, misión, visión, objetivos, mapa de procesos.			Equipo de auditoría
Ejecución de la auditoría	Elaboración de los instrumentos de recolección de información. Revisión documental. Aplicación de los instrumentos de recolección de información. Listas de chequeo			
Comunicación de resultados	Hallazgos encontrados Diseñar y preparar una estructura de informe. Elaboración del informe de auditoría.			

Fuente: Autores del proyecto

Evaluación del cumplimiento de la norma ISO/IEC 27001:2013 de la Secretaria de Hacienda de Rio de Oro-Cesar. En esta fase se realizó un análisis GAP de la situación inicial del SGSI de la Secretaria de Hacienda de Rio de Oro-Cesar, con el fin de determinar el nivel de cumplimiento de los dominios, objetivos de control y controles de seguridad de la información, conformes al estándar ISO/IEC 27002:2013.

El análisis GAP (análisis de brechas) es un estudio formal con respecto a los niveles de seguridad implementados actualmente por la dependencia y aquellos hacia los cuales se desea llegar en un futuro cercano, debe asegurar:

- La revisión y medición del nivel de cumplimiento de la entidad con respecto a la seguridad de la información.
- Provee un indicativo del esfuerzo, tiempo, dinero y recursos humanos que van a ser requeridos para obtener el objetivo deseado.
- Constituye el punto de arranque de la definición de una estrategia de la arquitectura de seguridad de la información, perfectamente alineada con la visión de la entidad, dentro de su entorno de operación.

Análisis e interpretación de la información. Con el fin de determinar el estado actual de la seguridad de la información de la Secretaria de Hacienda de Rio de Oro-Cesar, se realizaron visitas a la dependencia, donde se aplicaron los instrumentos de recolección de la información previamente seleccionados, además de entrevista directa con a la Secretaria de Hacienda y aplicación de encuestas y lista de chequeo al personal de la dependencia. Ver Apéndice 1

Para llevar a cabo la ponderación del cumplimiento se propuso la siguiente valorización, de acuerdo al Análisis GAP. Para llevar a cabo la ponderación del nivel de madurez del SGSI, de la Secretaria de Hacienda de Rio de Oro-Cesar, se utilizó la Tabla 4: *Valorización cláusulas requerimientos -ISO IEC 27001:2013.*

Tabla 4.
Valorización cláusulas re requerimientos -ISO IEC 27001:2013

%	ESTADO	DESCRIPCION
0	**No Existe**	Ausencia absoluta de una política reconocible, procedimiento, control, etc.
10	**Inicial**	El desarrollo apenas está iniciando y requerirá un trabajo significativo para cumplir con el requisito.
50	**Limitado**	Progresando muy bien pero aun incompleto.
90	**Definido**	El desarrollo está más o menos completo aunque se carece de detalle y/o aún no se ha implementado, impartido y promovido por la alta dirección.
95	**Gestionado**	El desarrollo está completo, el proceso/control se ha implementado y recientemente comenzó a operar.
100	**Optimizado**	El requisito está completamente cumplido, está funcionando completamente como se esperaba, está siendo monitoreado y mejorado constantemente, y hay evidencia sustancial para demostrarlo en una auditoria.
-	**No Aplicable**	TODOS los requisitos en el cuerpo principal de la norma ISO / IEC 27001 son obligatorios SI el SGSI es para ser certificado. De lo contrario, podrían ser ignorados.

Fuente. Autores del proyecto

A continuación se presenta la evaluación del nivel de cumplimiento de La Secretaria de Hacienda de Rio de Oro Cesar, basado en la Norma ISO-IEC 27001:2013.

Esta evaluación contemplo las etapas el diagnóstico del marco de seguridad y privacidad de la dependencia, que enmarca en la fase PLANEAR del ciclo PHVA. En esta etapa se |identifican las áreas susceptibles de mejora y se planificaron los objetivos a alcanzar, los resultados obtenidos se muestran en la tabla 5, Diagnóstico del marco de seguridad y privacidad secretaria de hacienda de la alcaldía de Rio de Oro – Cesar.

Tabla 5.
Diagnóstico del marco de seguridad y privacidad secretaria de hacienda de la alcaldía de Rio de Oro – Cesar.

DIAGNOSTICO DEL MARCO DE SEGURIDAD Y PRIVACIDAD SECRETARIA DE HACIENDA DE LA ALCALDÍA DE RIO DE ORO – CESAR, ISO-IEC 27001:2013				
ITEM	**ITEM A EVALUAR**	**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
1	La Secretaria de Hacienda cuenta con un autodiagnóstico realizado para medir el avance en el establecimiento, implementación, mantenimiento y mejora continua de su SGSI (Sistema de Gestión de Seguridad de la información?	NO EXISTE	0	En la dependencia no existe un SGSI. Por lo tanto no hay un parámetro que permita la medición.
2	La Secretaria de Hacienda creó un plan inicial del proyecto, donde se incluyen las prioridades y objetivos para la implementación del SGSI?	NO EXISTE	0	En la dependencia no existe un plan inicial para la implementación del SGSI.
3	La Secretaria de Hacienda contó con la aprobación de la dirección para iniciar el proyecto del SGSI?	**GESTIONADO**	95	Se gestionó y está autorizado por el Alcalde.
4	La Secretaria de Hacienda ha identificado los aspectos internos y externos que pueden afectar en el desarrollo del proyecto de implementación del sistema de gestión de seguridad de la información?	NO EXISTE	0	No se ha realizado la identificación del entorno, respecto al SGSI.
5	La Secretaria de Hacienda ha identificado las partes interesadas, necesidades y expectativas de estas respecto al Sistema de Gestión de Seguridad de la Información?	**INICIAL**	10	Se está haciendo de manera parcial, diferente a la norma y no está documentado.
6	La Secretaria de Hacienda ha evaluado los objetivos y las necesidades respecto a la Seguridad de la Información?	NO EXISTE	10	No se han evaluado los objetivos,.
7	En La Secretaria de Hacienda se ha definido un Comité de Seguridad de la Información?	NO EXISTE	0	No se ha definido.
8	La Secretaria de Hacienda cuenta con una definición del alcance y los límites del Sistema de Gestión de Seguridad de la Información?	NO EXISTE	0	No se ha definido el alcance, ni los límites del SGSI.

9	En La Secretaria de Hacienda existe un documento de política del Sistema de Gestión de Seguridad de la Información, el cual ha sido aprobado por la Dirección?	NO EXISTE	0	No existe ningún documento relacionado con el SGSI.
10	En La Secretaria de Hacienda existe un documento de roles, responsabilidades y autoridades en seguridad de la información?	**INICIAL**	10	Se está haciendo diferente, no está documentado.
11	La Secretaria de Hacienda tiene establecido algún proceso para identificar, analizar, valorar y tratar los riesgos de seguridad de la información?	NO EXISTE	0	No existe ningún documento relacionado con el tratamiento de los riesgos de la seguridad de la información.
12	La Secretaria de Hacienda ha realizado una declaración de aplicabilidad que contenga los controles requeridos por La Secretaria de Hacienda?	NO EXISTE	0	No se ha realizado.
13	La Secretaria de Hacienda ha evaluado las competencias de las personas que realizan, bajo su control, un trabajo que afecta el desempeño de la seguridad de la Información?	NO EXISTE	0	Se han establecido roles, pero no se han tomado en cuenta las competencias del talento humano. No está documentado.
14	La Secretaria de Hacienda tiene definido un modelo de comunicaciones tanto internas como externas respecto a la seguridad de la información?	NO EXISTE	0	No se ha definido.
15	La Secretaria de Hacienda tiene la información referente al Sistema de Gestión de Seguridad de la Información debidamente documentada y controlada?	NO EXISTE	0	No existe información del SGSI, al interior de la dependencia.
			125	NO EXISTE
	NIVEL DE CUMPLIMIENTO		8	

Fuente: Autores del proyecto

Una vez diligenciado los interrogantes de la tabla de diagnóstico del marco de seguridad y privacidad secretaria de hacienda de la alcaldía de Rio de Oro – Cesar, como resultado se obtuvo lo siguiente:

Tabla 6.
Consolidado de diagnóstico del marco de seguridad y privacidad secretaria de hacienda de la alcaldía de Rio de Oro – Cesar

ESTADO	FRECUENCIA	%
No existe	12	80
Inicial	2	13
Limitado	0	0
Definido	0	0
Gestionado	1	7
Optimizado	0	0
No aplica	0	0
TOTALES	**15**	**100**

Fuente: Autores del proyecto

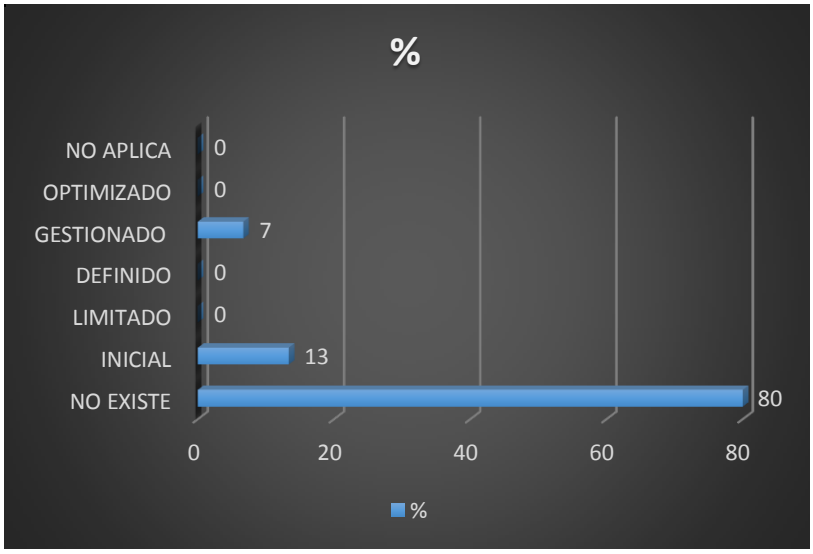

Figura 14. Diagnóstico consolidado del marco de seguridad y privacidad secretaria de hacienda de la alcaldía de Rio de Oro – Cesar
Fuente.Autores del proyecto

De acuerdo a los resultados obtenidos en la tabla 20 y la gráfica 20, se determinó que el nivel de cumplimiento en cuanto se refiere a la definición del Marco de Seguridad y Privacidad

de SGSI de la Secretaria de Hacienda de Rio de Oro-Cesar, respecto a la norma ISO-IEC 27001:2013, se encuentra **INEXISTENTE.** Lo anterior se pude sustentar en el hecho de que la mayor parte de los ítem evaluados no cuentan con un proceso reconocible respecto a la Seguridad de la Información, actualmente no existe un análisis, ni un plan inicial que le permita a la dependencia establecer las prioridades y objetivos para el diseño y posterior implementación SGSI. De igual forma la dependencia carece de un Sistema de Gestión Seguridad de la Información.

Las Directivas de la Secretaria reconocen que existen problemas a nivel de Seguridad de la información y necesitan resolverlos, sin embargo la gestión realizada hasta el momento no ha sido eficaz. Los procesos que existen tienden a ser aplicados en forma individual y los métodos en general de la administración de la Seguridad de la Información son desorganizados.

Los procedimientos no han sido estandarizados, ni documentados, no obstante, se cuenta con alguna información relacionada a los procesos de identificación de las partes interesadas del SGSI y de los roles, y responsabilidades de la Seguridad de la información, sin embargo los mismos no se han documentado, ni tampoco comunicado. El seguimiento de estos procesos se ha dejado en manos de las personas involucradas, por lo tanto se corre el riesgo que no se detecten desviaciones.

Por último, la Secretaria de Hacienda no tiene establecidos procesos de identificación, análisis, valoración y tratamiento de los riesgos de la seguridad de la información. Lo que la

expone a que se materialice una amenaza en los sistemas de información, que pueden ser utilizadas para vulnerar efectivamente su seguridad física y lógica.

4.2 Nivel de madurez de la Secretaria de Hacienda con respecto al modelo de seguridad de la información que plantea la norma ISO/IEC 27001:2013.

La versión 2013 de la norma ISO 27001, alineo su estructura conforme a los lineamientos definidos en el Anexo SL12 de las directivas ISO/IEC, con el objetivo de mantener la compatibilidad entre las normas ISO de sistemas de gestión que se han ajustado a este anexo.

El estándar ISO/IEC 27001 comprende dos secciones. En la primera sección se especifican cinco cláusulas enfocadas a características metodológicas del SGSI, que tienen estricto cumplimiento para obtener la certificación, que están comprendidos entre las secciones del 4 al 10 de la norma ISO 27001:2013. (Ver apéndice 7)

En la segunda fase se definen los controles para la gestión de la seguridad de la información que están determinados por el estándar ISO/IEC 27001 y asociados con cada uno de los dominios que están en el Anexo A, desde el dominio A5 hasta A18 de la versión 2013.

Para determinar el nivel de madurez de la Secretaria de Hacienda de Rio de Oro-Cesar, se tomó como criterio la norma ISO IEC 27001:2013, Los dominios de esta norma corresponden a los diferentes capítulos que establecen los requerimientos que las organizaciones deben cumplir

para el establecimiento de un Sistema de Gestión de Seguridad de la Información, los cuales se resumen a continuación:

Por otro lado el Anexo A de la Norma ISO IEC 27001:2013 proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 dominios.

Para determinar el nivel de madurez de la dependencia, se determinaron dos etapas. Inicialmente se seleccionaron los requisitos del numeral 4 hasta el numeral 10 de la Norma ISO IEC 27001:2013. Posteriormente, seleccionaron del Anexo A, los dominios del A5 al A18 y los controles que aplican en cada caso.

4.2.1 Nivel de madurez de los requerimientos de la Norma ISO-IEC 27001: 2013. A continuación se muestra le evaluación del nivel de madurez realizado a la Secretaría de Hacienda de Rio de Oro-Cesar de acuerdo a los requerimientos planteados por la Normas ISO 27001:2013.

Tabla 7.
Evaluación por requerimientos aplicados de la norma ISO 27001:2013

✓ SECRETARIA DE HACIENDA DE LA ALCALDÍA DE RIO DE ORO – CESAR NIVEL DE MADUREZ 4. CONTEXTO DE LA ORGANIZACIÓN				
DESCRIPCION DEL REQUISITO	**ITEM A EVALUAR**	**ESTADO**	**PONDERACION**	**ESTADO DE MADUREZ**
4.1 Conocimiento de la organización y de su contexto.	DOFA.	No existe	0	**16.35**
	Planes estratégicos.	No existe	0	
	Organigrama.	Limitado	50	
	Clasificación de la información	Limitado	50	
	Misión.	Limitado	50	
	Visión.	No existe	0	
	Valores.	No existe	0	
	Objetivos.	Limitado	50	
	Manuales de funciones y procedimientos	Limitado	50	
	Reglamento interno de trabajo	Limitado	50	
	Modelado de procesos	Limitado	50	
	Políticas de seguridad de la información	No existe	0	
	Promedio de madurez		**29.17**	
4.2 Comprensión de las necesidades y expectativas de las partes interesadas.	a) Partes interesadas que son pertinentes al SGSI:	Inicial	10	
	Inventarios de socios.	No aplica	0	
	Proveedores.	No existe	0	
	Aliados.	No existe	0	
	Clientes.	No existe	0	
	Requerimientos actuales del gobierno.	No existe	0	
	b) Los requisitos de las partes interesadas.	No existe	0	
	Metas y objetivos del area según el alcance.	No existe	0	
	Promedio de madurez		**1.25**	
4.3 Comprensión de las necesidades y expectativas de las partes interesadas.	c) Las interfaces y dependencias entre las actividades realizadas y las que realizan otras empresas.	No existe	0	
	Modelado de procesos	Limitado	50	
	Promedio de madurez		**25**	
4.4 Sistema de Gestión de Seguridad de la información	Norma 27001	Inicial	10	
	Promedio de madurez		**10**	
NIVEL DE MADUREZ REQUISITO CONTEXTO DE LA ORGANIZACIÓN				**INICIAL**

DESCRIPCION DEL REQUISITO	ITEM A EVALUAR	ESTADO	PONDERACION	ESTADO DE MADUREZ
5.1 Liderazgo y Compromiso	Políticas y Objetivos SGSI	No existe	0	**0.00**
	Integración de requisitos del SGSI-Procesos Negocio	No existe	0	
	Disponibilidad de recursos necesarios SGSI	No existe	0	
	Comunicación SGSI	No existe	0	
	Resultados del SGSI	No existe	0	
	Apoyo y dirección al personal involucrado SGSI	No existe	0	
	Mejora continua	No existe	0	
	Roles de áreas por responsabilidad	No existe	0	
	Promedio de madurez			**0**
5.2 Política	Adecuada a la dependencia	No existe	0	
	Proporciona el marco de establecimiento de los objetivos de la seguridad de la información	No existe	0	
	Compromisos aplicados a la seguridad de la información	No existe	0	
	Compromisos de mejora continua	No existe	0	
	Promedio de madurez			**0**
5.3 Roles, Responsabilidades y Autoridades en la organización.	Responsabilidad y autoridad para llevar a cabo los requisitos del SGSI, de acuerdo a la norma. Y el nivel de desempeño.	No existe	0	
	Promedio de madurez			**0**
	NIVEL DE MADUREZ REQUISITO LIDERAZGO			**NO EXISTE**

DESCRIPCION DEL REQUISITO	ITEM A EVALUAR	ESTADO	PONDERACION	ESTADO DE MADUREZ
6,1 Acciones para tratar el riesgo y oportunidades.	6,1,1 Generalidades		0	**1.67**
	Conocimiento de la organización y de su contexto	Inicial	10	
	Comprensión de las necesidades y expectativas de las partes interesadas.	No existe	0	
	Promedio de madurez		**5**	
	6,1,2 Evaluación de riesgo de la seguridad de la información			
	Criterios de identificación de riesgo	No existe	0	
	Criterios de evaluación de riesgo	No existe	0	
	Criterios de aceptación de riesgo	No existe	0	

	Criterios de evaluación de riesgo	No existe	0	
	Criterios de identificación de los dueños de los riesgos	No existe		
	Promedio de madurez		**0**	
	6,1,3 Tratamiento del riesgo.	No existe	0	
	Declaración de aplicabilidad	No existe	0	
	Plan de tratamiento de riesgo	No existe	0	
	Inventario de controles de mitigación del riesgo	No existe	0	
	Promedio de madurez		**0**	
NIVEL DE MADUREZ REQUISITO CONTEXTO PLANEACION				**NO EXISTE**
DESCRIPCION DEL REQUISITO	**ITEM A EVALUAR**	**ESTADO**	**PONDERACION**	**ESTADO DE MADUREZ**
7,1 Recursos	Recursos necesarios para establecer, implementar, mantener y mejorar el SGSI	No existe	0	**2.98**
	Promedio de madurez		**0**	
7,2 Competencias	Determinación de competencias personal involucrado en la seguridad de la información, respecto educación, formación y experiencia.	No existe	10	
	Promedio de madurez		**10.00**	
7,3 Toma de Conciencia	Conciencia de políticas de Seguridad de la información	Inicial	10	
	Conciencia de aportes al desempeño del SGSI	No existe	0	
	Conciencia de las no conformidades de SGSI	No existe	0	
	Promedio de madurez		**3.33**	
7,4 Comunicación	Determinación de contenido de la comunicación	No existe	0	
	Determinación de personal involucrado en la Seguridad de la información	No existe	0	
	Determinación de responsables de la comunicación	No existe	0	
	Determinación de procesos para llevar a cabo la comunicación	No existe	0	
	Promedio de madurez		**0.00**	
7,5 Información documentada	7,5,1 Generalidades			
	Información documentada requerida por la norma	No existe	0.00	

	Información documentada necearía para la eficacia del SGSI	Inicial	10.00	
	Promedio de madurez		**2.50**	
	7,5,2 Creación y actualización			
	Identificación y descripción de formatos necesarios SGSI	No existe	0.00	
	Creación de formatos y medios de soportes proceso de SGSI	No existe	0.00	
	Promedio de madurez		**0.00**	
	7,5,3 Control de la información documentada			
	Disponibilidad de la información documentada	Inicial	10	
	Protección de la información documentada	No existe	0	
	Control en el acceso, recuperación y uso de la documentación	No existe	0	
	Almacenamiento y preservación de la documentación	Inicial	10	
	Promedio de madurez		**5.00**	
	NIVEL DE MADUREZ REQUISITO SOPORTE			**NO EXISTE**
DESCRIPCION DEL REQUISITO	**ITEM A EVALUAR**	**ESTADO**	**VALORIZACION**	**ESTADO DE MADUREZ**
8,1 Planificación y control operacional	Planificación, implementación y control de procesos documentados necesarios para cumplir con los requisitos del SGSI y acciones para tratar el riesgo.	No existe	0	**0.00**
	Promedio de madurez		**0**	
	NIVEL DE MADUREZ REQUISITO OPERACIÓN			**NO EXISTE**
DESCRIPCION DEL REQUISITO	**ITEM A EVALUAR**	**ESTADO**	**PONDERACION**	**ESTADO DE MADUREZ**
9,1 Seguimiento, medición, análisis y evaluación.	Medición de indicadores (BSC)	No existe	0	**0.00**
	Evaluación de lo ejecutado vs planificado	No existe	0	
	Promedio de madurez		**0**	
9,2 Auditoria Interna.	Auditoria SGSI	No existe	0	
	Análisis GAP	No existe	0	
	Promedio de madurez		**0**	

9,3 Revisión por la dirección.	Documentos de compromisos de la dirección respecto a los resultados de la auditoria interna, análisis GAP, análisis de riesgos y análisis de cumplimiento. SGSI	No existe	0	
		Promedio de madurez	**0**	
	NIVEL DE MADUREZ REQUISITO EVALUACION DE DESEMPEÑO			**NO EXISTE**
DESCRIPCION DEL REQUISITO	**ITEM A EVALUAR**	**ESTADO**	**PONDERACION**	**ESTADO DE MADUREZ**
10,1 No conformidades y acciones correctivas.	Evidencia vs acciones tomadas no conformidades.	No existe	0	**0.00**
	Evidencia de indicadores.	No existe	0	
		Promedio de madurez	**0**	
10,2 Mejora continua.	Evidencia de reuniones, monitoreo toma de decisiones dirección.	No existe	0	
		Promedio de madurez	**0**	
	NIVEL DE MADUREZ REQUISITO MEJORA			**NO EXISTE**

Fuente. Autores del proyecto

Tabla 8.
Puntaje totalizado por requerimientos evaluados de la norma ISO 27001: 2013 a la Secretaría de Hacienda.

DOMINIO	ESTADO %	CALIFICACION
4 Contexto de la organización.	16.35	Inicial
5 Liderazgo.	0	No existe
6 Planeación.	1.67	No existe
7 Soporte.	2.98	**No existe Intuitivo Inicial**
8 Operación.	0	No existe
9 Evaluación.	0	No existe
10 Mejora.	0	No existe
TOTAL	3.00	NO EXISTE

Fuente. Autores del proyecto

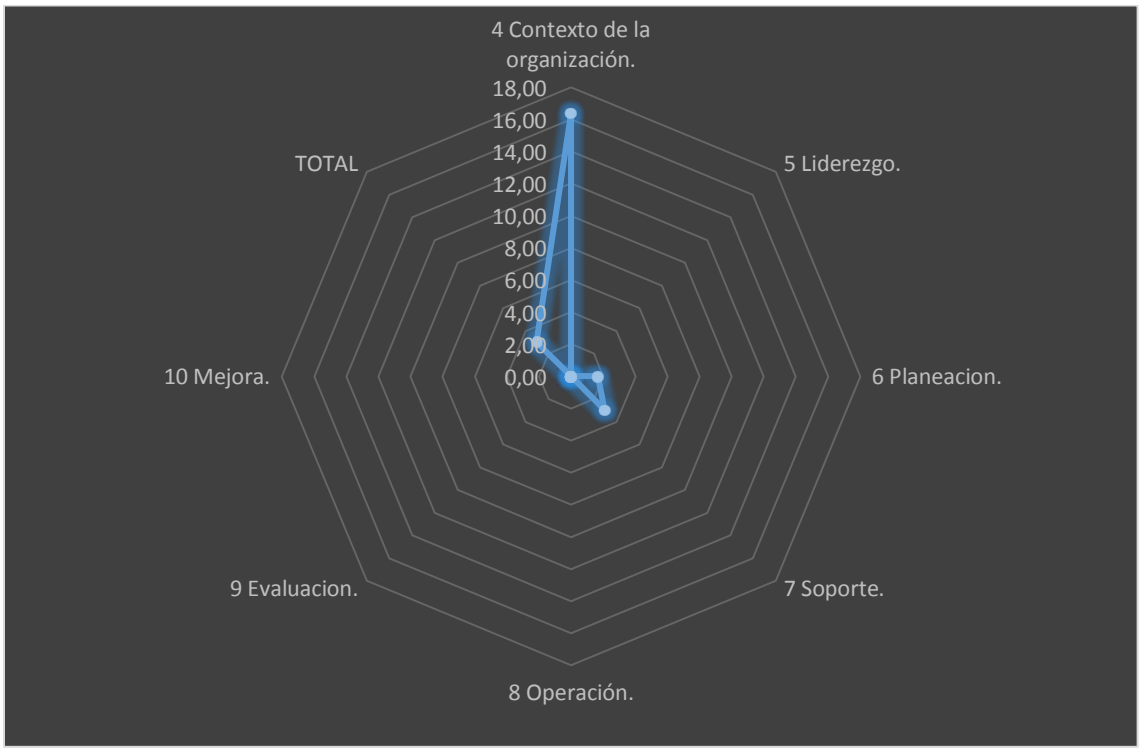

Figura 15. Grafica de red del Puntaje totalizado por requerimientos evaluados de la norma ISO 27001: 2013 a la Secretaría de Hacienda.
Fuente. Autores del proyecto

Con base a la evaluación realizada de los requerimientos y dominios de la norma ISO-IEC 27001:2013, se encontró que la situación actual de seguridad de la información, se encuentra en el nivel de madurez 3, considerado como "NO EXISTE". Para llegar a esta ponderación se tomó en cuenta los criterios definidos en la Tabla 9, donde se define claramente que la calificación

final se obtiene de promediar todas las calificaciones dadas, el valor resultante se aproximó a la cifra más baja y el resultado es el valor de la calificación.

Lo anterior indica que la Secretaria de Hacienda de Rio de Oro-Cesar, no está trabajando en estrategias para fortalecer la seguridad de la información en la dependencia, estas estrategias deben estar alineadas con los procesos misionales, para lograr un nivel de madurez mayor.

Lo anterior se evidencio en la falta de directrices a nivel de dirección y la escasa participación de las directivas respecto a la seguridad de la información. La alta dirección no ha establecido una política de seguridad de la información, además no tiene un estimativo de la asignación de recursos para el SGSI y tampoco ha establecido las responsabilidades y roles pertinentes a la seguridad de la información.

De igual forma se estableció que no existe participación de todos los involucrados de la dependencia con respecto al establecimiento de procedimientos adecuados y a la planeación e identificación de controles de seguridad de la información. Lo anterior obedece al escaso conocimiento y cultura, en temas de seguridad de la información, y a falta de interés por parte de los funcionarios en temas de seguridad.

Por otro lado cabe resaltar que la dependencia no ha establecido los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento. La dependencia carece de un sistema de información para la gestión de riesgos de seguridad, que le permita

inicialmente una valoración de riesgos de seguridad de los activos de información y seguidamente determinar las medidas y controles de seguridad, orientados a proteger la confidencialidad, la integridad y la disponibilidad de su información.

En cuanto se refiere al apartado de operación, se estipuló que la dependencia debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información, con el fin de definir los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y establecer el proceso de mejora del Sistema de Gestión de Seguridad de la Información, a partir de las no-conformidades con el objetivo de que no se repitan.

4.2.2 Nivel de madurez en cuanto al Anexo A de la Norma ISO-IEC 27001:2013. En el Apéndice 8, se describe el estado de madurez actual detallado para el Anexo A de la Norma ISO 27001:2013, de la Secretaria de Hacienda de Rio de Oro Cesar, luego de haber realizado esta evaluación se muestran los resultados obtenidos en la tabla 9.

Tabla 9.
Promedios del nivel de cumplimiento - Secretaria De Hacienda De Rio De Oro -Cesar.

DOMINIO EVALUADO	PONDERACION DE CUMPLIMIENTO POR DOMINIO
A5 políticas de seguridad de la información	0
A6 organización de la seguridad de la información	2
A7 seguridad de los recursos humanos	2
A8 gestión de activos	17
A9 control de acceso	0
A10 criptografía	0
A11 seguridad física y del entorno	0
A12 seguridad de las operaciones	3
A13 seguridad de las comunicaciones	2
A14 adquisición - desarrollo y mantenimiento de sistemas	0
A15 relación con los proveedores	0
A16 gestión de incidentes de la seguridad de la información	0
A17 aspectos de seguridad de la información de la gestión de continuidad de negocio	0
A18 cumplimiento	1
nivel de cumplimiento	**1.93**

Fuente. Autoras del proyecto

Luego de realizada la evaluación por dominios y con los resultados obtenidos de las tablas 16 y 17, se realizó un análisis de del estado actual de la gestión de la seguridad de la información que por cada dominio de la norma ISO/IEC 27001:2013:

Dominio 5. Políticas de Seguridad de la Información. Actualmente en la Secretaria de Hacienda de Rio de Oro-Cesar, no existen documentos que especifiquen los lineamientos en cuanto a la protección de la información sensible para la dependencia. La ausencia de unas Políticas de la Información no le permite el direccionamiento y soporte de los requerimientos de seguridad de sus activos informáticos y crea desorganización a la hora de llevar a cabo procedimientos, controles y de establecimiento de roles y responsabilidades respecto a la seguridad de la información.

Dominio 6. Aspectos organizativos de la seguridad de la información. La Secretaria de Hacienda de Rio de Oro-Cesar, no ha establecido las funciones y compromisos de la seguridad de la información, aunque los funcionarios se encuentran separado por áreas y tienen acceso a los activos y/o información necesaria para ejecutar sus actividades laborales, la Secretaria de Hacienda no tiene definida un área de sistemas, que se responsabilice de las actividades relacionadas con la gestión de la seguridad de la información. La dependencia carece de un marco referencial para iniciar y controlar la implementación de la seguridad de la información más relevante.

Así mismo, la dependencia no cuenta con procedimientos que especifiquen cuándo y cuáles autoridades contactar, y cómo se debieran reportar los incidentes de seguridad de la información que se puedan presentar en un momento determinado.

Por otro lado, en lo que respecta a los dispositivos móviles la dependencia carece de medidas de seguridad, para gestionar los riesgos introducidos por el uso de estos dispositivos.

Dominio 7. Seguridad ligada a los Recursos Humanos. Después de haber realizado una revisión a los métodos de selección y contratación de la Secretaria de Hacienda, se estableció que la dependencia selecciona al personal de acuerdo al perfil y la idoneidad del trabajo a ejecutar. De igual forma en el momento de contratación se toma en cuenta las leyes y reglamentaciones colombianas, sin embargo la dependencia no cuenta con una herramienta que garantice que su personal administrativo y contratistas, conozcan las responsabilidades y funciones en lo referente a seguridad información. Así mismo, los contratos que se suscriben con el personal a contratar y

con terceros no especifican un acuerdo de confidencialidad de la información, durante y después del contrato, lo que representa un riesgo para los principios básicos de la información.

Respecto a las faltas a los procesos disciplinarios en caso de incidencia de una violación a la seguridad de la información, la Secretaria no cuenta con proceso formal que le permita emprender acciones contra los infractores de la seguridad de la información.

Dominio 8. Gestión de Activos. La Secretaria de Hacienda actualmente tiene documentación relacionada con la identificación y clasificación de todos los activos ligados al sistema de información de la dependencia, de igual forma existe un documento donde se encuentran relacionados todos los propietarios de los activos informáticos inventariados. Sin embargo no se han implementado las reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. En lo que se refieren a la devolución de activos, existe un registro de paz y salvo, para empleados y usuarios de partes externas, donde se especifica la devolución de todos los activos de la dependencia, que se encuentren su cargo del responsable, al terminar su empleo, contrato o acuerdo.

Por otro lado, La Secretaria de Hacienda, no cuenta con un sistema de clasificación y etiquetado de información susceptibilidad a divulgación o a modificación no autorizada. Por último es necesario que la dependencia implante procedimientos para la gestión de medios removibles, debido a la frecuencia con que se usan y al riesgo que representan estos dispositivos para el uso y manejo de la información.

Dominio 9. Control de accesos. La Secretaria de Hacienda, carece de políticas de control de acceso a los sistemas de información, todos los usuarios tienen manejo de todos los equipos y permiso para la el manejo y uso de la red.

No se evidencia procesos respecto al registro y cancelación de acceso a los usuarios, ni durante la ejecución de su contrato laboral, ni posteriormente a la terminación del mismo. Además, aunque a cada usuario se le tiene asignada una contraseña, se evidencio que las claves, son compartidas y no se actualizan con frecuencia. Asimismo se determinó que la dependencia, no cuenta con un procedimiento para la asignación, control y restricción de derechos de acceso y privilegios sobre sus recursos tecnológicos y aplicaciones.

Dominio 10. Cifrado. La Secretaria de Hacienda carece de mecanismos, procedimientos y políticas orientados a establecer el uso de controles criptográficos para proteger la información.

D**ominio 11. Seguridad física y del entorno**. La Secretaria de Hacienda en lo referente a la protección contra amenazas externas y ambientales, no ha diseñado sistemas de protección física contra el daño causado por fuego, inundación, terremoto, explosión, revueltas sociales y otras formas de desastres naturales o provocados por el hombre. Igualmente no cuenta con sistemas contra robo o circuito cerrado de televisión.

Respecto a las áreas seguras de trabajo, se pudo observar que existe un perímetro físico delimitado, pero la dependencia no cuenta con personal de seguridad para el control de acceso a las instalaciones y por ende a la información.

En cuanto a los equipos es de resaltar, que los mismos están protegidos solo con una UPS, contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro. Respecto al sistema de cableado eléctrico y de telecomunicaciones que da soporte a los servicios de información, no se encuentran protegidos frente a interceptaciones o daños.

En lo relacionado con el mantenimiento de los equipos, se evidencio que solo reciben mantenimiento correctivo, no existen cronogramas anuales de mantenimientos preventivos que le permitan a los mismos asegurar la disponibilidad y la integridad de la información. Por otro lado la Secretaria de Hacienda para llevar a cabo el retiro de equipos, cuenta con un documento que se debe diligenciar y el cual debe estar autorizado por la Secretaria de Hacienda, no obstante los soportes de almacenamiento no son en su totalidad comprobados para confirmar que todo dato sensible y todas las licencias de software se han eliminado, borrado o sobrescrito de manera segura, antes de su retirada.

Por último, la dependencia carece de una política de puesto de trabajo despejado y bloqueo de pantalla. Se evidencio que muchos de los funcionarios poseen información confidencial de los usuarios del sistema.

Dominio 12. Seguridad en la Operativa. La Secretaria de Hacienda cuenta con alguna documentación de los procedimientos de operación, sin embargo, esto es iniciativa de los funcionarios, y los procedimientos existentes, no están a disposición de todos los usuarios. Además no se adaptan al criterio de evaluación. En cuanto a lo que tiene que ver con la Gestión

de cambios, se determinó que estos no se controlan, debido a que no existen procedimientos establecidos para ello.

Respecto a la protección contra del código malicioso, se evidencio que los usuarios son conscientes de la necesidad de mejorar aspectos relacionados a la implementación de controles de detección y prevención, pues hasta el momento el único mecanismo existente es la utilización de antimalware para los equipos.

Con relación a las copias de seguridad se estableció que a pesar de que la Secretaria de Hacienda no disponga de políticas al respecto, existen procedimientos que no están documentados, y cuya finalidad es llevar a cabo los procesos de respaldo de la información de los diferentes sistemas de información. No obstante, lo anterior se debe tomar en cuenta que estas copias de seguridad no son realizadas de acuerdo a un cronograma, se hacen por iniciativa de los usuarios.

En la Secretaria de Hacienda no se realiza ningún control de los cambios ocurridos en los equipos de los funcionarios, además los registros de eventos no están protegidos contra el acceso no autorizado y las manipulaciones indebidas. De igual forma no se registran las actividades del administrador y del operador del sistema. En lo que tiene que ver con la sincronización de los relojes, se constató que todos los sistemas están sincronizados bajo un único formato de tiempo y zona horaria

El Control del software en sistemas operativos, no se lleva a cabo al interior de la Secretaria, tampoco existe una metodología de gestión de la vulnerabilidad técnica, que permita adoptar las medidas necesarias para afrontar el riesgo asociado.

En el proceso de operación y uso no existen procesos de control, no cuentan con documentación de usuario, manuales de operación y material de entrenamiento que faciliten la operación y el uso de los aplicativos, solo se tiene el material entregado por los proveedores, el cual en ocasiones no es completo, tampoco se cuenta con un protocolo de resguardo del material de entregado por los proveedores de cada aplicación, software, etc.

Dominio 13. Seguridad en las telecomunicaciones. No existe ningún tipo de restricción en cuanto a la seguridad de la información que es consultada, descargada o subida a internet; de igual forma, la Secretaria de Hacienda, no cuenta con una infraestructura de red con protocolos de seguridad implementados en la dependencia, además la clave de la red al ser utilizada por personal externo a la dependencia hace vulnerable el tráfico de red de la oficina. No obstante la dependencia para mitigar el riesgo ha segregado su red por grupos de servicios de información, usuarios y sistemas de información.

En lo que se refiere al intercambio de información con partes externas, no hay políticas y procedimientos de intercambio de información, tampoco existen acuerdos de intercambio de información y de software entre la organización y los terceros. Así mismo la dependencia no tiene controles ni parámetros establecidos para proteger la que es objeto de mensajería

electrónica, por ultimo no existen cláusulas de confidencialidad en los contratos de los empleados o de terceros.

Dominio 14. Adquisición, desarrollo y mantenimiento de sistemas de información. La Secretaria de Hacienda, en sus procesos misionales no contempla el desarrollo y mantenimiento de sistemas, por lo tanto este dominio no aplica. No obstante, es importante mencionar que al interior de la dependencia lo relacionado con la adquisición de hardware y software, se realiza mediante contratación directa con terceros.

Los cambios de tecnología se administran de manera informal, no existe un proceso estructurado y es propenso a errores, ya que no hay planeación al momento de realizarlos, por lo tanto no se evalúa el impacto que un cambio en la infraestructura puede costar para la dependencia y la incidencia que este puede tener en los objetivos del negocio en cuanto a las metas propuesta.

Por otro lado, no se supervisan las soluciones tecnológicas implantadas, a pesar de que se confirma que cumpla con las condiciones iniciales pactadas en la contratación, y que suplan las necesidades de los usuarios finales. No existe un área de sistemas, que apruebe o acredite las instalaciones realizadas y los cambios en la infraestructura, esta acreditación la realiza personal específico asignado por el responsable de la dependencia, que en la mayoría de los casos no tiene las competencias para llevar a cabo dichos procesos de adquisición de tecnología.

Por último, se determinó que hay ausencia completa de procesos formales de instalación, ya que no existe una metodología de prueba que garantice pruebas de aceptación confiables. A pesar de que se realiza un acta de aceptación por parte de los usuarios entrenados y quienes luego operaran con la solución tecnológica instalada, no se garantiza la reducción del impacto negativo luego de la liberación, en ocasiones los proyectos tras su liberación han fracasado por la ausencia de metodología de pruebas de aceptación

Dominio 15. Relaciones con proveedores. En lo relacionado con los contratos llevados a cabo con terceros, la Secretaria de Hacienda de Rio de Oro-Cesar, tiene documentados los contratos y las condiciones de los mismos están de acuerdo a los requerimientos del Estado Colombiano, sin embargo los contratos, no incluyen una cláusula de confidencialidad, que le permita a la dependencia establecer los límites en cuanto al uso de información que se maneja entre las partes. Además en la alcaldía de Rio de Oro el tema de la contratación la maneja una dependencia encargada de ese tema.

Dominio 16. Gestión de incidentes en la seguridad de la información. La Secretaria de Hacienda, no cuenta con protocolos definidos, ni documentados para realizar el reporte de los incidentes internos y externos de seguridad, que puedan poner en riesgo la estabilidad y/o continuidad de sus procesos misionales.

Dominio 17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio. La dependencia carece de un plan de continuidad del negocio y de un plan de contingencias, que le permita determinar y documentar todas las acciones, procesos y

procedimientos, necesarios, orientados a restablecer sus procesos misionales, ante la presencia de un ataque al sistema de información de la Secretaria de Hacienda.

Dominio 18. Cumplimiento. La dependencia no realiza auditorías con entidades externas, la dependencia es auditada por entes de control, sin embargo no hay documentación de dichas auditorias y no existe un plan estipulado para las mismas. Por otro lado los sistemas de información se revisan, pero el hecho de que no existan políticas establecidas, no permite que haya un referente para poder evaluar o determinar el cumplimiento, tampoco hay documentación de las revisiones o actualizaciones realizadas.

4.3 Efectuar un diagnóstico de los riesgos de la seguridad de la información en la Secretaria de Hacienda de Rio de Oro-Cesar.

El propósito al analizar y evaluar el riesgo para La Secretaria de Hacienda de Rio de Oro Cesar, es determinar los riesgos basados en la identificación de los activos, de sus amenazas y vulnerabilidades y posteriormente a este análisis establecer los requerimientos necesarios para el manejo del riesgo.

La finalidad es proveer a la dependencia de los elementos necesarios para gestionar de manera eficiente el riesgo y la mitigación del mismo; facilitándole el establecimiento de un Gobierno de Seguridad que permita establecer parámetros coherentes a las buenas prácticas de manejo de la información.

Para llevar a cabo este objetivo, se tuvo en cuenta a todos los activos físicos y lógicos que están bajo la teneduría de la Secretaria de Hacienda de Rio de Oro Cesar. La información para el análisis y evaluación del riesgo se obtuvo a través de la observación, entrevistas directas a los funcionarios, la aplicación de encuestas, cuestionarios y listas de chequeo, y la revisión documental existente en la dependencia.

Para la identificación y evaluación del riesgo de La Secretaria de Hacienda de Rio de Oro Cesar, se utilizó la metodología estipulada en la norma ISO 27005:2011. Y cuyos procesos son los siguientes:

- Análisis de riesgos.
- Identificación de Amenazas
- Identificación de las Vulnerabilidades.
- Identificación y Valoración del Riesgo.
- Análisis y Evaluación del Riesgo.
- Tratamiento del Riesgo.

4.3.1 Análisis de riesgos*:* Con el fin de diagnosticar el estado de la seguridad de la información del de la Secretaria de Hacienda de Rio de Oro-Cesar, se realizó inicialmente la identificación de los activos de información y posteriormente se les dio una valoración con respecto a la magnitud del daño que sufriría el activo, en caso de materialización de alguna amenaza.

Identificación de Activos: Al realizar la identificación de los aspectos críticos de la seguridad física y lógica de la Secretaria de Hacienda de Rio de Oro Cesar, se identificaron todos los recursos que están en riesgo de vulneración de la seguridad de la información la Tabla 2: Inventario de equipos secretaría de hacienda hace una Clasificación General de Activos de la dependencia.

Valoración de Activos: La valoración de los activos busca establecer la importancia de los mismos tomando como criterios su disponibilidad, integridad y confidencialidad. Con el fin de establecer la importancia que tiene cada activo de la información identificado en cuanto a los principios de la información, se tomó como referencia la siguiente tabla basada en la norma ISO27005.

Tabla 10.
Grado de impacto vs Valor Activo.

VALOR	GRADO DE IMPACTO	DESCRIPCION
1	B: Bajo	Importancia menor para el desarrollo de las actividades de la Empresa
2	M: Medio	Importante para el desarrollo de las actividades de la Empresa
3	A: Alto	Altanamente importante para el desarrollo de las actividades de la Empresa
4	MA: Muy Alto.	De vital importancia para el desarrollo de actividades de la Empresa

Fuente ISO27005

Los activos de información seleccionados respecto al grado de impacto, de la Clasificación General de Activos de la Secretaria de Hacienda de Rio de Oro-Cesar se detallan a continuación:

Tabla 11.
Valoración de activos.

ACTIVO	PUNTAJE
Servidor	4
Equipos de Computo	4
Software-Sistemas de Información	4
Personas	4
Documentación	2
UPS	2

Fuente. Autoras del proyecto

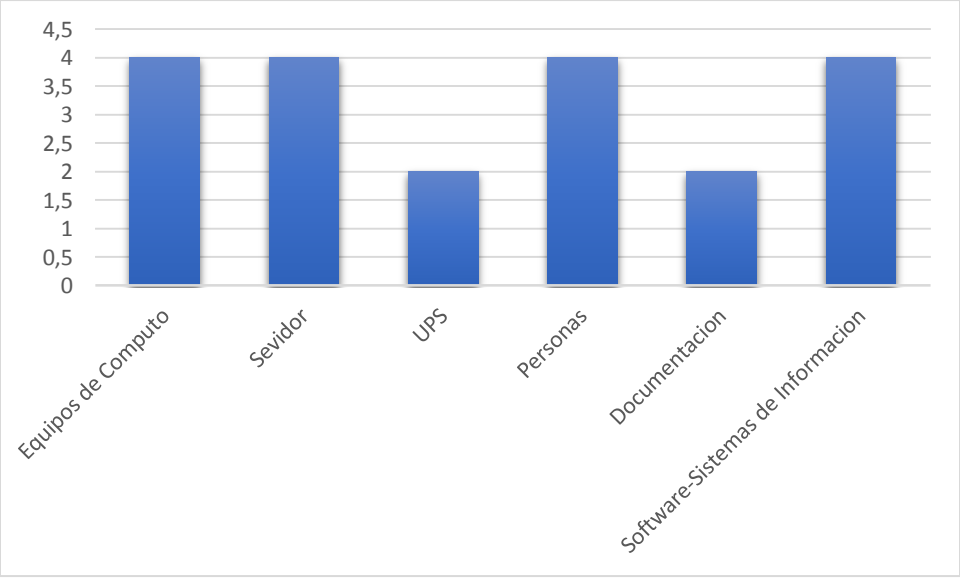

Figura 16. Grafica de valoración de activos
Fuente. Autoras del proyecto

De acuerdo a la gráfica anterior de puede terminar que los activos con mayor valoración son el Servidor, los equipos de cómputo, los Sistemas de Información y las personas o usuarios.

Una vez identificada la importancia de cada activo, se procedió a determinar los criterios de disponibilidad, confidencialidad e integridad de los activos de la Secretaria de Hacienda de Rio de Oro-Cesar.

Tabla 12.
Criterios de disponibilidad, confidencialidad e integridad de los activos de la Secretaria de Hacienda de Rio de Oro-Cesar

VALOR	PARAMETRO	DECRIPCION		
		DISPONIBILIDAD	**COFIDENCIALIDAD**	**INTEGRIDAD**
1	BAJO	La falta del activo no afecta los procesos o actividades soportadas.	El conocimiento de la información propia del proceso (archivos de configuración, datos de acceso, entre otros) no afecta la ejecución de las actividades soportadas por la dependencia.	La pérdida de veracidad y/o funcionalidad de los activos, impacta levemente a todas las actividades soportadas por la dependencia.
2	MEDIO	La falta del activo afecta medianamente los procesos o actividades soportadas.	El conocimiento de la información propia del proceso (archivos de configuración, datos de acceso, entre otros) afecta medianamente la ejecución de las actividades soportadas por la por la dependencia.	La pérdida de veracidad y/o funcionalidad de los activos, impacta medianamente a todas las actividades soportadas por la dependencia.
3	ALTO	La falta del activo afecta considerablemente los procesos o actividades soportadas.	El conocimiento de la información propia del proceso (archivos de configuración, datos de acceso, entre otros) afecta considerablemente la ejecución de las actividades soportadas por la por dependencia.	La pérdida de veracidad y/o funcionalidad de los activos, impacta considerablemente a todas las actividades soportadas por la dependencia.
4	MUY ALTO	La falta del activo es crítico para los procesos o actividades soportadas por la división de sistemas	El conocimiento de la información propia del proceso (archivos de configuración, datos de acceso, entre otros) es crítico para la ejecución de las actividades soportadas por la por la dependencia.	La pérdida de veracidad y/o funcionalidad de los activos, impacta críticamente a todas las actividades soportadas por la dependencia.

Fuente. Autoras del proyecto

Para calcular el nivel del riesgo se realiza la siguiente operación:

NI = (integridad) + (disponibilidad) + (confidencialidad)

El nivel de importancia (NI) del activo se debe tener encueta los niveles establecidos en los criterios

Tabla 13.
Valoración de activos de la Secretaria de Hacienda de Rio de Oro Cesar.

ACTIVO		DECRIPCION			TOTAL
		DISPONIBILIDAD	COFIDENCIALIDAD	INTEGRIDAD	
Hardware	5. Computadores de Escritorio	4	3	2	9
	UPS	2	2	2	6
	Servidor	4	4	4	12
Software	Visual TNS oficial, Neptuno Impuestos	4	4	4	12
Personas		4	4	4	12
Datos		4	4	4	12
Documentación		2	4	3	9

Fuente. Autoras del proyecto

Para cuantificar el valor de los activos, luego de haber tomado en cuenta los criterios de disponibilidad, confidencialidad e integridad y para mantener el rango de ponderación de los activos, se realizó una equivalencia, de donde se obtuvo lo siguiente:

Tabla 14.
Equivalencia del valor de los activos

VALOR	PARAMETRO	DESCRIPCION
1-3	No es importante	El activo es de muy baja importancia para los procesos misionales de la dependencia.
4-6	Poco importante	El activo tiene poca importancia para los procesos misionales de la dependencia.
7-9	Importante	El activo es importante para los procesos misionales de la dependencia.
10-12	Muy importante	El activo es de vital importancia para los procesos de la dependencia.

Fuente. Autoras del proyecto

4.3.2 Identificación de amenazas y controles. Tomando como referencia la Norma (ISO/IEC 27005), se realizó la identificación de las amenazas que reposan sobre cada uno de los activos de información anteriormente identificados para así continuar con el proceso de gestión del riesgo. De acuerdo a la Norma, las amenazas pueden ser:

- Deliberadas (D) Se utiliza para todas las acciones deliberadas que tienen como objetivo los activos de la información.
- Accidentales (A) Se utiliza para las acciones humanas que pueden dañar accidentalmente los activos de la información.
- Ambientales (E): Se utiliza para todos los incidentes que no se basa en las acciones humanas.

Tabla 15.
Identificación de Amenazas y Controles

TIPO	AMENAZA	ORIGEN	CONTROLES	DESCRIPCION
Daño Físico	Fuego	A.D.E	✓ No existen controles.	✓ Factor humano, manipulación de redes eléctricas, Sabotaje.
	Agua	A.D.E	✓ No existen controles.	✓ Condiciones ambientales. Redes de tuberías en mal estado.
	Destrucción de equipos o medios.	A.D.	✓ Copias de seguridad. ✓ Solicitud de contraseña de acceso.	✓ Manipulación de personal no autorizado o no capacitado.
	Temperatura	E.	✓ No existen controles.	✓ Condiciones ambientales.
Eventos Naturales	Fenómenos climáticos	E.	✓ No existen controles.	✓ Fenómenos de la naturaleza, inundaciones, terremotos, temblores.
	Fenómenos sísmicos	E.	✓ No existen controles.	
Perdida de los servicios esenciales.	Fallas en el suministro de energía eléctrica.	A.D.E.	✓ UPS	✓ Falta de mantenimiento, redes eléctricas en mal estado.
	Ausencia de Sistema de ventilación.	D.	✓ No existen controles.	
Compromiso de la información	Virus	D.	✓ Antivirus ✓ Cortafuegos.	✓ Desarrolladores Externos ✓ Acceso y manejo de la red. Espionaje. ✓ Empleados insatisfechos.
	Robo de equipos y documentos.	D.	✓ Inventario de equipos.	
	Recuperación de medio reciclados y/o desechados	D.	✓ No existen controles.	
	Manipulación de hardware	D.	✓ No existen controles.	
	Manipulación de	D.	✓ Contraseñas de	

	software			acceso.		
Fallas técnicas	Falla del equipo	A	✓	Mantenimiento Correctivo.	✓	Falta de mantenimiento, redes eléctricas en mal estado.
	Mal funcionamiento software.	E.A	✓	Licencias legales.		
Acciones no autorizadas	Corrupción de datos.	D.	✓	Copias de seguridad.	✓	Espionaje industrial intruso, empleado insatisfecho.
			✓	Solicitud de contraseña de acceso.		
	Uso no autorizado del equipos	D.	✓	Contraseñas de acceso.		
Compromiso de las funciones	Uso inadecuado de información.	A.	✓	Personal con experiencia en el cargo.	✓	Empleados insatisfechos.
	Disponibilidad del personal	A.D.E.	✓	Rotación de puestos.		

Fuente Autoras del proyecto.

4.3.3 Identificación de vulnerabilidades e impacto. Mediante la aplicación de listas de chequeo, encuestas, entrevistas al personal involucrado en el uso y manejo de la información de la Secretaria de Hacienda y visitas a la instalaciones de la dependencia; se identificaron las vulnerabilidades que pueden materializarse a través de una amenaza en los procesos misionales que presta la dependencia.

Tabla 16.
Identificación de Vulnerabilidades e Impacto

TIPO	AMENAZA	ORIGEN	VULENERABILIDAD	IMPACTO
Daño Físico	Fuego	A.D.E	✓ No hay sistema de alarma contra incendio. ✓ Existencia de materiales inflamables.	✓ Perdida de información. ✓ Daño en los equipos Recursos humano lastimado.
	Agua	A.D.E	✓ Filtraciones de agua por mal estado de tuberías de aguas limpias.	✓ Perdida de información. ✓ Daño en los equipos.
	Destrucción de equipos o medios.	A.D.	✓ No existe control de acceso a la dependencia.	✓ Pérdida parcial de información. ✓ Disponibilidad de los equipos.

	Temperatura	E.	✓ No hay sistema de ventilación. (Ausencia de aire acondicionado o de ventiladores)	✓ Perdida de información. ✓ Daño en los equipos.
Eventos Naturales	Fenómenos climáticos	E.	✓ Filtraciones por lluvia.	✓ Daño de equipos. ✓ Pérdida parcial de información. ✓ Daño de infraestructura física.
	Fenómenos sísmicos	E.	✓ Falta de señalización de evacuación en caso de emergencia. ✓ Falta de planes de contingencia para desastres naturales y humanos.	✓ Accidentes del Recurso Humano. ✓ Muerte del Recurso Humano. ✓ Pérdida total o parcial de información. ✓ Daño de equipos.
Perdida de los servicios esenciales.	Fallas en el suministro de energía eléctrica.	A.D.E.	✓ No existe planta eléctrica de respaldo. ✓ Sistema eléctrico en condiciones peligrosas.	✓ Disponibilidad de la información comprometida. ✓ Daños en los equipos por cambio inesperado de voltaje.
	Ausencia de Sistema de ventilación.	D.	✓ No existen ventiladores, ni sistema de aire acondicionado.	✓ Daño de equipos. ✓ Pérdida parcial de información.
Compromiso de la información.	Virus	D.	✓ Falta de actualización software. ✓ Licencia ilegales. Falta de licencias. Daño del código fuente de la aplicación.	✓ Perdida de información parcial o total. ✓ Daño parcial del software y del hardware.
	Robo de equipos y documentos.	D.	✓ Falta de controles de acceso al lugar donde están los equipos. ✓ Almacenamiento expuesto a personal ajeno a la dependencia.	✓ Perdida de la disponibilidad, confidencialidad e integralidad de la información. ✓ Perdida del software y del hardware.
	Recuperación de medio reciclados y/o desechados	D.	✓ Ausencias de políticas respecto a la destrucción de medios reciclados o desechados.	✓ Perdida de la confidencialidad de la información.
	Manipulación de hardware	D.	✓ Protección física de equipos inadecuada. ✓ Control de acceso inadecuado. ✓ Falta de un sistema para detección y monitoreo de intrusos dentro de la red de información.	✓ Perdida de la confidencialidad de la información. ✓ Daño parcial o total en equipos.
	Manipulación de software	D.	✓ Daño del código fuente de la aplicación. ✓ Ataque informático. ✓ Ausencia de control en la autenticación de usuarios. ✓ Cuenta de usuarios con claves inseguras	✓ Pérdida parcial o total de la información.
Fallas técnicas	Falla de equipos.	A	✓ Falta de mantenimiento preventivo. ✓ Falta de procedimientos para llevar a cabo la resolución de fallas.	✓ Perdida de información. ✓ Daño total o parcial de equipos.

	Mal funcionamiento software.	E.A	✓ Falta de actualización en las licencias. ✓ Daño del código fuente de la aplicación. ✓ Hardware no compatible con la versión de la aplicación.	✓ Disponibilidad de la información comprometida.
Acciones no autorizadas	Corrupción de datos.	D.	✓ Almacenamiento expuesto a personal ajeno a la dependencia. ✓ Ataques informáticos.	✓ Perdida de información. ✓ Modificación de la información ✓ Daño de equipos.
	Uso no autorizado del equipos	D.	✓ Ataques informáticos. Ausencia de control en la autenticación de usuarios. ✓ Falta de un sistema para detección y monitoreo de intrusos dentro de la red de información.	✓ Perdida de información parcial o total. ✓ Modificación de la información parcial o total. ✓ Daño a equipos.
Compromiso de las funciones	Uso inadecuado de información.	A.	✓ No existen procedimientos documentados en caso de que fallen los equipos y el software ✓ Almacenamiento de información sin acceso restringido.	✓ Daño de equipos por manipulación irresponsable. ✓ Perdida de información parcial o total.
	Disponibilidad del personal	A.D.E.	✓ Personal insatisfecho. Incapacidad, enfermedad del personal.	✓ Disponibilidad, confidencialidad e integralidad de la información comprometida. ✓ Imagen negativa de la dependencia.

Fuente. Autoras del proyecto

4.3.4 Identificación y valoración del riesgo. Para llevar a cabo la caracterización de la magnitud del riesgo que afecta a cada uno de los activos previamente identificados en la Secretaria de Hacienda de Rio de Oro-Cesar, inicialmente se contempla el impacto que podría presentarse en caso de que uno de estos se vieran afectados por factores internos o externos del entorno. Para llevar a cabo este proceso se utilizó un enfoque cualitativo y cuantitativo; usando una matriz que se forma de combinar la probabilidad de que ocurra una amenaza con la magnitud del daño de dicha amenaza, asignándole su valor correspondiente. En las siguientes tablas se establecen la Probabilidad de ocurrencia de una amenaza y la determinación del impacto.

Tabla 17.
Determinación de la probabilidad de ocurrencia de una amenaza.

ESTADO	DESCRIPCION
ALTA	La fuente de la amenaza está altamente motivada y capaz. controles para prevenir las vulnerabilidad son ineficaces
MEDIA	La fuente de la amenaza está motivada, pero hay controles que dificultan el ejercicio exitoso de la vulnerabilidad.
BAJA	La fuente de amenaza carece de motivación o capacidad, o los controles están previenen, o por lo menos obstaculizar significativamente, la vulnerabilidad de ser ejercida.

Fuente. Autores del proyecto

Tabla 18.
Determinación del impacto

ESTADO	DESCRIPCION
ALTA	(1) Puede resultar en la pérdida altamente costosa de Activos o recursos tangibles importantes; (2) puede violar, dañar o Impedir la misión, reputación o interés de una organización; (3) puede resultar en la muerte humana o lesiones graves.
MEDIA	(1) Puede resultar en la costosa pérdida de Bienes o recursos; (2) puede violar, dañar o impedir la Misión, reputación o interés (3) puede resultar en lesiones humanas
BAJA	(1) Puede resultar en la pérdida de algo tangible Activos o recursos (2) puede afectar no notablemente Misión, reputación o interés.

Fuente. Autores del proyecto

Para determinar el riesgo para cada uno de los activos identificados como importantes para llevar a cabo el cumplimiento de los procesos misionales de la Secretaria de Hacienda de Rio de Oro-Cesar, se utilizó una matriz 3x3. Para el análisis del riesgo se aplicó una escala de valor que permitió valorar los activos, se pondero su impacto con relación a su confidencialidad, integridad y disponibilidad. Se estableció utilizar la escala cualitativa de: Alto, Mediano y Bajo.

Tabla 19.
Determinación del riesgo.

Probabilidad de amenaza		Impacto		
	%	Bajo	Medio	Alto
		10	50	100
Alto	1	Bajo	Medio	Alto
Medio	0,5	Bajo	Medio	Medio
Bajo	0,1	Bajo	Bajo	Bajo

Fuente. Autores del proyecto

Escala: Alta (>50 - 100); Medio (>10 - 50); Bajo (1 - 10)

Riesgo = Probabilidad de ocurrencia de la Amenaza x Magnitud del impacto

Tabla 20.
Valorización del riesgo Sistemas de Información.

TIPO	AMENAZA	ORIGEN	VULENERABILIDAD	DESCRIPCION DE IMPACTO	CONTROL	PA	I	R
Daño Físico	Fuego.	A.D.E	✓ Sistema de cableado en mal estado. ✓ No hay sistema de alarma contra incendio	✓ Perdida de información ✓ Daño en los equipos Recursos humano lastimado	✓ No existen controles.	0,5	100	50
	Destrucción de equipos o medios.	A.D.	✓ No existe control de acceso a la dependencia.	✓ Pérdida parcial de información. ✓ Disponibilidad de los equipos.	✓ No existen controles.	0,5	50	25
	Agua.	A.D.E	✓ Filtraciones de agua por mal estado de tuberías de aguas limpias.	✓ Perdida de información. ✓ Daño en los equipos	✓ No existen controles.	0,5	100	50
Eventos Naturales	Fenómenos climáticos.	E.	✓ Filtraciones por lluvia.	✓ Daño de equipos. ✓ Pérdida parcial de información. ✓ Daño de infraestructura física.	✓ No existen controles.	0,5	100	50
Perdida de los servicios esenciales.	Fallas en el suministro de energía eléctrica.	A.D.E.	✓ Sistema eléctrico en condiciones peligrosas.	✓ Disponibilidad de la información comprometida. ✓ Daños en los equipos por cambio inesperado de voltaje.	✓ UPS	1	50	50
	Ausencia de Sistema de ventilación.	D.	✓ No existen ventiladores, ni sistema de aire acondicionado.	✓ Daño de equipos. ✓ Pérdida parcial de información.	✓ No existen controles.	0,5	50	25
Compromiso de la información	Virus	D.	✓ Falta de actualización software.	✓ Perdida de información parcial o total. ✓ Daño parcial del software y del hardware.	✓ Antivirus ✓ Cortafuegos.	1	50	50

	Robo de equipos y documentos.	D.	✓ Falta de controles de acceso al lugar donde están los equipos.	✓ Perdida de la disponibilidad, confidencialidad e integralidad de la información. ✓ Pérdida del software y del hardware.	✓ Inventario de equipos.	0,5	50	25
	Recuperación de medio reciclados y/o desechados	D.	✓ Ausencias de políticas respecto a la destrucción de medios reciclados o desechados.	✓ Perdida de la confidencialidad de la información.	✓ No existen controles.	1	100	100
	Manipulación de hardware	D.	✓ Protección física de equipos inadecuada y control de acceso inadecuado.	✓ Perdida de la confidencialidad de la información. ✓ Daño parcial o total en equipos.	✓ No existen controles.	0,5	100	50
	Manipulación de software	D.	✓ Falta de un sistema para detección y monitoreo de intrusos dentro de la red de información.	✓ Pérdida parcial o total de la información.	✓ Contraseñas de acceso.	0,5	100	50
Fallas técnicas	Falla de equipos.	A	✓ Falta de mantenimiento preventivo. ✓ Falta de procedimientos para llevar a cabo la resolución de fallas.	✓ Perdida de información. ✓ Daño total o parcial de equipos.	✓ Mantenimiento Correctivo.	0,5	50	25
	Mal funcionamiento software.	E.A	✓ Falta de actualización en las licencias.	✓ Disponibilidad de la información comprometida.	✓ Licencias legales.	0,5	50	25
Acciones no autorizadas	Uso no autorizado del equipos	D.	✓ Ausencia de control en la autenticación de usuarios. ✓ Falta de un sistema para detección y monitoreo de intrusos dentro de la red de información.	✓ Perdida de información parcial o total. ✓ Modificación de la información parcial o total. Daño a equipos.	✓ Contraseñas de acceso.	0,5	100	50
Compromiso de las funciones	Uso inadecuado de información.	A.	✓ No existen procedimientos documentados en caso de que fallen los equipos y el software. ✓ Almacenamiento de información sin acceso restringido.	✓ Daño de equipos por manipulación irresponsable. ✓ Perdida de información parcial o total.	✓ Personal con experiencia en el cargo.	0,5	50	25

	Disponibilidad del personal	A.D.E.	✓ Incapacidad, enfermedad del personal.	✓ Disponibilidad, confidencialidad e integralidad de la información comprometida. ✓ Imagen negativa de la dependencia.	✓ Rotación de puestos.	0,5	50	25

Tabla 21.
Valoración del riesgo servidor y computadores de escritorio.

TIPO	AMENAZA	ORIGEN	VULENERABILIDAD	IMPACTO	CONTROL	PA	I	R
Daño Físico	Fuego	A.D.E	✓ Sistema de cableado en mal estado. ✓ No hay sistema de alarma contra incendio	✓ Perdida de información. ✓ Daño en los equipos. ✓ Recursos humano lastimado	✓ No existen controles.	1	100	100
	Agua	A.D.E	✓ Filtraciones de agua por mal estado de tuberías de aguas limpias.	✓ Perdida de información Daño en los equipos	✓ No existen controles.	0,5	50	25
	Destrucción de equipos o medios.	A.D.	✓ No existe control de acceso a la dependencia.	✓ Pérdida parcial de información.Disponibilidad de los equipos.	✓ Copias de seguridad. ✓ Autenticador de identidad. ✓ Solicitud de contraseña de acceso.	0,5	50	25
Eventos Naturales	Fenómenos climáticos	E.	✓ Filtraciones por lluvia.	✓ Daño de equipos. ✓ Pérdida parcial de información. ✓ Daño de infraestructura física.	✓ No existen controles.	0,5	100	50
	Fenómenos sísmicos	E.	✓ Falta de señalización de evacuación en caso de emergencia. Falta de contingencia para desastres naturales y humanos.	✓ Accidentes del Recurso Humano. ✓ Perdida del Recurso Humano. Muerte. ✓ Pérdida total o parcial de información. ✓ Daño de equipos.	✓ No existen controles.	1	100	100
Perdida de los servicios esenciales.	Fallas en el suministro de energía eléctrica.	A.D.E.	✓ No existe planta eléctrica de respaldo. ✓ Sistema eléctrico en condiciones peligrosas.	✓ Disponibilidad de la información comprometida ✓ Daños en los equipos por cambio inesperado de voltaje.	✓ UPS	0,5	50	25

	Ausencia de Sistema de ventilación.	D.	✓ No existen ventiladores, ni sistema de aire acondicionado.	✓ Daño de equipos. Pérdida parcial de información.	✓ No existen controles.	0,5	50	25
Compromiso de la información	Virus.	D.	✓ Falta de actualización software. ✓ Licencia ilegales. ✓ Falta de licencias. ✓ Daño del código fuente de la aplicación.	✓ Perdida de información parcial o total. ✓ Daño parcial del software y del hardware.	✓ Antivirus Cortafuegos.	0,5	100	50
	Robo de equipos y documentos.	D.	✓ Falta de controles de acceso al lugar donde están los equipos. ✓ Almacenamiento expuesto a personal ajeno a la dependencia.	✓ Perdida de la disponibilidad, confidencialidad e integralidad de la información. ✓ Perdida del software y del hardware.	✓ Inventario de equipos.	1	50	50
	Recuperación de medio reciclado y/o desechado.	D.	✓ Ausencias de políticas respecto a la destrucción de medios reciclados o desechados.	✓ Perdida de la confidencialidad de la información.	✓ No existen controles.	0,5	50	25
	Manipulación de hardware.	D.	✓ Protección física de equipos inadecuada. Control de acceso inadecuado. Falta de un sistema para detección y monitoreo de intrusos dentro de la red de información	✓ Perdida de la confidencialidad de la información. Daño parcial o total en equipos.	✓ No existen controles.	1	50	50
	Manipulación de software.	D.	✓ Daño del código fuente de la aplicación. Ataque informático.Ausencia de control en la autenticación de usuarios.Cuenta de usuarios con claves inseguras	✓ Pérdida parcial o total de la información.	✓ Contraseñas de acceso.	1	50	50
Fallas técnicas	Falla de equipos.	A	✓ Falta de mantenimiento preventivo. Falta de procedimientos para llevar a cabo la resolución de fallas.	✓ Perdida de información. Daño total o parcial de equipos.	✓ Mantenimiento Correctivo.	0,5	50	25
Acciones no autorizadas	Uso no autorizado del equipos	D.	✓ Falta de un sistema para detección y monitoreo de intrusos dentro de la red de información.	✓ Perdida de información parcial o total. ✓ Modificación de la información parcial o total. ✓ Daño a equipos.	✓ Contraseñas de acceso.	0,5	50	25

Compromiso de las funciones	Uso inadecuado de información.	A.	✓ Almacenamiento de información sin acceso restringido.	✓ Daño de equipos por manipulación irresponsable. ✓ Perdida de información parcial o total.	✓ Personal con experiencia en el cargo.	0,5	50	25
	Disponibilidad del personal	A.D.E.	✓ Personal insatisfecho.	✓ Disponibilidad, confidencialidad e integralidad de la información comprometida ✓ Imagen negativa de la dependencia.	✓ Rotación de puestos.	0,5	50	25

Fuente. Autores del proyecto

Tabla 22. *Valoración del riesgo en el personal involucrado.*

TIPO	AMENAZA	ORIGEN	VULENERABILIDAD	IMPACTO	CONTROL	PA	I	R
Daño Físico	Fuego	A.D.E	✓ Sistema de cableado en mal estado. ✓ No hay sistema de alarma contra incendio.	✓ Perdida de información Daño en los equipos Recursos humano lastimado	✓ No existen controles.	1	100	100
Eventos Naturales	Fenómenos sísmicos	E.	✓ Falta de planes contingencia para desastres naturales y humanos.	✓ Accidentes del Recurso Humano. ✓ Perdida del Recursos Humano. Muerte ✓ Pérdida total o parcial de información. ✓ Daño de equipos.	✓ No existen controles.	1	100	100
Perdida de los servicios esenciales.	Fallas en el suministro de energía eléctrica.	A.D.E.	✓ Sistema eléctrico en condiciones peligrosas.	✓ Disponibilidad de la información comprometida. ✓ Daños en los equipos por cambio inesperado de voltaje. ✓ Accidentes de Recursos Humano.	✓ UPS	0,5	100	50
	Ausencia de Sistema de ventilación.	D.	✓ No existen ventiladores, ni sistema de aire acondicionado.	✓ Daño de equipos. ✓ Pérdida parcial de información.	✓ No existen controles.	0,5	50	25
Compromiso de la información	Recuperación de medios reciclados y/o desechados.	D.	✓ Ausencias de políticas respecto a la destrucción de medios reciclados o desechados.	✓ Perdida de la confidencialidad de la información.	✓ No existen controles.	0,5	50	25
	Manipulación de hardware.	D.	✓ Protección física de equipos inadecuada.	✓ Perdida de la confidencialidad de la información ✓ Daño parcial o total en equipos.	✓ No existen controles.	0,5	50	25

	Manipulación de software.	D.	✓ Cuenta de usuarios con claves inseguras	✓ Pérdida parcial o total de la información.	✓ Contraseñas de acceso.	0,5	50	25
Fallas técnicas	Falla de equipos.	A	✓ Falta de mantenimiento preventivo. Falta de procedimientos para llevar a cabo la resolución de fallas.	✓ Perdida de información. Daño total o parcial de equipos.	✓ Mantenimiento Correctivo.	0,5	50	25
Acciones no autorizadas	Uso no autorizado del equipos	D.	✓ Falta de un sistema para detección y monitoreo de intrusos dentro de la red de información.	✓ Perdida de información parcial o total. ✓ Modificación de la información parcial o total. ✓ Daño a equipos.	✓ Contraseñas de acceso.	0,5	50	25
Compromiso de las funciones	Uso inadecuado de información.	A.	✓ Almacenamiento de información sin acceso restringido.	✓ Daño de equipos por manipulación irresponsable. ✓ Perdida de información parcial o total.	✓ Personal con experiencia en el cargo.	0,5	50	25
	Incumplimiento en la disponibilidad del personal	A.D.E.	✓ Personal insatisfecho.	✓ Disponibilidad, confidencialidad e integralidad de la información comprometida. ✓ Imagen negativa de la dependencia.	✓ No existen controles.	1	100	100

Fuente. Autoras del proyecto

4.3.5 Análisis y evaluación del riesgo. Con el fin de definir las acciones a emprender para tratar el riesgo identificado en la Secretaria de Hacienda de rio de Oro-Cesar, se realiza el proceso identificación de controles para cada uno de los riesgos previamente evaluados y que se ponderan de acuerdo a la siguiente tabla:

Tabla 23.
Descripción del Riesgo

ALTO	**Necesidad de medidas correctivas. Un sistema existente puede continuar funcionando, pero debe establecerse un plan de acción correctiva tan pronto como sea posible.**
MEDIO	Las acciones correctivas se deben desarrollar un plan para incorporar estas acciones Dentro de un plazo razonable.
BAJO	Determinar si aún se requieren medidas correctivas o decidir si se acepta el riesgo.

Fuente. Autoras del proyecto

Al realizar el análisis y la evaluación de riesgo para la Secretaria de Hacienda de Rio de Oro-Cesar, se han determinado las diferentes amenazas asociadas a sus fuentes y las vulnerabilidades que pueden activar dichas amenazas y afectar seriamente los activos físicos y lógicos de la dependencia

En cuento se refiere a la valoración de riesgos en los Sistemas de Información, se determinó que el riesgo más alto está relacionado con la amenaza de Recuperación de medios reciclados y/o desechados, la dependencia no cuenta con políticas y/o procedimientos que le permitan al personal hacer el uso correcto de los medios reciclados, lo anterior compromete la confidencialidad de la información por cuanto, la dependencia no cuenta con ningún control para mitigar el riesgo.

Por otro lado, se evidencio que en lo concerniente a la valoración del riesgo del servidor y los computadores de escritorio, los riegos más altos se encuentran en las amenazas por fuego, debido a que la dependencia tiene un sistema de cableado eléctrico deteriorado, además no cuenta con un sistema contra incendios. De igual forma otra amenaza relevante es la relacionada con los fenómenos sísmicos, ya que la Secretaria de Hacienda actualmente no cuenta con un adecuado modelo de Seguridad y Salud Laboral, no existe señalización para la evacuación, no hay documentados planes de contingencia y no existe capacitación para el personal en caso que se hagan efectivas dichas amenazas. De llegarse a presentar estos eventos habría pérdida parcial o total de información, daño parcial o total de equipos y accidentes graves o muerte de los empleados.

En lo relacionado con el personal o usuarios involucrados en el manejo y uso de la información, se pudo determinar que los riesgos más altos están relacionados con el fuego, fenómenos sísmicos y el incumplimiento en la disponibilidad del personal, Este último es de resaltar debido al impacto generado si se llegara a potencializar la vulnerabilidad, puesto que compromete la disponibilidad, confidencialidad e integralidad de la información y por lo tanto la imagen de la dependencia. Actualmente la Secretaria de Hacienda carece de una cláusula de confidencialidad en sus contratos con empleados y terceros.

Tomando en cuenta todo lo anterior, se concluye que la probabilidad de que ocurra el evento de amenaza tiene un porcentaje de valoración MEDIA, que corresponde a 86 % y una probabilidad de amenaza media del 79%. De lo anterior se puede analizar que el impacto de la probabilidad de amenaza de ponderación media tiene un alto impacto en los activos físicos y lógicos de la dependencia. Y que las principales amenazas asociadas al impacto, tienen una probabilidad del 81% de afectar al inventario físico y lógico de los activos de la dependencia.

4.3.6 Tratamiento del riesgo. Del análisis y la evaluación de riesgos realizado en la Secretaria de Hacienda de Rio de Oro-Cesar, se describen los riesgos que fueron detectados y se indican los controles que deben tenerse en cuenta para lograr la minimización del mismo.

Riesgo - probabilidad de incendio: El sistema de cableado eléctrico de la Secretaria de Hacienda de Rio de Oro-Cesar, se encuentra en mal estado, hay algunos tramos con cables expuestos a manipulación, además hay varios interruptores que no cuentan con cajas de protección. Lo anterior pone en riesgo no solo la integridad del sistema de información, sí no que expone al recurso humano a accidentes o incluso la muerte.

Controles:

- Reparar el sistema de cableado eléctrico.
- Utilizar normas de cableado estructurado para la organización de los equipos de cómputo, redes de datos y equipos de red.
- Gestionar la instalación de equipos básicos de sistema contra incendios.
- Capacitar al personal en el manejo de extintores.

Riesgo – Fallas del fluido eléctrico: La Secretaria de Hacienda de Rio de Oro-Cesar, no cuenta con una planta eléctrica, que le permita solventar de manera inmediata la falta de energía, en dado caso de que ocurra un corte prolongado. Solo tiene el tiempo de espera que le brindan las UPS conectadas a sus equipos de cómputo. Lo anterior aunado a las deficientes instalaciones eléctricas, pone en riesgo la integridad de la información y la falta de continuidad en procesamiento de la información y la entrega de resultados, por altos tiempo en el restablecimiento y/o continuidad de los servicios.

Controles:

- Gestionar la adquisición de una planta eléctrica.
- Se recomienda gestionar la creación un plan de continuidad para todos los procedimientos y/o actividades que soporta la dependencia.

Riesgo- Daño de los equipos de procesamiento: La dependencia no cuenta con políticas de mantenimiento preventivo de equipos, además está expuesta a fallos de energía lo que puede

provocar en los equipos averías por cambio repentino de voltaje. La ubicación de los equipos especialmente del servidor no es la adecuada.

Lo anterior puede generar interrupción del procesamiento de información y pérdida parcial de registros de información.

Controles:

- Crear políticas y procedimientos para llevar a cabo la solución a fallas técnicas de los equipos.
- Establecer un plan de mantenimiento preventivo y correctivo.
- Realizar reubicación de equipos y servidor.

Riego- Corrupción de datos y programas por virus: Aunque la dependencia cuenta con antivirus y cortafuegos, los mismos son genéricos y no cuentan con las licencias respectivas. Lo anterior pondría en riesgo la integridad del software, la integridad de la información y de igual forma la paralización temporal de los procesos; en caso que se presentara un evento de esta magnitud.

Controles:

- Adquirir software legal.
- Mantener actualizadas las licencias.
- Realizar copias de seguridad con frecuencia.

- Realizar la configuración de un sistema de prevención de intrusos.

Riesgo- Pérdida, alteración o manipulación de la información - Recuperación de medios reciclados y/o desechados: Aunque la dependencia cuenta con contraseñas para el uso de los sistemas y equipos, hay una inadecuada asignación de perfiles y no existe autenticación de usuarios. Además las instalaciones no cuentan con control de acceso a visitantes. En cuanto se refiere a recuperación de medios reciclados, no existen documentados procedimientos. Lo anterior puede provocar modificación o fraude en la información contenida en las base de datos, expone a la información a la perdida de la confidencialidad y por ende a la pérdida de confianza y credibilidad en los procesos de la dependencia.

Controles:

- Crear políticas y procedimientos de cambio de contraseñas y/o usuarios.
- Revisión y actualización de los usuarios del sistema, con el fin de eliminar usuarios no autorizados.
- Crear procedimientos y políticas respecto a la recuperación de medios reciclados y/o desechados.

Riesgo- Acceso no autorizado a las instalaciones y a los equipos: En la investigación realizada se determinó que los controles de acceso a las instalaciones de la Secretaria de Hacienda son débiles, no tiene una puerta en la entrada que restrinja el fluido de visitantes, además no hay personal asignado para llevar un control de las personas autorizadas y el nivel de seguridad para acceder a las aplicaciones no es el adecuado. Lo anterior puede generar en caso que se presente un robo de equipos o documentos, la pérdida o alteración de la información y por ende la pérdida de confianza y credibilidad en los procesos.

Controles:

- Asignación de un responsable para controlar el ingreso al personal autorizado.
- Gestionar la instalación de una puerta en la entrada principal.
- Gestionar la instalación de cámaras de Circuito Cerrado de TV.

Riesgo- Daño total o parcial de las instalaciones y personal: Aunque un desastre natural no se puede evitar, si es posible minimizar las consecuencias del mismo. En cuanto a la Secretaria de Hacienda de Rio de Oro-Cesar, en la actualidad carece de plan de contingencia para el caso de un desastre, además no tiene implementadas las medidas de seguridad para la protección del personal, no existen señales de evacuación y el personal no cuenta con la capacitación para atender y reaccionar ante este tipo de eventos. Las consecuencias dependiendo de la magnitud del desastre serian incalculables para la dependencia, no solo por la pérdida total o parcial de información, la perdida de continuidad de los procesos, sino porque además de los daños económicos, están expuestas las personas que laboran en la Secretaria.

Controles:

- Gestionar un plan de atención a desastres.
- Realizar la señalización respectiva de las áreas críticas y la señalización de las rutas de evacuación.
- Realizar simulacros para capacitar al personal ante este tipo de eventos.
- Mantener copias de seguridad de la información en un lugar seguro fuera de la dependencia.

Riesgo- Divulgación no autorizado de información: El manejo que se le da al interior de la dependencia a la contratación de empleados y terceros, no es el adecuado en cuanto a la seguridad de la información que manejan las partes. Un empleado insatisfecho, puede emprender acciones encaminadas a violar los principios de confidencialidad de la información. Lo anterior puede acarrear una pérdida de confianza de la Secretaria de Hacienda.

Controles:

- Crear Políticas de Seguridad de la información y socializarla con los empleados.
- Incluir cláusulas de confidencialidad en los contratos, con consecuencias disciplinarias y penales para los involucrados.

Riesgo- Falta de políticas y procedimientos de Seguridad de la Información.

Actualmente la Secretaria de Hacienda no realiza un tratamiento adecuado de los componentes del sistema de información. Lo anterior obedece a la escasa gestión que se ha realizado en la dependencia en cuanto a seguridad de la información se refiere.

Controles:

- Designar a un responsable de la seguridad de la información.
- Crear lineamientos de Seguridad de la información, capacitar al personal y retroalimentarlo constantemente.

4.4 Documentar las buenas prácticas de Seguridad de la Información de la Secretaria de Hacienda de Rio de Oro-Cesar tomando como base la norma ISO 27001:2013.

Después de haber realizado un diagnóstico con relación a la Gestión de la Seguridad de la Información en la Secretaria de Hacienda de Rio de Oro-Cesar, haber determinado el nivel de madurez de la dependencia respecto a la norma ISO 27001:2013 y haber efectuado el diagnóstico de los riesgos de la seguridad de la información se logró conocer a fondo el estado actual de la dependencia en cuanto a la gestión de la seguridad de la información y con base en esto se pudo establecer una serie de buenas prácticas de Seguridad de la Información con el objetivo de preservar la integridad, la confidencialidad y disponibilidad de la misma a fin de que los procesos misionales de la dependencia no resulten afectados.

Se determinó la siguiente política de Seguridad de la Información teniendo en cuenta los criterios establecidos en la ISO 27001:2013:

4.4.1 Política de seguridad de la información

Introducción. La Secretaría de Hacienda del Municipio de Río de Oro, Cesar, consciente de que la información es el activo más importante de cualquier organización y sabiendo de los riesgos a los que se ve sometida la información propende por una política que salvaguarde este activo. Por tal razón ha definido la Política de Seguridad de la Información, teniendo en cuenta los lineamientos de la norma ISO 27001:2013.

Esta política contribuye al cumplimiento de los objetivos institucionales puesto que es un elemento fundamental para el mejoramiento continuo y la alineación a los estándares internacionales.

Misión Secretaría de Hacienda del Municipio de Río de Oro, Cesar. 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.

Objetivo. Propender por la protección de la información de la Secretaría de Hacienda, de tal modo que se garantice, como mínimo, la confidencialidad, disponibilidad e integridad de este activo.

Alcance. Este documento proporciona el conjunto de políticas para proteger los activos de información que están a cargo de la Secretaría de Hacienda y servirá como guía para la implementación de la seguridad de la información, este documento es aplicable a todos los servidores públicos y contratistas de la de la dependencia y otras personas vinculadas que utilicen los recursos informáticos y físicos de ella.

Se tienen en cuenta los aspectos relacionados con: equipos de cómputo, mecanismos de seguridad informática y demás elementos tecnológicos que apoyan las actividades de Secretaría

de Hacienda. Finalmente, esta política no estipula las sanciones para quienes la incumplan, puesto que esto es propio del área de control interno de la alcaldía Municipal.

Referencias normativas. La presente política fue elaborada teniendo en cuentas las directrices de control contemplados en la norma ISO/IEC 27001:2013.

Responsabilidades. Es responsabilidad del jefe de despacho de la Secretaría de Hacienda comunicar la Política de Seguridad de la Información a todo el personal a su cargo y a terceros que, por razón de sus funciones, presten servicios o estén involucrados con las actividades de esta dependencia.

Políticas de seguridad de la información: Se debe adoptar una política de seguridad de la información que establezca las acciones necesarias y los procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información, protejan, preserven y administren correctamente los activos de la dependencia así como los mecanismos utilizados para la implementación de los mismos, junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas.

Organización de la seguridad de la información. En la alcaldía Municipal de Rio de Oro, no existe un área de sistemas que apoye a todas las dependencias en lo relacionado con las tecnologías de la información por tanto se debe crear un Área de Sistemas, encargada de la administración del manejo de la información, creando roles y responsabilidades entre los

empleados participantes para que apoye las actividades de la Secretaría de Hacienda, dependencia que maneja el mayor flujo de información dentro de la administración Municipal.

Se debe organizar un comité de seguridad de la información que esté integrado por los funcionarios de la dependencia.

El Comité de Seguridad de la Información debe estar integrado por:

- Alcalde Municipal (Coordinador del Comité de Seguridad de la Información)
- Ingeniero de Sistemas (Responsable de los sistemas de información)
- Secretaria de Hacienda (Responsable de los procesos contables)
- Coordinadora de rentas (Responsable de los procesos de rentas)

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

- Revisar el estado general de la seguridad de la información periódicamente.
- Inspeccionar y monitorear los incidentes de seguridad de la información.
- Dar cumplimiento a las políticas de seguridad que se hayan establecido.
- Revisar, analizar y aprobar los proyectos de seguridad de la información.
- Aprobar las modificaciones o nuevas políticas de seguridad de la información que se quieran implementar.
- Realizar análisis de riesgos a los sistemas de información que se manejan.

- Mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes

Seguridad de los recursos humanos. Se deben implementar estrategias orientadas a reducir los riesgos de error humano, comisión de ilícitos contra uso inadecuado de instalaciones, es fundamental tener en cuenta el recurso humano que labora en la dependencia con el fin de garantizar la integridad, confidencialidad y disponibilidad de la información para ello se deben seguir los siguientes controles:

Incluir una cláusula de confidencialidad de la información que tendrán a su cargo los funcionarios de la dependencia y quienes laboran en Secretaría de Hacienda o tiene actividades relacionadas con la información que se maneja.

Se debe crear conciencia en los funcionarios sobre la importancia de la seguridad de la información, esto se puede hacer por medio de capacitaciones periódicas.

Se debe asignar responsabilidades a los funcionarios en cuanto a los activos que tiene a su cargo.

Se debe definir los perfiles de los cargos, para identificar las necesidades de los procesos que va a manejar el funcionario y realizar la clasificación de la información a la que se va a tener acceso, y los riesgos asociados a ésta.

Gestión de activos. Hace referencia al manejo que debe hacerse sobre los bienes de la Secretaría de Hacienda, dentro de los que se incluye la información.

Se deben aplicar las Tablas de Retención Documental para organizar el archivo físico de la dependencia.

Se debe mantener actualizado el inventario de activos.

Control de acceso. Los controles para el acceso a la información de la Secretaría de Hacienda deben seguir unos parámetros para asegurar la disponibilidad, integridad y confidencialidad de la información:

Se deben gestionar las cuentas de usuario para el uso de servicios de la red, sistemas de información y quipos de la dependencia.

Cuando un empleado se retire del área, debe informar al coordinador de seguridad con por lo menos un día de antelación, para realizar el correspondiente backup y cambios o eliminación de usuarios.

Se debe concientizar a los funcionarios de la importancia de mantener en secreto y de uso personal las claves de seguridad

Se debe coordinar con el Jefe de Recursos Humanos las tareas de concientización a todos los funcionarios y contratistas de la dependencia, 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.

Solo se deberá permitir el ingreso al área de archivo de información al personal autorizado, entendiéndose por ello, funcionarios y personas externas previa autorización.

Seguridad física y del entorno. Se deben crear controles de acceso a las instalaciones de la dependencia con el objetivo de prevenir accesos físicos no autorizados, así como mantener en buen estado documentos que por su valor institucional deben ser conservados.

Se debe reubicar el servidor y los equipos de red que se encuentran en la oficina de la secretaria de hacienda en un sitio que cumpla con los requisitos de un área de sistemas protegida y que este aislado del público que se atiende en la dependencia.

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.

Se debe utilizar normas de cableado estructurado para aislar los cables que transportan datos y corriente eléctrica con el fin de evitar interferencias o cortocircuitos por la exposición.

Los funcionarios que laboran en la dependencia no deben descuidar documentos que contengan información, ya que esto ocasionara la consulta, copia o pérdida de la información por parte de personas no autorizadas.

Se debe restringir el acceso a personal no autorizado a las zonas de archivo.

Los funcionarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada con el fin de evitar accesos a los mismos de personal no autorizado.

Copias de respaldo. Se debe concientizar a los funcionarios de la dependencia sobre la importancia de la realización periódica de copias de seguridad de la información.

Se deben realizar copias de respaldo diariamente.

Se debe ubicar un área de seguridad para el almacenamiento de las copas de respaldo

Protección contra códigos maliciosos. Se debe implementar el uso de antivirus con licencias, además de establecer controles para detectar, prevenir y recuperar la información evitando los ataques de código malicioso

Gestión de incidentes de seguridad de la información. La gestión de incidentes hace referencia al tratamiento que se le debe dar a todas aquellas situaciones no comunes que puedan presentarse y que se consideren puedan dañar, alterar, la información.

Cuando se presente un incidente de seguridad el funcionario deberá reportar a su jefe inmediato en el menor tiempo posible, los eventos asociados al daño, deterioro, pérdida o destrucción de archivos, así como cualquier situación o debilidad que ponga en riesgo los activos de información.

- Una adecuada gestión de incidentes le permitirá a la Secretaría de Hacienda:
- 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 una base de conocimientos sobre Incidentes;
- Evitar en lo posible, incidentes repetitivos.

Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información.

Continuidad del negocio. Se debe crear un plan de contingencia que haga frente a cualquier eventualidad de tipo natural, social, o maliciosa, que afecte el normal funcionamiento de la entidad para el cumplimiento de sus procesos misionales.

Cumplimiento. Todos los requisitos legales, estatutarios, reglamentarios y contractuales pertinentes a las administraciones públicas, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.

5. Conclusiones

Con la ejecución de este proyecto se diseñó un Sistema de Seguridad de la Información para la Secretaria de Hacienda de Rio de Oro-Cesar, para lo cual se decidió utilizar como marco de referencia la norma ISO 27001:2013.

Una vez aplicados los diferentes instrumentos de recolección de la información, las matrices de comprobación de la Norma ISO/IEC 27001: 2013 y la Norma ISO/IEC 27005:2011, se logró obtener un diagnóstico del estado actual de la seguridad de la información en la dependencia que permitieron establecer el nivel de madurez de la entidad en cuanto a la gestión de la seguridad de la información y la gestión del riesgo y con esto se pudo proponer unas políticas de seguridad de la información.

El nivel de cumplimiento de la norma ISO/IEC 27001:2013 en la Secretaría de Hacienda, en lo relacionado con la gestión de la seguridad de la información no cuenta con un proceso reconocible, no existe un diagnóstico inicial, ni un plan que le permita a la dependencia establecer las prioridades y objetivos para el diseño y posterior implementación SGSI.

Se determinó que la situación actual de la seguridad de la información asociado a los requerimientos del estándar ISO-IEC 27001:2013, se encuentra en el nivel de madurez 3, lo que significa que no existe participación activa respecto a la gestión de la información por parte de la alta dirección de la Secretaria de Hacienda y de los involucrados en el uso y manejo de la información.

Una vez aplicada la metodología contemplada en la Norma ISO/IEC 27005:2011, se pudo establecer el grado de riesgo asociado al sistema de información, al que se encuentra expuesta la Secretaria de Hacienda de Rio de Oro-Cesar. El diagnóstico realizado del riesgo de la seguridad física y lógica de la información, permito definir el tratamiento del riesgo acorde a las necesidades de la dependencia.

Con base en todo lo anterior, se diseñó el marco de las políticas de la seguridad de la información para la Secretaria de Hacienda de Rio de Oro-Cesar, con la finalidad de proveer a la dependencia de herramientas orientadas mejorar el tratamiento de la información.

6. Recomendaciones

Se recomienda a la Secretaria de Hacienda de la Alcaldía de Rio de Oro-Cesar, lo siguiente:

Asumir y priorizar la responsabilidad de la seguridad de la información en la dependencia.

Realizar capacitaciones y sensibilización a todos los empleados en la Secretaria de Hacienda, en cuanto se refiere a la seguridad de la información, con la finalidad crear cultura y modos de trabajo eficaces, orientados a mitigar los riesgos.

Aprobar y dar a conocer las políticas de seguridad de la información, planteadas en este proyecto, a todos los involucrados.

Abordar las fases siguientes para el desarrollo del Sistema de Gestión de Seguridad de la Información, además de expandir su implementación a los procesos desarrollados por toda la dependencia.

Realizar auditorías internas una vez implementado el SGSI en la dependencia, con la finalidad de favorecer la mejora continua en los procesos de misión crítica.

Referencias

Alexander, A. G. B. D., Alexander, L. J. A. G., & Buitrago, L. J. (2007). *Diseño de un sistema de gestión de seguridad de información: Óptica ISO 27001: 2005*.

ÁLVAREZ ANGARITA, M. T., & DURAN ALVERNIA, L. (16 de 05 de 2017). *universidad francisco de paula santander ocaña.* Obtenido de http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/1611

Argüello, G. (15 de 10 de 2014). *academia.edu.* Recuperado de http://www.academia.edu/19202037/Historia_de_la_seguridad_de_la_informacion

CNB - INDECOPI. (2008). NTP-ISO/IEC 27001:2008. EDI Tecnología de la información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la información. Requisitos. Lima.

Congreso de Colombia. (1 de agosto de 2015). Recuperado de Ley estatutaria No. 1266 del 31 de diciembre de 2008: http://www.sic.gov.co/drupal/sites/default/files/files/ley1266_31_12_2008(1).pdf.

Consultores, B. (S.F.). Bsc Consultores. Obtenido de http://www.bscconsultores.cl/

Doria Corcho, A. F. (2015). Diseño De Un Sistema De Gestión De Seguridad De La Información Mediante La Aplicación De La Norma Internacional Iso/Iec 27001:2013 En La Oficina De Sistemas De Información Y Telecomunicaciones De La Universidad De Córdoba,. Montería.

DIARIO OFICIAL. (5 de enero de 2009). *DIARIO OFICIAL*. Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

ICETEX (s.f.).Recuperado el 3 de junio de 2017, de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/ACUERDONo.003del17deFebrerode2015.pdf

ICONTEC, "Estándar Internacional ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition)," ed, 2011.

ICONTEC (s.f.). 5 de julio de 2013, de http://tienda.icontec.org/brief/NTC-ISO-IEC27001.pdf

ISACA. (2012). CISM – Certified Information Security Manager – Review Manual 2013. ISACA.

ISO (2005).Recuperado el 8 de agosto de 2015, de https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

ISO 27001. (2013). ISO 27001:2013. Information technology – Security techniques – Information Security management systems - Requirements.

Ministerio de tecnologia de la infromación y la comunicacion. (12 de julio de 2012). *mintic*. Obtenido de http://www.mintic.gov.co/portal/604/articles-5259_doc_pdf.pdf. Obtenido de Infrome de

República de Colombia. (2012). Constitucion Política de Colombia. En R. d. Colombia. Bogotá.

Prezi.com. (2 de mayo de 2014). *Auditoría de sistemas.* Recuperado el 9 de mayo de 2016, de https://prezi.com/q-i08kniv6rb/auditoria-de-sistemas/

Salinas, J., & Isabel, Z. (2015). Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001: 2013.

Sanchez, K., & Areniz, Y. (2014). *Diseño de las políticas de la seguridad de la información para la alcaldía municipal de Río de Oro, Cesar* (Tesis de pregrado). Universidad Francisco de Paula Santander, Ocaña.

Apéndices

Apéndice 1 **Entrevista dirigida a la secretaria de hacienda**

ENTREVISTA DIRIGIDA A LA SECRETARIA DE HACIENDA				HOJA 1/2
EMPRESA	**AREA AUDITADA**	**FECHA**		
Alcaldía de Río de Oro - Cesar	Secretaria de hacienda	DD	MM	AAAA
Objetivo: Indagar sobre la seguridad de la información en el área de sistemas de la secretaria de hacienda del Municipio de Río de Oro				
Funcionario entrevistado: Mayra Vanegas	Cargo: secretaria de hacienda			
Inicio de la entrevista con saludo y explicación breve de objetivo de la entrevista.				

Por favor comente los requisitos mínimos que exige la Secretaria de Hacienda de Rio de Oro-Cesar, en cuanto a escolaridad, experiencia y conocimientos técnico-teóricos, para desempeñar su cargo.

1. Haga un breve comentario sobre el equipo de colaboradores, en cuanto a cantidad de funcionarios vs cargos, nivel de escolaridad, experiencia y conocimientos técnico-teóricos de los mismos.

2. ¿De qué manera se le da a conocer al equipo de colaboradores sus funciones, responsabilidades y la forma de realizar sus actividades?

3. ¿Haga un breve comentario respecto al concepto de seguridad física y lógica de la información desde su punto de vista como jefe de la dependencia?

4. ¿Cuáles son los puntos críticos que afronta dentro del área de sistemas y no permiten el logro de los objetivos?

5. De acuerdo a los puntos críticos antes mencionados, ¿Cómo cree usted que se pueden mejorar o corregir?

6. ¿Existe una política de seguridad de la información para Secretaría de Hacienda? Si existe, ¿se ha socializado a los funcionarios de la dependencia?

7. ¿Se especifican términos y condiciones de contratación para el personal de la Secretaría de Hacienda, teniendo en cuenta la información que manejan en el desempeño de sus funciones?

8. ¿Existen requerimientos a los funcionarios de la dependencia para que se aplique la seguridad de la información?

9. ¿Qué sistemas de información existen en esta dependencia y quienes son responsables de los mismos?

10. ¿Cómo se realiza el acceso a los sistemas de información existentes en la dependencia y que controles de seguridad se tienen para dicho acceso?

11. ¿Qué tipos de restricciones existen al sistema de información y de qué manera se hace la socialización de estas restricciones?

12. Explique el proceso y la frecuencia con que se hace respaldo de la información. Además enuncie el o los responsables de realizarlos.

13. ¿Cree usted que la ubicación del área de sistemas es la adecuada, o si por el contario debería tener ciertas características que la diferencian de una oficina de trabajo?

14. ¿Es importante para usted y los demás miembros de la dependencia el uso de usuarios con roles asignados y claves de acceso a los sistemas de información?

15. ¿Cada cuánto realizan mantenimiento preventivo y correctivo a los equipos de cómputo y quien realiza dicho mantenimiento?

16. ¿Cuentan con dispositivos para evitar que los computadores sufran averías por descargas eléctricas? Mencione cuáles

Apéndice 2 Encuesta dirigida a la los funcionarios de la secretaria de hacienda.

ENCUESTA DIRIGIDA A LA LOS FUNCIONARIOS DE LA SECRETARIA DE HACIENDA				HOJA 1/6
	EMPRESA	**AREA AUDITADA**	**FECHA**	
	Alcaldía de Río de Oro – Cesar	Secretaria de hacienda	DD MM AAAA	
Objetivo: Indagar sobre la seguridad física, seguridad de la secretaria de hacienda del Municipio de Río de Oro				
Funcionario entrevistado: todos los funcionarios de la dependencia	Cargo: contador. Coordinador de rentas, auxiliar de archivo, asesor de presupuesto, secretaria ejecutiva			

I. INFRAESTRUCTURA

EVALUACION DE UBICACION-ADECUACION-ACESSO – SEGURIDAD

1- Las instalaciones son las adecuadas específicamente para funcionar el área de sistemas?

Si_____ No_____

Observaciones._____

2- ¿Se cuenta con una distribución del espacio adecuada en el área de sistemas, de forma tal que facilite el trabajo y permita la circulación fluida?

Si_____ No_____

Observaciones._____

3- ¿El o los lugares de acceso al área de sistemas es o son los más adecuadas respecto a:

Visibilidad

Existe señalización de salida y entrada

Si_____ No_____

Observaciones._____

Amplitud

Si_____ No_____

Observaciones._____

Transito

Si_____ No_____

Observaciones._____

Seguridad

El área de sistemas cuenta con personal de seguridad que restrinja y controle el acceso a las instalaciones.

Si_____ No_____

Observaciones._____

4- ¿Para acceder al área de sistemas se necesita algún tipo de autorización?

Si_____ No_____

Observaciones._____

5- ¿Existe alguna clase de sistema de verificación de entrada y salida de las instalaciones del área de informática?

Si_____ No_____

Observaciones._____

6- Señale con una x los sistemas con los que cuenta el área de sistemas:

Electricidad	**Ventilación**	**Iluminación**
Seguridad		
Circuito cerrado de tv	**Incendio**	**Robo**
Plagas o animales	**Acceso**	**Otro cual**

7- ¿Se realiza mantenimiento a los diferentes sistemas que conforman el área de informática?

Si_____ No_____

Observaciones._____

8- En la siguiente tabla enuncie el tipo de mantenimiento que se realiza, especificando si es contratado con terceros o interno, frecuencia del mismo.

Sistema	**Tipo de Mantenimiento**	**Tipo de Contrato**	**Frecuencia**
Eléctrico e iluminación			
Ventilación			
Seguridad			
Circuito cerrado tv			
Incendios			
Robo			
Plagas animales			
Otro			

9- ¿El sistema de instalaciones eléctricas se encuentra debidamente cableado a la caja de distribución?

Si_____ No_____

Observaciones._____

10- ¿El cableado y el tablero de distribución están debidamente señalizados?

Si_____ No_____

Observaciones._____

11- ¿Los tomacorrientes y los interruptores de conexión se encuentran bien distribuidos en el área de sistemas respecto a los equipos?

Si_____ No_____

Observaciones._____

12- ¿En cuanto al estado de los tomacorrientes e interruptores se puede decir que están?

Bien _____ Regular _____ Mal_____
Observaciones._____

13- ¿Se cuenta con instalación con polo a tierra para todos los equipos?
Si_____ No_____
Observaciones._____

14- ¿Existe algún sistema de contingencia en dado caso que falle el suministro de energía?
Si_____ No_____
Observaciones._____

15- Señale la existencia de detectores de humo y cantidad de los mismos.
Si_____ No_____ Cantidad_____
16- Señale la existencia de alarma de seguridad en caso de incendio y cantidad de los mismos.
Si_____ No_____ Cantidad_____

II INVENTARIOS

17- ¿Los equipos y accesorios que integran el área de sistemas se encuentran inventariados?
Si_____ No_____
Observaciones._____
(si la respuesta es negativa pase a la pregunta 20)

18- Señale con una x las especificaciones del inventario:

Cantidad	
Descripción	
Marca	
Serie	
Ubicación	
Registro de averías por unidad	
Otro cual	

19- Señale la frecuencia con que se realiza la actualización de inventarios
_____

20- Señale si existen controles para verificar la existencia y estado de.

Adquisición de nuevos equipos	
Equipos en garantía	
Equipos extraviados y o robados	
Equipos dados de baja	
Equipos averiados	
Tenencia y responsabilidad de equipos	

21- ¿Se cuenta con servicio de mantenimiento para todos los equipos?
Si_____ No_____
Observaciones._____

22- ¿Se cuenta con servicio de mantenimiento para todos los equipos?

Sí_____ No_____

Observaciones._____

23- ¿Qué tipo de mantenimiento se realiza en los equipos?

Preventivo _____ Correctivo_____ No se realiza_____

24- ¿Tiene conocimiento respecto a equipos o dispositivos extraviados y o robados. En dado caso que la respuesta sea positiva por favor enuncie el o el equipo dispositivo extraviado y la cantidad de los mismos?

Sí_____ No_____

Observaciones._____

25- Tiene conocimiento respecto a equipos o dispositivos dañados o averiados por:

Uso y manejo del personal
Deterioro vida útil
Incendio
Humedad
Ventilación
Bebidas y alimentos
Instalaciones eléctricas

Sí_____ No_____

Observaciones._____

26- En dado caso que la respuesta sea positiva por favor enuncie el o el equipo dispositivo extraviado y la cantidad de los mismos.

27- ¿Es conocedor de políticas y procedimientos para el uso y manejo de seguridad de los equipos de cómputo? Por favor enuncie las que conoce:

28- ¿La dependencia cuenta con programas de capacitación en el uso y manejo de seguridad de los equipos del área de sistemas?

Sí_____ No_____

Observaciones._____

29- ¿Hay prohibición en el consumo de bebidas y alimentos dentro del área de sistemas?

Sí_____ No_____

Observaciones._____

30- ¿Hay avisos que adviertan la prohibición de consumo de bebidas y alimentos dentro del área de sistemas?

Sí_____ No_____

Observaciones._____

Apéndice 3. Encuesta dirigida a la los funcionarios de la secretaria de hacienda.

ENCUESTA DIRIGIDA A LA LOS FUNCIONARIOS DE LA SECRETARIA DE HACIENDA					HOJA 1/4
	EMPRESA	**AREA AUDITADA**	**FECHA**		
	Alcaldía de Río de Oro – Cesar	Secretaria de hacienda	DD	MM	AAAA
Objetivo: Indagar sobre la seguridad lógica, seguridad de la secretaria de hacienda del Municipio de Río de Oro					
Funcionario entrevistado: todos los funcionarios de la dependencia	Cargo: contador. Coordinador de rentas, auxiliar de archivo, asesor de presupuesto, secretaria ejecutiva				

1. Los programas instalados del área de sistemas se encuentran inventariados?

Si_____ No_____
Observaciones._____

2. Los programas inventariados del área de sistemas tienen sus respectivas licencias. ? En dado caso que escoja la opción algunos relacione los que no tienen licencia.

Si_____ No_____
Observaciones._____

3. Los programas inventariados del área de sistemas tienen sus respectivos manuales de usuario?.

Si_____ No_____
Observaciones._____

4. Se tiene algún tipo de control respecto a las licencias. ?

Si_____ No_____
Observaciones._____

5. De los programas inventariados del área de sistemas. Sabe usted de algunos que no estén instalados. ? Si su respuesta es sí relacione cuales no se están utilizando y las causas porque no se se están ejecutando.

Si_____ No_____
cuáles? _____
Causas_____

6. Existen políticas y procedimientos estipulados para el uso de los programas del área de sistemas. ? Si su respuesta es sí relacione los existentes.

Si_____ No_____
Observaciones._____

7. Sabe usted si hay registros de las incidencias presentadas en los programas del área de sistemas. ?

Si_____ No_____

Observaciones._____

8. Con que frecuencia se actualizan los programas. ?

9. Existe código de acceso y contraseña para acceder a los programas. ?

Si_____ No_____

Observaciones._____

10. Los programas permiten que los códigos y contraseñas estén encriptados. ?

Si_____ No_____

Observaciones._____

11. Con que frecuencia se cambian los códigos y contraseñas de los equipos y programas. ?

12. Existen procedimientos de asignación y distribución de contraseñas. ?

Si_____ No_____

Observaciones._____

13. Cada usuario tiene asignado un código y una contraseña para acceder a los programas. ?

Si_____ No_____

Observaciones._____

14. Los programas cuentan con algún tipo de bloqueo cuando el sistema no es utilizado por un tiempo determinado. ?

Si_____ No_____

Observaciones._____

15. Cuándo se presenta cambios de personal, que manejo se le dan los códigos y contraseñas. ?

16. Conoce usted si los usuarios prestan sus equipos a otros usuarios. ?

Si_____ No_____

Observaciones._____

17. Conoce usted si los usuarios prestan sus códigos y contraseñas de acceso a otros usuarios?

Si_____ No_____

Observaciones._____

18. Existe registro clasificado del tipo de información que se maneja en el área de sistemas. ?

Si_____ No_____

Observaciones._____

Apéndice 4. Lista de chequeo seguridad fisica

LISTA DE CHEQUEO				HOJA 1/1
	**EMPRESA/AREA**	**RESPONSABLE**	**FECHA**	
	Alcaldía de Rio de Oro	Secretaria de hacienda	DD MM AAAA	
Objetivo: Conocer los controles existentes en cuanto a la seguridad física del hardware, de la Secretaria de Hacienda de Rio de Oro Cesar.				

No	**Preguntas**	**Cumple**	**No Cumple**	**Observación**
	A. Acceso físico			
1	**¿**El sitio donde está ubicada el área de sistemas		**X**	
2	tiene acceso restringido?		**X**	
3	¿Existen mecanismos de identificación al personal que ingrese al área de sistemas?		**X**	
4.	¿Existe localización y señalización adecuada de áreas sensibles?		**X**	
	¿La ubicación área de sistemas es independiente de otras oficinas y es la adecuada?			
	B. Aspectos relacionados con el hardware			
5	¿Se encuentra inventariado el hardware que reposa en el área de sistemas?		**X**	
6	¿Cada dispositivo o periférico tiene la numeración		**X**	
7	respectiva del inventario?		**X**	
8	¿Existe personal autorizado para controlar la salida de dispositivos del área de la dependencia?		**X**	
9	¿Tiene conocimiento de algún faltante del inventario de hardware como periféricos, equipos de cómputo o algún dispositivo?		**X**	
	¿Se realizan mantenimientos preventivos a los dispositivos de cómputo?			
	C. Plan de desastres			
11	¿Cuentan con un plan de desastres?		**X**	
12	¿Existen planes y manuales sobre normas de actuación en caso de emergencia?		**X**	
13	¿Existe señalizacion para la evacuacion en caso		**X**	
14	de desanstres?		**X**	
15	¿Se realizan simulacros de emergencia para saber cómo actuar y qué hacer con los dispositivos en caso de que ocurra una eventualidad?		**X**	
	¿Existe salida de emergencias?			
	D. Instalaciones eléctricas			
16	¿Tienen contrato con algún electricista para que revisen las instalaciones eléctricas?		**X**	
17	¿Se revisan las instalaciones eléctricas?		**X**	
18	¿Las instalaciones eléctricas y el cableado		**X**	
19	cumplen con los estándares?		**X**	

20	¿Se han generado cortos circuitos en las instalaciones?		**X**	
21	¿Hay extintores en la dependencia? ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?		**X**	
	E. Seguridad Física			
22	¿El área de sistemas se encuentra ubicada en un cuarto o cubículo independiente?		**X**	
23	¿El sitio donde reposan los dispositivos del área de sistemas es idóneo, no hay humedad ni calor excesivo?	**X**		
24	¿Se permite el consumo de alimentos y bebidas en el interior del área de sistemas?	**X**		
25	¿Existen avisos en el interior del área de sistemas que recuerden que está prohibido ingerir alimentos o bebidas dentro del mismo?		**X**	
26	¿Son controladas las entradas en el área de sistemas? ¿Se registra el acceso al área de sistemas a personas ajenas a este?		**X**	

Apéndice 5. Lista de chequeo seguridad lógica

LISTA DE CHEQUEO				HOJA 1/1
	**EMPRESA/AREA**	**RESPONSABLE**	**FECHA**	
	Alcaldía de Río de oro	Secretaria de hacienda	DD MM AAAA	
Objetivo: **Conocer los controles existentes en cuanto a la seguridad lógica de la información que se tiene la secretaria de Hacienda**				

No	**Preguntas**	**Cumple**	**No Cumple**	**Observación**
	Acceso a la información			
1	¿Los equipos de cómputo tienen claves de acceso asignadas a los funcionarios de acuerdo al computador en que laboran?		**X**	
2	¿Las personas que laboran en esta dependencia son conscientes de la importancia de proteger la información que manejan?	**X**		
3	¿Las claves de acceso son únicas para cada usuario y para cada aplicación?		**X**	
4	¿Se cuenta con una copia de las claves de acceso de los usuarios en un lugar seguro?		**X**	
5	¿Existe un acuerdo de confidencialidad entre la dependencia y los empleados para la protección de la información que ha sido encomendada?		**X**	
6	En caso de incumplimiento de dicho acuerdo ¿Se emprenden acciones por parte de la dependencia contra quien lo comete?		**X**	
7	¿Cuándo se presenta cambios de personal, se inhabilitan las claves de acceso de los usuarios que ya no utilizan el sistema?			
8	¿Se limita el uso del equipo a los usuarios autorizados únicamente?	**X**	**X**	

9	¿Se capacitan periódicamente a los usuarios en el adecuado manejo de los equipos y de los aplicativos?		**X**	
10	¿Es suficiente el plan de capacitación establecido para los usuarios?	**X**		
11	¿Se limita el acceso a los programas y archivos mediante el uso de contraseñas o algún otro mecanismo para el ingreso a aplicaciones o programas?		**X**	
12	¿Se realizan copias de seguridad de la información que se genera al interior del establecimiento?		**X**	
13	¿El establecimiento cuenta con programas utilitarios que permitan la recuperación de archivos en caso de fallas de los equipos?		**X**	
14	¿En los equipos de la dependencia hay software para la detección de intrusos?	**X**		
15	¿Los equipos tienen instalado software antivirus?		**X**	
	¿Las bases de datos de estos antivirus se encuentran actualizadas?			

Apéndice 6. Dictamen de auditoria

Ocaña, 07 de Agosto de 2017
Señora
MAYRA ALEJANDRA VANEGAS PICON
Secretaria de Hacienda
Alcaldía de Rio de Oro-Cesar

Cordial Saludo.

Con la presente me permito remitirle el dictamen de la auditoría realizada durante el periodo del 10 de julio al 04 de agosto del año en curso, en la dependencia que está a su cargo, y cuyo objetivo fue Evaluar la existencia y eficiencia de controles de seguridad de la información en La Secretaria de Hacienda de Rio de Oro-Cesar, de acuerdo con los dominios contemplados en el estándar ISO/IEC 27001:2013.

En cuanto a los resultados obtenidos en la evaluación efectuada a través de la observación directa, entrevistas, encuestas, cuestionarios y listas de chequeo, me permito comunicarle las desviaciones encontradas:

El área de sistemas no cuenta con Políticas de seguridad de manejo y uso e información. Lo que dificulta al equipo de colaboradores ejecutar sus funciones de manera óptima y pone en riesgo la seguridad de personas, equipos, programas e información.

La ubicación del área de sistemas no es la adecuada, debido a que se encuentra al interior de la dependencia de la Secretaria de Hacienda y esto limita la distribución en planta para equipos y enseres y vulnera la seguridad de la información, ya que no existe restricción en el ingreso de personal.

El sistema eléctrico no cumple con los estándares de seguridad, se detectaron cables expuestos, interruptores sin señalización y tomas sin protección. Lo que puede ocasionar daños en equipos y pérdida de información por cortos circuito, o falta de señalización en los interruptores, y exposición a accidentes de trabajo por contacto con cables expuestos o tomas sin tapas de protección.
El acceso al área de sistemas no es restringido, lo que expone al riesgo a personas, equipos e información.
La dependencia no realiza mantenimientos preventivos a los equipos de cómputo y a sus dispositivos. Lo que puede ocasionar daño permanente en piezas básicas del ordenadores y haber posible pérdida total o parcial de la información.

No se realizan copias de seguridad de la información periódicamente. Lo que vulnera el sistema información en cuanto a base de datos y programas, en casos de imprevistos ocasionados

condiciones ambientales, desastres naturales, fallas de energía, daños en equipos, uso inadecuado por usuarios o pérdida por robo.

Las contraseñas de ingreso a los sistemas de información son conocidas y compartidas por todos los funcionarios de la dependencia. Lo que supone un riesgo alto en el manejo que se le da a la información.

De acuerdo a con las pruebas realizadas respecto a las situaciones encontradas me permito hacerle las siguientes recomendaciones:

Designar un responsable de sistemas, que se encargue de gestionar e implementar las políticas de seguridad de la información del área de sistemas.

Ubicar la oficina del área de sistemas en un sitio idóneo fuera de la dependencia de Secretaria de Hacienda o adecuar al interior de las oficinas de la Secretaria de Hacienda, un cubículo independiente que cumpla con las condiciones de espacio, seguridad y privacidad.

En cuanto al sistema eléctrico se deben cubrir los cables expuestos con canaletas, y realizar la debida señalización de los interruptores y proteger los toma-corrientes con tapa.

Para restringir el acceso al área de sistemas es necesario instalar una puerta que permita la privacidad de la dependencia y un aviso legible y de tamaño adecuado que indique que solo puede ingresar personal autorizado. Además se debe crear e implementar un sistema de control de ingreso de personal.

Respecto a los mantenimientos se debe definir e implementar un plan de mantenimiento preventivo y correctivo periódico para los equipos de cómputo y dispositivos.

Crear políticas que contemplen los procedimientos necesarios para realizar con frecuencia copias de seguridad de la información que maneja cada funcionario. Designar un lugar seguro para almacenar las copias de respaldo de de toda la información y capacitar al personal en las políticas seguridad.

Crear políticas de acceso y control a los sistemas donde se especifique la asignación y el uso de claves secretas y roles a cada funcionario.

Atentamente,

Auditor Líder

Apéndice 7 Secciones NORMA ISO IEC 27001:2013

REQUERIMIENTOS SECCIONES	CONTENIDO
Sección 0 Introducción	Explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.
Sección 1 Alcance	Explica que esta norma es aplicable a cualquier tipo de organización.
Sección 2 Referencias normativas.	Hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.
Sección 4 Contexto de la organización.	Esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.
Sección 5 Liderazgo	Esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.
Sección 6 Planificación	Esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.
Sección 7 Soporte	Esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.
Sección 8 Operación	Esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.
Sección 9 Evaluación y Desempeño.	Esta sección forma parte de la fase de Revisión del ciclo PDCA
Sección 10. Mejora.	Define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

Apéndice 8: Matriz de aplicabilidad por dominio y objetivos de control secretaria de hacienda de la alcaldía de Rio de Oro – cesar

A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**				
A5.1	Orientación de la dirección para la gestión de la seguridad de la información				
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	NO EXISTE	0	La Secretaria de Hacienda, actualmente no tiene implementado un SGSI y no existe un documento que contemple políticas de seguridad de la información.
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	NO EXISTE	0	No existe, actualmente la Secretaria no cuenta con políticas de seguridad de la información.
NIVEL DE CUMPLIMIENTO DOMINIO A5				0	NO EXISTE
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**				
A6.1	Organización interna				
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**

A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	NO EXISTE	0	No están definidos los roles y responsabilidades relativas a la seguridad de la información, puesto que no se tiene implementado un SGSI en la dependencia.
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	**INICIAL**	10	Los funcionarios se encuentran separado por áreas y tienen acceso a los activos y/o información necesaria para ejecutar sus actividades laborales.
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes, para reportar las incidencias de la SI.	NO EXISTE	0	No se tiene contacto con autoridades nacionales, departamentales o locales, para reportar los incidentes de seguridad que la Secretaria presenta, los mismos se resuelven internamente.
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	NO EXISTE	0	No se tiene contacto con autoridades nacionales, departamentales o locales, para temas relacionados con SGSI.
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	NO EXISTE	0	Los proyectos que se presentan en la dependencia están relacionados con las TIC, sin embargo son presentados pero no contemplan los riegos referentes a la seguridad de la información.
A6.2	Dispositivos móviles y teletrabajo				
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**NIVEL DE CUMPLIMIENTO% CMM CMM**

A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	NO EXISTE	0	No existe una política de seguridad al interior de la dependencia.
A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	NO APLICA	0	No se implementa el teletrabajo.
NIVEL DE CUMPLIMIENTO DOMINIO A6				2	NO EXISTE
A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**				
A7.1	Antes de asumir el empleo				
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la	**INICIAL**	10	El personal se selecciona de acuerdo al perfil y la idoneidad del trabajo a ejecutar.

		clasificación de la información a que se va a tener acceso y a los riesgos percibidos.			
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	NO EXISTE	0	En los contratos que lleva a cabo la dependencia, no existe una cláusula que resguarde los principios básicos de la SI.
A7.2	Durante la ejecución del empleo				
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	NO EXISTE	0	No existen políticas de seguridad de la información.
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y	NO EXISTE	0	No se tiene implementado un SGSI ni un plan de concientización, capacitación formal relativa a la seguridad de la información.

		procedimientos de la organización pertinentes para su cargo.			
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	NO EXISTE	0	La Secretaria no cuenta con un SGSI, no tiene políticas de seguridad de la información, ni tiene documentado ningún proceso disciplinario en caso de incidencia, está sujeta a la normatividad laboral vigente colombiana para la celebración de contratos laborales. Y la contratación con terceros.
A7.3	Terminación y cambio de empleo				
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	NO EXISTE	0	No existen cláusulas de confidencialidad de la información en el contrato que el funcionario firma al momento de ingresar a la empresa.
NIVEL DE CUMPLIMIENTO DOMINIO A7				2	NO EXISTE
A8	**GESTION DE ACTIVOS**				
A8.1	Responsabilidad por los activos				
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.			**ESTADO DE CUMPLIMIENT**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**

			O		
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	LIMITADO	50	Existe un documento con la clasificación de todos los activos ligados al sistema de información.
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	LIMITADO	50	Existe un documento donde especifican los propietarios de los activos informáticos inventariados.
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	NO EXISTE	0	Actualmente no existe ningún documento relacionado con reglas específicas para el manejo y buen uso de los activos.
A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	LIMITADO	50	Existen registros de paz y salvo donde se especifica la devolución de los activos entregados por los empleados al momento de retirarse de la dependencia.
A8.2	Clasificación de la información				
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y	NO EXISTE	0	No existe un documento que clasifique la criticidad de la información.

		susceptibilidad a divulgación o a modificación no autorizada.			
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	NO EXISTE	0	No existe procedimiento alguno para el etiquetado y/o clasificación de la información.
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	NO EXISTE	0	No existen procedimientos para el manejo de la información, ya que ésta no está clasificada
A8.3	Manejo de medios				
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	NO EXISTE	0	No se cuenta con un procedimiento para la gestión de los medios removibles que pueda manejar la dependencia.
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	NO EXISTE	0	No se dispone de un procedimiento debidamente documentado para la disposición de medios.

A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	NO APLICA	0	No se transportan medios informáticos.
NIVEL DE CUMPLIMIENTO DOMINIO A8				17	**INICIAL**
A9	**CONTROL DE ACCESO**				
A9.1	Requisitos del negocio para el control de acceso				
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	NO EXISTE	0	No existe una política de control de acceso para la secretaría de Hacienda, más cuando es una dependencia que tiene acceso independiente al resto del edificio de la Alcaldía
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	NO EXISTE	0	El acceso a las redes no está protegido a personas no autorizadas, todos los usuarios tienen manejo de todos los equipos.
A9.2	Gestión de acceso de usuarios				
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los	NO EXISTE	0	No existe documento alguno respecto asignación de registro y cancelación, cuando una persona se retira de la dependencia no tiene el proceso para la cancelación del registro.

		derechos de acceso.			
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	NO EXISTE	0	No hay existencia de documento relacionado con el proceso al acceso de los usuarios.
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	NO EXISTE	0	No hay evidencia de restricción y control de acceso privilegiado.
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	NO EXISTE	0	No existe un mecanismo para llevar un control.
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	NO EXISTE	0	No hay documentación al respecto.
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar	NO EXISTE	0	No existe documentación formal de remoción de los privilegios de acceso de los empleados que cambian el cargo o terminan contrato, pero cada vez que un usuario ya no trabaja en la compañía se le es retirado todos los permisos para ingresar a los diferentes sistemas de información.

		cuando se hagan cambios.			
A9.3	Responsabilidades de los usuarios				
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	NO EXISTE	0	La información de autenticación del empleado en los sistemas y acceso a información no es confidencial.
A9.4	Control de acceso a sistemas y aplicaciones				
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	NO EXISTE	0	Aunque se manejan pasword de entrada a los sistemas de información, las mismas son conocidas por todo el personal. No hay confidencialidad.
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	NO EXISTE	0	Los sistemas no están protegidos mediante un mecanismo de inicio de sesión seguro.
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y	NO EXISTE	0	Existen sistemas que la contraseña fue suministrada manualmente y este no posee el mecanismo de obligar al usuario a cambiarla

		deben asegurar la calidad de las contraseñas.			
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	NO EXISTE	0	Los sistemas se pueden instalar software, ya que a los funcionarios se les suministra la clave del administrador para llevar a cabo esta tarea
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	NO EXISTE	0	Se utilizan los sistemas de información pero no se hacen implementaciones.
NIVEL DE CUMPLIMIENTO DOMINIO A9				0	NO EXISTE
A10	**CRIPTOGRAFIA**				
A10.1	Controles criptográficos				
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	NO EXISTE	0	No existe una política sobre el uso de algoritmos de encriptación para el cifrado de la información transmitida.
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	NO EXISTE	0	No existe una política sobre el uso y distribución de llaves criptográficas
NIVEL DE CUMPLIMIENTO DOMINIO A10				0	NO EXISTE
A11	**SEGURIDAD FISICA Y DEL ENTORNO**				

A11.1	Áreas seguras				
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.			**ESTADO DE CUMPLIMIENTO**		**OBSERVACION**
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	NO EXISTE	0	Existe un perímetro físico, pero no existe personal de seguridad para el control de acceso a las instalaciones y por ende a la información.
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	NO EXISTE	0	No existe un mecanismo, que permita el control del personal que ingresa, no hay guardia de seguridad a la entrada de las instalaciones.
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones..	NO EXISTE	0	Las oficinas y lugares de trabajo no están protegidas por medios físicos para controlar el acceso.
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	NO EXISTE	0	No existe protección física contra los desastres naturales y ataques o amenazas humanas.
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	NO EXISTE	0	Debido al espacio reducido de las instalaciones, no están diseñadas áreas seguras para la ejecución del trabajo.
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no	NO EXISTE	0	La entrega de equipos y otros dispositivos ocurre al interior de la oficina de sistemas de la empresa

		autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.			
A11.2	Equipos				
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	NO EXISTE	0	Los equipos que se encuentra en la empresa no se encuentran protegidos físicamente contra amenazas ambientales tales como fuego, incendio, agua, humo. No existe sistema contra robo, ni circuito cerrado de TV, ni tampoco sistemas contra incendio.
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	NO EXISTE	0	Algunos equipos cuentan con UPS, sin embargo los servicios de suministros de energía, ventilación no están acordes a las características de los equipos.
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	NO EXISTE	0	El cableado eléctrico que dispone la Secretaria de Hacienda, se encuentra expuesto sin las acometidas que aíslen la interferencia y el cableado de datos no está diseñado con las normas necesarias para una arquitectura de red segura.
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad	NO EXISTE	0	El mantenimiento que lleva a cabo es correctivo, no disponen de un cronograma donde se pueda controlar el mantenimiento preventivo de los equipos y dispositivos.

		continuas.			
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	**INICIAL**	10	Para el retiro de equipos se debe diligenciar un documento de autorización por parte de la Secretaria de Hacienda.
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	NO APLICA	0	
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso.	NO APLICA	0	
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	NO APLICA	0	
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una	NO EXISTE	0	No existe una política debidamente documentada, se evidencio que muchos de los funcionarios poseen información confidencial de los usuarios del sistema.

		política de pantalla limpia en las instalaciones de procesamiento de información.			
NIVEL DE CUMPLIMIENTO DOMINIO A11				0	NO EXISTE
A12	**SEGURIDAD DE LAS OPERACIONES**				
A12.1	Procedimientos operacionales y responsabilidades				
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	NO EXISTE	0	La dependencia cuenta con algunos documentos donde se encuentras procedimientos operacionales. Sin embargo esto es iniciativa de los funcionarios. No hay políticas al respecto.
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	NO EXISTE	0	No existen procedimientos de control de cambios.
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	NO APLICA	0	No posee ambiente de desarrollo y prueba.
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no	NO APLICA	0	No posee ambiente de desarrollo y prueba.

		autorizados al ambiente de operación.			
A12.2	Protección contra códigos maliciosos				
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	**INICIAL**	10	Aunque no existe una política definida contra el los códigos maliciosos, los usuarios son conscientes de los efectos que éstos podrían tener sobre el sistema de información. De igual forma, los equipos poseen software antimalware.
A12.3	Copias de respaldo				
Objetivo: Proteger contra la perdida de datos			**ESTADO DE CUMPLIMIENTO**		**OBSERVACION**
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	**INICIAL**	10	Aunque la empresa no disponga de políticas, existe un procedimiento para llevar a cabo las copias de seguridad y realizar los procesos de respaldo de la información de los diferentes sistemas de información.
A12.4	Registro y seguimiento				
Objetivo: Registrar eventos y generar evidencia			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del	NO EXISTE	0	No se realiza un control de los cambios ocurridos en los equipos de los funcionarios.

		usuario, excepciones, fallas y eventos de seguridad de la información.			
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	NO EXISTE	0	Los registros de eventos no están protegidos contra el acceso no autorizado.
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	NO EXISTE	0	Las acciones y registros de los administradores de los sistemas de información de la dependencia no son almacenados, ni protegidos de cualquier modificación.
A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	**INICIAL**	10	Aunque no se tiene una política documentada sobre la sincronización de los relojes, todos los sistemas están sincronizados bajo un único formato de tiempo y zona horaria.
A12.5	Control de software operacional				
Objetivo: Asegurarse de la integridad de los sistemas operacionales			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	NO EXISTE	0	No existe una política o procedimiento documentado respecto a la autorización para la instalación de software en los sistemas operativos.
A12.6	Gestión de la vulnerabilidad técnica				
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**

A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	NO EXISTE	0	Aunque existe un inventario de los activos físicos y del software operacional, no se tiene una metodología de riesgos que los evalúe.
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	NO EXISTE	0	No existen políticas o procedimientos que definan la instalación de software por parte de los usuarios.
A12.7	Consideraciones sobre auditorias de sistemas de información				
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	NO EXISTE	0	No se dispone un plan de auditoría para la verificación de los sistemas operativos.
NIVEL DE CUMPLIMIENTO DOMINIO A12				3	NO EXISTE
A13	**SEGURIDAD DE LAS COMUNICACIONES**				
A13.1	Gestión de la seguridad de las redes				
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.			**ESTADO DE CUMPLIMIENT**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**

			O		
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	NO EXISTE	0	No existe una infraestructura de red con protocolos de seguridad implementados en la dependencia, además la clave de la red al ser utilizada por personal externo a la dependencia hace vulnerable el tráfico de red de la oficina
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	NO EXISTE	0	No se exige a los contratistas que suministran los servicios de redes y comunicaciones la implementación de políticas de seguridad para salvaguardar la información.
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	**INICIAL**	10	Se encuentra separadas en equipos de comunicación, servidor y usuarios.
A13.2	Transferencia de información				
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de	NO EXISTE	0	No existe una política o documentación sobre los procedimientos y controles para la transferencia segura de la información.

		todo tipo de instalaciones de comunicaciones.			
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	NO EXISTE	0	No se han implementado controles criptográficos que garanticen la seguridad en la transmisión de la información
A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	NO EXISTE	0	No se han implementado controles criptográficos que garanticen la seguridad en la transmisión de la información.
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	NO EXISTE	0	En los contratos de los empleados no se estipula el compromiso con la confidencialidad de la información.
NIVEL DE CUMPLIMIENTO DOMINIO A13				2	NO EXISTE
A14	**ADQUISICION , DESARROLLO y MANTENIMIENTO DE SISTEMAS**				
A14.1	Requisitos de seguridad de los sistemas de información				
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos	NO EXISTE	0	No existe una política o documentación sobre los procedimientos mencionado

		para nuevos sistemas de información o para mejoras a los sistemas de información existentes.			
A.14. 1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	NO APLICA	0	
A.14. 1.3	Protección de transaccione s de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	NO APLICA	0	
A14.2	Seguridad en los procesos de Desarrollo y de Soporte				
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A.14. 2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los	NO APLICA	0	La dependencia no lleva a cabo el desarrollo de software.

		desarrollos dentro de la organización.			
A.14. 2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	NO APLICA	0	La dependencia no lleva a cabo el desarrollo de software.
A.14. 2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	NO EXISTE	0	No dispone un procedimiento establecido para realizar esta tarea
A.14. 2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	NO APLICA	0	La empresa no realiza desarrollo de software y las actualizaciones y modificaciones de software son desarrolladas por la empresa encargada.
A.14. 2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	NO APLICA	0	La dependencia no lleva a cabo el desarrollo de software.

A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	NO APLICA	0	La dependencia no lleva a cabo el desarrollo de software.
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	NO APLICA	0	La dependencia no lleva a cabo el desarrollo de software.
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	NO APLICA	0	La dependencia no lleva a cabo el desarrollo de software.
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	NO EXISTE	0	No se realizan las pruebas de seguridad debido a que aún no existen los lineamientos o políticas de la seguridad de la información.
A14.3	Datos de prueba				
Objetivo: Asegurar la protección de los datos usados para pruebas.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y	NO APLICA	0	La dependencia no lleva a cabo el desarrollo de software.

		controlar cuidadosamente.			
NIVEL DE CUMPLIMIENTO DOMINIO A14				0	NO EXISTE
A15	**RELACIONES CON LOS PROVEEDORES**				
A15.1	Seguridad de la información en las relaciones con los proveedores.				
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	OBSERVACION
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	NO EXISTE	0	No existen políticas de seguridad de la información.
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	NO EXISTE	0	No se llevan a cabo acuerdos documentados ya que no existe una clasificación de seguridad de la información, así como tampoco las políticas y procedimientos
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y	NO EXISTE	0	No se llevan a cabo acuerdos documentados ya que no existe una clasificación de seguridad de la información, así como tampoco las políticas y procedimientos

		servicios de tecnología de información y comunicación.			
A15.2	Gestión de la prestación de servicios de proveedores				
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	NO EXISTE	0	No existen políticas de seguridad de la información.
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	NO EXISTE	0	No se llevan a cabo acuerdos documentados ya que no existe una clasificación de seguridad de la información, así como tampoco las políticas y procedimientos
NIVEL DE CUMPLIMIENTO DOMINIO A15				0	NO EXISTE
A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**				
A16.1	Gestión de incidentes y mejoras en la seguridad de la información				

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	NO EXISTE	0	No existen procedimientos documentados para gestionar los incidentes relativos a la seguridad de la información.
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	NO EXISTE	0	El canal de gestión para dar a conocer los eventos relacionados con la seguridad de la información, no está definidos ni documentados.
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	NO EXISTE	0	Cualquier eventualidad es informada por los usuarios de los sistemas, sin embargo no se encuentra un procedimiento formalmente definido.
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	NO EXISTE	0	Aunque existe una clasificación de activos, no existe una metodología de análisis y evaluación de riesgos ligados a la seguridad de la información.

A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	NO EXISTE	0	Aunque las respuestas son inmediatas, los procedimientos de respuesta no están documentados, así como tampoco existe un Plan de Continuidad del Negocio
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	NO EXISTE	0	No existen procedimientos documentados para gestionar los incidentes relativos a la seguridad de la información.
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	NO EXISTE		La dependencia no tiene procedimientos definidos para el manejo de la información
NIVEL DE CUMPLIMIENTO DOMINIO A16				0	NO EXISTE
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**				
A17.1	Continuidad de Seguridad de la información				
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante	NO EXISTE	0	No existe un plan de contingencia para la continuidad del negocio, en el momento de ser afectado por algún incidente interno o externo.

		una crisis o desastre.			
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	NO EXISTE	0	No existe un plan de contingencia para la continuidad del negocio, en el momento de ser afectado por algún incidente interno o externo.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	NO EXISTE	0	No existe un plan de contingencia para la continuidad del negocio, en el momento de ser afectado por algún incidente interno o externo.
A17.2	Redundancias				
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	NO APLICA	0	
NIVEL DE CUMPLIMIENTO DOMINIO A17				0	NO EXISTE
A18	**CUMPLIMIENTO**				

A18.1	Cumplimiento de requisitos legales y contractuales				
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	**INICIAL**	10	Algunos requisitos contractuales están identificados, sin embargo, no cumplen con los requerimientos exigidos por la ley, en la mayoría de los casos.
A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	NO APLICA	0	La dependencia no lleva a cabo el desarrollo de software.
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación,	NO EXISTE	0	No existe un nivel de clasificación formal de confidencialidad de los registros.

		contractuales y de negocio.			
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	NO EXISTE	0	No existen políticas de seguridad de la información.
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	NO EXISTE	0	No existe una Infraestructura de Llave Pública implementada que garantice que la información transmitida y/o almacenada sea segura.
A18.2	Revisiones de seguridad de la información				
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.			**ESTADO DE CUMPLIMIENTO**	**NIVEL DE CUMPLIMIENTO% CMM**	**OBSERVACION**
A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	NO EXISTE	0	No se realizan auditorías con entidades externas, la dependencia es auditada por entes de control, sin embargo no hay documentación de dichas auditorias. Y no existe un plan estipulado para las mismas.

A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	NO EXISTE	0	No existen políticas de seguridad de la información.
A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	NO EXISTE	0	Los sistemas de información se revisan, sin embargo no hay políticas establecidas, para poder evaluar o determinar el cumplimiento. Tampoco se documentan dichas revisiones o actualizaciones.
NIVEL DE CUMPLIMIENTO DOMINIO A18				1	NO EXISTE
La calificación final se obtiene de promediar todas las calificaciones dadas en cada ítem evaluado, el valor resultante se debe aproximar a la cifra más baja.					

Apéndice 9 Acta de apertura

ACTA DE APERTURA AUDITORIA INTERNA

Proceso Auditado: SECRETARÍA DE HACIENDA

Responsable Proceso Auditado: MAYRA ALEJANDRA VANEGAS

Auditor Líder: MAIRE LISNETH SERNA VEGA

Fecha: 10 de julio de 2017 Lugar: ALCALDIA DE RÍO DE ORO

Hora de Inicio 08: 00 am Hora de Terminación 09:00 am

Asistencia:
La reunión de apertura contó con la asistencia de los siguientes funcionarios:
MAYRA ALEJANDRA VANEGAS: Secretaria de hacienda
FABIAN RUEDAS: Contador
NOHORA HERRERA: Secretaria ejecutiva de hacienda

Presentación
El auditor líder realizó la presentación de cada uno de los integrantes del equipo de auditoría. Se explicó por parte del auditor líder el contenido del plan de trabajo.

Propósitos y Objetivos de la Auditoria
El auditor líder explico a los asistentes el propósito principal de la Auditoria a realizar que es evaluar la existencia y eficiencia de los controles de seguridad de la información en La Secretaria de Hacienda de Rio de Oro-Cesar, de acuerdo con los dominios contemplados en el estándar ISO/IEC 27001:2013.

Reunión de Cierre e informe de la auditoria
El día 04 del mes agosto se realizará la reunión de cierre para presentar las observaciones y el informe definitivo se presentará a la secretaria de Hacienda Municipal

Auditor Lider **Auditado (s)**

MAIRE LISNETH SERNA VEGA

MAYRA ALEJANDRA VANEGAS PICON

Apéndice 10. Acta de cierre

	ACTA REUNION CIERRE DE AUDITORIA	

Sitio de la reunión:	SECRETARÍA DE HACIENDA DE RIO DE ORO - CESAR	Fecha y Hora	04/08/2017
Proceso/Proyecto/Servicio Social:	SECRETARÍA DE HACIENDA		

ORDEN DEL DIA.

1- Presentación de los participantes
2. Exposición de la metodología aplicada.
3. Presentación de los hallazgos y verificación de ajustes sugeridos.
4. Concretar fechas para el Plan de mejoramiento
5. Otros.

DESARROLLO TEMATICO

PUNTO A TRATAR	RESULTADO
1- Presentación de los participantes	Se realizó la presentación de los participantes de la auditoria y los funcionarios de la dependencia
2. Exposición de la metodología aplicada.	Se dio a conocer la metodología aplicada para la realización de la auditoria que comprendió un examen a los elementos existentes para garantizar la gestión de la seguridad de la información en la Secretaría de Hacienda del Municipio de Rio de Oro – Cesar mediante los lineamientos de la norma ISO 27001:2013. Se Utilizó la Observación y Entrevista como herramienta para verificar el estado Físico y ambiental donde se encuentran ubicados los equipos de computo
3. Presentación de los hallazgos y verificación de ajustes sugeridos.	El área de sistemas está expuesta a todo el público que entra al despacho de la secretaria de hacienda por lo cual su acceso no es restringido y se permite el consumo de alimentos cerca de los aparatos de computo. Se evidenció que no existen controles eficientes para resguardar la parte física de los dispositivos que almacenan la información Se evidenció que no existen controles eficientes para resguardar la parte lógica la información. No se tiene programación para realizar mantenimientos preventivos a los dispositivos del área de sistemas, ni se reconoce la importancia de estos. No existe un SGSI

	ACTA REUNION CIERRE DE AUDITORIA	

4. Otros.	

CONCLUSIONES. (Acuerdos, compromisos y responsables).

HORA DE TERMINACION: 04:35pm

NOMBRE Y FIRMA DE LOS PARTICIPANTES

Nombre y Apellidos	Cargo	Firma
MAYRA ALEJANDRA VANEGAS	Secretaria de hacienda	
FABIAN RUEDAS	Contador	
NOHORA HERRERA	Secretaria ejecutiva de hacienda	

NOMBRE Y FIRMA DE LOS AUDITORES

Nombre y Apellidos	Cargo	Firma
Maire Lisneth Serna Vega	Auditor líder	
Aleida Duran Peñaranda	Auditor 1	
Rosy Sánchez Acosta	Auditor 2	