	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
	Documento	Código	Fecha	Revisión
FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO		F-AC-DBL-007	10-04-2012	A
DIVISIÓN DE BIBLIOTECA		Dependencia	Aprobado	Pág.
		SUBDIRECTOR ACADEMICO		1(142)

RESUMEN – TRABAJO DE GRADO

AUTORES	HAINETH PARRA ALVERNIA JAVIER CONTRERAS NAVARRO DIANA YISNEY DÍAZ PACHECO EDWIN JESÚS LÓPEZ OVALLE		
FACULTAD	INGENIERÍAS		
PLAN DE ESTUDIOS	ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS		
DIRECTOR	ISBELIA KARINA RINCÓN PARADA		
TÍTULO DE LA TESIS	DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RÍO DE ORO, CESAR “EMCAR”		
RESUMEN (70 palabras aproximadamente)			
<p>EL DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR, “EMCAR”, DESARROLLADO MEDIANTE UN ANÁLISIS DE RIESGOS Y/O AMENAZAS QUE ENFRENTA LA ORGANIZACIÓN, PERMITIRÁ LA ELABORACIÓN DEL DOCUMENTO FINAL ESTABLECIENDO LOS DOMINIOS Y OBJETIVOS DE CONTROL, SUSTENTADA, APLICADA Y SOCIALIZADA GARANTIZARÁ LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN, QUE ES EL OBJETIVO PRINCIPAL DEL PRESENTE TRABAJO DE INVESTIGACIÓN.</p>			
CARACTERÍSTICAS			
PÁGINAS: 142	PLANOS:	ILUSTRACIONES:	CD-ROM: 1



**DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA
LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR
“EMCAR”**

**HAINETH PARRA ALVERNIA
JAVIER CONTRERAS NAVARRO
DIANA YISNEY DÍAZ PACHECO
EDWIN JESÚS LÓPEZ OVALLE**

**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS
OCAÑA
2015**

**DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA
LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR
“EMCAR”**

**HAINETH PARRA ALVERNIA
JAVIER CONTRERAS NAVARRO
DIANA YISNEY DÍAZ PACHECO
EDWIN JESÚS LÓPEZ OVALLE**

Proyecto para optar al título de Especialistas en Auditoría de Sistemas

**Directora
Msc. ISBELIA KARINA RINCÓN PARADA
Ingeniero de Sistemas**

**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS
OCAÑA
2015**

AGRADECIMIENTOS

Los autores dan los agradecimientos a:

La Doctora María Fernanda Carrascal Vega, Gerente de la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”, por facilitarnos la información para el desarrollo del presente trabajo de investigación.

A la directora del proyecto MSC. Isbelia Karina Rincón Parada, por su dedicación, esmero e incondicional apoyo al desarrollo de este proyecto.

A los profesores y demás personas por sus aportes para realizar este proyecto de investigación.

CONTENIDO

INTRODUCCIÓN	12
1. DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RÍO DE ORO, CESAR “EMCAR”.	14
1.1 PLANTEAMIENTO DEL PROBLEMA.....	14
1.2 FORMULACIÓN DEL PROBLEMA.	14
1.3 OBJETIVOS.....	14
1.3.1 General.....	14
1.3.2. Específicos.....	15
1.4. JUSTIFICACIÓN.....	15
1.5 HIPÓTESIS.....	16
1.6 DELIMITACIONES.....	16
1.6.1 Geográficas.	16
1.6.2 Temporales..	16
1.6.3 Conceptuales.....	16
1.6.4 Operativa..	17
2 MARCO REFERENCIAL.	18
2.1 MARCO HISTÓRICO.....	18
2.1.1 Historia de la seguridad de la información.....	18
2.1.2 Antecedentes.....	20
2.2 MARCO CONCEPTUAL.....	22
2.3 MARCO CONTEXTUAL.....	26
2.3.1 La organización.....	26
2.4 MARCO TEÓRICO.....	27
2.4.1 Norma ISO/IEC 27001.....	27
2.4.2 Administración de la Seguridad.....	30
2.4.3 Análisis de Riesgos..	30
2.4.4 Políticas de Seguridad..	31
2.5 MARCO LEGAL.....	31
2.5.1 Constitución Política de Colombia.	31
3 DISEÑO METODOLÓGICO.	37
3.1 TIPO DE INVESTIGACIÓN.....	37
3.2. POBLACIÓN Y MUESTRA.....	37
3.3 TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN.....	37
3.3.1 Fuentes primarias.	37
3.3.2 Fuentes secundarias.....	37
4. PRESENTACIÓN DE RESULTADOS	38

4.1 IDENTIFICACIÓN DE AMENAZAS EXISTENTES EN LA EMPRESA A TRAVÉS DE LA NORMA ISO 27001.	40
4.1.1 Misión.	40
4.1.2 Visión.	40
4.1.3 Principios corporativos.	40
4.1.4 Valores institucionales.	41
4.1.5 Objetivos.	41
4.1.6 Estructura organizacional.	43
4.1.7 Objetivos de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar.	44
4.1.8 Cadena de valor de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar.	45
4.1.9 Proceso de Distribución de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.	45
4.1.10 Proceso Alcantarillado de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.	46
4.1.11 Proceso Acueducto de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.	47
4.1.12 Proceso Aseo de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.	48
4.1.13 Proceso Facturación de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.	49
4.1.14 Resultados de la entrevista.	50
4.1.15 Resultados de las encuestas.	51
4.1.16 Matriz de riesgos. Código identificador del riesgo.	61
4.2 DOMINIOS DE LA NORMA ISO 27001.	69
4.3 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RÍO DE ORO, CESAR, “EMCAR”, DE ACUERDO A LA NORMA ISO 27001.	73
CONCLUSIONES	123
RECOMENDACIONES	124
BIBLIOGRAFÍA	125
FUENTES ELECTRÓNICAS	127
ANEXOS	129

LISTA DE GRÁFICAS

Grafica 1. Estructura organizacional.....	43
Grafica 2. Objetivos EMCAR.....	44
Grafica 3. Cadena de valor de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar.	45
Grafica 4. Proceso de Distribución de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.....	46
Grafica 5. Proceso Alcantarillado de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.....	47
Grafica 6. Proceso Acueducto de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.....	48
Grafica 7. Proceso Aseo de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.....	49
Grafica 8. Proceso Facturación de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.....	50
Grafica 9. Utilización del equipo de cómputo para el desempeño de funciones.	52
Grafica 10. Perímetros de seguridad que protegen las áreas de los equipos de cómputo. ...	53
Grafica 11. Copias de seguridad de la información.	54
Grafica 12. Controles para el ingreso de personal.	55
Grafica 13. Mecanismos de seguridad.	56
Grafica 14. Aplicaciones con contraseña.	57
Grafica 15. Lineamientos para la seguridad de la información.	58
Grafica 16. Conocimiento de la existencia de una guía de políticas de seguridad de la información.	59
Grafica 17. La política de seguridad de la información está aprobada, establecida y publicada.	60
Grafica 18. Comité de seguridad de la información.	61

LISTA DE TABLAS

Tabla 1. Objetivos y actividades.	38
Tabla 2. Utilización del equipo de cómputo para el desempeño de funciones.	51
Tabla 3. Perímetros de seguridad que protegen las áreas de los equipos de cómputo.	52
Tabla 4. Copias de seguridad de la información.	53
Tabla 5. Controles para el ingreso de personal.	54
Tabla 6. Mecanismos de seguridad.	55
Tabla 7. Aplicaciones con contraseña.	56
Tabla 8. Lineamientos para la seguridad de la información.	57
Tabla 9. Conocimiento de la existencia de una guía de políticas de seguridad de la información.	58
Tabla 10. La política de seguridad de la información está aprobada, establecida y publicada.	59
Tabla 11. Comité de seguridad de la información.	60
Tabla 12. Probabilidad.	62
Tabla 13. Impacto.	62
Tabla 14. Marcador de riesgo para un riesgo específico.	62
Tabla 15. Riesgo.	63
Tabla 16. Matriz de riesgos EMCAR.	64
Tabla 17. Dominios Norma ISO 27001.	69

LISTA DE ANEXOS

Anexo A. ENTREVISTA A LA GERENTE DE LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR “EMCAR”	130
Anexo B. ENCUESTA A LA GERENTE DE LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR “EMCAR”	132
Anexo C. ENCUESTA AL PERSONAL DE LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR “EMCAR”	135
Anexo D. OFICIO SOLICITUD CAPACITACIÓN.	137
Anexo E. ACTA DE CAPACITACIÓN.	138
Anexo F. FOTOGRAFÍAS DE LA CAPACITACIÓN.	140
Anexo G. EVALUACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR “EMCAR”	141
Anexo H. CONSTANCIA CAPACITACIÓN Y ENTREGA DE LAS POLÍTICAS.	142

INTRODUCCIÓN

Actualmente toda empresa sea grande, mediana o pequeña, tienen implementado algún sistema de información para el manejo de sus activos, por esta razón han optado por utilizar normas nacionales e internacionales eficientes que permitan salvaguardar la información que hoy en día es lo más importante.

A medida que las empresas crecen, la tecnología y los sistemas de información deben avanzar significativamente de la mano con ella y cada día apoyarse más en los procesos de misión y visión para su fortalecimiento en el tiempo¹.

Toda organización se enfrenta a distintos tipos de amenazas de seguridad que incluyen: El fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación, entre otras más². Por lo tanto, es importante tener un buen manejo de la seguridad de la información de la empresa, utilizando las diferentes normas que puedan garantizar el uso adecuado de la misma, que para este caso se implementara la ISO 27001 que está enfocada en las políticas de seguridad de la información³.

Por esta razón, con la puesta en marcha del presente documento de Políticas de Seguridad de la información para la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”, se busca fortalecer el compromiso con los procesos de gestión responsable de la información; que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad, teniendo como eje el cumplimiento de los objetivos misionales.

El enfoque de esta investigación es cuantitativo y se fundamenta en un proceso deductivo, al plantear como hipótesis que las políticas de seguridad de la información contribuyen a dar un manejo adecuado de la información que se opera en la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar.

Teniendo en cuenta lo anterior, este proyecto busca dar respuesta a la pregunta ¿Con el diseño de las políticas de seguridad de la información, permitirá a la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”, proteger y salvaguardar su información en caso de pérdida o daño?, la cual se quiere comprobar en esta investigación.

¹ GIL PECHUÁN, Ignacio. Sistemas y Tecnologías de la Información para la Gestión. Madrid, McGraw-Hill, 1997.

² ANGARITA LÓPEZ, Liseth Tatiana. Diseño del plan de gestión de seguridad de la información para controlar el acceso a las áreas restringidas de la empresa Ingepec LTDA en la ciudad de Ocaña: Tesis de grado para especialización en auditoría de sistemas, 2014.

³ ISOTools. La norma ISO 27001 y la importancia de la gestión de la seguridad de la información. [En línea]. [Citado el 21 octubre de 2014]. Disponible en internet <<http://www.isotools.org/pdfs/Monografico-ISO-27001-ISOTools.pdf>>

Para tal fin se plantea desarrollar como objetivo diseñar las políticas de seguridad de la información de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar “EMCAR”, la cual permitirá a la organización definir de forma adecuada los lineamientos de seguridad.

1. DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RÍO DE ORO, CESAR “EMCAR”.

1.1 PLANTEAMIENTO DEL PROBLEMA.

La Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”, en la actualidad brinda un servicio muy importante a la comunidad, encargándose de suministrar los diferentes servicios públicos como son: Servicio de aseo, alcantarillado y de acueducto a toda la zona urbana del Municipio; a su vez cuenta con unas instalaciones para el manejo de la información, ya que es considerado como un activo importante para la organización.

Además se hicieron visitas a la entidad, donde se realizaron unas auditorias posteriores para conocer las diferentes amenazas en cuanto a la seguridad de la información, como resultado de la misma se encontraron hallazgos como: No hay un manejo adecuado de los equipos, no se realizan copias de seguridad, las contraseñas no se cambian periódicamente, no hay perfiles de usuario definidos para cada empleado, personas externas a la empresa pueden acceder a la información; teniendo en cuenta lo hallado se evidencia que en la empresa no existe un documento formal que exprese las políticas que debe tener la organización en cuanto a la seguridad de la información.

Por esta razón, la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar, contiene información muy valiosa, donde está registrado todos los datos de los usuarios del municipio a los cuales se les ofrece el servicio y pueden estar expuestos a una pérdida de información si no se cuenta con una política de seguridad.

Por tal motivo, se requiere proteger la información de la empresa de las diferentes amenazas que podrían generar traumatismos en el manejo; a su vez se debe garantizar que los datos están siendo manejados en un ambiente seguro, que no sean alterados y modificados.

1.2 FORMULACIÓN DEL PROBLEMA.

¿Con el diseño de las políticas de seguridad de la información, permitirá a la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”, proteger y salvaguardar su información en caso de pérdida o daño?

1.3 OBJETIVOS.

1.3.1 General. Diseñar las políticas de seguridad de la información de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar “EMCAR”.

1.3.2. Específicos. Identificar las amenazas existentes de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”, a través de la Norma ISO 27001.

Identificar cuales dominios de la Norma ISO 27001 son aptos para ser implementados en la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.

Elaborar un documento formal que contenga las políticas de seguridad de la información de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”, de acuerdo a la Norma ISO 27001.

1.4. JUSTIFICACIÓN.

Hoy en día vivimos en una sociedad donde uno de los principales activos de cualquier organización es la información, sin importar su tamaño o giro del negocio.

El factor humano junto con la tecnología, permite gestionar y manejar la información de las empresas. A medida que la tecnología va avanzando, de la misma forma se deberá alinear y sincronizar cada vez más a los objetivos y procesos del negocio, como soporte para su correspondiente cumplimiento⁴. En la actualidad, se puede evidenciar como las organizaciones han automatizado los diferentes procesos utilizando algún software o haciendo uso de la tecnología.

Como resultado del incremento de la dependencia de las organizaciones, respecto a la tecnología e interconectividad para el uso de la información en el ambiente comercial, cada vez está expuesta a una variedad más amplia y sofisticada de amenazas y vulnerabilidades⁵. A su vez estas amenazas pueden ser internas, externas, premeditadas, accidentales, entre otras. En muchos de los casos anteriormente se generan diversas pérdidas dentro de la organización, siendo las más difíciles de contrarrestar.

Por esta razón, la Empresa Comunitaria de Acueducto de Río de Oro, Cesar “EMCAR”, no tiene implementado las políticas de seguridad de la información, ya que no han tenido algún incidente de seguridad relativamente grave, lo cual comprueba que la entidad sigue siendo reaccionaria y no preventiva, tampoco cuenta con un plan de procedimientos internos para custodiar los datos, ni planes de acción para dar a entender la importancia del uso y manejo adecuado de la información.

⁴ VEGA BRICEÑO, Edgar Armando. Los sistemas de información y su importancia para las organizaciones y empresas. [En línea]. [Citado el 23 octubre de 2014]. Disponible en internet <<http://www.gestiopolis.com/Canales4/mkt/simparalas.htm>>

⁵ ALIAGA FLORES, Luis Carlos. Diseño de un sistema de gestión de seguridad de la información para un instituto educativo: Tesis de grado, Pontificia Universidad Católica del Perú, 2013.

Para que estos principios de seguridad de la información sean efectivos, es necesario implementar la Norma ISO/IEC 27001, para que forme parte de la cultura organizacional de la empresa y que implica el compromiso de todos los empleados vinculados a la gestión de la misma y así contribuir con los objetivos misionales.

Por último, el diseño de las políticas es crucial para en un futuro desarrollar y poner en funcionamiento un sistema de seguridad de la información en la empresa.

1.5 HIPÓTESIS.

Las políticas de seguridad de la información contribuyen al buen manejo y uso de la información, teniendo en cuenta que es el activo más importante de la misma.

Por lo tanto, se pretende diseñar las políticas de seguridad de la información para la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”, para garantizar la seguridad y veracidad de la información, contando con el apoyo y participación de los empleados y la Junta Directiva para la realización de dicho proyecto.

1.6 DELIMITACIONES.

1.6.1 Geográficas. El proyecto cubrirá la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”.

1.6.2 Temporales. El trabajo de grado conllevará un tiempo de cuatro (4) meses, tal como se programa en el cronograma de actividades.

1.6.3 Conceptuales. El proyecto que se plantea en el presente documento se enfoca a brindar una herramienta metodológica que sirva como modelo para la aplicación de un plan de acción para el tratamiento de los riesgos e implementar controles para detectar y dar respuesta oportuna a incidentes de seguridad de la información según la norma ISO 27001.

De igual forma, propiciar los fundamentos para elaborar estrategias de formación y toma de conciencia, que desarrolle competencias para la aplicación de la herramienta, también brindar una guía documental que plantee una metodología que permitan detectar y dar respuesta oportuna a los incidentes de seguridad; tomando como base la norma ISO 27001, haciendo referencia a modelar los procesos de buenas prácticas de seguridad de la información.

1.6.4 Operativa. Durante el desarrollo del proyecto de investigación es posible que se presente algunos inconvenientes como son: Escasas fuentes de información, debiendo orientar otras opciones, con base al criterio del director del trabajo de grado.

2 MARCO REFERENCIAL.

2.1 MARCO HISTÓRICO.

2.1.1 Historia de la seguridad de la información. La seguridad es un concepto que ha venido en constante evolución, desde tiempo remotos el hombre ha protegido y resguardado con celo sus conocimientos dado que son estos los que le proporcionan ventajas competitivas frente a los demás individuos de la sociedad. El concepto de seguridad de la información no es un tema nuevo, se puede partir desde los primeros intentos criptográficos que realizó el hombre en busca de la protección de información. Con el paso del tiempo y debido a los avances significativos que se han presentado en cuanto a tecnologías de información y comunicaciones el hombre se ha visto en la necesidad de crear cada vez sistemas más robustos que permitan salvaguardar el activo más valioso con el que cuentan las organizaciones “la información”, dado que, junto con este avance también se han desarrollado amenazas y delitos informáticos que están a la espera de cualquier descuido o vulnerabilidad para ser aprovechado en contra de las organizaciones⁶.

A continuación se realizará un resumen de aquellos sucesos más destacados a través de la historia que demostraron la vulnerabilidad de los sistemas como consecuencia de la no implantación de políticas de seguridad de la información. El 1 de enero de 1980 se fundamentan las bases de la seguridad de la información, en el año de 1980, James P. Anderson escribe un documento titulado “Computer Security Threat Monitoring and Surveillance” (Monitoreo de Amenazas de Seguridad Informática y Vigilancia). Lo más interesante de este documento es que James Anderson da una definición de los principales agentes de las amenazas informáticas.

En 1985 aparecieron los primeros Troyanos (caballo de troya), escondidos como un programa de mejora de gráficos llamado EGABTR y un juego llamado NUKE-LA que fueron los primeros virus conocidos en la historia, seguido en 1987 hace su aparición el virus Jerusalén o Viernes 13, que era capaz de infectar archivos .EXE y .COM, su primera aparición fue reportada desde la Universidad Hebrea de Jerusalén y ha llegado a ser uno de los virus más famosos de la historia.

El 3 de noviembre de 1988, equipos como VAX y SUN conectados a Internet se vieron afectados en su rendimiento y posteriormente se paralizaron afectando adicionalmente Bancos, Universidades e instituciones de gobierno, la causa fue un Gusano, desarrollado por Morris, recién graduado en Computer Science en la Universidad de Cornell.

⁶ ISCALA TOBITO, Nancy Auristela. Diseño de un protocolo de seguridad de la información del área financiera de la secretaria de educación departamental de Norte de Santander Ocaña: Tesis de grado para especialización en auditoría de sistemas, 2014.

En el año 2003, en Ginebra, se realiza por primera vez la Cumbre Mundial sobre la Sociedad de la Información. Bajo el lema amenazas y vulnerabilidades se celebró el primer día Internacional de Seguridad de la Información, que tuvo lugar en noviembre de 2006 en la Escuela Universitaria de Ingeniería Técnica de Telecomunicación EUITT de la Universidad Politécnica de Madrid y por último un suceso muy importante SEGURINFO Colombia 2011 XVI Congreso Interamericano de Seguridad de la Información, el encuentro se realizó con el objetivo de informar y discutir sobre temas de actualidad en la materia para sustentar las decisiones gerenciales en el ámbito de la Seguridad en la Información.⁷

Actualmente, ya en el siglo XXI, en un corto período de tiempo, el mundo desarrollado se ha propuesto lograr la globalización del acceso a los enormes volúmenes de información existentes en medios cada vez más complejos, con capacidades exponencialmente crecientes de almacenamiento y en soportes cada vez más reducidos.⁸ Antes de la aparición de las primeras redes de computadores, prácticamente toda la información sensible de una organización se guardaba en un formato físico: bodegas repletas de grandes archivadores y toneladas de papeles eran los encargados de guardar los datos de una empresa. Las principales amenazas a la seguridad de dicha información se podían encontrar en desastres naturales, y el robo de información era algo bastante complejo más que ahora. Pero con la aparición de la computación y el auge de las redes, la información comenzó a digitalizarse de una manera impresionante, y una bodega llena de archivadores con datos de una organización ahora podía resumirse al contenido de un disco duro de un equipo que podría ocupar menos de un metro cuadrado de superficie. Este avance en la tecnología, aparte de las múltiples ventajas en el procesamiento y análisis de la información, trajo consigo un nuevo problema al mundo de la informática. La información en formato digital, es más fácil de transportar, por lo que las posibilidades de hurtarla o alterarla no son despreciables.

La seguridad de la información es un conjunto de herramientas y procedimientos, tecnológicos, sociales y culturales que buscan proteger y defender nuestra información de cualquier agente interno y/o externo que pueda afectar cualquiera de sus tres principios básicos. Integridad, Confidencialidad y Disponibilidad. La seguridad no es un término estrictamente tecnológico; de nada servirá tener una red saturada de complejos Firewalls, sistemas de detección de intrusos, políticas y contraseñas complejas si el administrador de la red deja su contraseña escrita en un papel y pegada en una esquina del monitor, por lo que un descuido por parte de una persona puede ser fatal para la seguridad a nivel global de una organización.

Hasta hace un tiempo atrás, muchos creían que el villano de la información era el hacker, sin embargo, esto ha pasado a ser un mito de la informática. Muchas veces el enemigo puede estar dentro de la misma organización, y no necesariamente es un experto en

⁷ TIMETOAST. [En línea]. [Citado el 25 Septiembre de 2014]. Disponible en internet <<http://www.timetoast.com/timelines/historia-de-la-seguridad-informatica>>

⁸ TIMERIME. [En línea]. [Citado el 12 Septiembre de 2014]. Disponible en internet <<http://timerime.com/es/evento/1870578/Siglo+XXI+Procesamiento+de+datos/>>

programación ni un maestro en informática, uno de los errores humanos con respecto a la seguridad de la información es creer que todos los posibles factores de peligro de la información se encuentran en el exterior. Este error ha sido reafirmado por numerosas estadísticas que demuestran que un gran porcentaje de los problemas de seguridad se producen en el interior mismo de las organizaciones. Empleados insatisfechos, usuarios curiosos y por sobre todo poco conscientes del impacto que pueden tomar sus acciones en una red, pueden ser parte importante de los dolores de cabeza que los encargados de seguridad tienen.

La seguridad de la información es algo dinámico y que sufre una constante evolución. Cada día aparecen nuevas amenazas a la seguridad y así como aparecen nuevas amenazas, los expertos en seguridad se esmeran en crear nuevos programas, protocolos y equipos dedicados a mejorar la seguridad a nivel informático. En estos últimos años en cuanto a seguridad, sobre todo para la región de América Latina las empresas de tecnología han estado trabajando fuertemente en dos ámbitos. Ámbito tecnológico y el ámbito humano/social. Por el lado tecnológico han focalizado sus esfuerzos en el concepto de desarrollo seguro. Por el ámbito humano/social muchas organizaciones han iniciado campañas para generar conciencia de seguridad en las personas, campañas que buscan capacitar a los usuarios y profesionales del área en seguridad.

En resumen, es muy importante recordar que la seguridad no es un problema meramente tecnológico. Con la importancia que ha adquirido hoy en día la información, es necesario adoptar no solo una actitud, si no que un estilo de vida seguro. Debemos aprender a estar conscientes del valor de nuestra información, y usar en cada una de nuestras actividades diarias dicha conciencia. Sólo así tendremos posibilidades de ganar esta loca carrera entre las amenazas y los amenazados.⁹

2.1.2 Antecedentes.

2.1.2.1 Plan de Gestión de Seguridad de la Información basado en TIC'S para la Facultad de Ingeniería de Sistemas de la Escuela Politécnica Nacional. Mireya Isabel Vasco Aguas y Mercedes Estefanía Verdezoto Saltos. Quito, Ecuador. 2009. El presente plan constituye el establecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) que consiste en establecer la política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la Facultad, para ella se contempla los requerimientos de seguridad basándose en el estudio de los riesgos de seguridad y en la recopilación y estudio de los documentos organizacionales y legales para

⁹ MONTENEGRO, Luis. Artículo: Seguridad de la Información: Más que una actitud, un estilo de vida. [En línea]. [Citado el 28 Septiembre de 2014]. Disponible en internet <<http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/>>

la selección de los objetivos de control y controles incluidos en los estándares ISO/IEC 27001:2005 e ISO/IEC 17799:20052. ¹⁰

2.1.2.2 Plan de Propuesta para la Implantación de la Norma de Seguridad Informática ISO 27001:2005, para el Grupo Social Fondo Ecuatoriano Populorum Progressio (GSFEPP). Oscar Eduardo Campaña Tenesaca. Quito, Ecuador. 2010. Implantar un Sistema de Gestión de Seguridad de la Información (SGSI), es de mucha ayuda para entidades que basan su sostenibilidad en la claridad y respaldo de la información que esta genera en el aspecto de manejo financiero y de proyectos, ya que así seguirán recibiendo financiamiento de entidades extranjeras, pero las dificultades aparecen duramente la explicación del proceso de análisis de riesgos y vulnerabilidades y se intensifican con la necesidad de colaboración de una parte importante de las personas de la empresa con la dirección al frente, esto se debe a la cultura poco participativa de nuestra sociedad. ¹¹

2.1.2.3 Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa Comware S.A. en la ciudad de Quito, aplicando la norma ISO/IEC 27001. Diego Calderón y David Sánchez. Quito, Ecuador. 2012. El presente proyecto de titulación tiene como objetivo el diseño de un Sistema de Gestión de Seguridad de la Información para la empresa Comware S.A. en la ciudad de Quito basado en la Norma ISO 27001, con el fin de lograr un esquema que sirva como guía para la posterior implementación y certificación de la Norma en la empresa. Se realizó un análisis por medio de varios software que permitieron ver algunas falencias dentro de los sistemas que se manejan en la empresa y de esta forma realizar un análisis de las amenazas que se encuentran latentes en los sistemas informáticos. ¹²

2.1.2.4. Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial. María Gabriela Hernández Pinto. Quayaquil, Ecuador. 2006. El contenido de este trabajo ayudará a las organizaciones comerciales a tener una concienciación permanente de mantener seguros sus activos, teniendo en cuenta que la

¹⁰ VASCO AGUAS, Mireya I y VERDEZOTO SALTOS, Mercedes E. Plan de Gestión de Seguridad de la Información basado en TIC'S para la Facultad de Ingeniería de Sistemas de la Escuela Politécnica Nacional. Quito, Ecuador.. 2009. 226 h. Escuela Politécnica Nacional. [en línea]. <<http://bibdigital.epn.edu.ec/handle/15000/4370?mode=full> >

¹¹ CAMPAÑA TENESACA, Oscar E. Plan de Propuesta para la Implantación de la Norma de Seguridad Informática ISO 27001:2005, para el Grupo Social Fondo Ecuatoriano Populorum Progressio (GSFEPP). Quito, Ecuador. 2010. 207h. [en línea] <<http://dspace.ups.edu.ec/handle/123456789/4468?mode=full>>

¹² CALDERÓN, Diego y SÁNCHEZ, David. Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa Comware S.A. en la ciudad de Quito, aplicando la norma ISO/IEC 27001. Quito, Ecuador. 2012. 216h. Universidad Politécnica Salesiana. [en línea] <[21](https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCwQFjAA&url=http%3A%2F%2Fdspace.ups.edu.ec%2Fbitstream%2F123456789%2F3901%2F1%2FUPS-ST000906.pdf&ei=GDsSUR0EJaa02wWI7YCYAQ&usg=AFQjCNFsKFoVxj06G_YJYJx906JAEUBptQ&si g2=CxONXw8ZwdZkaOorjVnyxw&bvm=bv.50768961,d.b2I></p></div><div data-bbox=)

palabra activo son todos los recursos informáticos o relacionados con éste para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección¹³.

La meta de obtener un nivel considerable de seguridad se logrará con la propuesta que ofrece este proyecto mediante el “Diseño de un Plan Estratégico de Seguridad de Información” que puede ser aplicado por entidades dedicadas a cualquier tipo de actividad comercial que se proponga llevarlo a cabo.

2.1.2.5 Diseño de Políticas de Seguridad de la Información para la Oficina de Archivo y Correspondencia de la Universidad Francisco de Paula Santander Ocaña. En la presente investigación se realizó el diseño de políticas de seguridad de la información para la oficina de archivo y correspondencia de la UFPSO siguiendo una metodología con miras a la mejora continua, donde en un inicio se efectuó el análisis de la situación actual de la oficina en materia de seguridad para esto se contó con técnicas de recolección de información como encuestas, análisis y evaluación de riesgos y auditorías.

Identificado las amenazas latentes se procedió con un proceso de planificación donde se estudió las diferentes normas existentes para la gestión de la seguridad de la información y con esto poder decidir qué modelo seguir para el diseño de las políticas. Se continuó documentando el modelo elegido para poder tener las pautas que permitan dictaminar los controles y la creación de un documento formal que contenga las políticas de seguridad de la información. Por último se realizó un proceso de verificación de controles donde se pretende evaluar y confirmar que efectivamente las políticas dictadas cumplen con su propósito de mitigar los riesgos detectados al interior de la oficina, permitiendo así que se preserven los tres elementos principales de la información. Integridad, confidencialidad y disponibilidad.¹⁴

2.2 MARCO CONCEPTUAL.

En el presente trabajo investigativo, es necesario generar un marco que permita definir conceptos que son relevantes para el tema de seguridad de la información.

Como se percibirá a continuación se han definido fundamentales a saber: seguridad informática, seguridad de la información e inseguridad de la información.

La necesidad de preservar y custodiar de manera efectiva y adecuada la información al interior de una organización, y más aún, en la transmisión de la misma, es un tema que se convierte en un requisito funcional dentro de las políticas organizacionales; es un factor

¹³ HERNÁNDEZ PINTO, María Gabriela. Tesis Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial, Escuela Superior Politécnica del Litoral.2006. Guayaquil, Ecuador.

¹⁴ REYES CASADIEGOS, María Teresa. Álvarez Cabrales, Andru. Tesis Diseño de Políticas de Seguridad de la Información para la Oficina de Archivo y Correspondencia de la Universidad Francisco de Paula Santander Ocaña. Universidad Francisco de Paula Santander Ocaña. 2013. Colombia

determinante para la credibilidad de la organización frente a sus clientes y usuarios, y un paso de adelanto hacia la excelencia en la calidad de sus procesos.

El riesgo en la información ha aumentado a medida que ésta ya no es controlada en un solo lugar como lo era un sistema centralizado para las organizaciones; ahora la información se distribuye de tal forma que se encuentra en varios lugares como lo son sedes o sucursales, por ésta razón se desconoce qué información puede ser almacenada en puestos específicos de trabajo, que muchas veces son usados como equipos personales en las organizaciones.

Técnicamente es imposible lograr sistemas informáticos ciento por ciento seguros, "El único sistema realmente seguro es aquel que esté desconectado de la línea eléctrica, incrustado dentro de un bloque de concreto, encerrado herméticamente en una habitación revestida de plomo y protegido por guardias armados y aun así, se puede dudar",¹⁵ pero buenas prácticas de seguridad evitan posibles daños y problemas que pueden ocasionar las incidencias de seguridad de la información en la organización.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma y que posea valor para la organización. Cualquier cosa que tenga que ver con la organización.¹⁶

Administración de Usuarios. Son los parámetros definidos para la asignación y uso de los recursos informáticos.

Autorización. Proceso de determinar las actividades permitidas para ser ejecutadas por un usuario.

Control. Las políticas, los procedimientos, las prácticas y las estructuras organizativas admitidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Documentos. Son documentos los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares.

Integridad. Mantenimiento de la exactitud y veracidad de la información.

¹⁵ GÓMEZ VIEITES, Álvaro., Enciclopedia de la Seguridad Informática, Alfa omega Grupo editor, México, Primera Edición, 2007.

¹⁶ NTC ISO/IEC 5411 - 1:2006. Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la tecnología de la información y las comunicaciones. Parte 1: Conceptos y modelos para la gestión de la tecnología de la información y las comunicaciones (ISO/IEC 13335-1:2004).

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

Amenaza. Declaración intencionada de hacer un daño (Virus, acceso no autorizado, robo) Eventos naturales que pueden desencadenar daños materiales o pérdidas inmateriales en sus activos. Las amenazas se pueden materializar y transformarse en agresiones.

Perfil de Usuario. Es el permiso asignado a cada usuario para el uso de cada uno de los sistemas operacionales, bases de datos y aplicativos.

Política de seguridad. Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Seguridad de la Información. La seguridad de la información se entiende como la preservación de la información a través del tiempo, aplica las siguientes características:

Confidencialidad. Acceso a la información por parte únicamente de quien está autorizado. Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.¹⁷

Integridad. Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: Acceso a la información y/o los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

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

Auditabilidad. Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la duplicación. Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

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

¹⁷ Ibid, p. 10

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

Confiabilidad de la Información. Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

ISO/IEC 27001. Es un estándar para la seguridad de la información; Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información.

Sistema de Información. Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información. Se refiere al hardware y software operado por el organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Universidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Comité de Seguridad de la Información. El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

Responsable de Seguridad Informática. Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

Evento de Seguridad de la Información. Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.¹⁸

Incidente de Seguridad de la Información. Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Sistema de Gestión de la Seguridad de la Información (SGSI): Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

¹⁸ Ibid., p. 11

Red de Computadoras: También llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Red LAN. Local Área Network (Red de área local)

Red WAN. Wide Área Network (Red de área amplia)

Riesgo. Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Rol. Se refiere al papel, área de responsabilidad y actividades que debe desempeñar una persona para contribuir al cumplimiento de la meta organizacional de proteger la información. El criterio en cuanto a la capacidad para desempeñar determinado rol está determinado por la posesión por parte del funcionario, del nivel de destrezas requeridas para cada rol.

Vulnerabilidad. Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

2.3 MARCO CONTEXTUAL.

2.3.1 La organización.

Administración Pública Cooperada Empresa Comunitaria de Acueducto de Río de Oro, es una Empresa descentralizada de la Alcaldía Municipal de Río de Oro-Cesar formada mediante acta de asamblea general de constitución N° 001 del 25 de Octubre del 2004, creando a la Administración Pública Cooperada Empresa Comunitaria de Acueducto de Río de Oro “A.P.C EMCAR ESP”, Entidad prestadora de los servicios públicos de Acueducto, Alcantarillado y Aseo.¹⁹

Servicio de Agua Potable: El sistema de acueducto del municipio de Río de Oro se abastece de tres fuentes mediante bocatomas: La Toma de la Cordillera, Las Marcelina y El Gitano son las tres que se encuentran en uso en este momento;

El casco urbano del municipio de Río de Oro tiene un sistema de acueducto que opera por gravedad desde el desarenador hasta la Planta de Tratamiento, cuenta con tres, uno por cada fuente de captación, el cual opera normalmente.

¹⁹ EMCAR. (2015). Empresa Comunitaria de Acueducto de Río de Oro, Cesar. www.emcar.com.co.

La Empresa cuenta con una planta de tratamiento compacta tipo Pulsator (degremont) de 18 litros por segundo de capacidad, la Planta de Tratamiento existen tres tanques de almacenamiento semienterrados, ubicados debajo del edificio de operaciones con capacidad de:

Tanque No. 1: 246.50 m³.

Tanque No. 2: 227 m³.

Tanque No. 3: 217 m³.

Servicio de Alcantarillado: El Sistema de Alcantarillado del municipio de Río de Oro no responde a una planeación correctamente ejecutada. Las variaciones que se han hecho a las redes se ejecutan más como soluciones puntuales.

Servicio de Aseo: La limpieza, barrido de vías y áreas públicas del municipio de Río de oro en el área urbana se presta en un 100% y en los Centros poblados de Montecitos, el Márquez, los Ángeles, Platanal y Morrison, así como también la Recolección, el transporte y la disposición final de los residuos sólidos que se producen.

Cabe resaltar que la limpieza y disposición final de los residuos sólidos de los Centros Poblados se realiza a través de convenios Institucionales con la Alcaldía Municipal.

Servicio de Laboratorio: Toma de muestras de fisicoquímicas y microbiológicas de agua tratada.

2.4 MARCO TEÓRICO.

Desde una óptica teórica propiamente dicha (sin tener en cuenta la normatividad y los estándares mencionados en los capítulos anteriores), se ha escrito muy poco sobre la seguridad de la información y su papel desempeñado dentro de la organización; por eso, en éste marco se pretende mostrar los aportes que han enriquecido los estándares de prácticas de seguridad de la información, y desde la perspectiva de los autores, esbozar un posible direccionamiento de la norma ISO 27001,²⁰ desde el punto de vista de la aplicación de la guía de buenas prácticas de seguridad de la información -propuesto y desarrollado - en el proyecto.

2.4.1 Norma ISO/IEC 27001. Es un estándar internacional que mejora la seguridad de la información en las organizaciones que deciden implantar un Sistema de Gestión en Seguridad de la Información. Durante este post vamos a hablar sobre el control que se debe tener en cuenta a la hora de acceder a los sistemas operativos de la organización.²¹

²⁰ Norma Técnica NTC ISO/IEC 27001:201, Sistemas de Gestión de la Seguridad de la Información (SGSI).

²¹ TORO Raquel, ISO 27001 ¿Cómo mejorar la seguridad de la información en las organizaciones. [En línea]. [Citado el 20 Octubre de 2014]. Disponible en internet <<http://www.pmg-ssi.com/2014/10/iso-27001-como-mejorar-la-seguridad-de-la-informacion-en-las-organizaciones/>>

Por la función que realizan los sistemas operativos, estos suelen resultar críticos en el funcionamiento de las aplicaciones. Por lo que surge la necesidad de controlar el acceso mediante una configuración del sistema.

Según establece la norma **ISO 27001**, es recomendable tener definido un procedimiento que controle la entrada en los sistemas operativos, donde se debe indicar la gestión de todos los eventos que se encuentren asociados. Todo el proceso de debe ser lo más confidencial posible, para lograrlo no se debe mostrar información o ayuda alguna a la hora de acceder al sistema operativo de la organización. Otra cosa a tener en cuenta es el registro de todos los intentos de acceso al sistema, tanto los que se produzcan exitosamente como los fallidos y si se alcanza un número determinado de intentos fallidos se interrumpa inmediatamente el proceso.

Cada uno de los usuarios del sistema debe tener su propio identificador, de uso exclusivo que le sirva para poder asignar las diferentes responsabilidades sobre las acciones que han quedado registradas. Si se dispone de un identificador que se encuentra asociado a diferentes grupos de personas, este grupo debe ser autorizado por la alta dirección de la organización y se deben implicar un mínimo de controles de monitorización adicionales. El control que se lleve a cabo para la autenticación del usuario debe ir en concordancia con la importancia de los datos que deba manejar y el tratamiento que se proporciona para que puedan acceder a estos.

Si la autenticación del usuario es mediante contraseña, se tiene que establecer una política de gestión que asegure la eficacia y la fortaleza de esta. Las cosas más importantes a tener en cuenta en estos casos son:

Definir un procedimiento de registro de nuevos usuarios, así como la retirada de este una vez ya no esté disponible.

Los usuarios deben disponer de un identificador personal, dependiendo de su cargo en la empresa.

Restringir el uso de privilegios, que deben ser otorgados según las necesidades de uso que tengan.

Se debe definir un procedimiento de asignación de contraseñas.

Revisar los derechos de acceso de los usuarios de forma regular, por si cambia algo tenerlo actualizado.

En cada uno de los equipos existen aplicaciones que solo pueden ser manejadas por el administrador del sistema, que tiene la capacidad de invalidar los controles de acceso al mismo. La utilización de estos programas debe estar perfectamente controlada y restringida. Para ello se pueden usar controles que limiten el uso y disminuyan la utilización de recursos al mínimo número de usuarios disponibles, se pueden segregar las tareas pendientes y se deben registrar todas las acciones realizadas.

Se deben realizar unos controles básicos de seguridad que pueden equivaler a la desconexión de la sesión de usuario después de cierto tiempo de inactividad. Se debe cerrar por completo la aplicación o recurrir a un protector de pantalla protegido con contraseña. Se debe limitar el tiempo de conexión, incluye sin que haya periodo de inactividad, con esto se controlan los tiempos habituales de realización de las diferentes actividad y se puede prevenir la utilización no autorizada del sistema.

En conclusión hacia esto poder hacer el siguiente resumen. El principal objetivo es prevenir el acceso no autorizado al sistema de la organización y para ello se deben de seguir una serie de pautas básicas, las cuales son recomendadas a la hora de implantar un Sistema de Gestión de la Seguridad de la Información basado en la norma **ISO-27001** :

Se deben establecer controles de acceso a los sistemas operativos de la organización. El procedimiento a seguir para entrar en el sistema debe seguir una serie de reglas básicas de información sobre el sistema operativo.

Identificación única para cada usuario, que corresponda con el cargo que tenga en la organización para poder generar las responsabilidades.

Establecer los suficientes controles para gestionar las contraseñas. Se deben modificar cada cierto tiempo, además se debe controlar las nuevas contraseñas y las obsoletas.

Se deben restringir la utilización de programas informáticos que invalida controles.

Se deben cerrar las sesiones en un periodo de tiempo estipulado si no se está produciendo actividad.

Limitar el tiempo de conexión para reforzar la seguridad de las aplicaciones.

Se debe llevar a cabo un control exhaustivo del acceso a las aplicaciones que se ocupan de los activos de la organización. Este control debe permitir el acceso solo de los usuarios autorizados según la política de privilegios que se encuentre perfectamente definida.

Dentro de cada aplicación utilizada por la empresa, se debe controlar todos los posibles accesos a dichas aplicaciones. La norma ISO 27001 puede implementar los controles necesarios que garanticen el respeto de los privilegios que determinan acciones, como se deben crear y ejecutar, insertar, modificar o borrar la información o consultar todos los datos de alto nivel de privacidad de la organización. Otro factor importante es controlar que todas las aplicaciones de la organización se conectan y con qué privilegios. La salida de la información hacia otras aplicaciones debe estar registrada para poder llevar a cabo su monitorización.

La organización debe disponer de alguna aplicación que se encargue de la información de alto nivel de sensibilidad y que requiera que los equipos de acceso encuentren un entorno aislado, este aislamiento puede ser:

Físico: se llevar a cabo en un equipo exclusivamente.

Lógico: se comparte recursos mediante aplicaciones de confianza.

2.4.2 Administración de la Seguridad. Las buenas prácticas de administración indican que el establecimiento claro de la misión de una organización es indispensable para que todos los funcionarios ubiquen sus propios esfuerzos y los direccionen en bien de la misma. [Glueck, W. – Lawrence, J, Business Policy and Strategic Management -Hill, 1984], además permite elaborar políticas operativas que facilitan el cumplimiento de la misión de la organización, que pueden entenderse como reglas que hay que seguir obligatoriamente.

Es usual que la alta gerencia cometa errores en cuanto a la seguridad de la información de sus organizaciones, como por ejemplo suponer que los problemas desaparecen si se ignoran, no entender cuánto dinero vale su información y que tanto depende la organización de ella, no lidiar con los aspectos operacionales de la seguridad, no entender la relación que existe entre la seguridad y los problemas de funcionamiento y marcha de la organización, entre otros. Si la administración empresarial propone una misión para direccionar estratégicamente la organización es posible hacer una analogía con la “administración de la seguridad”, y es posible entonces ejecutar una “Misión de Seguridad”, que solucione las falencias, ubicando la seguridad informática al mismo nivel que otras actividades sustantivas de la organización, elaborando un plan de seguridad informática clara, promulgando políticas que se derivan de dicha misión y determinando que mecanismos se requieren para implementar esas políticas.²²

2.4.3 Análisis de Riesgos. Un paso intermedio entre la administración de la seguridad, - que desemboca en la generación del plan estratégico de seguridad (misión de seguridad)- , y las políticas de seguridad, es el análisis de riesgos de la información dentro de la organización; es aquí donde "se analiza una metodología práctica para el desarrollo de planes de contingencia de los sistemas de información, que comprende: la identificación de riesgos, calificación del impacto del mismo si se hiciera realidad, evaluación del impacto en los procesos críticos y la creación de estrategias de contingencias".²³

Salvaguardar la confidencialidad, la integridad, la autenticidad y la disponibilidad de la información es la característica que en el fondo define el modelo que se quiere diseñar en el presente proyecto. Aunque estas características soportan como tal la seguridad de la información. “No todas deben estar vigentes simultáneamente, ni tienen toda la misma importancia en todas las circunstancias”.²⁴ Existen casos de aplicación en que en ocasiones es más importante la confidencialidad que la disponibilidad,

²² DALTABUIT GODAS Enrique, VÁSQUEZ José de Jesús, La seguridad de la información”. Limusa Noriega Editores, 2007. p. 215

²³ NIMA RAMOS Jonathan D, Guía para la elaboración de planes de recuperación para sistemas de información empresarial y de negocios, Universidad de Plura, 2014.

²⁴ DALTABUIT GODAS Enrique, VÁSQUEZ José de Jesús, La seguridad de la información”. Limusa Noriega Editores, 2007. p. 26

otros casos en que la información debe ser auténtica. Debe determinarse en qué casos, cuáles de las propiedades son necesarias o importantes.

La seguridad de la información, como disciplina, trata precisamente de establecer metodologías para determinar cuáles de las cuatro características son deseables en alguna circunstancia y de encontrar la forma de lograr que se apliquen.

En el proceso de análisis de riesgos de la información se pueden diferenciar dos módulos: a) La Evaluación del riesgo, orientado a determinar los sistemas de información y sus componentes, que pueden ser afectados directa o indirectamente por agentes externos, y b) La Gestión del riesgo, que implica la identificación, selección, aprobación y administración de las defensas para eliminar, o reducir a niveles aceptables, los riesgos evaluados. En conclusión, su papel es reducir la posibilidad de que una amenaza ocurra, si ocurre, limitar su impacto, eliminar la vulnerabilidad existente y retroalimentar para futuras eventualidades.

2.4.4 Políticas de Seguridad. Posterior al establecimiento de la misión de seguridad, se requiere redactar las políticas en las que se basará el cumplimiento de la misión. La importancia de la implantación de políticas radica en que sin ellas “no se tiene un marco de referencia general de seguridad, puesto que permiten definir los procedimientos y herramientas necesarias del sistema de seguridad”.²⁵

Los beneficios del establecimiento de las políticas de seguridad de la información ayudan a tomar decisiones sobre otros tipos de política empresarial (propiedad intelectual, destrucción de información, etc.), que al final de cuentas redundan en una estructura de calidad de servicio, seguridad en el servicio y dispone un ambiente propicio para suministrar una guía, ya que si ocurre un incidente, las políticas constituyen un marco referencial sobre quién hace qué acciones que minimicen el impacto de los mismos.

2.5 MARCO LEGAL.

2.5.1 Constitución Política de Colombia. Ley Estatutaria No. 1581 por la cual se dictan disposiciones generales para la protección de datos personales, publicada el pasado 17 de Octubre de 2012 por el Congreso de Colombia.²⁶

La Ley “tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a

²⁵ DALTABUIT GODAS Enrique, VÁSQUEZ José de Jesús, La seguridad de la información”. Limusa Noriega Editores, 2007. p. 221.

²⁶ CONSTITUCIÓN POLÍTICA DE COLOMBIA, Ley Estatutaria 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013.

que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma”.

Artículo 1°. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Artículo 2°. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

- A.** A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.
- B.** Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley;
- C.** A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;
- D.** A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;
- E.** A las bases de datos y archivos de información periodística y otros contenidos editoriales;
- F.** A las bases de datos y archivos regulados por la Ley 1266 de 2008;
- G.** A las bases de datos y archivos regulados por la Ley 79 de 1993.

Parágrafo. Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.

Artículo 3°. Definiciones. Para los efectos de la presente ley, se entiende por:

- A. Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;
- B. Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento;
- C. Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;
- D. Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;
- E. Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;
- F. Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento;
- G. Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Artículo 4°. Principios para el Tratamiento de datos personales. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

- A. Principio de legalidad en materia de Tratamiento de datos:** El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;
- B. Principio de finalidad:** El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;
- C. Principio de libertad:** El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;
- D. Principio de veracidad o calidad:** La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;
- E. Principio de transparencia:** En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;
- F. Principio de acceso y circulación restringida:** El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley; Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

G. Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

H. Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

Artículo 19. Autoridad de Protección de Datos. La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

Parágrafo 1°. El Gobierno Nacional en el plazo de seis (6) meses contados a partir de la fecha de entrada en vigencia de la presente ley incorporará dentro de la estructura de la Superintendencia de Industria y Comercio un despacho de Superintendente Delegado para ejercer las funciones de Autoridad de Protección de Datos.

Parágrafo 2°. La vigilancia del tratamiento de los datos personales regulados en la Ley 1266 de 2008 se sujetará a lo previsto en dicha norma.

Artículo 20. Recursos para el ejercicio de sus funciones. La Superintendencia de Industria y Comercio contará con los siguientes recursos para ejercer las funciones que le son atribuidas por la presente ley:

A. Los recursos que le sean destinados en el Presupuesto General de la Nación.

Artículo 21. Funciones. La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:

A. Velar por el cumplimiento de la legislación en materia de protección de datos personales;

B. Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos;

C. Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva;

- D.** Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementará campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos;
- E.** Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley;
- F.** Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones.
- G.** Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos;
- H.** Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento;
- I.** Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional;
- J.** Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personajés;
- K.** Las demás que le sean asignadas por ley.

Artículo 25. Definición. Reglamentado por el Decreto Nacional 886 de 2014 El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.

El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.

Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley.

Parágrafo. El Gobierno Nacional reglamentará, dentro del año siguiente a la promulgación de la presente ley, la información mínima que debe contener el Registro, y los términos y condiciones bajo los cuales se deben inscribir en este los Responsables del Tratamiento.

Artículo 26. Prohibición. Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.

Esta prohibición no regirá cuando se trate de:

- A.** Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia;

- B.** Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública;
- C.** Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;
- D.** Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;
- E.** Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular;
- F.** Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Parágrafo 1°. En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Parágrafo 2°. Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008.

3 DISEÑO METODOLÓGICO.

3.1 TIPO DE INVESTIGACIÓN.

La presente investigación tiene como propósito diseñar las políticas de seguridad de la información para la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”, que ayudará a mejorar los procesos que presenten alguna amenaza relacionada con la información, por lo tanto se hace uso de una investigación cuantitativa y se fundamenta en un proceso deductivo que permitirá dar solución al problema planteado en la empresa objeto de estudio.

3.2. POBLACIÓN Y MUESTRA.

La población a estudiar para la realización de la investigación está conformada por los integrantes del Área Administrativa, Gerente, Contador Público, Auxiliar Contable, Auxiliar Administrativo y Auxiliar Comercial.

Para la realización de la investigación se tomó como muestra el total de la población el 100%, debido a que todos conforman el grupo de trabajo y es fácilmente abarcarlos.

3.3 TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN.

3.3.1 Fuentes primarias.

Entrevista a la Gerente de la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”.

Encuesta a la Gerente de la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”.

Encuesta al personal administrativo de la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”.

Visita de observación y aplicación de los instrumentos de recolección de la información en la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”.

3.3.2 Fuentes secundarias.

Soporte en leyes, normas y estándares relacionados con la seguridad de la información, administración y control de riesgos.

4. PRESENTACIÓN DE RESULTADOS

Para el cumplimiento de los objetivos planteados, se efectuaron las siguientes actividades, evidenciando de esta manera las amenazas a las que está expuesta la empresa, cuyo objeto es de estudio para la realización del proyecto.

Tabla 1. Objetivos y actividades.

	OBJETIVOS ESPECÍFICOS	ACTIVIDADES	RESULTADO/ENTREGABLE
4.1	Identificar las amenazas existentes de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”, a través de la Norma ISO 27001.	<ol style="list-style-type: none"> 1. Inspección a cada una de las áreas administrativas de la empresa como son: Gerencia, Revisoría Fiscal, Contabilidad, Secretaria, Tesorería y Facturación. 2. Aplicación de las técnicas e instrumentos de recolección de evidencias, las cuales fueron realizadas de la siguiente manera: Entrevista a la Gerente y encuestas al Revisor Fiscal, Contador Público, Auxiliar, Contable, Auxiliar Comercial y la secretaria. 	<p>Como resultado de la aplicación de los instrumentos como: Entrevista y encuesta al personal administrativo de EMCAR, los cuales arrojaron información primordial que ayudaron al cumplimiento de este objetivo; mostrando así la cantidad de amenazas a las que enfrentan la organización día a día.</p> <p>Para este caso la cantidad de riesgos fueron catorce (14), los cuales muestran un código del riesgo, la causa, descripción, la probabilidad, el impacto, Rango (probabilidad por impacto), acciones, señales y responsables, donde se debe calificar el nivel del riesgo de acuerdo al rango y debe ser identificado por un color, el cual dio como resultado un nivel Alto (Rojo) (Ver Tabla 12. Matriz de Riesgos).</p>
4.2	Identificar cuales dominios de la Norma ISO 27001 son aptos para ser implementados en la Empresa	<ol style="list-style-type: none"> 1. Consultar la Norma ISO 27001. 2. Identificar los dominios aptos para aplicar a la empresa de 	<p>Para este objetivo se hizo un estudio de la Norma ISO 27001, el cual se utilizaron en los siguientes dominios:</p>

	Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.	acuerdo a la Norma ISO 27001.	<p>Política de Seguridad de la Información.</p> <p>Organización de la Seguridad de la Información.</p> <p>Seguridad de los Recursos Humanos.</p> <p>Gestión de Activos.</p> <p>Control de Acceso.</p> <p>Seguridad Física y Ambiental.</p> <p>Seguridad de las Operaciones.</p> <p>Seguridad de las Comunicaciones.</p> <p>Gestión de Incidentes de Seguridad de la Información.</p> <p>Aspectos de Seguridad de la Información de la Continuidad del Negocio.</p> <p>Cumplimiento.</p>
4.3	Elaborar un documento formal que contenga las políticas de seguridad de la información de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”, de acuerdo a la Norma ISO 27001.	<ol style="list-style-type: none"> 1. Aplicar los pasos sugeridos en la norma para el desarrollo del documento. 2. Crear el documento con las políticas de seguridad para la empresa objeto de estudio. 	El documento de las políticas de seguridad de la información para la empresa EMCAR tiene como fin establecer una cultura e indicar el conjunto de instrucciones o normas generales necesarias para la operación y buscar mejor disponibilidad, integridad y confiabilidad de la información

Fuente: Autores del proyecto.

4.1 IDENTIFICACIÓN DE AMENAZAS EXISTENTES EN LA EMPRESA A TRAVÉS DE LA NORMA ISO 27001.

En este objetivo se aplicaron los instrumentos de recolección de la información del área administrativa de la empresa, los cuales dieron como resultado información fundamental para el desarrollo de los objetivos propuestos.

Teniendo en cuenta, que para una investigación de tipo cuantitativo, los instrumentos que se usaron fue la entrevista y la encuesta.

Analizando la información obtenida, se evidenció que la organización tiene un nivel alto de amenazas que originan los riesgos, a los cuales se ven expuestos permanentemente, los cuales comprometen las características de la seguridad de la información que son: Disponibilidad, integridad y confidencialidad. Con el objetivo de apoyar la seguridad de dicha información se plantea el diseño de las Políticas de Seguridad de la Información.

4.1.1 Misión. Mejoraremos la calidad de vida de nuestros usuarios, satisfaciendo sus necesidades de agua potable y saneamiento básico, con conciencia ambiental, generando desarrollo para el municipio y valor para nuestros socios, soportados en la efectividad del servicio y el bienestar de nuestra gente.

4.1.2 Visión. Consolidarnos como una empresa comunitaria modelo y líder en la prestación del servicio integral de acueducto y saneamiento básico en el municipio y la provincia, con inspiración para el desarrollo de nuevos negocios complementarios, para el 2018 ser una empresa de ejemplo y altamente sostenible.

4.1.3 Principios corporativos. Calidad En cumplimiento de los servicios requeridos por los usuarios y público en general.

Eficacia. En el desarrollo de los procesos y procedimientos que se realicen.

Preservación del Medio Ambiente. Como parte social de la Empresa en la calidad de vida del ser humano.

Cordialidad y Amabilidad. En atención del público, usuarios y en toda las relaciones humanas.

Lealtad de Competencias. Al establecer y promover sanas estrategias de acción dentro de las normas establecidas

4.1.4 Valores institucionales. LA CALIDAD, EL RESPETO, LA ETICA, LA SENSIBILIDAD SOCIAL, EL LIDERAZGO, y EL COMPROMISO son pilares de la actitud y desarrollo de las actividades que al interior y hacia el exterior de la empresa se realizan.

Calidad: Resultado de una serie de procesos que llevan a un desarrollo oportuno y efectivo de cada acción en la organización.

Respeto: Capacidad de aceptar los diferentes criterios y actitudes dentro de la filosofía de la organización

Ética: Comportamiento individual y colectivo basado en la honestidad, lealtad y transparencia que hacen de EMCAR una organización integral.

Sensibilidad social: Conciencia de solidaridad y servicio, identificándonos con los problemas sociales y económicos de la comunidad, atendiendo sus necesidades, contribuyendo al mejoramiento de la calidad de vida.

Liderazgo: Capacidad de gestión organizacional para el logro de la excelencia en la prestación del servicio

Compromiso: Actitud positiva, participativa y responsable para el logro de los objetivos de la organización en el cual cada persona aporta lo mejor de sí misma con gran sentido de pertenencia.

4.1.5 Objetivos.

Proporcionar al interior de la organización un cambio cultural positivo.

Suministrar a nuestros usuarios agua potable de conformidad con la normativa legal vigente.

Ofrecer un servicio confiable de acuerdo con las condiciones preestablecidas de suministro.

Mantener un rendimiento óptimo de la red de distribución, minimizando las posibles pérdidas de agua.

Atender en mínimo tiempo posible las averías que se presenten en el sistema de saneamiento.

Optimizar el estado de la redes de alcantarillado.

Suministrar a nuestros usuarios un servicio de recolección domiciliaria de calidad y de conformidad con la normatividad legal vigente.

Disponer las basuras de manera técnica produciendo el mínimo impacto ambiental de los mismos

Erradicar puntos clandestinos de disposición de basuras.

Atender las solicitudes de servicios adicionales de los usuarios en el mínimo tiempo posible

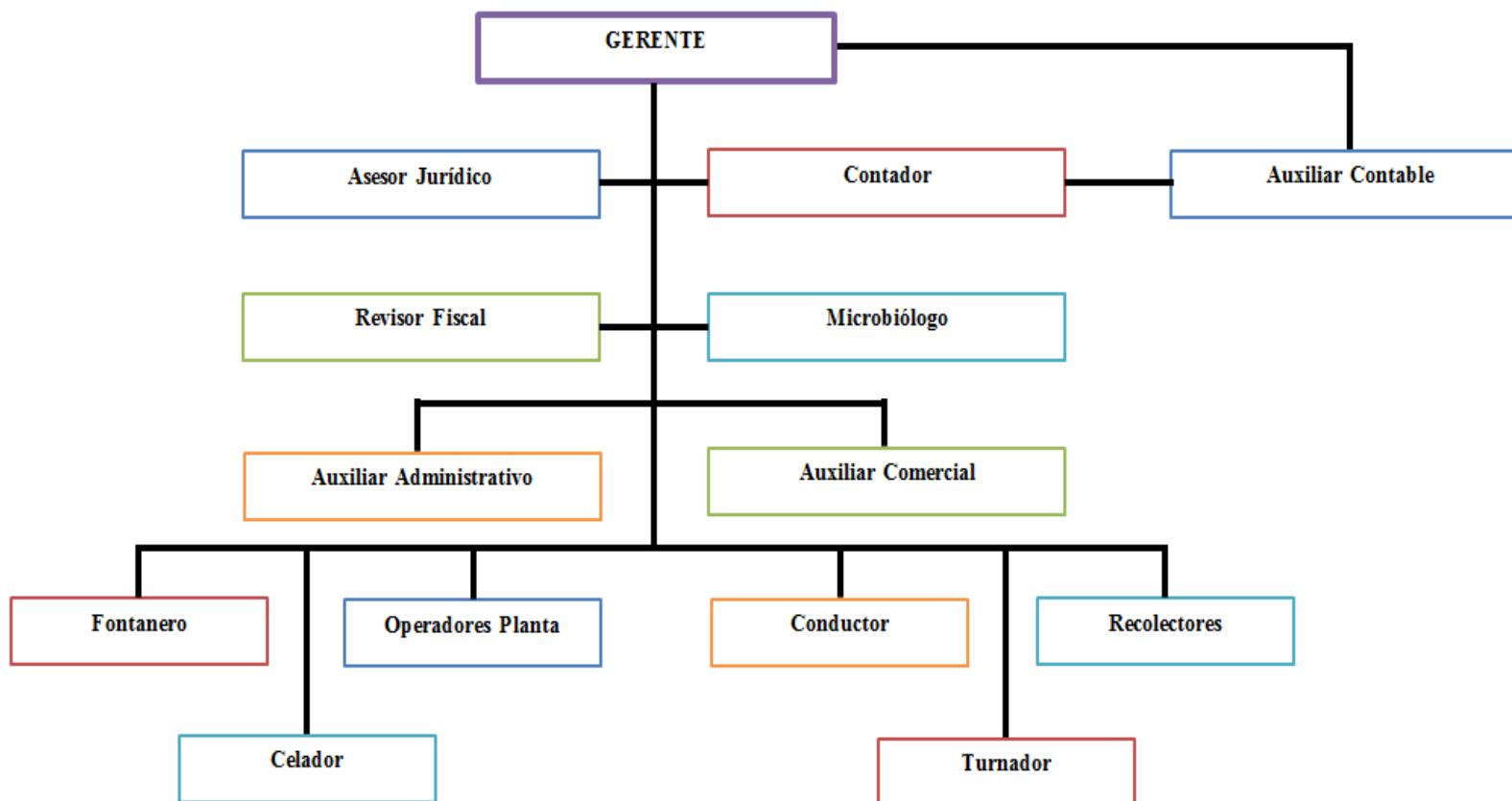
Efectuar la facturación y el cobro de acuerdo con las lecturas, tarifas vigentes y calendario previsto.

Atender los requerimientos de nuestros usuarios, suministrando los recursos necesarios para hacerlo.

Realizar los proyectos y la interventora necesaria de las obras de infraestructura necesaria para la adecuada prestación del servicio de acueducto y alcantarillado.

4.1.6 Estructura organizacional. La estructura organizacional de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”, define las responsabilidades de las diferentes funciones y procesos a diferentes personas, dependencias o áreas.

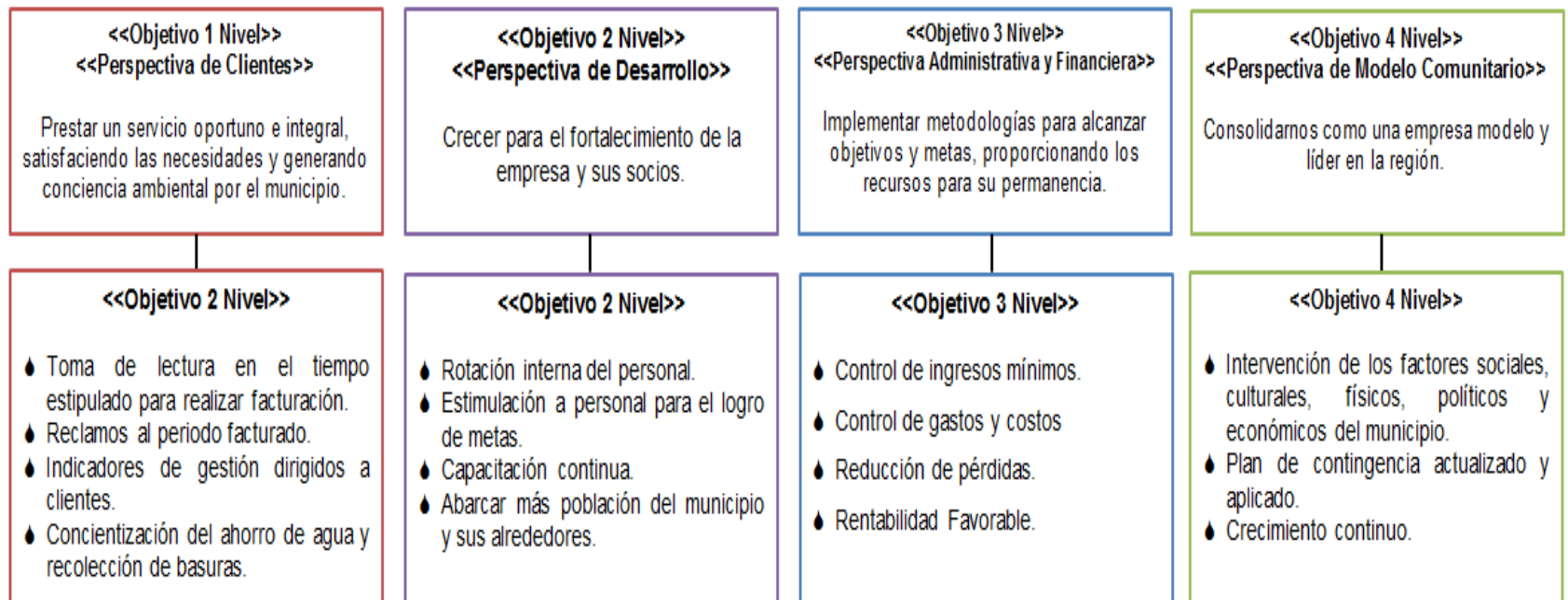
Grafica 1. Estructura organizacional.



Fuente: Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.

4.1.7 Objetivos de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar. La perspectiva de clientes, el desarrollo, la administración, financiera y el modelo comunitario, son las bases para los objetivos propuestos para la empresa, que conllevará al crecimiento y progreso, logrando satisfacer las necesidades de los usuarios, fortaleciendo la organización y permanecer como una entidad de modelo a seguir.

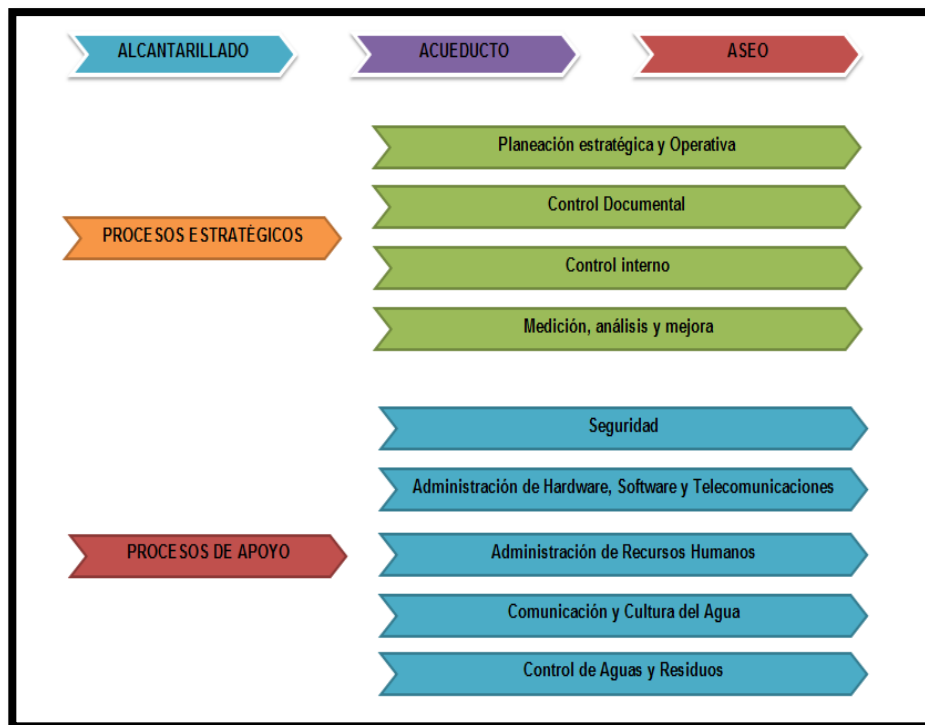
Grafica 2. Objetivos EMCAR.



Fuente: Autores del proyecto.

4.1.8 Cadena de valor de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar. La Empresa Comunitaria de Acueducto de Río de Oro, Cesar, tiene cinco (5) procesos principales que son: Distribución, alcantarillado, acueducto, aseo y facturación. Para tener un buen resultado en sus procesos tiene dependencias de apoyo que suministran información, teniendo como fin los logros de los objetivos.

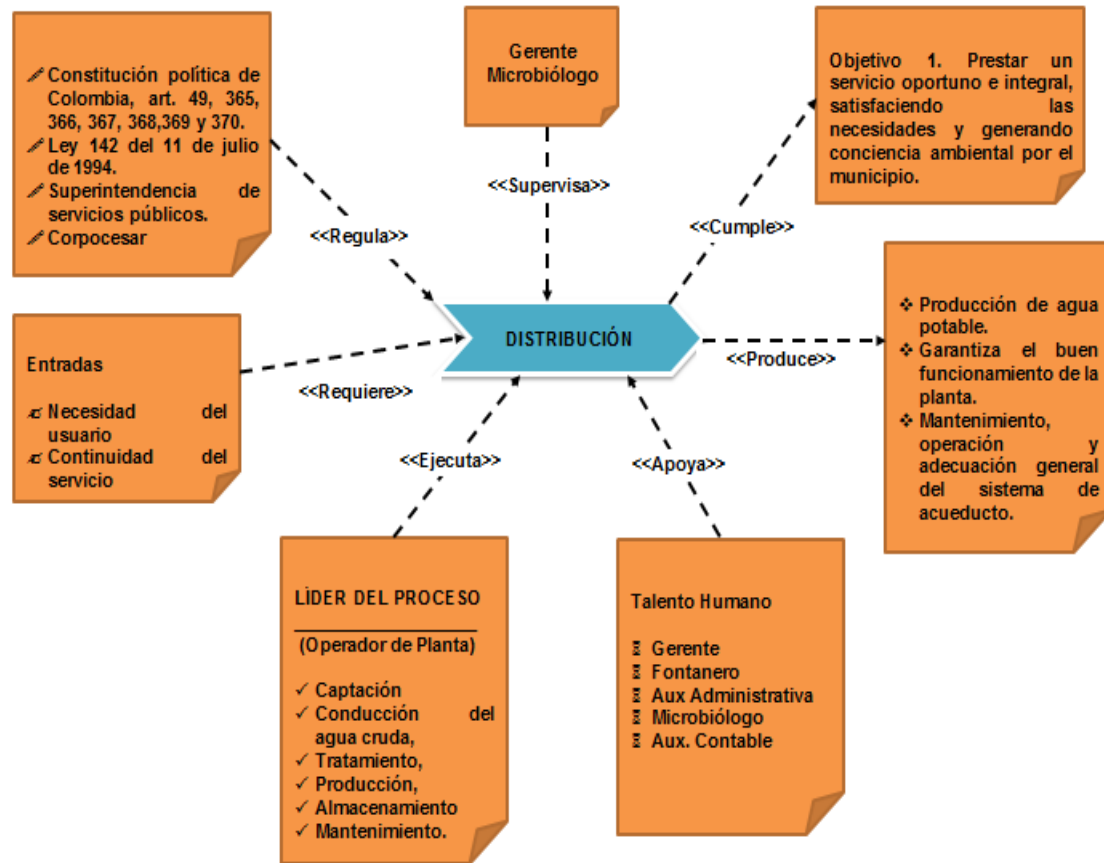
Grafica 3. Cadena de valor de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar.



Fuente: Autores del proyecto.

4.1.9 Proceso de Distribución de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”. El proceso de distribución, contempla el agua potable que es suministrada a cada una de las viviendas de los usuarios, satisfaciendo de esta manera sus necesidades y generando conciencia ambiental por el Municipio; este proceso está basado en normas, leyes y/o decretos, el cual requiere que sea continuo y cuente con un recurso humano idóneo para garantizar la prestación del servicio.

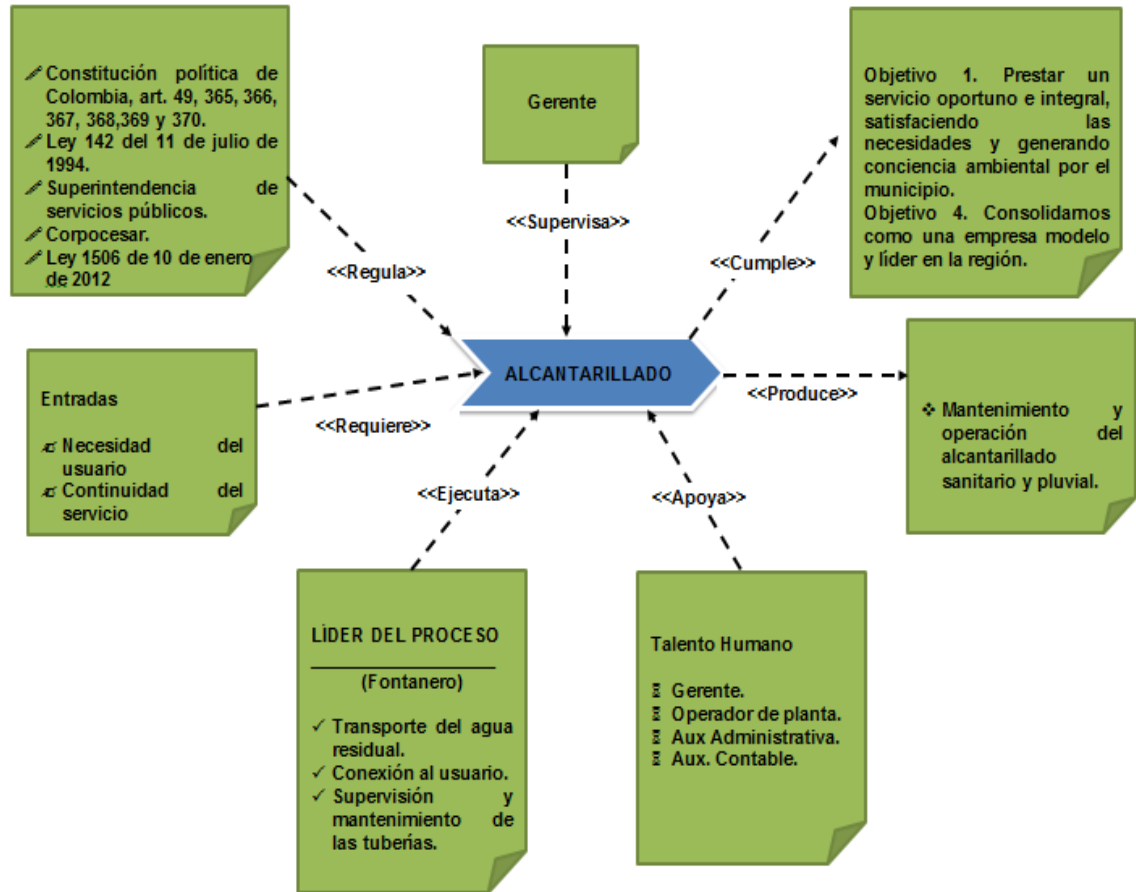
Grafica 4. Proceso de Distribución de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.



Fuente: Autores del proyecto.

4.1.10 Proceso Alcantarillado de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”. El proceso de alcantarillado tiene un sistema de estructuras y tuberías que es usado para la recogida y transporte de las aguas residuales, aguas industriales y aguas lluvias del Municipio desde el lugar en que desembocan en un río de aguas sucias. Este proceso se rige por norma, leyes y/o decretos, que ayuden a controlar el adecuado tratamiento a estas aguas residuales; debe contar con un mantenimiento a las tuberías para evitar problemas de contaminación ambiental.

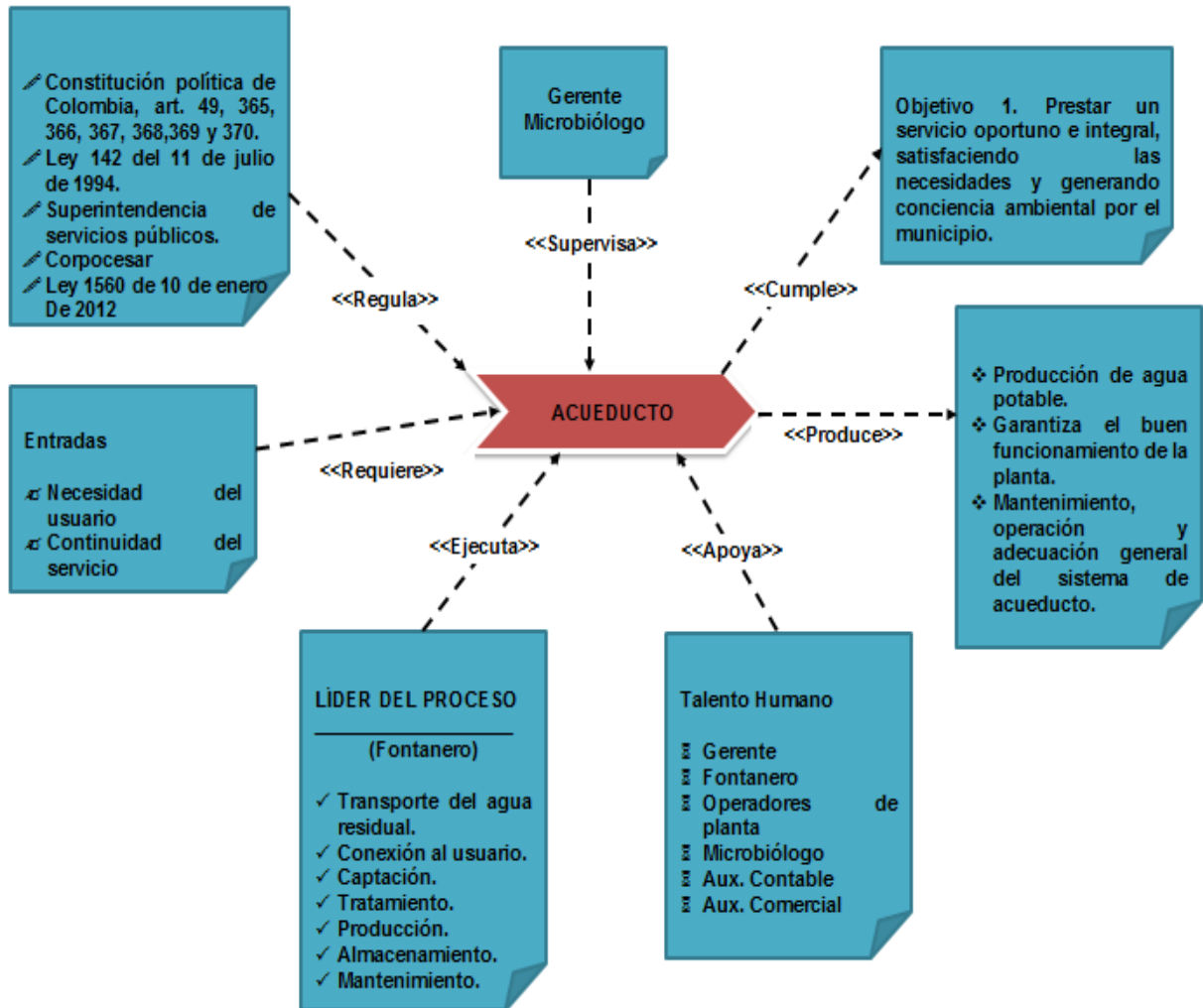
Grafica 5. Proceso Alcantarillado de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.



Fuente: Autores del proyecto.

4.1.11 Proceso Acueducto de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”. El proceso de acueducto, es el encargado de transportar agua en forma continua a cada una de las viviendas del Municipio de Río de Oro, Cesar, prestando un servicio oportuno e integral, satisfaciendo las necesidades de los usuarios.

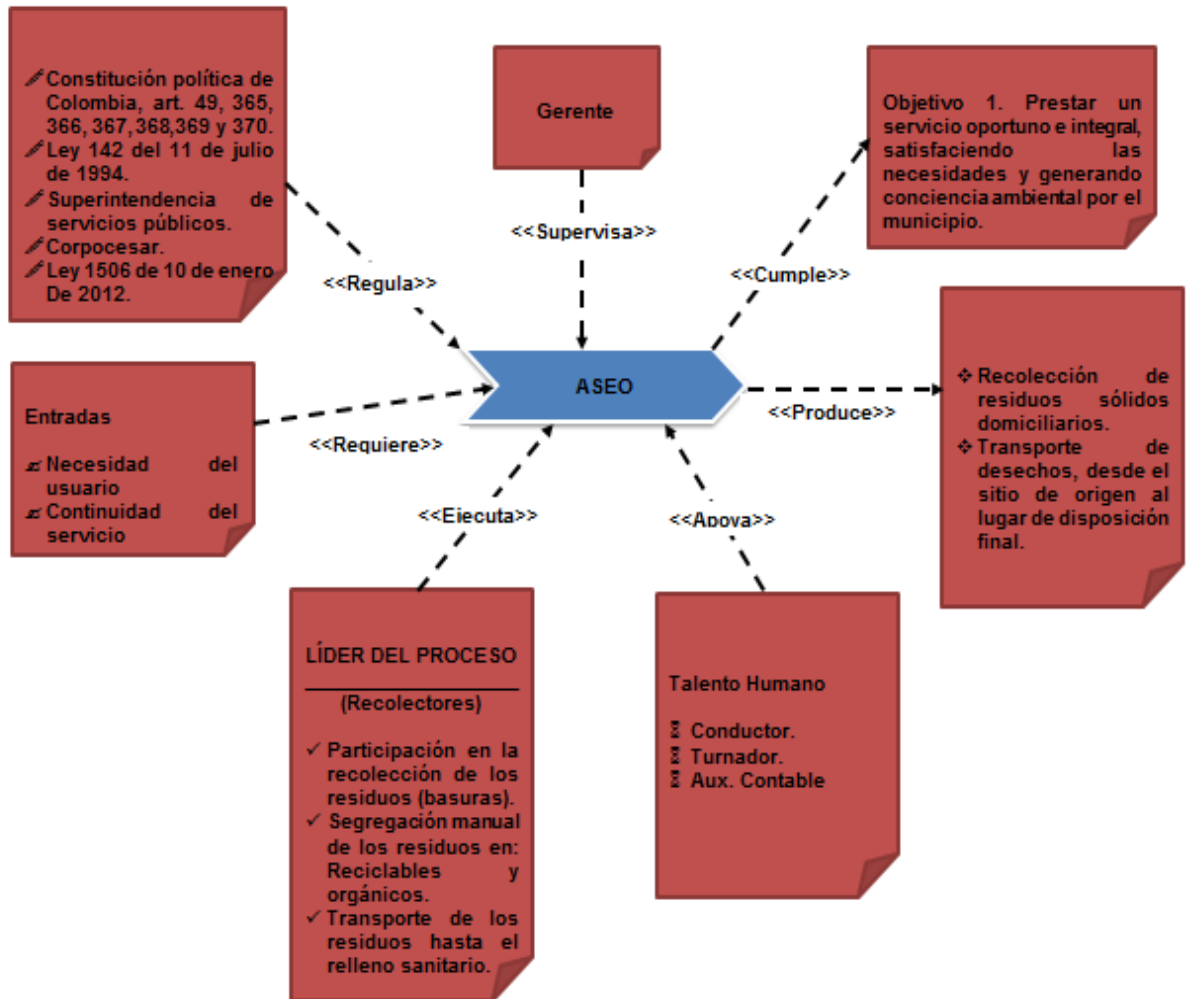
Grafica 6. Proceso Acueducto de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.



Fuente: Autores del proyecto.

4.1.12 Proceso Aseo de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”. El proceso de aseo, consiste en la limpieza, barrido de vías y áreas públicas del Municipio de Río de Oro, Cesar, regido por normas, leyes y/o decretos, los cuales permiten la prestación de un servicio oportuno.

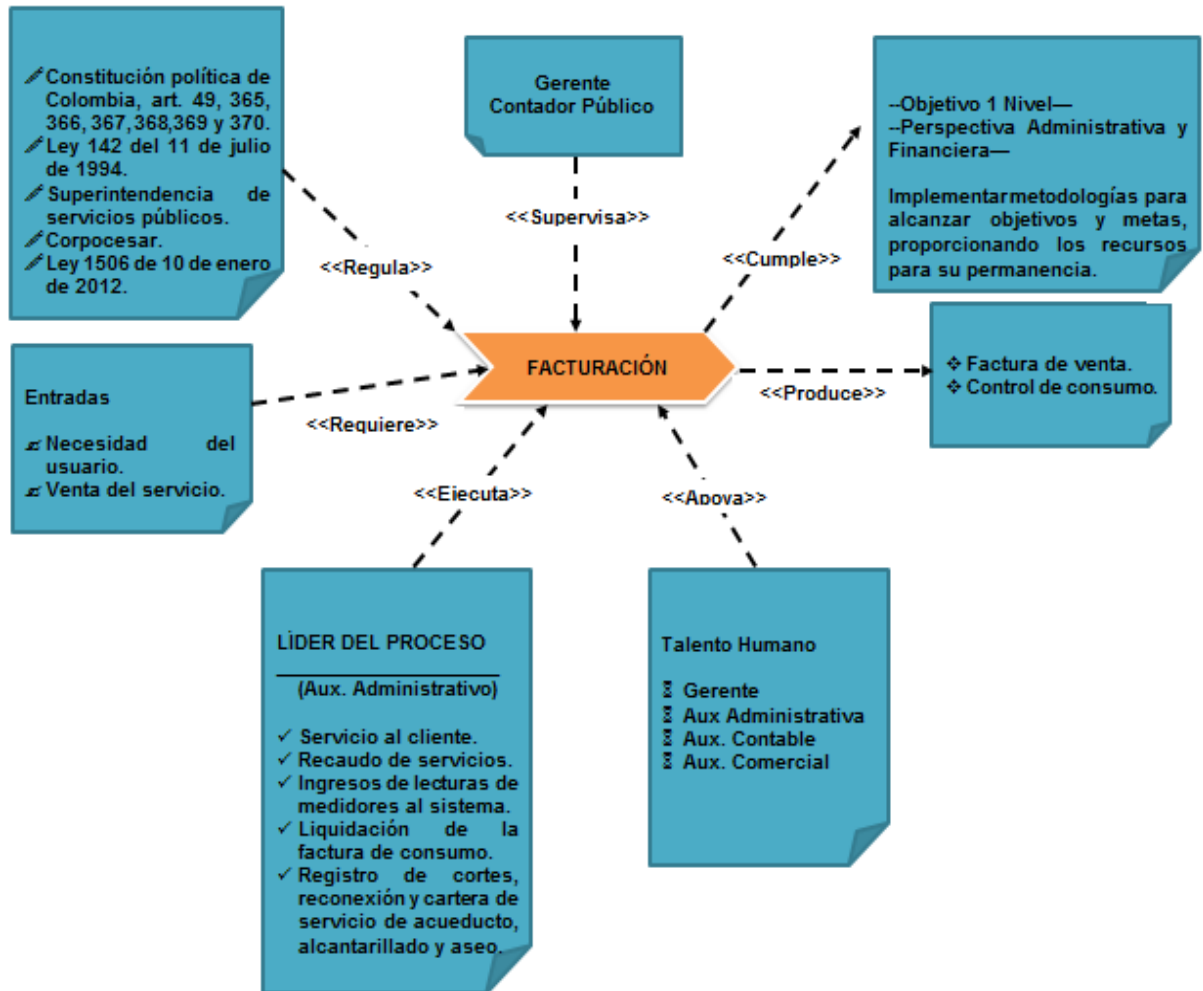
Grafica 7. Proceso Aseo de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.



Fuente: Autores del proyecto.

4.1.13 Proceso Facturación de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”. El proceso de facturación, permite el registro de los servicios de acueducto, alcantarillado y aseo de cada uno de los usuarios del Municipio de Río de Oro, Cesar.

Grafica 8. Proceso Facturación de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.



Fuente: Autores del proyecto.

4.1.14 Resultados de la entrevista. Para la aplicación de este instrumento se elaboró un formato de entrevista de acuerdo a la Norma ISO 27001, para la Gerente de la empresa. El cual se le da a conocer el objetivo de estudio de la investigación que es obtener información acerca de las políticas de seguridad de la información.

Como resultado de la recolección de la información, se obtuvo el siguiente análisis:

La Empresa Comunitaria de Acueducto de Río de Oro, Cesar, reconoce que no cuenta con una política, normas y/o procedimientos de seguridad de la información, la cual nunca ha sido establecida, publicada y aprobada formalmente por la organización. Al no existir una política solo generaría que la entidad enfrente amenazas de seguridad que incluyen: Fraude, espionaje, sabotaje, fuego, robo e inundación.

A parte de no contar con unas políticas definidas, se evidencia que el personal administrativo de la organización, no tiene un conocimiento, entrenamiento o capacitación a cerca de la seguridad de la información, y por tal razón, no hay conciencia de que se pueda presentar un incidente o desastre natural, que termine afectando a los sistemas de información de la empresa.

La Gerencia a la hora de contratar personal, no define entre sus términos y condiciones, la confidencialidad, integridad y disponibilidad de la información contenida de la empresa.

Por último, se encontró que la empresa nunca ha conformado un Comité de Seguridad de la información, el cual sea el encargado de aprobar políticas, establecer penalidades al momento de atentar contra la identidad organizativa y promover el objetivo e importancia de la necesidad de creación de un documento formal de políticas.

4.1.15 Resultados de las encuestas. Para la aplicación de este instrumento se diseñó un formato de preguntas, el cual fue dirigido al Personal Administrativo, dando a conocer el objetivo principal que es conocer la necesidad de diseñar las políticas de seguridad de la información.

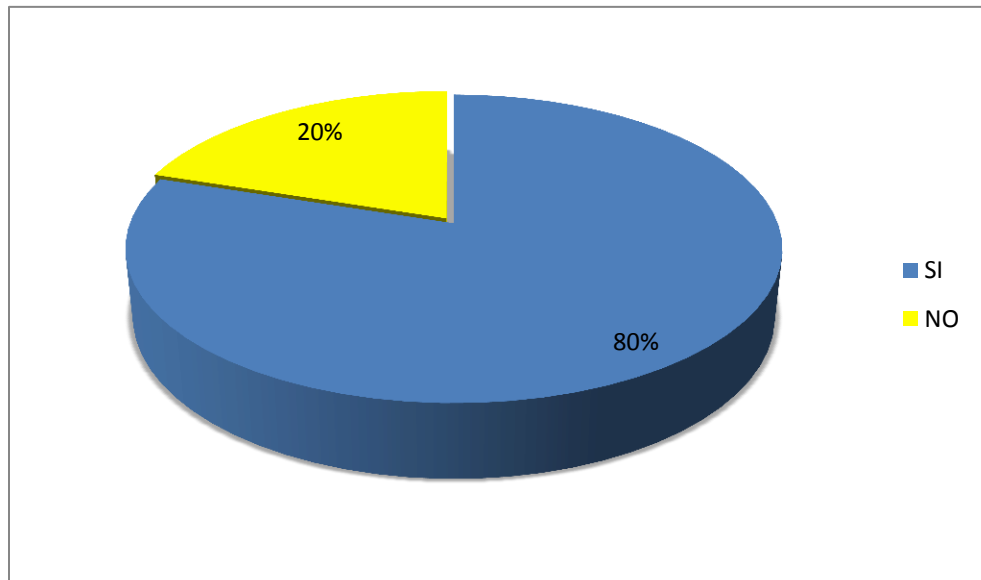
A continuación se presentan los resultados en cuadros, gráficos y análisis cuantitativo arrojado por las encuestas aplicadas a 5 empleados de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar.

Tabla 2. Utilización del equipo de cómputo para el desempeño de funciones.

PERSONAS ENCUESTADAS	RESPUESTAS	FRECUENCIA	%
5	SI	4	80
	NO	1	20
	TOTAL		100

Fuentes: Autores del proyecto.

Grafica 9. Utilización del equipo de cómputo para el desempeño de funciones.



Fuentes: Autores del proyecto.

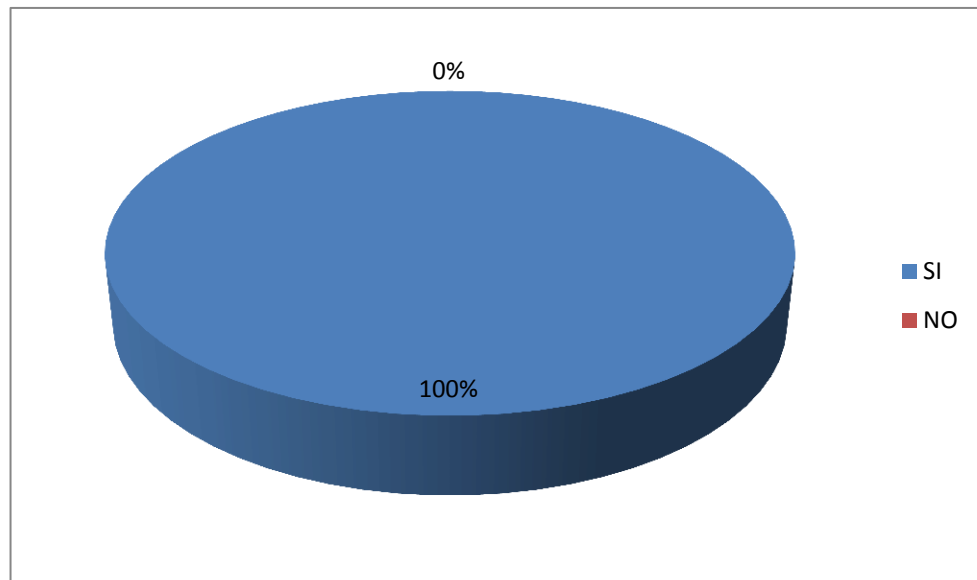
La gráfica nos indica que el personal administrativo, no siempre utiliza el equipo de cómputo que les fue asignado para desempeñar funciones propias de la empresa, en conclusión, se afirma que la organización no monitorea al personal administrativo en función de sus labores.

Tabla 3. Perímetros de seguridad que protegen las áreas de los equipos de cómputo.

PERSONAS ENCUESTADAS	RESPUESTAS	FRECUENCIA	%
5	SI	5	100
	NO	0	0
	TOTAL		100

Fuentes: Autores del proyecto.

Grafica 10. Perímetros de seguridad que protegen las áreas de los equipos de cómputo.



Fuentes: Autores del proyecto.

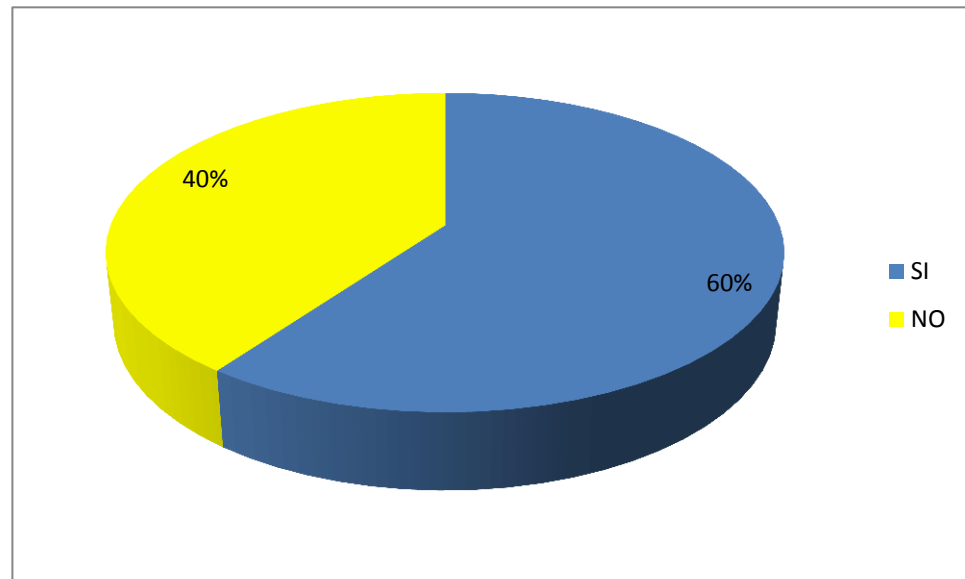
La gráfica anterior, muestra que todo el personal utiliza los perímetros de seguridad como: Acceso restringido o carnet de identificación, para proteger las áreas que tienen equipos; por lo tanto conocen la importancia de proteger los diferentes departamentos que contengan información y recursos para su procesamiento.

Tabla 4. Copias de seguridad de la información.

PERSONAS ENCUESTADAS	RESPUESTAS	FRECUENCIA	%
5	SI	3	60
	NO	2	40
	TOTAL		100

Fuentes: Autores del proyecto.

Grafica 11. Copias de seguridad de la información.



Fuentes: Autores del proyecto.

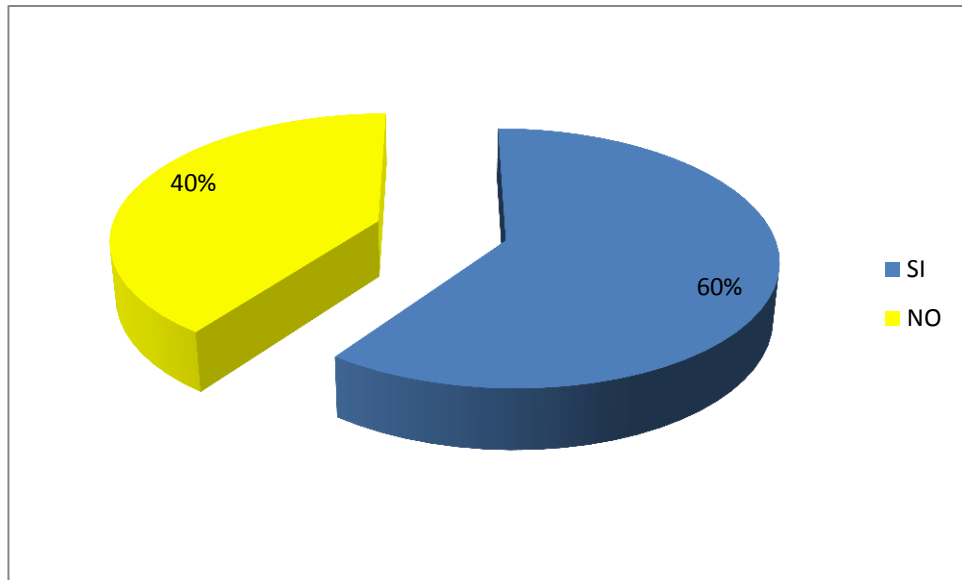
Como se evidencia en la gráfica, gran parte del personal de la empresa, no conoce la importancia de realizar copias de seguridad de los equipos, teniendo en cuenta que no tienen conocimiento o no han sido capacitados para mitigar o eliminar el riesgo de pérdida de información.

Tabla 5. Controles para el ingreso de personal.

PERSONAS ENCUESTADAS	RESPUESTAS	FRECUENCIA	%
5	SI	3	60
	NO	2	40
	TOTAL		100

Fuentes: Autores del proyecto.

Grafica 12. Controles para el ingreso de personal.



Fuentes: Autores del proyecto.

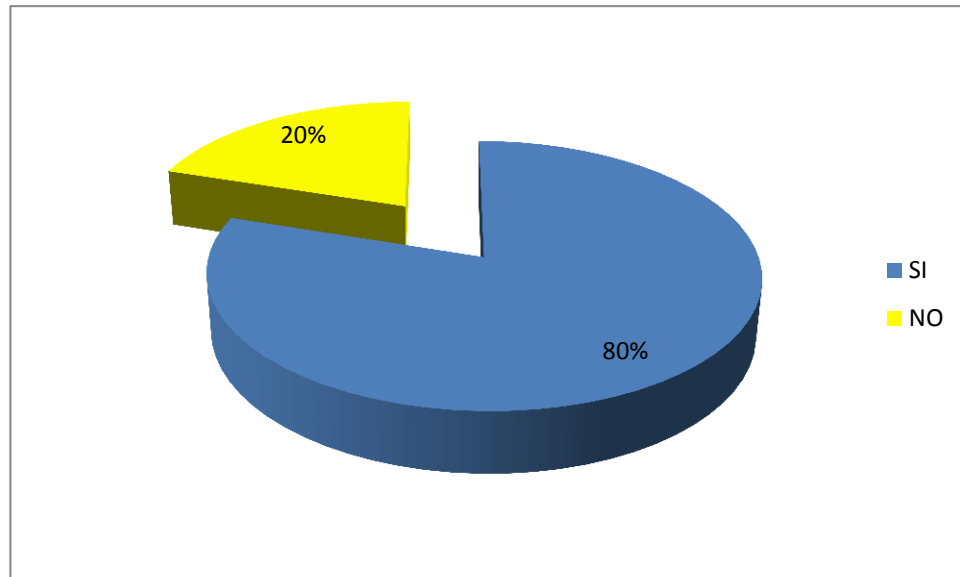
Como se observa en la gráfica, aunque existen controles de ingreso de personal no autorizado a algunas áreas, se evidenció que en otras dependencias puede acceder personal externo ocasionando que la información no sea confidencial, íntegra y disponible.

Tabla 6. Mecanismos de seguridad.

PERSONAS ENCUESTADAS	RESPUESTAS	FRECUENCIA	%
5	SI	4	80
	NO	1	20
	TOTAL		100

Fuentes: Autores del proyecto.

Grafica 13. Mecanismos de seguridad.



Fuentes: Autores del proyecto.

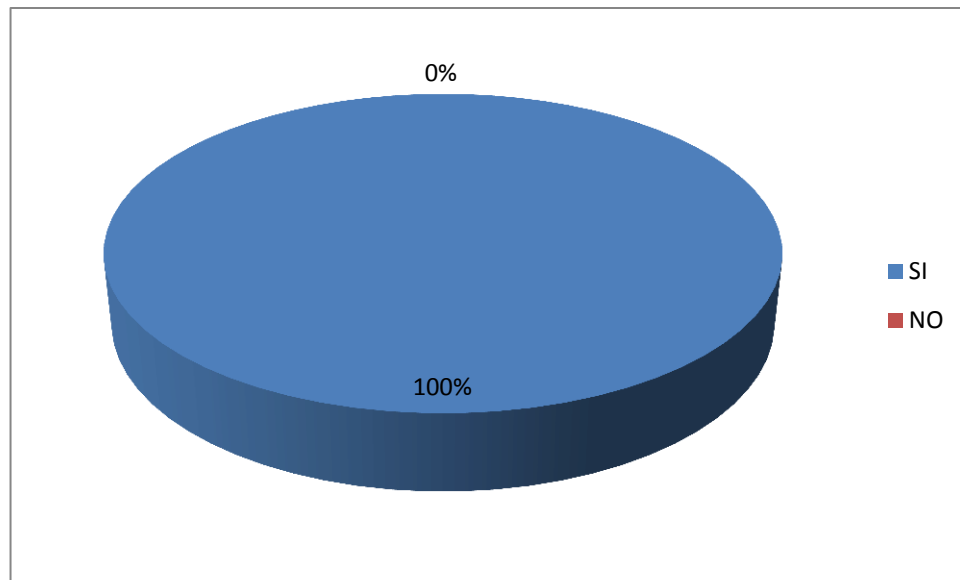
En la gráfica anterior los resultados muestran que si existe un mecanismo de control de acceso a la organización, pero se evidencia que no hay una bitácora donde se registre la entrada y salida del personal que ingresa a la empresa

Tabla 7. Aplicaciones con contraseña.

PERSONAS ENCUESTADAS	RESPUESTAS	FRECUENCIA	%
5	SI	5	100
	NO	0	0
	TOTAL		100

Fuentes: Autores del proyecto.

Grafica 14. Aplicaciones con contraseña.



Fuentes: Autores del proyecto.

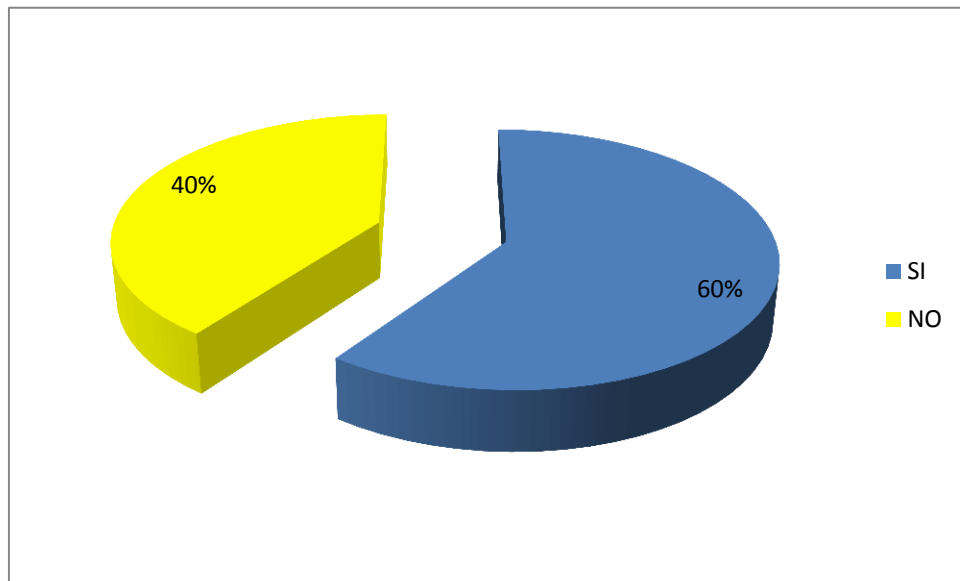
En la gráfica anterior, se evidenció que el personal administrativo es consciente de la protección de los equipos con contraseña, pero dicha autenticación no cumple con las características establecidas para asegurar la información.

Tabla 8. Lineamientos para la seguridad de la información.

PERSONAS ENCUESTADAS	RESPUESTAS	FRECUENCIA	%
5	SI	3	60
	NO	2	40
	TOTAL		100

Fuentes: Autores del proyecto.

Grafica 15. Lineamientos para la seguridad de la información.



Fuentes: Autores del proyecto.

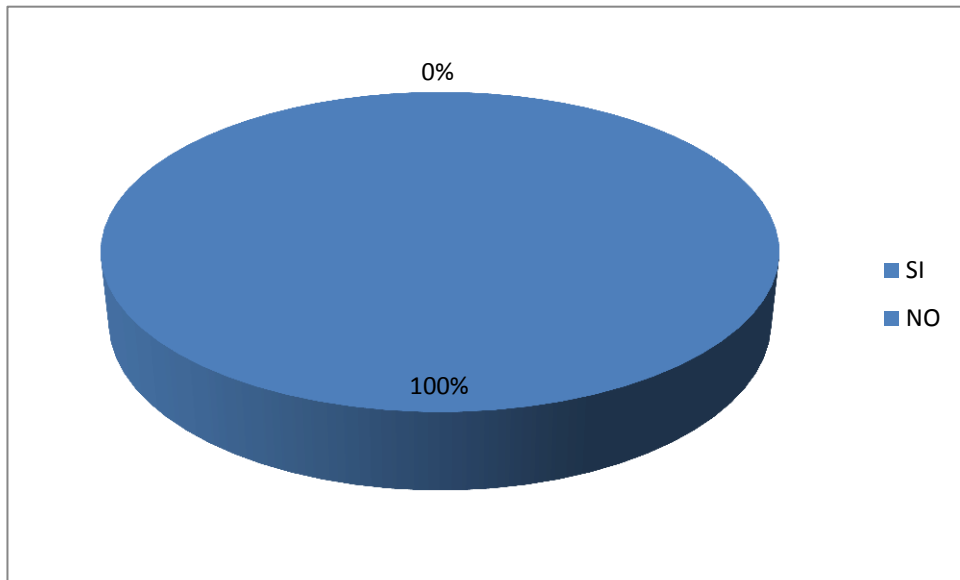
En la gráfica se evidencia que el personal administrativo dice conocer sobre los lineamientos de seguridad de la información, pero la Gerencia manifiesta no tener implementadas las políticas necesarias para la seguridad de la información.

Tabla 9. Conocimiento de la existencia de una guía de políticas de seguridad de la información.

PERSONAS ENCUESTADAS	RESPUESTAS	FRECUENCIA	%
5	SI	0	0
	NO	5	100
	TOTAL		100

Fuentes: Autores del proyecto.

Grafica 16. Conocimiento de la existencia de una guía de políticas de seguridad de la información.



Fuentes: Autores del proyecto.

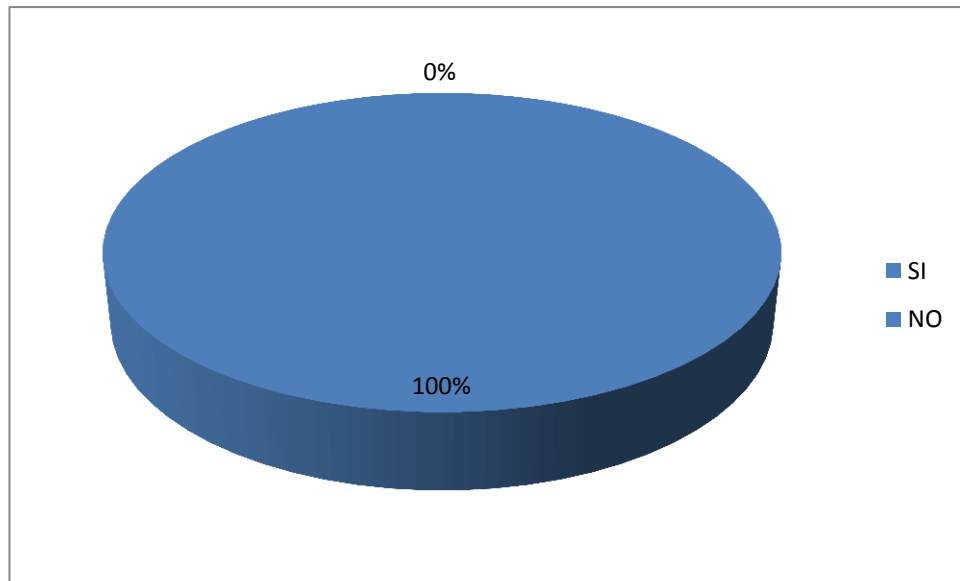
En la gráfica se evidencia la falta de conocimiento e implementación de unas políticas de seguridad de la información, para la protección de sus activos, garantizar la continuidad del negocio, reportar los incidentes ocurridos y buscar una mejor disponibilidad, integridad y confiabilidad de la información de la empresa.

Tabla 10. La política de seguridad de la información está aprobada, establecida y publicada.

PERSONAS ENCUESTADAS	RESPUESTAS	FRECUENCIA	%
5	SI	0	0
	NO	5	100
	TOTAL		100

Fuentes: Autores del proyecto.

Grafica 17. La política de seguridad de la información está aprobada, establecida y publicada.



Fuentes: Autores del proyecto.

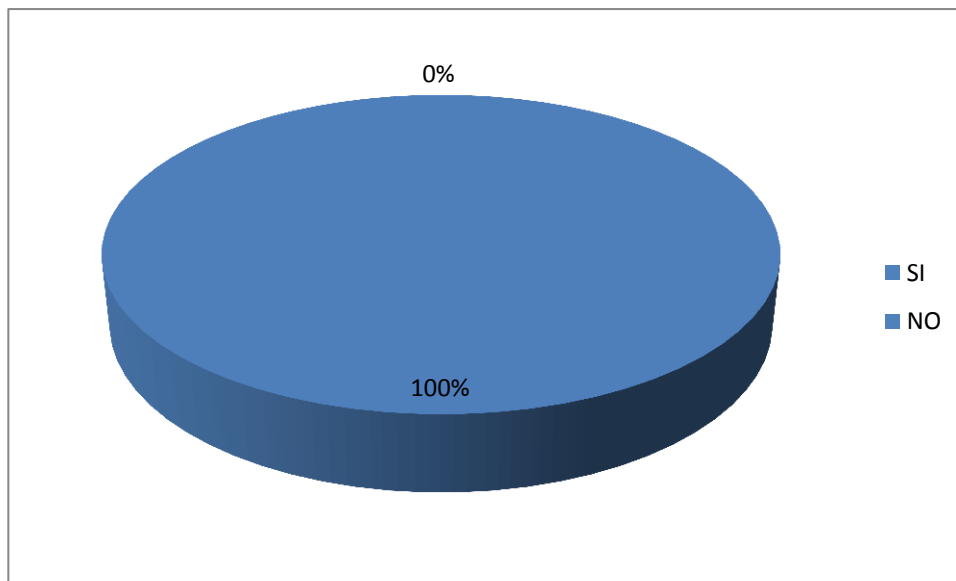
La grafica anterior, indica que la empresa desconoce la importancia de crear e implementar políticas de seguridad de la información, no garantizando la confidencialidad, disponibilidad e integridad de los datos.

Tabla 11. Comité de seguridad de la información.

PERSONAS ENCUESTADAS	RESPUESTAS	FRECUENCIA	%
5	SI	0	0
	NO	5	100
	TOTAL		100

Fuentes: Autores del proyecto.

Grafica 18. Comité de seguridad de la información.



Fuentes: Autores del proyecto.

En la gráfica se evidencia que la empresa no tiene conocimiento de la importancia de crear un comité de seguridad, que proponga soluciones a la hora de que la organización sufra un incidente o cualquier evento inesperado.

4.1.16 Matriz de riesgos. Código identificador del riesgo.

El código de identificación nos permite trabajar de forma estandarizada y ser incluido en una base de datos de riesgos. Este podría tener, por ejemplo, la estructura RX999, donde 999 es un consecutivo y la "X" es la Categoría del Riesgo:

RA: Riesgo de Administración

RE: Riesgo Externo

RO: Riesgo Organizacional

RT: Riesgo Técnico

Causa del riesgo.

El evento que causa el riesgo. Nivel más bajo de la RBS (Estructura de Desglose del Riesgo) que se establece. En caso de no existir en la RBS, señalar en fuente de color rojo, con el objetivo de actualizar posteriormente la RBS para futuros proyectos.

Descripción del Riesgo.

Las características y la forma en que se especifican los riesgos varían según la organización. Para esta práctica utilice la siguiente sintaxis: SI sucede el evento **QUE** consecuencias sobre los objetivos del proyecto traería.

Tabla 12. Probabilidad.

Muy Probable	0.9
Bastante Probable	0.7
Probable	0.5
Poco Probable	0.3
Improbable	0.1

Fuente: Autores del proyecto.

Tabla 13. Impacto.

Muy Alto	0.8
Alto	0.4
Moderado	0.2
Bajo	0.1
Muy Bajo	0.05

Fuente: Autores del proyecto.

Tabla 14 Marcador de riesgo para un riesgo específico

(P x I)

Impacto	Muy bajo	Bajo	Moderado	Alto	Muy Alto
Probabilidad	.05	.1	.2	.4	.8
0.9	0.05	0.09	0.18	0.36	0.72
0.7	0.04	0.07	0.14	0.28	0.56
0.5	0.03	0.05	0.10	0.20	0.40
0.3	0.02	0.03	0.06	0.12	0.24
0.1	0.01	0.01	0.02	0.04	0.08

Verde: Riesgo Bajo – Amarillo: Riesgo Moderado – Rojo: Riesgo Alto

Fuente: Autores del proyecto.

Combinando las escalas de la probabilidad y del impacto obtenemos la matriz P x I, que se muestra arriba, la cual nos permite calificar cada riesgo según la escala:

Tabla 15. Riesgo.

Alto	0.99 - 0.18
Moderado	0.17 - 0.05
Bajo	0.04 - 0.01

Fuente: Autores del proyecto.

Probabilidad.

Para cada riesgo, utilizando la escala de probabilidad, le asignamos el valor correspondiente.

Impacto.

Para cada riesgo, utilizando la escala de impacto, le asignamos el valor correspondiente.

Rango (P x I).

Multiplicación de la probabilidad por el impacto.

Señales.

En la manera de lo posible indicar una señal de que el riesgo va a suceder.

Responsable.

Miembro del equipo o de la organización que debe responder por la ejecución de las acciones planeadas para ese riesgo.

Una vez aplicado los instrumentos como: entrevista y encuesta a la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, se hizo notable un análisis de la información suministrada, la cual se encontraron riesgos, que pueden afectar la seguridad de la información contenida en EMCAR.

Se evidencia en los resultados que los riesgos a los que se enfrenta EMCAR son de un nivel alto; por consiguiente, se debe mejorar o tomar medidas al respecto, para evitar que la organización sea vulnerable a cualquier tipo de amenaza que afecte su activo más importante que es la información.

A continuación, se muestra el análisis de los riesgos, con su respectivo impacto y probabilidad.

Tabla 16. Matriz de riesgos EMCAR.

CÓDIGO	CAUSA	DESCRIPCIÓN DEL RIESGO	PROBABILIDAD	IMPACTO	RANGO PXI	ACCIONES	SEÑALES	RESPONSABLE
RT - 02	Utilización de perímetros de seguridad para protección de las áreas de la empresa.	Infraestructura tecnológica no cumple con las normas y estándares técnicos.	0,70	0,40	0,28	Aplicación de la norma para la instalación del cableado.	Conexiones eléctricas mal estructuradas, tanto de equipos de cómputo como de seguridad, cableado suelto.	Gerente
RT - 03	Realización de copias de seguridad, de la información de los equipos de la organización.	Pérdida irreparable de la información, ocasionando digitalización de los datos perdidos nuevamente al sistema, afectando la integridad, disponibilidad y confidencialidad.	0,90	0,80	0,72	Realización de backups diarios de seguridad de la información de la empresa.	Pérdida de la información.	Empleados
RO - 01	Controles para el ingreso de personal no autorizado.	No hay un control de acceso a algunas áreas de la empresa, debido a que no se cuentan con cubículos para atención al usuario.	0,70	0,40	0,28	Implementar un programa para el registro de entrada y salida de los usuarios.	Ingreso de personal no autorizado, visibilidad física y lógica de la información.	Gerente y empleados.

RO - 02	Mecanismos de seguridad para el control de acceso a la empresa.	Ingreso de personas externas a la empresa (Usuarios), sin ningún tipo de identificación, tiempo de permanencia y actividad a realizar.	0,70	0,40	0,28	Implementar un mecanismo de seguridad como: Carnet de visitante y tiempo de permanencia máximo en la organización, con el fin de tener un control más exacto del ingreso del personal externo.	Usuarios dentro de la empresa, sin ningún tipo de identificación y actividades a realizar.	Gerente
RO - 03	Lineamientos de seguridad de la información, desconocidos por los funcionarios de la empresa.	Pérdida, alteración, sabotaje, borrado, desastres naturales (Incendios, inundaciones) de la información.	0,70	0,40	0,28	Elaboración de un documento que describa los lineamientos que se deben tener en cuenta para la seguridad de la información.	No existe un plan de contingencia, para mitigar los diferentes accidentes presentados.	Gerente
RO - 04	Existencia de una guía y/o norma formal de políticas de seguridad de la información.	Con la no existencia de una guía de las políticas de seguridad de la información, puede ocasionar la pérdida absoluta de los datos.	0,70	0,40	0,28	Documentar las políticas de seguridad de la información, para evitar incidentes informáticos, incluir penalidades para aquellos que incumplan la política y tener claro el	Sensibilidad de la empresa a las amenazas y riesgos informáticos a los que se ven expuesto día a día.	Gerente

						objetivo principal del mismo.		
RO - 06	No existe comité de seguridad de la información.	La no protección de la información.	0,70	0,40	0,28	Conformación de un comité de seguridad, con la representación de todos los funcionarios de la empresa.	Falta de organización y socialización de incidentes presentados.	Gerente
RO - 07	Existencia de un responsable de las políticas, normas y procedimientos.	No hay una persona encargada de realizar capacitaciones periódicas y actualizaciones de las políticas.	0,70	0,40	0,28	Asignar a una persona que sea la encargada de las políticas, normas y procedimientos.	No existe concientización y participación por parte de la empresa para definir roles y responsabilidades.	Gerente y empleados.
RO - 08	Acuerdos de confidencialidad de la información.	Información puede ser alterada por: Divulgación, medios físicos y electrónicos, conversaciones.	0,70	0,40	0,28	Crear para cada empleado un formato de confidencialidad o incluido en una cláusula de la hoja de vida, donde estén estipulados todos los compromisos a adquirir.	Información robada y divulgada.	Gerente y empleados.

RO - 09	Limpieza del puesto de trabajo.	Deterioro, daños irreversibles a los equipos, impidiendo el normal funcionamiento de las funciones.	0,90	0,80	0,72	Socialización de la política de ingerir alimentos en el puesto de trabajo.	Suciedad, deterioro del equipo de cómputo.	Gerente y empleados.
RO - 10	Planes, procedimientos y entrenamiento para el manejo de una crisis.	Pérdida de la información por un inadecuado manejo del software.	0,90	0,80	0,72	Crear copias de seguridad para salvaguardar la información.	Bajonazos de luz, descargas eléctricas y catástrofes naturales que ocasionan daños en la disponibilidad, integridad y confidencialidad de la información.	Gerente
RT-01	Utilización de equipos de cómputo de la empresa para desempeñar otras funciones diferentes a las institucionales.	Navegación de páginas no autorizadas y descarga de aplicaciones que causan amenazas en la seguridad de la información.	0,50	0,20	0,10	Bloqueo de páginas.	Navegación en páginas no seguras y permitidas por la empresa.	Gerente
RT - 05	Inventario de activos.	Desactualización, la no realización de mantenimiento correctivo y preventivo de los equipos.	0,50	0,20	0,10	Actualización periódica de los activos de la organización.	Robo o intercambio de activos de la empresa, no existe un responsable de los mismos.	Empleados

RT - 04	Control de contraseñas para el ingreso de personal administrativo a las aplicaciones de los equipos.	Acceso a la información, ocasionando pérdida de los datos, mal uso de las aplicaciones y un borrado accidental o provocado.	0,30	0,10	0,03	Cambio de contraseñas periódicas, que cumplan con los requisitos que debe tener como: Mayúsculas, minúsculas, números y caracteres.	Existen equipos sin contraseña y otros que no la han actualizado.	Gerente y empleados.
			PROMEDIO		0,33			
CALIFICACIÓN GENERAL DEL RIESGO: ALTO								

Fuentes: Autores del proyecto.

4.2 DOMINIOS DE LA NORMA ISO 27001.

Mediante un análisis de la información suministrada por la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, se hizo un estudio de los dominios, objetivos de control y los controles para la creación de un documento de las políticas de seguridad de la información.

Enunciado los dominios a utilizar de la siguiente manera:

Tabla 17. Dominios Norma ISO 27001.

DOMINIOS	OBJETIVOS DE CONTROL	CONTROLES
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Brindar orientación y soporte.	Definir políticas para la seguridad de la información.
		Revisión constante de las políticas de seguridad de la información.
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Organización interna para iniciar y controlar la implementación y operación del SGSI.	Seguridad de la información roles y responsabilidades.
		Separación de deberes.
		Contacto con las autoridades.
		Contacto con grupos de interés especial.
	Seguridad en Dispositivos Móviles y Teletrabajo.	Política para dispositivos móviles.
SEGURIDAD DE LOS RECURSOS HUMANOS	Antes de Asumir el Empleo	Teletrabajo
		Selección.
	Durante la Ejecución del Empleo	Términos y condiciones del empleo.
		Responsabilidades de la dirección.
		Toma de conciencia, educación y formación de la seguridad de la información
	Terminación y Cambio de Empleo	Proceso disciplinario.
		Terminación o cambio de responsabilidades de empleo.

GESTIÓN DE ACTIVOS	Responsabilidad por los Activos	Inventarios de activos.
		Propiedad de los activos.
		Uso aceptable de los activos.
		Devolución de activos.
	Clasificación de la Información.	Clasificación de la información.
		Etiquetado de la información.
		Manejo de activos.
	Manejo de Medios de Soporte	Gestión de medios de soporte removibles.
		Disposición de los medios de soporte.
Transferencia de medios de soporte físico.		
CONTROL DE ACCESO	Requisitos del Negocio para Control de Acceso	Política de control de accesos.
		Acceso a redes y a servicios en red.
	Gestión de Acceso de Usuarios	Revisión de derechos de acceso de usuarios.
		Cancelación o ajuste de los derechos de acceso.
	Responsabilidades de los Usuarios	Uso de información secreta.
		Control de acceso a sistemas y aplicaciones.
		Restricción de acceso a información.
		Sistema de gestión de contraseñas.
SEGURIDAD FÍSICA Y AMBIENTAL	Áreas Seguras	Perímetros de seguridad física.
		Controles físicos de entrada.
		Seguridad de oficina, salones e instalaciones.
		Protección contra amenazas externas y ambientales.
		Trabajo en áreas seguras.

	Equipos	Ubicación y protección de los equipos.
		Servicios públicos de soporte.
		Seguridad del cableado.
		Mantenimiento de equipos.
		Retiro de activos.
		Seguridad de equipos y activos fuera del predio.
		Disposición segura o reutilización de equipos.
		Política de escritorio limpio y pantalla limpia
SEGURIDAD DE LAS OPERACIONES	Procedimientos Operacionales y Responsabilidades	Procedimientos de operación documentada.
		Protección contra códigos maliciosos.
		Realización de copias de seguridad contra pérdida de datos.
	Registro y Seguimiento	Registrar eventos y generar evidencia.
	Proteger la información de registro contra alteración y registro no autorizado.	
SEGURIDAD DE LAS COMUNICACIONES	Gestión de Seguridad de Redes	Controles de redes.
		Seguridad de los servicios de red.
		Separación en las redes.
	Transferencia de Información	Políticas y procedimientos de transferencia de información.
		Acuerdos sobre transferencia de información.
		Mensajes electrónicos.
		Acuerdos de confidencialidad o de no divulgación.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Gestión de Incidentes y Mejoras en Seguridad de la Información.	Responsabilidades y procedimientos.
		Informe de eventos de seguridad de la información
		Informe de debilidades de seguridad de la información
		Evaluación de eventos de seguridad de la información.
		Respuesta a incidentes de seguridad de la información.
		Aprendizaje obtenido de los incidentes de seguridad de la información.
		Recopilación de evidencia.
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA CONTINUIDAD DEL NEGOCIO	Continuidad de Seguridad de la Información	Planificación de la continuidad de la seguridad de la información.
		Implementación de la continuidad de la seguridad de la información.
		Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
	Redundancia	Disponibilidad de instalaciones de procesamiento de información

CUMPLIMIENTO	Cumplimiento	Cumplimiento de requisitos legales y contractuales.
		Identificación de los requisitos de legislación y contractuales aplicables.
		Derechos de propiedad intelectual.
		Protección de registros.
		Privacidad y protección de la información identificable personalmente.
	Revisiones de Seguridad de la Información	Revisión independiente de la seguridad de la información.
		Cumplimiento con las políticas y normas de seguridad.
		Revisión del cumplimiento técnico.

Fuentes: Autores del proyecto.

4.3 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RÍO DE ORO, CESAR, “EMCAR”, DE ACUERDO A LA NORMA ISO 27001.

Para el presente objetivo se diseñó el documento de las Políticas de Seguridad de la Información para la Empresa Comunitaria de Acueducto de Río de Oro, Cesar. El cual se tomó como referencia la Norma ISO/IEC 27001:2013, donde establece unos lineamientos y principios generales para iniciar, implementar, mantener y mejorar la seguridad de la información de la organización.

Para su elaboración se tuvieron en cuenta, los dominios, objetivos de control y los controles los cuales deben ser implementados para mitigar los riesgos encontrados en la empresa.

**POLÍTICA DE SEGURIDAD DE LA
INFORMACIÓN PARA LA EMPRESA
COMUNITARIA DE ACUEDUCTO DE RÍO DE
ORO, CESAR, “EMCAR”**



INTRODUCCIÓN

La información es el activo que representa gran valor para la Empresa Comunitaria de Acueducto y Alcantarillado de Río de Oro, Cesar “EMCAR”, garantizando la disponibilidad, integridad y confidencialidad de la información, contribuyendo de esta manera a una mejor gestión, garantizando la continuidad del negocio y minimizando los riesgos que pueden presentarse.

Las Políticas de Seguridad de la Información a implementar, necesitan que tengan un contenido cultural para EMCAR, por el cual debe contarse con el compromiso de todos y cada uno de los funcionarios, contratistas y todo aquel que haga parte de la organización empresarial y así cumplir con el propósito de este proyecto.

Lo anteriormente expuesto, la Empresa Comunitaria de Acueducto y Alcantarillado de Río de Oro, Cesar “EMCAR”, busca implementar sus propias políticas de seguridad de la información, basándose en los dominios establecidos en la norma internacional ISO/IEC 27001 segunda edición, que describe los requisitos para la implementación del Sistema de Gestión de Seguridad de la Información SGSI.

Por esta razón, el propósito de la implementación de estas políticas de seguridad, es de realizarse de forma ordenada y sucesiva, EMCAR ha dispuesto la conformación de un comité de Seguridad de la Información y unos objetivos a cumplir en un tiempo determinado.

• OBJETIVO

Presentar una política de uso adecuado de la tecnología para el procesamiento de la información.

Establecer una cultura e indicar el conjunto de instrucciones o normas generales necesarias para la operación y buscar mejor disponibilidad, integridad y confiabilidad de la información procesada por los diferentes sistemas de información de EMCAR.

Este documento describe el uso adecuado de los servicios, aplicativos, equipos de cómputo y la red.

• TÉRMINOS Y DEFINICIONES

Para el presente documento se aplican las siguientes definiciones:

• SEGURIDAD DE LA INFORMACIÓN.

La seguridad de la información se entiende como la preservación de las siguientes características²⁷:

Confidencialidad: Se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada: las líneas “pinchadas” la interceptación o recepción electromagnética no autorizada o la simple intrusión directa en los equipos donde la información está físicamente almacenada.

Integridad: Se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

Disponibilidad: La disponibilidad de la información se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

Adicionalmente, deberán considerarse los conceptos de:

²⁷ Norma ISO 27000 – 27001 Versión 2013 – Seguridad de la Información.

Activo de información: Un activo en relación a la presente política de seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para EMCAR, incluyendo bases de datos, documentación, manuales, software, hardware, contratos de equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, quienes los generan, transmiten y destruyen información. Todos los activos deberán estar claramente identificados manteniendo un inventario con los más importantes.

Seguridad de la información: Es el conjunto de medidas preventivas y correctivas para proteger la información manteniendo la confidencialidad, disponibilidad e integridad de la misma.

Virus: Son programas creados para infectar sistemas y otros programas creándoles modificaciones y daños que hacen que estos funcionen incorrectamente.

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

Auditabilidad: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la duplicación: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grave una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

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

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

Confiability de la Información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

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

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información: Se refiere al hardware y software operados por la empresa o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la entidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

• EVALUACIÓN DE RIESGOS.

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de la empresa.

• ADMINISTRACIÓN DE RIESGOS.

Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

• COMITÉ DE SEGURIDAD DE LA INFORMACIÓN.

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

• RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN.

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la entidad que así lo requieran.

• INCIDENTE DE SEGURIDAD.

Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

• **ALCANCE**

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico en la Empresa Comunitaria de Acueducto y Alcantarillado de Rio de Oro, Cesar.

Debe ser conocida y cumplida por todo el personal administrativo y operativo de la empresa, tanto para funcionarios internos o externos.

• **GESTIÓN Y TRATAMIENTO DE ACTIVOS DE INFORMACIÓN.**

PRINCIPAL CONCEPTO DE ACTIVOS DE INFORMACIÓN.

Los activos de información se clasifican para indicar la necesidad, las prioridades y el grado esperado de protección al manejar la información. Por lo anterior, EMCAR debe definir los controles para salvaguardar la información creada, procesada, transmitida y/o almacenada de sus procesos, con el fin de minimizar impactos financieros, operativos y/o legales debido al uso incorrecto de la misma.

La Información que EMCAR utilice para el desarrollo de sus objetivos tiene asignado un responsable, quién la utiliza y es el que responde por su correcto tratamiento. Así, él toma las decisiones que son requeridas para la protección de su información y determina quiénes son los usuarios y sus privilegios de tratamiento.

Cada responsable de la información debe cuidar y vigilar su correcto tratamiento, los lugares donde reside y los usuarios de la misma. Dichos usuarios deben demostrar una necesidad de negocio para su acceso, el cual debe ser vigilado por el responsable. La Información provista por los clientes, proveedores, terceros, y funcionarios es privada y su tratamiento dentro de las premisas de EMCAR está enmarcado para los fines que fue obtenida.

EMCAR provee los medios necesarios para asegurarse de que cada usuario preserve y proteja los activos de información de una manera consistente y confiable. Cualquier persona que intente inhabilitar, vencer o sobrepasar cualquier control de Seguridad de la Información en forma no autorizada será sujeto de las acciones legales correspondientes.

Los recursos de información de EMCAR son exclusivamente para propósitos de la organización y deben ser tratados como activos dedicados a proveer las herramientas para realizar el trabajo requerido.

EMCAR promueve el buen uso de los recursos de Información, conservando el derecho a la intimidad, la privacidad, el habeas data, y la protección de los datos de sus propietarios.

EMCAR, se reserva el derecho de restringir el acceso a cualquier Información en el momento que lo considere conveniente.

INCIDENTE DE SEGURIDAD.

Se deberá notificar al Gerente:

- En caso de un evento adverso en la computadora asignada, o en la red de la empresa.
- Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización.
- Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de EMCAR.

El Gerente, tiene establecidas las responsabilidades y procedimientos que aseguren una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información que se llegasen a presentar en la organización.

• POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN²⁸.

Generalidades.

La información es un recurso que, como el resto de los activos, tiene valor para la empresa y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la empresa.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Para esto, se debe asegurar un compromiso por parte de todo el personal que conforma la organización y a su vez entidades gubernamentales que brindan apoyo a la misma, con el fin de difundir, consolidar y cumplir la presente política.

²⁸ Visión General – ISO 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información Requisitos. Pág. 10.

Objetivo.

Proteger los recursos de información de la empresa y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, brindando orientación y soporte constante sobre el buen uso del mismo y mantenerla actualizada, acorde a los objetivos misionales de la organización.

Alcance.

Esta Política se aplica en todo el ámbito de la empresa, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Responsabilidad.

Todo el personal que hace parte de la empresa tanto, la Asamblea General, el Gerente, los empleados y personas externas vinculadas a la empresa, son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la empresa y cualquiera sea el nivel de las tareas que desempeñe.

Las máximas autoridades de la organización aprueban esta Política y son responsables de la autorización de sus modificaciones.

El Comité de Seguridad de la Información de la empresa, procederá a revisar y proponer a la máxima autoridad del mismo para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad; aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información; garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios; promover la difusión y apoyo a la seguridad de la información dentro de la empresa y coordinar el proceso de administración de la continuidad de las actividades de la entidad.

El Gerente será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

El Responsable de Seguridad Informática cumplirá funciones relativas a la seguridad de los sistemas de información de la empresa, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

Los Propietarios de la Información son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

El Gerente cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Así mismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad y las tareas de capacitación continua en materia de seguridad.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

Políticas para la seguridad de la información.

EMCAR se compromete a producir, proveer y divulgar información y conocimiento confiable y oportuno preservando la confidencialidad, integridad y disponibilidad de la información misional de acuerdo a las disposiciones legales y técnicas y a las responsabilidades adquiridas para la satisfacción de los clientes y la protección de la información contra amenazas internas y externas, mediante la implementación de buenas prácticas en la gestión de riesgos, el fortalecimiento de la capacidad institucional y la operación bajo un sistema de gestión integrado que mejore continuamente su eficacia, eficiencia y efectividad.

Revisión de las políticas para la seguridad de la información.

Las políticas de seguridad de la información se revisarán periódicamente (mínimo una vez por año), o antes, en caso de producirse cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, que puedan afectar su continuidad. La aprobación de las actualizaciones y/o modificaciones, se realizará por parte del Comité de Seguridad de la Información.

• ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN²⁹.

Generalidades.

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la empresa.

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Así mismo, se contemplará la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Por otro lado, debe tenerse en cuenta que ciertas actividades de la empresa pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Objetivo.

Administrar la seguridad de la información dentro de la organización y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la empresa.

Alcance.

Esta política se aplica a todos los recursos de la empresa y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

²⁹ Visión General – ISO 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información Requisitos. Pág. 10.

Responsabilidad.

El Gerente será el responsable de impulsar la implementación de la presente Política.

El Comité de Seguridad de la Información tendrá a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante la máxima autoridad de la organización, el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización) y la proposición de asignación de funciones.

El Responsable de Seguridad Informática asistirá al personal de la empresa en materia de seguridad de la información y coordinará la interacción con organismos especializados. Así mismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información de la empresa y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

El Responsable del Área de Administración cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

ORGANIZACIÓN INTERNA.

El GERENTE DE EMCAR, tiene toda la responsabilidad máxima respecto a la seguridad de la información.

Comité de Seguridad de la Información.

El Comité de Seguridad de la Información, integrado por entidades externas, Gerente General, representantes de las áreas administrativas de EMCAR, su objetivo es: “Asegurar que exista dirección y apoyo gerencial para establecer, implementar y monitorear las estrategias de Seguridad de la Información que requiera la entidad”.

Para efectos de desarrollo de la presente Política, se efectuará a través del Comité de Seguridad de la Información.

Dentro de la organización interna de Seguridad de la Información se identificarán roles a saber: Custodio, Usuario o Propietario de la información, cada rol debe identificar, analizar, evaluar, tratar y monitorear el cumplimiento de la Política.

Custodio: Tienen la responsabilidad de monitorear el cumplimiento de las actividades encargadas.

Usuario o Propietario: Debe verificar la integridad de la información y velar por que se mantenga la disponibilidad y confiabilidad de la misma.

Seguridad de la información roles y responsabilidades.

Las responsabilidades de seguridad de la información están definidas y asignadas de acuerdo a la clasificación dada a la información.

Separación de deberes.

La responsabilidad de la información deberá estar en cabeza de una sola persona para evitar conflicto en cuanto a responsabilidades. Lo anterior permite reducir oportunidades de modificación (intencional o no) no autorizada o mal uso de los activos de la organización.

Contacto con las autoridades.

Se mantendrán los contactos apropiados con las autoridades pertinentes, en caso de encontrar violación a la presente política de seguridad de la información.

Contacto con grupos de interés especial.

Se mantendrán los contactos apropiados con los grupos de interés especial (Policía, Bomberos, Defensa Civil) y asociaciones profesionales para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad de la información.

DISPOSITIVOS MÓVILES Y TELETRABAJO.

Política para dispositivos móviles.

El uso de los equipos portátiles fuera de las instalaciones de EMCAR únicamente se permitirá a usuarios autorizados por el Gerente, previa solicitud de la dependencia respectiva, y éstos se protegerán mediante el uso de los siguientes controles tecnológicos:

- Antivirus.
- Cifrado de datos.
- Restricción en la ejecución de aplicaciones.
- Restricción de conexión de dispositivos USB.
- Protección física mediante la guaya de seguridad.

La sincronización de dispositivos móviles con cualquier sistema de información de EMCAR, sólo estará permitido para personal autorizado por el Gerente y la dependencia respectiva.

Teletrabajo.

Cualquier funcionario de EMCAR, autorizado por el Gerente, que requiera tener acceso a la información de la empresa desde redes externas, podrá acceder remotamente mediante un proceso de autenticación; uso de conexiones seguras. Lo anterior asegurando el cumplimiento de requisitos de seguridad de los equipos desde los que se accede.

•SEGURIDAD DE LOS RECURSOS HUMANOS³⁰.

Generalidades.

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales repeticiones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

Objetivo.

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

³⁰ Visión General – ISO 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información Requisitos. Pág. 10.

Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la empresa en el transcurso de sus tareas normales.

Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Alcance.

Esta Política se aplica a todo el personal de la organización, cualquiera sea su situación, y al personal externo que efectúe tareas dentro del ámbito de la organización.

Responsabilidad.

El Gerente incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

El Gerente tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al Comité de Seguridad de la Información, a los propietarios de la información.

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Gerente maneje los reportes de incidentes y anomalías de los sistemas. Así mismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

Todo el personal de la empresa es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.

ANTES DE ASUMIR EL EMPLEO.

Selección.

Se realiza la verificación de antecedentes judiciales, disciplinarios, fiscales y seguimiento a la hoja de vida de todos los candidatos a emplear de conformidad con el reglamento interno de EMCAR y las leyes y regulaciones del estado colombiano.

Términos y condiciones del empleo.

Los acuerdos contractuales con los empleados y los contratistas deberán establecer las responsabilidades establecidas por EMCAR en el cumplimiento de la presente Política de Seguridad de la Información.

DURANTE LA EJECUCIÓN DEL EMPLEO.

Responsabilidades de la dirección.

La administración pedirá a todos los empleados y contratistas, aplicar la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización. Todos los empleados y/o contratistas tendrán acceso permanente a la política y se obligan a cumplirla.

El personal que ingrese vinculado de manera temporal y/o indefinida a EMCAR, deberá firmar que conoce y acepta lo definido en la política de Seguridad de manera obligatoria.

Toma de conciencia, educación y formación de la seguridad de la información.

El Gerente realizará capacitaciones a todos los empleados y contratistas de la organización de sensibilización, educación y formación adecuada y actualizaciones periódicas en las políticas y procedimientos de la organización, que sea relevante para su función laboral.

Proceso disciplinario.

Se solicitará proceso disciplinario formal y comunicado en lugar de tomar medidas contra los empleados que hayan cometido una violación de la seguridad de la información, y según corresponda la investigación será tramitada por el Proceso de Control Interno Disciplinario de la Entidad o la Procuraduría General de la Nación.

TERMINACIÓN Y CAMBIO DE EMPLEO.

Terminación o cambio de responsabilidades de empleo.

Las responsabilidades de seguridad de la Información y deberes que siguen vigentes después de la terminación o cambio de empleo, se deben definir y comunicarse al empleado o contratista y se deben hacer cumplir.

Es responsabilidad del Gerente asegurar que en el evento de la terminación y/o cambio de cargo al interior de EMCAR, el servidor hace la devolución de todos los activos de información y elementos asignados durante su relación.

La vigencia de los derechos de acceso y su revocatoria, debe estar estrechamente relacionados con la terminación de la relación laboral y/o contractual del servidor público y/o cambio del rol del servidor público en la empresa.

• **GESTIÓN DE ACTIVOS**³¹.

Generalidades.

La organización debe tener un acabado conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

• **Recursos de información:** bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada³².

• **Recursos de software:** software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios.

• **Activos físicos:** equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, máquinas de fax), medios magnéticos (discos), otros equipos técnicos (Relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento.

• **Servicios:** servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

³¹ Visión General – ISO 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información Requisitos. Pág. 11.

³² Norma ISO 27000. [En línea]. [Citado el 24 de enero de 2015]. Disponible en internet <http://www.iso27000.es/iso27002_8.html>

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para la entidad.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Objetivo.

Garantizar que los activos de información reciban un apropiado nivel de protección.

Clasificar la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Alcance.

Esta Política se aplica a toda la información administrada en la organización, cualquiera sea el soporte en que se encuentre.

Responsabilidad.

El Gerente y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Así mismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental.

El Gerente definirá las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. A su vez, controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones de la empresa.

RESPONSABILIDAD POR LOS ACTIVOS.

Inventarios de activos.

Los activos relacionados con la información y las instalaciones de procesamiento de información deben ser identificados dentro del inventario de activos de la empresa.

Propiedad de los activos.

Los activos involucrados dentro del inventario deben ser propios de la organización.

Uso aceptable de los activos.

Las normas para el uso aceptable de la información y de los activos asociados a la información y las instalaciones de procesamiento de información están identificadas en el presente documento y deben cumplirse de forma obligatoria por sus responsables.

Devolución de activos.

Todos los empleados y contratistas deberán devolver todos los activos de la organización en su poder a la terminación de su empleo, contrato o acuerdo.

CLASIFICACIÓN DE LA INFORMACIÓN.

Clasificación de la información.

La información se clasificará en función de los requisitos legales, el valor, criticidad y sensibilidad a la divulgación o modificación no autorizada.

Todos los activos de información en EMCAR serán clasificados según el contenido y los controles adecuados serán implementados de acuerdo a su importancia en la organización. Esta clasificación será realizada por el responsable de la misma, teniendo en cuenta: Su valor relativo, su privacidad, sensibilidad, el nivel de riesgo a que está expuesta y/o requerimientos legales de retención.

Estos niveles serán divulgados y oficializados a los usuarios de la información para asegurar que los niveles de protección son entendidos y se mantienen a través de la organización. Cada nivel de clasificación tendrá un conjunto de controles determinados por EMCAR, los que podrán ser complementados y aumentados, nunca disminuidos, por el Gerente. Dichos controles se utilizan para proveer un nivel de protección de la información apropiado y consistente dentro de la organización, sin importar el medio, formato o lugar donde se encuentre. Estos controles se aplican y mantienen durante el ciclo de vida de la información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción.

Si la información clasificada de EMCAR debe ser entregada a contratistas, asociados y terceros por efectos del negocio, previamente se deben firmar los acuerdos de

confidencialidad respectivos, que incluyan el seguimiento y cumplimiento de las prácticas de gestión segura establecido en la Política. Igualmente si la información clasificada de la EMPRESA es requerida por algún ente externo o ciudadano en donde opere EMCAR, su entrega está supeditada a la aprobación previa de su responsable y de las instancias establecidas.

EMCAR establece los controles de protección a la información.

Datos e información publicable: Aquellos en los que la Ley no ha dado el carácter de reservado y obliga a su publicación, si esta definidos como datos abiertos.

Datos e información no publicable: Aquellos en los que la Ley ha otorgado el carácter de reservados y de protección legal, por tal motivo no puede ser publicada.

Datos e información personal semiprivada: Datos e información personal que no es de dominio público, pero que ha sido obtenida u ofrecida por orden de una autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de administración de datos personales. Esta información puede ser o no sujeta a reserva por su titular.

Información que requiere protección por razones de seguridad nacional.

Top Secret: El acceso a la información por parte de personal no autorizado, así como la alteración en la integridad de la información podría dañar los intereses nacionales de manera grave y tendrá un alto impacto sobre la empresa.

Secreta: El acceso a la información por parte de personal no autorizado, así como la alteración en la integridad de la información podría dañar los intereses nacionales de manera seria y tendría un medio impacto sobre la empresa.

Confidencial: El acceso a la información por parte de personal no autorizado, así como la alteración en la integridad de la información podría dañar los intereses nacionales de manera significativa y tendría un bajo impacto sobre la empresa.

Restringida: El acceso a la información por parte de personal no autorizado, así como la alteración en la integridad de la información podría dañar los intereses nacionales y de la empresa de manera adversa.

Información que requiere protección por razones de privacidad personal.

Sensitiva: El acceso a la información por parte de personal no autorizado, así como la alteración en la integridad de la información podría dañar los intereses del estado o poner en peligro la seguridad de los ciudadanos.

En confianza: El acceso a la información por parte de personal no autorizado, así como la alteración en la integridad de la información podría perjudicar el mantenimiento de la Ley y

el orden, impedir la conducta efectiva del Gobierno o afectar adversamente la privacidad de sus ciudadanos.

Acceso a información TOP SECRET, SECRETA CONFIDENCIAL Y RESTRINGIDA.

- Las terceras partes que requieran acceso a información en medio físico y/o electrónico, deben presentar a EMCAR una autorización por parte del dueño de la información y se debe firmar un acuerdo de confidencialidad indicando las restricciones de uso de dicha información.
- Se deben utilizar los mecanismos apropiados de control de acceso a la información dependiendo de su nivel de clasificación.
- Los servicios públicos, contratistas, pasantes o estudiantes no pueden tomar información top secret, secreta, confidencial, y/o restringida cuando termine su vínculo con la empresa.
- La destrucción de información secreta, confidencial y restringida se realizará de acuerdo a métodos aprobados por el responsable de seguridad de la información. El único impedimento para la destrucción de la información puede ser una restricción señalada expresamente por parte del Asesor Jurídico, de acuerdo a la estructura orgánica de EMCAR, y/o radicada en las tablas de retención documental.

Almacenamiento de Información.

La información top secret, secreta confidencial y/o restringida almacenada en cualquier medio electrónico, o físico, debe ser protegida por medio de mecanismos de cifrado.

Los equipos de cómputo y/o portátiles que almacenen información top secret, secreta confidencial y/o restringida deben estar protegidos con mecanismos de seguridad para evitar que ante la pérdida del equipo una persona no autorizada pueda acceder a la información allí almacenada. Así mismo si son reasignados a usuarios diferentes, se debe borrar la información del disco de forma segura, de acuerdo a los lineamientos dados por el responsable de seguridad de la información.

Impresión de información.

La información clasificada como top secret, secreta confidencial y/o restringida debe ser enviada a la impresora y recogida inmediatamente, evitando que personal no autorizado tenga acceso a ésta.

Divulgación de información a terceros.

Los servidores públicos no deben divulgar información a terceros acerca de las vulnerabilidades de los sistemas lógicos o físicos de EMCAR, sin la previa autorización por

parte de los responsables de Seguridad de la Información y la firma de un acuerdo de confidencialidad.

Etiquetado de la información.

Los procedimientos para el etiquetado de la información serán aplicados de acuerdo con el esquema de clasificación de la información aprobada por la entidad, lo anterior teniendo en cuenta las Tablas de Retención Documental aprobadas para las diferentes áreas.

Manejo de activos.

Se aplicarán los procedimientos para el manejo de los activos de conformidad con el esquema de clasificación de la información aprobada por la empresa y presentada en este documento.

MANEJO DE MEDIOS DE SOPORTE.

Gestión de medios de soporte removibles.

La gestión de medios extraíbles se realizará de acuerdo con el esquema de clasificación adoptado por la entidad.

Los equipos de cómputo que tienen autorizado el manejo de USB y unidades reproductoras de CD/DVD, deben cumplir los siguientes requisitos.

- Tener habilitado el escaneo automático de virus
- Tener configurada en la herramienta de antivirus institucional, el bloqueo de la reproducción automática de archivos ejecutables.

Disposición de los medios de soporte.

La información será eliminada de los medios de comunicación de forma segura cuando ya no sea necesaria, utilizando procedimientos formales.

Transferencia de medios de soporte físico.

Los medios que contienen información deben estar protegidos contra el acceso no autorizado, mal uso o corrupción durante el transporte.

Se debe implementar la utilización de protocolos de seguridad para la encriptación de las claves más sofisticados.

• CONTROL DE ACCESO³³.

Generalidades.

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Objetivo.

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.

Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Controlar la seguridad en la conexión entre la red de la organización y otras redes públicas o privadas.

Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

³³ Visión General – ISO 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información Requisitos. Pág. 12.

Alcance

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información de la organización, cualquiera sea la función que desempeñe.

Así mismo, se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Responsabilidad.

El Gerente estará a cargo de:

- Definir normas y procedimientos para: La gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades; y el ajuste de relojes de acuerdo a un estándar preestablecido.
- Definir pautas de utilización de Internet para todos los usuarios.
- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways,) y validarlos periódicamente.
- Controlar la asignación de privilegios a usuarios.
- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones a la red, control de ruteo de red.
- Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.
- Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

- ✓ Evaluar los riesgos a los cuales se expone la información con el objeto de:
 - Determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
 - Definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.
 - Aprobar y solicitar la asignación de privilegios a usuarios.
 - Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.
 - Definir un cronograma de depuración de registros de auditoría en línea.

Los Propietarios de la Información o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

Los Responsable de las Unidades Organizativas, junto con el Gerente, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Así mismo, autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

El Responsable de la información cumplirá las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Evaluar el costo y el impacto de la implementación de “enrutadores” o “gateways” adecuados para subdividir la red y recomendar el esquema apropiado.
- Implementar el control de puertos, de conexión a la red y de ruteo de red.
- Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.

- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

El Comité de Seguridad de la Información aprobará el análisis de riesgos de la información efectuado. Así mismo, aprobará el período definido para el mantenimiento de los registros de auditoría generados.

REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO.

Política de control de accesos.

EMCAR garantiza entornos con controles de acceso idóneos, los cuales aseguran el perímetro, tanto en oficinas, recintos, áreas de carga y descarga, así como en entornos abiertos para evitar el acceso no autorizado a ellos. Del mismo modo, controla las amenazas físicas externas y vela por proveer las condiciones medioambientales requeridas para el funcionamiento de la plataforma tecnológica y para la preservación de sus activos de información documentales.

Así mismo, exige a los proveedores de servicios de tecnología, el cumplimiento de la implantación y efectividad de mecanismos de seguridad física, controles de acceso físico y condiciones medioambientales con que éste debe contar.

Los servidores públicos responsables de las áreas seguras tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- Las áreas de producción se catalogan como seguras y deben permanecer cerradas y custodiadas.
- El acceso a áreas seguras donde se procesa o almacena información top secret, confidencial y restringida, es limitado únicamente a personas autorizadas.
- El acceso a áreas seguras requieren esquemas de control de acceso, como tarjetas, llaves o candados.
- El responsable de un área segura debe asegurar que no ingresen cámaras fotográficas, videos, teléfonos móviles con cámaras.
- Se utilizan planillas para registrar la entrada y salida del personal.
- Se restringe el acceso físico a dispositivos como: puntos de acceso inalámbricos, puertas de enlace a redes y terminales de red que estén ubicadas en las áreas seguras.

Acceso a redes y a servicios en red.

Los usuarios que dispongan de acceso y servicios de la red son los que han sido específicamente autorizados para su uso.

Cada usuario es responsable por sus acciones mientras usa cualquier recurso de Información de EMCAR. Por lo tanto, la identidad de cada Usuario de los recursos de información está establecida de una manera única. Esta identidad de ninguna manera o por ninguna circunstancia podrá ser compartida. El sobrepaso a éste medio será tratado como una infracción a seguridad de la información.

Los niveles de acceso deben reflejar permanentemente una necesidad clara y demostrada de negocio y no deben comprometer la segregación de funciones y responsabilidades.

GESTIÓN DE ACCESO DE USUARIOS.

El acceso a la información de EMCAR, es otorgado sólo a usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad o tipo de servicio. El acceso a los recursos de información, es restringido en todos los casos sin excepción, y se da específicamente a quienes lo requieran en razón de sus funciones, con los privilegios apropiados y por un tiempo limitado.

Se debe identificar y autenticar a cualquier usuario que de manera local o remota, requiera utilizar los Recursos de Tecnología y operación, para lo que se requiere contar con sistemas de seguridad que cumplan con las siguientes características:

- Debe estar activo para acceder a la plataforma tecnológica y de operación, lo que significa que cada usuario tiene que identificarse y autenticarse antes de acceder a un recurso de tecnología por medio de un usuario y una contraseña.

- Una vez se han identificado y autenticado, los usuarios sólo podrán acceder a los recursos sobre los cuales están autorizados.
- Los eventos de ingreso y autenticación de usuarios serán registrados y monitoreados por los responsables de la información.

El acceso a los Activos de Información de EMCAR, debe ser controlado mediante un proceso formal de creación, modificación y eliminación del identificador de usuario.

Únicamente el responsable de la información, puede autorizar la creación de un usuario, este identificador de usuario debe ser asociado sólo a un individuo y la solicitud debe obedecer a una razón legítima de negocio.

El uso remoto de los activos de información y la computación móvil será realizado bajo una autorización previa de los responsables de la información, junto con su respectivo manejo de riesgo aprobado por EMCAR.

Ningún rol puede tener acceso a más de un ambiente.

Revisión de derechos de acceso de usuarios.

Los propietarios de activos deben revisar los derechos de acceso de los usuarios a intervalos regulares. Cualquier desviación será tratada como un incidente en seguridad de la información.

Los responsables deben dejar trazas del ejercicio de ésta actividad, las que serán objeto de revisiones de parte de EMCAR.

Cancelación o ajuste de los derechos de acceso.

Los derechos de acceso de todos los empleados y/o contratistas de la información e instalaciones de informática serán retirados en el momento de retiro de su empleo y/o terminación de contrato.

RESPONSABILIDADES DE LOS USUARIOS.

Uso de información secreta.

Se exigirá a los usuarios que sigan prácticas de la organización en el uso de información secreta de autenticación.

Control de acceso a sistemas y aplicaciones.

EMCAR tiene establecidos controles físicos y de acceso lógico para los ambientes de desarrollo, pruebas y producción de los Activos de Información para que permanezcan completamente separados.

El acceso a la información debe hacerse únicamente por los aplicativos y sistemas autorizados. En ningún caso la información puede ser accedida directamente.

Si entes externos tienen acceso a información crítica de EMCAR se deben suscribir acuerdos para la salvaguarda de la información. La información que está en manos de personas externas debe tener el mismo o mayor nivel de protección como si estuviera administrada por la empresa, por lo cual es necesario efectuar revisiones a fin de conocer cómo se está manejando y protegiendo la información externamente

Restricción de acceso a información.

El acceso a la información estará restringido de conformidad con la política de Control de acceso.

Sistema de gestión de contraseñas.

Junto con el nombre de usuario el funcionario recibirá una contraseña o clave para acceder a los recursos informáticos de la Entidad, la cual es de cambio obligatorio en el primer uso garantizando así su responsabilidad y único conocimiento sobre la misma. Dicha contraseña debe tener una longitud mínima de 8 (ocho) caracteres alfanuméricos, diferentes a nombres propios o cualquier otra palabra de fácil identificación.

Por seguridad se recomienda el cambio de dichas claves con una periodicidad de 90 (noventa) días.

Después de 3 (tres) intentos no exitosos de digitar la contraseña el usuario será bloqueado de manera inmediata y deberá solicitar el desbloqueo a la persona encargada de manejar la información.

Se prohíbe el uso de contraseñas compartidas. La contraseña es personal e intransferible. Las contraseñas nunca serán modificadas telefónicamente.

•SEGURIDAD FÍSICA Y AMBIENTAL³⁴.

Generalidades.

³⁴ Visión General – ISO 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información Requisitos. Pág. 13.

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones de la empresa. Así mismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible de la empresa, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones de la organización como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas de la entidad. Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente a la entidad pero situado físicamente fuera del mismo así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación.

Objetivo.

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de la empresa.

Proteger el equipamiento de procesamiento de información crítica de la empresa ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Así mismo, contemplar la

protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento de equipamiento informático que alberga la información.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Proporcionar protección proporcional a los riesgos identificados.

Alcance.

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información de la empresa: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, entre otros.

Responsabilidad.

El Gerente y los Propietarios de Información, según corresponda, las medidas de seguridad Física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Así mismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental.

El Gerente define las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Así mismo, controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones de la empresa.

Los Responsables de Unidades Organizativas definirán los niveles de acceso físico del personal de la organización a las áreas restringidas bajo su responsabilidad.

Los propietarios de la información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los empleados de la entidad cuando lo crean conveniente.

Todo el personal de la organización es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

ÁREAS SEGURAS.

Perímetros de seguridad física.

El perímetro de las áreas que contienen la información y sus instalaciones de procesamiento o bien sensibles o críticos estarán protegidos de acceso no permitidos.

Controles físicos de entrada.

Las áreas seguras se protegerán mediante controles de entrada adecuados para garantizar que se le permita el acceso únicamente al personal autorizado.

Para el ingreso de terceros, se tienen que registrar en la bitácora ubicada en un lugar visible a la entrada a este lugar.

Los privilegios (de los funcionarios y/o contratistas) de acceso físico deben ser eliminados o modificados oportunamente a la terminación, transferencia o cambio en las labores de un funcionario autorizado.

Las oficinas e instalaciones donde haya atención al público no deben permanecer abiertas cuando los funcionarios se levantan de sus puestos de trabajo, así sea por periodos cortos de tiempo.

Las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a las oficinas solo deben ser utilizadas por los funcionarios y/o contratistas autorizados y salvo situaciones de emergencia, estos no deben ser transferidos a otros funcionarios de la empresa o funcionarios provistos por terceras partes.

Las oficinas e instalaciones donde se maneje información sensible deben contar con sistemas de alarmas y cámaras.

Todos los funcionarios deben permanecer con el carnet que los identifica como funcionarios y/o contratistas de EMCAR, mientras permanezcan en las instalaciones.

Todos los funcionarios deben reportar, a la mayor brevedad, cualquier sospecha de pérdida o robo de carnet de identificación y tarjetas de acceso físico a las instalaciones.

Los funcionarios de EMCAR no deben intentar ingresar a áreas a las cuales no tengan la debida autorización.

Todos los visitantes que ingresan a la entidad, deben ser recibidos y estar acompañados por la persona a quien visitan durante su permanencia en las instalaciones del mismo.

Todos los visitantes que ingresan a la empresa, deben ser registrados en bitácora de visitantes con los datos personales y hora de entrada y salida de las instalaciones.

La documentación física generada, recibida y, en general, manipulada por los funcionarios de la organización y los funcionarios provistos por terceras partes deben estar ubicados en

archivos o repositorios con condiciones de temperatura y humedad adecuadas, de acuerdo con las directrices de la función archivística.

Seguridad de oficina, salones e instalaciones.

Las áreas administrativas deben contar con mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistema de alarmas.

El ingreso de terceros a las áreas administrativas debe estar debidamente registrado mediante una bitácora ubicada en un lugar visible a la entrada de estos lugares.

Los ingresos a las áreas administrativas deben ser monitoreados regularmente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.

Los departamentos deben estar separados de áreas que tengan líquidos inflamables o estén en riesgo de inundaciones e incendios.

Deben existir mecanismos de revisión y control del ingreso de cualquier tipo de material a los equipos.

En las áreas administrativas deberán existir sistemas de detección y extinción automáticas de incendios e inundación y alarmas en caso de detectarse condiciones inapropiadas.

Se debe monitorear y revisar de manera permanente el estado de los componentes de soporte físico, eléctrico y ambiental que hacen parte de las áreas administrativas, como son el sistema de aire acondicionado y el sistema de detección y extinción de incendios, entre otros.

Los trabajos de mantenimiento de redes eléctricas, cableados de datos y voz, deben ser realizados por personal especialista y debidamente autorizado e identificado.

Se deben realizar mantenimientos preventivos y pruebas de funcionalidad del sistema de UPS y/o plantas eléctricas, de los sistemas de detección y extinción de incendios y del sistema de aire acondicionado.

Se deben realizar mantenimientos preventivos y correctivos de los servidores, equipos de comunicaciones y de seguridad que conforman la plataforma tecnológica de EMCAR.

Se debe proveer un procedimiento, que garantice la realización del mantenimiento preventivo y correctivo de las estaciones de trabajo y equipos portátiles, así como su adecuación para la reutilización o reasignación de manera segura en el cual se conserve la disponibilidad, integridad y confidencialidad de la información contenida en los mismos.

El Gerente debe garantizar la adopción de los controles necesarios para asegurar que los suministros de electricidad así como las redes de comunicaciones se encuentran protegidos.

Protección contra amenazas externas y ambientales.

El Gerente debe monitorear las variables de temperatura y humedad de las áreas de procesamiento de datos.

Trabajo en áreas seguras.

EMCAR a través del responsable de seguridad de la información, debe establecer controles ante las diferentes amenazas que pueden afectar la normal operación. Los controles a implementar son:

Medio ambiente: El Gerente deberá monitorear las variables de temperatura y humedad de las áreas de procesamiento de información.

Identificación de terceros, explosivos y corrosivos: Todos los visitantes o terceras personas, que ingresan a las instalaciones de la empresa, deben poseer una identificación a la vista. Por ninguna razón se podrá tener material explosivo o corrosivo dentro o en sitio cercano a áreas definidas como seguras.

Fuego: En los centros de procesamiento deben instalarse detectores de humo, en forma adecuada y en número suficiente, para detectar conato o indicio de incendios. En las áreas seguras no se debe tener material inflamable tales como: Cajas, manuales, formas continuas, papel.

Los detectores deben probarse de acuerdo a las recomendaciones del fabricante o al menos una vez cada seis meses.

Se deben tener extintores debidamente aprovisionados, con carga vigente y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales.

Interferencia eléctrica y/o radiación electromagnética: El cableado lógico, debe estar protegido de las interferencias electromagnéticas producidas por equipos eléctricos y/o industriales.

Los cables de potencia deben estar separados de los cables de comunicación, siguiendo normas técnicas. Los equipos deben protegerse de fallas de potencia u otras anomalías de tipo eléctrico.

Sistema de abastecimiento de Potencia: El correcto uso de las UPS, se debe probar según las recomendaciones del fabricante, de tal forma que se garantice su operación y el suficiente tiempo para realizar las funciones de respaldo servidores y aplicaciones.

La planta eléctrica debe probarse regularmente, de acuerdo a las recomendaciones del fabricante y por lo menos una vez cada quince días.

Se deben tener interruptores eléctricos adicionales, localizados cerca de las salidas de emergencia, para lograr un rápido apagado de los sistemas en caso de una falla o contingencia. Las luces de emergencia deben funcionar en caso de fallas en la potencia eléctrica del proveedor del servicio público.

El cableado de la red lógica y eléctrica debe estar instalado y mantenido por ingenieros calificados con el fin de garantizar su integridad, operación y cumplimiento de normatividad de instalación.

Se deben realizar mantenimientos sobre los equipos de acuerdo a las recomendaciones del fabricante y realizarse únicamente por soporte técnico o personal autorizado. Si se tiene que enviar fuera de las instalaciones de la entidad, se debe asegurar la información y verificar la vigencia y alcance de las pólizas de seguro.

EQUIPOS.

Ubicación y protección de los equipos.

Los equipos de cómputo deben estar situados y protegidos para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado.

Servicios públicos de soporte.

El equipo deberá estar protegido contra fallas de energía y otras interrupciones causadas por fallas en el soporte de los servicios públicos.

Seguridad del cableado.

El cableado que transporta datos, energía y telecomunicaciones o el soporte de los servicios de información debe estar protegido contra la interceptación, interferencia o daños.

Mantenimiento de equipos.

Los equipos de cómputo deben tener un correcto mantenimiento para asegurar su continua disponibilidad e integridad.

Retiro de activos.

Los equipos, información o software no se deben retirar de sus sitios sin autorización previa.

Seguridad de equipos y activos fuera del predio.

Se aplicará seguridad a los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

Disposición segura o reutilización de equipos.

Todos los elementos del equipo que contienen los medios de almacenamiento deberán ser verificados para garantizar que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Política de escritorio limpio y pantalla limpia

Los puestos de trabajo deben estar limpios de papeles, soportes de almacenamiento extraíbles y cuando un computador este desatendido deberá bloquearse la pantalla.

Cuando sea apropiado, papeles y medios de información deben estar asegurados en armarios especiales, especialmente en horas fuera de las normales de trabajo.

Información confidencial y crítica para la empresa debe ser asegurada preferiblemente en armarios resistentes a impacto, fuego e inundación. Los computadores personales no se deben dejar dentro de sesión, se recomienda el uso de llaves físicas, contraseñas, y otro tipo de controles cuando no estén en uso.

Puntos de envío y recepción del correo, máquinas de fax, deben ser protegidos de acceso no autorizado.

Las fotocopiadoras deben estar protegidas de uso no autorizado.

•SEGURIDAD DE LAS OPERACIONES³⁵.

Generalidades.

EMCAR establecerá que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispysware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso.

³⁵ Visión General – ISO 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información Requisitos. Pág. 14

Será responsabilidad del Gerente autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

Así mismo, EMCAR define los siguientes lineamientos:

No está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad aprobadas previamente por EMCAR.
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.
- El uso de código móvil. Éste sólo podrá ser utilizado si opera de acuerdo con las políticas y normas de seguridad definidas y debidamente autorizado por el Gerente.

Objetivo.

Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

Alcance.

Todas las instalaciones de procesamiento y transmisión de información de la empresa.

PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES.

Procedimientos de operación documentada.

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad Informática. Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

- Procesamiento y manejo de la información.
- Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
- Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
- Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
- Instrucciones especiales para el manejo de “salidas”, como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.

- Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

EMCAR debe proveer a sus funcionarios los manuales de configuración y operación de los sistemas operativos, servicios de red, bases de datos y sistemas de información (comunicaciones y servicios como correo, intranet, WEB) así como todos los componentes de la plataforma tecnológica de la entidad.

Protección contra códigos maliciosos.

Se aplicarán controles de detección, prevención y recuperación para protegerse contra el código malicioso, en combinación con el conocimiento del usuario correspondiente.

EMCAR proveerá los recursos necesarios que garanticen la protección de la información y los recursos de procesamiento de la misma adoptando controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por la contaminación y/o el contagio de software malicioso.

El Gerente debe garantizar que los activos de información, así como, los recursos tecnológicos son actualizados periódicamente, evitando que código malicioso y virus ejecuten vulnerabilidades del sistema de los mismos.

EMCAR debe garantizar:

- Que el software usado para la mitigación de virus informáticos cuenta con las licencias de uso aprobadas, garantizando su autenticidad y su periódica actualización.
- La información almacenada en los activos de información tecnológicos que es transportada por la red de datos, es escaneada con una periodicidad establecida para garantizar así la seguridad de la misma.
- Los usuarios de los activos de información tecnológicos no pueden modificar la configuración establecida para el software antivirus.

Realización de copias de seguridad contra pérdida de datos.

EMCAR debe asegurar que la información en servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que sean confiables en caso de emergencia y guardadas por un periodo de tiempo determinado.

El Gerente establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma.

Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

REGISTRO Y SEGUIMIENTO.

Registrar eventos y generar evidencia.

Se producirán revisiones regulares y cuidadosas a los registros de eventos que se graban de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Proteger la información de registro contra alteración y registro no autorizado.

Los registros de información se protegerán contra la manipulación y el acceso no autorizado.

•SEGURIDAD DE LAS COMUNICACIONES³⁶.

Generalidades.

Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos equipos de cómputo.

Objetivo.

Garantizar la protección de la información en las redes y sus instalaciones de apoyo de procesamiento de información.

Alcance.

³⁶ Visión General – ISO 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información Requisitos. Pág. 15.

Todas las instalaciones de procesamiento y transmisión de información de la empresa.

GESTIÓN DE SEGURIDAD DE REDES.

Controles de redes.

Las redes deberán ser administradas y controladas para proteger la información en los sistemas y aplicaciones.

Seguridad de los servicios de red.

Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de la red deben ser identificados e incluidos en los acuerdos de servicios de red.

Separación en las redes.

La plataforma tecnológica de EMCAR que soporta los sistemas de información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. El Gerente es el encargado de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

EMCAR debe establecer mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la entidad.

Es responsabilidad de los administradores de recursos tecnológicos garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

TRANSFERENCIA DE INFORMACIÓN.

Políticas y procedimientos de transferencia de información.

Las políticas formales de transferencia, procedimientos y controles deberán estar en posición de proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.

Acuerdos sobre transferencia de información.

Dichos acuerdos deberán dirigirse a la transferencia segura de información comercial entre la organización y las partes externas.

EMCAR en su intención de proteger la información de la empresa, indistintamente del lugar o forma en que está se encuentre almacenada, proveerá los recursos necesarios para garantizar la protección de la misma al momento de ser transferida, comunicada a un tercero o al salir de sus instalaciones según necesidad de la actividad o proceso particular.

El intercambio electrónico de información utilizando el canal de internet institucional, se debe realizar con base en estándares de documentos electrónicos y mensajes de datos de dominio público, regidas por organismos idóneos de carácter nacional e internacional y utilizando mecanismos criptográficos de clave pública que garanticen la integridad, confidencialidad, autenticidad y aceptación de la información.

Cuando se considere necesario, los servicios de intercambio de información también incluirán garantías de “no repudio”.

El Gerente velará por la protección de la información, sin embargo el contenido de los archivos enviados a través del canal de Internet de la entidad será directamente responsabilidad del funcionario y/o contratista.

Los responsables del intercambio de información con entidades externas deben definir en compañía del Gerente las estrategias para la correcta gestión e intercambio seguro de la misma.

Los responsables del intercambio de información con entidades externas deben diseñar, establecer y aplicar acuerdos en los cuales se definan las responsabilidades en el intercambio de información de las partes que interactúen en el mismo.

El Gerente debe proveer los recursos necesarios con los cuales sea posible garantizar el correcto, adecuado y seguro intercambio de información desde estaciones de trabajo y equipos portátiles, así, como desde los dispositivos externos o móviles. Así mismo, debe garantizar que las transacciones de EMCAR realizadas de manera electrónica o haciendo uso de las redes de comunicaciones y las estaciones de trabajo de la misma, cuentan con los controles suficientes para evitar transmisiones incompletas, enrutamiento no apropiado o erróneo, repeticiones de las mismas no autorizadas, pérdida de confidencialidad, integridad de las mismas y pérdida de disponibilidad del servicio.

Los administradores de los activos de información tecnológicos y recursos informáticos deben aplicar los controles necesarios que garantizan la disponibilidad, confidencialidad e integridad de la información transmitida electrónicamente por medio de recursos tecnológicos de propiedad o provistos por la organización, según necesidad o el nivel de criticidad de la misma.

Los usuarios o funcionarios tanto directos como los provistos por terceras partes que interactúen en procesos de intercambio de información al exterior de la empresa deben cumplir los lineamientos, recomendaciones y/o estrategias establecidas para este propósito en EMCAR.

Mensajes electrónicos.

La información involucrada en la mensajería electrónica será debidamente protegida.

Acuerdos de confidencialidad o de no divulgación.

Se debe revisar, identificar y documentar regularmente los diferentes requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información.

• GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN³⁷.

Generalidades.

Establecer los lineamientos generales para la gestión de incidentes de seguridad de la información, con el fin de prevenir y limitar el impacto de los mismos.

Objetivo.

Garantizar un enfoque coherente y eficaz para la gestión de incidentes en la seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.

Alcance.

La política de gestión de incidentes de seguridad de la información está dirigida a toda persona que tenga legítimo acceso a los sistemas informáticos de la organización, incluso aquellos gestionados mediante contratos con terceros y lugares relacionados.

GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN.

Responsabilidades y procedimientos.

La responsabilidad y el procedimiento de manejo para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información está en cabeza del Gerente.

Informe de eventos de seguridad de la información.

³⁷ Visión General – ISO 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información Requisitos. Pág. 17.

Los eventos de seguridad de información se comunicarán a través de canales de gestión adecuadas tan pronto como sea posible.

Informe de debilidades de seguridad de la información.

Los funcionarios y contratistas que utilizan los sistemas y servicios de información deben observar y reportar cualquier debilidad de seguridad de información observada o sospechada en los sistemas o servicios.

Evaluación de eventos de seguridad de la información.

El Gerente es el encargado de valorar los eventos de seguridad de información y decidir si han de ser clasificados como incidentes de seguridad de la información.

Respuesta a incidentes de seguridad de la información.

Los incidentes de seguridad de información deberán recibir una respuesta de conformidad con los procedimientos documentados.

Aprendizaje obtenido de los incidentes de seguridad de la información.

Los conocimientos adquiridos a partir del análisis y la resolución de incidentes de seguridad de información se deben utilizar para reducir la probabilidad o el impacto de los incidentes en el futuro.

Recopilación de evidencia.

EMCAR debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como evidencia.

• ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO³⁸.

Generalidades.

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles de la empresa.

³⁸ Visión General – ISO 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información Requisitos. Pág. 17

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades de la organización puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades de la empresa y asegurar la reanudación oportuna de las operaciones indispensables.

Objetivo.

Minimizar los efectos de las posibles interrupciones de las actividades normales de la organización (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

Maximizar la efectividad de las operaciones de contingencia de la entidad con el establecimiento de planes que incluyan al menos las siguientes etapas:

- **Notificación / Activación:** Consistente en la detección y determinación del daño y la activación del plan.
- **Reanudación:** Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
- **Recuperación:** Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal de la empresa y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

Alcance.

Esta Política se aplica a todos los procesos críticos identificados de la empresa.

Responsabilidad.

El Gerente participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

El Gerente y los empleados cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la organización.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la empresa.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la organización.

El Gerente revisará periódicamente los planes bajo su incumbencia, como así también identificar cambios en las disposiciones relativas a las actividades de la empresa aún no reflejadas en los planes de continuidad.

Los administradores de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

El Comité de Seguridad de la Información tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información de la empresa frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

- Identificar y priorizar los procesos críticos de las actividades de la organización.
- Asegurar que todos los integrantes de la entidad comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad de la empresa.
- Elaborar y documentar una estrategia de continuidad de las actividades de la organización consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de las actividades de la empresa de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades.
- Proponer las modificaciones a los planes de contingencia.

CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN.

Planificación de la continuidad de la seguridad de la información.

Análisis de riesgos enfocado específicamente a valorar el impacto de incidentes que comprometen la continuidad del negocio teniendo en cuenta que este impacto será mayor cuanto más dure el incidente. Los pasos a seguir para realizarlo son los habituales de un análisis de riesgos:

- Se identifican los procesos críticos de negocio.
- Se identifican los eventos que pueden provocar interrupciones en los procesos de negocio de la organización, por ejemplo: fallos de los equipos, errores humanos, robos, incendios, desastres naturales y actos terroristas.
- Se evalúan los riesgos para determinar la probabilidad y los efectos de dichas interrupciones en cuanto a tiempo, escala de daños y período de recuperación.
- Identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información en el ámbito del sistema de gestión de la seguridad de información, y establecer acciones de control y responsables de contribuir en la mitigación de los riesgos.

Implementación de la continuidad de la seguridad de la información.

Establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.

Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Verificar la información de continuidad de los controles de seguridad establecidos y aplicados a intervalos regulares con el fin de asegurarse de que son válidos y eficaces en situaciones adversas.

REDUNDANCIA.

Disponibilidad de instalaciones de procesamiento de información.

Las instalaciones para el procesamiento de información deben contar con la suficiente redundancia para satisfacer los requisitos de disponibilidad.

• CUMPLIMIENTO³⁹.

Generalidades.

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados.

Objetivos.

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la empresa y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de la organización.

Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la empresa.

Alcance.

Esta Política se aplica a todo el personal de la empresa, cualquiera sea su situación.

Así mismo, se aplica a los sistemas de información, normas, procedimientos, documentación y plataformas técnicas de la empresa y a las auditorías efectuadas sobre los mismos.

³⁹ Visión General – ISO 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información Requisitos. Pág. 18.

Responsabilidad.

El Gerente cumplirá las siguientes funciones:

- Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.
- Realizar revisiones periódicas de todas las áreas de la organización a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
- Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos.
- Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

CUMPLIMIENTO.

Cumplimiento de requisitos legales y contractuales.

Las situaciones o acciones que violen la presente Política deben ser detectadas, registradas, analizadas, resueltas y reportadas de manera inmediata a través de los canales señalados para el efecto.

Se entenderán incluidas a la Política las regulaciones nacionales e internacionales que de tiempo en tiempo se expidieren y que se relacionen con la misma.

Cuando de la aplicación de tales normas se presentare un conflicto, se entenderá que aplica la más restrictiva, es decir, aquella que exija el mayor grado de seguridad.

Así mismo y con el fin de mantener un nivel de seguridad adecuado con el negocio de EMCAR, esta Política se debe apoyar en las mejores prácticas de seguridad de la información.

Periódicamente se debe evaluar el cumplimiento de los requerimientos de seguridad por parte de los Usuarios. El incumplimiento de los requerimientos de seguridad, se debe registrar como un incidente a la Política de Seguridad de la Información que debe ser resuelto de acuerdo con los procedimientos de manejo de incidentes de EMCAR.

Deben establecerse procedimientos apropiados para asegurar el cumplimiento con las restricciones de carácter legal en el uso de material que puede estar sujeto a derechos de propiedad intelectual tales como derechos de autor y derechos de diseño.

Identificación de los requisitos de legislación y contractuales aplicables.

Todos los requisitos pertinentes, legislativos estatutarios, reglamentarios y contractuales, y el planteamiento de la entidad para cumplir con estos requisitos deberán estar explícitamente identificados, documentados y protegidos al día para cada sistema de información y la organización.

Derechos de propiedad intelectual.

Se aplicarán procedimientos apropiados para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales, relacionados con los derechos de propiedad intelectual y uso de productos de software propietario.

Se debe establecer en los contratos de trabajo de empleados y en los contratos de desarrollo realizados por proveedores y contratistas, cláusulas respecto a la propiedad intelectual de EMCAR, al material y productos generados en el desarrollo del negocio.

Protección de registros.

Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de conformidad con los requisitos de legalidad, reglamentarias, contractuales y comerciales.

Privacidad y protección de la información identificable personalmente.

Se garantizará la privacidad y la protección de la información de identificación personal a lo dispuesto en la legislación y la reglamentación pertinente en su caso.

REVISIONES DE SEGURIDAD DE LA INFORMACIÓN.

Revisión independiente de la seguridad de la información.

El enfoque de la organización para la gestión de seguridad de la información y su aplicación (es decir, los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

Cumplimiento con las políticas y normas de seguridad.

El Gerente deberá comprobar periódicamente el cumplimiento de los procedimientos de procesamiento de la información dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad.

Revisión del cumplimiento técnico.

Los sistemas de información deben ser revisados regularmente para cerciorarse que se da cumplimiento a las políticas y normas de seguridad de la información de la entidad.

Las situaciones o acciones que violen la presente Política deben ser detectadas, registradas, analizadas, resueltas e informadas al comité de Seguridad de la Información y a las áreas responsables por su tratamiento de manera inmediata.

CONCLUSIONES

En el proceso de la realización de auditorías, entrevistas y encuestas en la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”, permitió la identificación de amenazas y/o riesgos en cuanto a la seguridad de la información, tales como: Conexiones eléctricas no organizadas, pérdida de los datos por falta de copias de seguridad periódicas, ingreso de personal no autorizado a las instalaciones u oficinas de la empresa, plan de contingencia no elaborado, ni publicado, no hay roles y responsabilidades asignadas, no hay restricción de páginas web para los empleados, en algunos equipos de cómputo no hay asignación de usuarios, ni claves de acceso, tampoco los permisos para el ingreso al sistema, dispositivos expuestos a robos (portátiles y aparatos móviles), entre otros; por este motivo, se propuso el diseño de las políticas de seguridad de la información, buscando su confidencialidad, integridad y disponibilidad.

La creación de las políticas de seguridad de la información se basaron en la Norma ISO 27001:2013, tomando los dominios más aplicables a los requerimientos informáticos de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR” que fueron en total 11 (once), que darán los controles para el mejoramiento de la administración de la información, cumpliendo así los objetivos propuestos del presente proyecto.

Siendo la información el activo más importante de la organización, los riesgos y/o amenazas se deben reducir o mitigar, por lo que la empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR” no es ajena a que estos posibles ataques informáticos pongan en peligro los datos, es aquí donde las políticas de seguridad de la información deben ponerse en práctica y aplicarlas.

RECOMENDACIONES

Socializar e implementar el documento de Políticas de Seguridad de la Información con la Gerente, el personal administrativo y personas externas vinculadas a la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”.

El Gerente será el encargado que las políticas de seguridad de la información deben revisarse periódicamente (mínimo una vez por año), o antes, en caso de producirse cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, que puedan afectar su continuidad. La aprobación de las actualizaciones y/o modificaciones, se realizará por parte del Comité de Seguridad de la Información.

El Gerente realizará capacitaciones a todos los empleados y contratistas de la organización de sensibilización, educación y formación adecuada y actualizaciones periódicas en las políticas y procedimientos de la organización, que sea relevante para su función laboral.

El responsable de un área segura debe vigilar que no ingresen cámaras fotográficas, videos, teléfonos móviles con cámaras.

El personal de la empresa junto con el nombre de usuario recibirá una contraseña o clave para acceder a los recursos informáticos de la Entidad, la cual es de cambio obligatorio en el primer uso garantizando así su responsabilidad y único conocimiento sobre la misma. Dicha contraseña debe tener una longitud mínima de 8 (ocho) caracteres alfanuméricos, diferentes a nombres propios o cualquier otra palabra de fácil identificación.

Por seguridad se recomienda el cambio de dichas claves con una periodicidad de 90 (noventa) días. Se prohíbe el uso de contraseñas compartidas, la cual debe ser personal e intransferible.

BIBLIOGRAFÍA

GIL PECHUÁN, Ignacio. Sistemas y Tecnologías de la Información para la Gestión. Madrid, McGraw-Hill, 1997.

ANGARITA LÓPEZ, Liseth Tatiana. Diseño del plan de gestión de seguridad de la información para controlar el acceso a las áreas restringidas de la empresa Ingepec LTDA en la ciudad de Ocaña: Tesis de grado para especialización en auditoría de sistemas, 2014.

ALIAGA FLORES, Luis Carlos. Diseño de un sistema de gestión de seguridad de la información para un instituto educativo: Tesis de grado, Pontificia Universidad Católica del Perú, 2013.

ISCALA TOBITO, Nancy Auristela. Diseño de un protocolo de seguridad de la información del área financiera de la secretaria de educación departamental de Norte de Santander Ocaña: Tesis de grado para especialización en auditoría de sistemas, 2014.

HERNÁNDEZ PINTO, María Gabriela. Tesis Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial, Escuela Superior Politécnica del Litoral.2006. Guayaquil, Ecuador.

REYES CASADIEGOS, María Teresa. Álvarez Cabrales, Andru. Tesis Diseño de Políticas de Seguridad de la Información para la Oficina de Archivo y Correspondencia de la Universidad Francisco de Paula Santander Ocaña. Universidad Francisco de Paula Santander Ocaña. 2013. Colombia

GÓMEZ VIEITES, Álvaro., Enciclopedia de la Seguridad Informática, Alfa omega Grupo editor, México, Primera Edición, 2007.

NTC ISO/IEC 5411 - 1:2006. Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la tecnología de la información y las comunicaciones. Parte 1: Conceptos y modelos para la gestión de la tecnología de la información y las comunicaciones (ISO/IEC 13335-1:2004).

Norma Técnica NTC ISO/IEC 27001:201, Sistemas de Gestión de la Seguridad de la Información (SGSI).

DALTABUIT GODAS Enrique, VÁSQUEZ José de Jesús, La seguridad de la información”. Limusa Noriega Editores, 2007. p. 215

NIMA RAMOS Jonathan D, Guía para la elaboración de planes de recuperación para sistemas de información empresarial y de negocios, Universidad de Plura, 2014.

DALTABUIT GODAS Enrique, VÁSQUEZ José de Jesús, La seguridad de la información”. Limusa Noriega Editores, 2007. p. 26

DALTABUIT GODAS Enrique, VÁSQUEZ José de Jesús, La seguridad de la información”. Limusa Noriega Editores, 2007. p. 221.

CONSTITUCIÓN POLÍTICA DE COLOMBIA, Ley Estatutaria 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013.

FUENTES ELECTRÓNICAS

ISOTools. La norma ISO 27001 y la importancia de la gestión de la seguridad de la información. [En línea]. [Citado el 21 octubre de 2014]. Disponible en internet <<http://www.isotools.org/pdfs/Monografico-ISO-27001-ISOTools.pdf>>

VEGA BRICEÑO, Edgar Armando. Los sistemas de información y su importancia para las organizaciones y empresas. [En línea]. [Citado el 23 octubre de 2014]. Disponible en internet <<http://www.gestiopolis.com/Canales4/mkt/simparalas.htm>>

TIMETOAST. [En línea]. [Citado el 25 Septiembre de 2014]. Disponible en internet <<http://www.timetoast.com/timelines/historia-de-la-seguridad-informatica>>

TIMERIME. [En línea]. [Citado el 12 Septiembre de 2014]. Disponible en internet <<http://timerime.com/es/evento/1870578/Siglo+XXI+Procesamiento+de+datos/>>

MONTENEGRO, Luis. Artículo: Seguridad de la Información: Más que una actitud, un estilo de vida. [En línea]. [Citado el 28 Septiembre de 2014]. Disponible en internet <<http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/>>

VASCO AGUAS, Mireya I y VERDEZOTO SALTOS, Mercedes E. Plan de Gestión de Seguridad de la Información basado en TIC'S para la Facultad de Ingeniería de Sistemas de la Escuela Politécnica Nacional. Quito, Ecuador.. 2009. 226 h. Escuela Politécnica Nacional. [en línea]. <<http://bibdigital.epn.edu.ec/handle/15000/4370?mode=full>>

CAMPAÑA TENESACA, Oscar E. Plan de Propuesta para la Implantación de la Norma de Seguridad Informática ISO 27001:2005, para el Grupo Social Fondo Ecuatoriano Populorum Progressio (GSFEPP). Quito, Ecuador. 2010. 207h. [en línea] <<http://dspace.ups.edu.ec/handle/123456789/4468?mode=full>>

CALDERÓN, Diego y SÁNCHEZ, David. Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa Comware S.A. en la ciudad de Quito, aplicando la norma ISO/IEC 27001. Quito, Ecuador. 2012. 216h. Universidad Politécnica Salesiana. [En línea] <https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCwQFjAA&url=http%3A%2F%2Fdspace.ups.edu.ec%2Fbitstream%2F123456789%2F3901%2F1%2FUPSST000906.pdf&ei=GDsSUrOEJao2wWI7YCYAQ&usg=AFQjCNFsKFoVxj06G_YJYJx906JAEUBptQ&sig2=CxONXw8ZwdZkaOorjVnyxw&bvm=bv.50768961,d.b2I>

EMCAR. (2014). Empresa Comunitaria de Acueducto de Rio de Oro, Cesar. www.emcar.com.co.

TORO Raquel, ISO 27001 ¿Cómo mejorar la seguridad de la información en las organizaciones. [En línea]. [Citado el 20 Octubre de 2014]. Disponible en internet <<http://www.pmg-ssi.com/2014/10/iso-27001-como-mejorar-la-seguridad-de-la-informacion-en-las-organizaciones/>>

ANEXOS

Anexo A. ENTREVISTA A LA GERENTE DE LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR “EMCAR”.

Objetivo: Entrevista dirigida a la gerente de la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”, con el fin de obtener información acerca de las políticas de seguridad de la información.

1. ¿La empresa cuenta con una política de seguridad de la información, que este formalmente establecida, publicada y aprobada por la misma?
2. ¿La política de seguridad de la información de la organización incluye normas y/o procedimientos para garantizar el uso adecuado de la información?
3. ¿El personal administrativo ha sido concientizado sobre la importancia de contar con unas políticas de seguridad de la información?
4. ¿La empresa en sus respectivos contratos cuenta con condiciones de confidencialidad y responsabilidades de la información al personal encargado de administrar la información?
5. ¿Cuenta en la actualidad con un comité de seguridad en su empresa?
6. ¿Está consciente de la necesidad de incluir penalidades para aquellos que incumplan la política de seguridad?
7. ¿Cree necesario formar un comité encargado del análisis de los casos que llegasen a ocurrir?
8. ¿Tiene claro el objetivo principal de la política de seguridad de la información en su empresa?
9. ¿Ha recibido un entrenamiento o capacitación de seguridad de la información su personal?
10. En su empresa, ¿Existen planes, procedimientos y entrenamiento para el manejo de una crisis?
11. ¿Todas las partes interesadas de la empresa entienden la importancia de la seguridad de la información?

12. ¿Los computadores de su empresa cumplen con la política de seguridad para asegurar la información?

Anexo B. ENCUESTA A LA GERENTE DE LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR “EMCAR”.

Objetivo: Encuesta dirigida a la gerente de la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”, con el objetivo de conocer más a fondo sobre las políticas de seguridad de la información.

1. ¿Existen documentos de políticas de seguridad de la información?

SI _____ NO _____

2. ¿Existe una normativa relativa a la seguridad de la información?

SI _____ NO _____

3. ¿Existen procedimientos relativos a la seguridad de la información?

SI _____ NO _____

4. ¿Existe un responsable de las políticas, normas y procedimientos?

SI _____ NO _____

5. ¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad?

SI _____ NO _____

6. ¿La dirección y las áreas de la empresa participan en temas de seguridad?

SI _____ NO _____

7. ¿Existe un acuerdo de confidencialidad de la información que se accesa?

SI _____ NO _____

8. ¿Existe un inventario de activos actualizado?

SI _____ NO _____

9. ¿El inventario contiene activos de datos, software, equipos y servicios?

SI _____ NO _____

10. ¿Existe un responsable de los activos?

SI _____ NO _____

11. ¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?

SI _____ NO _____

12. ¿Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad?

SI _____ NO _____

13. ¿Se recogen los datos de los incidentes de forma detallada?

SI _____ NO _____

14. ¿Informan a los usuarios de las vulnerabilidades observadas o sospechadas?

SI _____ NO _____

15. ¿Existen controles de entrada para protegerse frente al acceso de personal no autorizado?

SI _____ NO _____

16. ¿La ubicación de los equipos está de tal manera para minimizar accesos innecesarios?

SI _____ NO _____

17. ¿Existen protecciones frente a fallos en la alimentación eléctrica?

SI _____ NO _____

18. ¿Existe seguridad en el cableado frente a daños e interceptaciones?

SI _____ NO _____

19. ¿Se asegura la disponibilidad e integridad de todos los equipos?

SI _____ NO _____

20. ¿Existe una gestión de los password de usuarios?

SI _____ NO _____

21. ¿Existe una revisión de los derechos de accesos de los usuarios?

SI _____ NO _____

22. ¿Existen políticas de limpieza en el puesto de trabajo?

SI _____ NO _____

Anexo C. ENCUESTA AL PERSONAL DE LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR “EMCAR”.

Objetivo: Encuesta dirigida a los empleados de la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”, con el objetivo de conocer la necesidad de diseñar las políticas de seguridad de la información.

NOMBRE DEL EMPLEADO: _____ **CARGO:** _____

1. ¿Utiliza usted el equipo de cómputo de la empresa para desempeñar sus funciones?
SI _____ NO _____
2. ¿Se utilizan perímetros de seguridad para proteger las áreas que contienen de la misma?
SI _____ NO _____
3. ¿Realiza copias de seguridad de la información que maneja dentro de sus funciones?
SI _____ NO _____
4. ¿Se tienen controles apropiados para el ingreso de personal no autorizado?
SI _____ NO _____
5. ¿Utiliza mecanismos de seguridad para el control de acceso a la organización?
SI _____ NO _____
6. ¿Las aplicaciones a las que accede usted, cuentan con contraseña para permitir el ingreso de los usuarios?
SI _____ NO _____
7. ¿Tiene conocimiento si dentro de la organización existen lineamientos para la seguridad de la información?
SI _____ NO _____
8. ¿Conoce usted de la existencia de una guía y/o norma formal de políticas de seguridad de la información?

SI _____ NO _____

9. ¿La política de seguridad de la información, está formalmente aprobada, establecida y publicada?

SI _____ NO _____

10. ¿Sabe usted si existe un comité de seguridad de la información?

SI _____ NO _____

Anexo D. OFICIO SOLICITUD CAPACITACIÓN.

Ocaña, febrero 10 de 2015

Gerente

MARÍA FERNANDA CARRASCAL VEGA

Empresa Comunitaria de Acueducto de Rio de Oro, Cesar "EMCAR"
Rio de Oro, Cesar.

Asunto: Solicitud

Cordial saludo.

Por medio de la presente me permito solicitar llevar a cabo la capacitación de las políticas de seguridad de la información para la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar "EMCAR", como proyecto de grado de los estudiantes Haineth Parra Alvernia, Javier Contreras Navarro, Diana Yisney Díaz Pacheco y Edwin Jesús López Ovalle, el cual tiene como título **DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR "EMCAR"**, este incluye al personal administrativo y aquellos a los cuales usted considere deben hacer parte de esta información.


La capacitación está contemplada para el día martes 10 de febrero del presente año, cuya duración será de una hora.

Por lo anterior, agradezco la atención a la presente.


Atentamente,

HAINETH PARRA ALVERNIA
HAINETH PARRA ALVERNIA
Estudiante

Diana Yisney Díaz Pacheco
DIANA YISNEY DÍAZ PACHECO
Estudiante

 **EMCAR**
RECIBIDO
Fecha: 10-02-15
Hora: 6:45 pm
María Fernanda Carrascal V.
JAVIER CONTRERAS NAVARRO
Estudiante
Edwin Jesús López Ovalle
EDWIN JESÚS LÓPEZ OVALLE
Estudiante

Anexo E. ACTA DE CAPACITACIÓN.

EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR 		Acta de Capacitación	
Código: 001	Versión: 1	Fecha de emisión: 2015-02-10	Pág. 1 de 2
Capacitación dirigida por: HAINETH PARRA ALVERNIA JAVIER CONTRERAS NAVARRO DIANA YISNEY DÍAZ PACHECO EDWIN JESÚS LÓPEZ OVALLE		Fecha de la capacitación: 10 -Febrero - 2015	Acta No:
		Lugar: EMCAR	Duración: 2 Horas
Objetivo de la capacitación: Brindar orientación sobre la puesta en marcha de la Política de Seguridad de la Información.			
Temas tratados: Políticas de Seguridad de la Información. Dominios Objetivos de control		Controles Riesgos y/o amenazas	
Conclusiones y observaciones: <ul style="list-style-type: none"> • Las buenas prácticas de las políticas de seguridad de la información busca brindar la mejora continua a la organización. • Vincular al personal administrativo en el buen uso de las políticas de seguridad de la información. 			

EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR



Acta de Capacitación

Código: 001

Versión: 1

Fecha de emisión: 2015-02-10

Pág. 2 de 2

Nombre y Apellidos	N° Cédula	Cargo	Dependencia	Correo Electrónico	Firma
Betty Donado Pinón	1064836685	Aux Contable	Contabilidad	contabilidad@emcar.com	
Norelys Chinchilla S.	1064837745	Aux comercial		norelys-101002@hotmail.com	Norelys Chinchilla S.
Aura Carina Ruedas Osorio	1064836392	Aux. Administrativa		auracarinaruedasosorio@hotmail.es	
Van's Fernando Camacho	26.864.146	Gerente	Activo	vianale@Uninil.com	Van's Camacho U.

Anexo F. FOTOGRAFÍAS DE LA CAPACITACIÓN.



Anexo G. EVALUACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR “EMCAR”.

Objetivo: Brindar orientación sobre la puesta en marcha de las políticas de seguridad de la información de la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”, con el objetivo de conocer más a fondo sobre las políticas de seguridad de la información.

NOMBRE: _____

CARGO: _____

1. ¿Qué entiende usted por políticas de seguridad de la información?

2. ¿Defina que son roles y responsabilidades?


3. ¿Sabe usted realizar copias de seguridad y cada cuanto las realiza?

4. ¿Cuáles son las características mínimas que debe contener su contraseña para el ingreso al sistema?

5. ¿Conoce usted que es un acceso restringido o no autorizado?

6. ¿Informa a la Gerencia cualquier irregularidad de la seguridad de la información?

Anexo H. CONSTANCIA CAPACITACIÓN Y ENTREGA DE LAS POLÍTICAS.



**LA SUSCRITA GERENTE DE LA
ADMINISTRACION PÚBLICA COOPERADA EMPRESA
COMUNITARIA DE ACUEDUCTO DE RIO DE ORO
A.P.C. EMCAR E.S.P.**

HACE CONSTAR

Que los estudiantes **HAINETH PARRA ALVERNIA** con código **850106**, **JAVIER CONTRERAS NAVARRO** con código **850115** y **EDWIN JESÚS LÓPEZ OVALLE** con código **850108**, brindaron capacitación en **POLITICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RÍO DE ORO, CESAR "A.P.C. EMCAR E.S.P.**, dejando como evidencia el documento de dichas políticas.

Dado en Rio de Oro – Cesar, a los diez (10) días del mes de febrero de 2015

**ADMINISTRACIÓN PÚBLICA COOPERADA
EMPRESA COMUNITARIA DE
ACUEDUCTO DE RIO DE ORO
A.P.C. EMCAR E.S.P.
C.P. 5687 del 15 de Feb. de 2005
M.A. 500.003.372.2
MARIA FERNANDA CÁRRASCAL VEGA
Gerente A.P.C EMCAR E.S.P.**

Calle Humareda No. 3-01 - Rio de Oro - Cesar – Colombia
Teléfonos: (7) 5619091 - (7) 5619447
E-mail: info@emcar.com.co / Sitio Web: www.emcar.com.co