PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS



ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TRABAJO DE GRADO

INFORME FINAL:

"PLANES Y CONTROLES DE TRATAMIENTO DE RIESGOS TECNOLÓGICOS PARA LA GESTIÓN DE INFORMACIÓN BASADO EN NORMAS DE SEGURIDAD: CASO GADPE"

PREVIA OBTENCIÓN DEL TÍTULO:

INGENIERO EN SISTEMAS Y COMPUTACIÓN

LÍNEA DE INVESTIGACIÓN:

GOBIERNO Y ADMINISTRACIÓN DE TECNOLOGÍA DE INFORMACIÓN

AUTOR:

CEDEÑO ROSERO DAVID ABSALON

ASESORA:

ING. SUSANA PATIÑO

Esmeraldas-Ecuador

Julio, 2017

Disertación aprobada luego de haber dado cumplimiento a los requisitos exigidos por el reglamento de grado de la PUCESE, previa a la obtención del título de Ingeniero de Sistemas y Computación.

_____

PRESIDENTE DEL TRIBUNAL DE GRADUACIÓN.

_____

Ing. Kléber Vera T.

LECTOR 1.

_____

Mgt. David Rodríguez

LECTOR 2.

_____

Ing. Susana Patiño

DIRECTOR DE TESIS.

_____

Mgt. Xavier Quiñonez Ku

DIRECTOR DE ESCUELA.

FECHA:……

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, Cedeño Rosero David Absalon, portadora de la cédula de identidad No. 0803847540, declaro que los resultados obtenidos en la investigación que presento como informe final, previo a la obtención del título de **Ingeniero en Sistemas y Computación** son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola, exclusiva responsabilidad legal y académica.

David Cedeño Rosero

CI 0803847540

DEDICATORIA

Dedico el trabajo de grado a Dios, mi familia, maestros y amigos.

A Dios, puesto que nada se puede lograr sin su bendición y voluntad, y gracias a tales bendiciones he logrado culminar esta etapa.

A mi madre, cuyo apoyo incondicional y dedicación son la causa principal de la consecución de mis logros personales y profesionales, sin ella esto no sería posible.

A mi padre, por ser una de las bases principales en mi formación como ser humano y profesional.

A mi esposa, por estar siempre a mi lado y apoyarme en cada paso de mi vida.

A mi familia, quiénes de una forma u otra me han brindado su apoyo incondicional.

A mis maestros, quiénes a diario me heredaban un poco de sus conocimientos y experiencia, además de alimentar mi amor por esta profesión.

A mi asesora, por su inacabable paciencia y enorme dedicación, su apoyo y consejos fueron pilares fundamentales para mí en este proceso.

A mis amigos, por ser incondicionales en su apoyo y estar siempre presentes sin importar las circunstancias.

AGRADECIMIENTO

Agradezco a todas la personas cuyo apoyo y colaboración fueron fundamentales para la culminación de este proyecto.

A Dios ya que sin el nada es posible.

A mis padres que son los principales responsables de todo lo que he logrado hasta hoy, su apoyo in condicional y su enorme sacrificio para educarme han sido la base de todo en mi vida.

A mi esposa, que está siempre apoyándome para que siga adelante y me supere cada vez más.

A mis maestros, por su dedicación absoluta a su profesión y por el conocimiento brindado durante mis estudios profesionales.

A la Ing. Susana Patiño, por su paciencia, disponibilidad, buen trato y asesoría durante todo este proceso desde su inicio hasta su culminación.

A cada uno de los lectores cuyos consejos y correcciones fueron fundamentales para la mejora y finalización de mi trabajo de grado.

A mis amigos, por ser un apoyo sin estar obligados a serlo.

RESUMEN

La presente investigación es muy importante para el departamento de TIC del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas, ya que su finalidad es garantizar la protección del activo más importante de la institución, la información, garantizando su disponibilidad, accesibilidad e integridad.

La importancia de la información para el crecimiento de las organizaciones, y el éxito de sus objetivos ha aumentado la necesidad de protegerla y para ello muchas organizaciones en el mundo han optado por el uso de la norma de seguridad de la información ISO 27001, y confiado en su aplicación, la seguridad de la información con resultados excelentes, minimizando el riesgo y evitando las amenazas. Aplicando de la forma correcta la norma, la organización garantizaría la correcta protección de la información.

El principal problema encontrado durante el desarrollo del proyecto fue identificar y organizar cada uno de los controles a aplicar para la creación de las políticas de seguridad; con la aplicación de las políticas, el departamento de TIC minimizará los riesgos y amenazas a los que está expuesta la información, garantizando una gestión adecuada y un correcto manejo de los activos.

Palabras claves: Procesos, Políticas, Métricas, Información, Seguridad, Activos, Riegos.

ABSTRACT

The present investigation is very important for the TIC´s department of the Autonomous Government Decentralized of the Province of Esmeraldas, since your finality is guarantee the protection of the most important active of the institution, the information, guaranteeing your availability, accessibility and integrity.

The importance of information for the growth of the organizations, and the success of your objectives has increased the need to protect it, and for this many organizations in the world had opted by the use of the safety regulation of ISO information 27001, and trusted in your application, the security of information with excellent results, minimizing the risk and preventing the threats. Applying of the correct form the norm, the organization would guarantee the correct protection of the information.

The principal problem encountered during the development of the project was to identify and organize each of the controls to applied for the creation of security politics; with the implementation of politics, the TIC´s department will minimize the risks and threats to which the information is exposed, guaranteeing adequate management and proper asset management.

Keywords: Processes, Politics, Metrics, Information, Security, Assets, Risks.

ÍNDICE GENERAL

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD iii
DEDICATORIA iv
AGRADECIMIENTO v
RESUMEN vi
ABSTRACT vii
INTRODUCCIÓN 12
Presentación de la investigación 12
Planteamiento del problema 13
Justificación 14
Objetivos 15
Objetivo general 15
Objetivos específicos 15
CAPÍTULO I 16
1. MARCO DE REFERENCIA 16
1.1. Antecedentes 16
1.2. Bases teóricas científicas 17
1.2.1. Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas 17
1.2.1.1. Ubicación geográfica. 17
1.2.1.2. Visión 18
1.2.1.3. Misión 18
1.2.1.4. Objetivos estratégicos 18
1.2.1.5. Plan Estratégico Informática 19
1.2.1.6. Disposiciones Legales 19
1.2.1.7. Misión de la dirección de TIC 19
1.2.1.8. Visión de la dirección de TIC 20
1.2.2. Tecnología de la Información y Comunicaciones (TIC's) 20
1.2.2.1. Definición 20
1.2.2.2. Las tecnologías 21
1.2.2.3. Papel de las TIC's en las empresas 21

1.2.3. Gestión de la Seguridad de la información 22
1.2.3.1. Definición 22
1.2.3.2. Planificación 22
1.2.3.3. Análisis y evaluación de Riesgos 23
1.2.3.4. Selección de Controles 24
1.2.3.5. Tratamiento de Riesgos 25
1.2.3.6. Técnicas de manejo de riesgos 25
1.2.2.6.1. Evitar 25
1.2.2.6.2. Reducir 26
1.2.2.6.3. Asumir 26
1.2.2.6.4. Transferir 26
1.2.3.7. Objetivo del tratamiento de riesgos 26
1.2.3.8. Medios de transmisión de ataques 27
1.2.3.9. Actores que amenazan la seguridad 28
1.2.4. Tecnologías de la Seguridad 28
1.2.5. Familia ISO 27000 29
1.2.5.1. ISO/IEC 27000 29
1.2.5.2. ISO/IEC 27001 29
1.2.5.2.1. Objetivo de la Norma 30
1.2.5.2.2. Controles del anexo A de la norma 30
1.2.5.3. ISO/IEC 27002 32
1.2.5.4. ISO/IEC 27003 32
1.2.5.5. ISO/IEC 27004 33
1.2.5.6. ISO/IEC 27005 33
1.2.5.7. ISO/IEC 27006 33
1.2.5.8. Certificación 33
1.2.6. CICLO DE DEMING 34
1.2.6.1. ¿Qué es el ciclo de DEMING? 34
1.2.6.2. Definición de las etapas del ciclo de DEMING 35
1.2.6.2.1. Planificar (Plan) 35
1.2.6.2.2. Hacer (Do) 35

1.2.6.2.3. Controlar o Verificar (Check) 35
1.2.6.2.4. Actuar (Act) 35
1.2.6.3. Aplicación del ciclo de DEMING en la norma ISO 27001 36
1.2.6.3.1. Definición de un SGSI 36
1.2.6.3.2. Fundamentos 36
1.2.6.3.3. ¿Para qué sirve un SGSI? 37
1.3. Marco Legal 38
CAPITULO II 39
2. METODOLOGÍA 39
2.1. Descripción y caracterización del lugar 39
2.2. Tipo de investigación 40
2.2.1. Descriptiva 40
2.2.2. Explicativa 40
2.2.3. De Campo 40
2.3. Métodos y técnicas 41
2.3.1 Métodos 41
2.3.2. Técnicas 41
2.4. Población y muestra de estudio (técnicas de muestreo) 42
2.4.1. Población 42
2.4.2. Muestra 42
2.5. Descripción del instrumento 42
2.5.1. Entrevista 42
2.6. Técnicas de procesamiento y análisis de datos 42
2.7. Normas éticas 43
CAPITULO III 44
3. RESULTADOS 44
3.1. Análisis e interpretación de resultados 44
CAPITULO IV 47
4. PROPUESTA 47
4.1. Políticas de seguridad de la información 47
4.1.1. Seguridad ligada a los recursos humanos 51

4.1.2. Gestión de activos 54
4.1.3. Control de accesos 56
4.1.4. Cifrado 62
4.1.5. Seguridad Física y ambiental 64
4.1.6. Seguridad en la operativa 67
4.1.7. Seguridad en las telecomunicaciones 73
4.1.8. Adquisición desarrollo y mantenimiento de los sistemas de información 75
4.1.9. Relaciones con suministradores 79
4.1.10. Gestión de incidentes en la seguridad de la información 81
4.1.11. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio 82
4.1.12. Cumplimiento 84
4.1.13. Control del documento e historia de cambios 85
4.2. Plan para la implementación de políticas 87
CAPITULO V 97
5. CONCLUSIONES Y RECOMENDACIONES 97
5.1. Conclusiones 97
5.2. Recomendaciones 97
REFERENCIAS 98
ANEXOS 102

ÍNDICE DE TABLAS

Tabla 1 Área segura del departamento de TIC 65
Tabla 2 Plan para la implementación de políticas 96
Tabla 3 Matriz de Riesgo 121

ÍNDICE DE ILUSTRACIONES

Ilustración 1 Controles ISO/IEC 27002 106

INTRODUCCIÓN

Presentación de la investigación

Diversas han sido las herramientas que se han desarrollado o mejorado a fin de tratar de reducir los riesgos asociados con el manejo de la información y uso de la tecnología que administra la seguridad de dicha información. Sin embargo, ha sido evidente que ningún mecanismo de seguridad, logra ser completamente efectivo, e incluso deja de cumplir su propósito si no se controla el elemento más sensible, el recurso humano.

La seguridad de la información consiste en combinar las herramientas, técnicas de seguridad y el factor humano para detectar fugas de información, ataques de hackers y dejar de lado las vulnerabilidades o amenazas que atenten, contra la seguridad de la información.

Los Sistemas de Gestión de Seguridad de la Información son descritos por la ISO/IEC 27001 e ISO/IEC 27002, definido por un conjunto de políticas o reglas para la correcta administración de la Información, dentro de las empresas u organizaciones, incluyendo el diseño, implantación, mantenimiento de los procesos que gestionan de manera eficiente la accesibilidad de la información asegurando la confidencialidad, integridad y disponibilidad de la información minimizando los riesgos.

El departamento de TIC del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas es una entidad integrada bajo la necesidad de brindar servicios tecnológicos eficientes como implementación y manejo de infraestructura tecnológica, redes, desarrollo de aplicaciones y servicios de capacitación tecnológica a la ciudadanía esmeraldeña.

Al ser el departamento de TIC el encargado del manejo de la infraestructura tecnológica y los sistemas de información es por obvias razones el principal responsable de la seguridad de los activos de información de la institución por lo cual las falencias por la falta de controles oportunos y de un plan de tratamiento de riesgos para su gestión se convierte en un factor

crítico en contra del cumplimiento de los objetivos de la institución, por lo cual es de importancia la implantación de plan efectivo y controles que minimicen los riesgos, amenazas y las consecuencias en caso de hacerse efectiva alguna de estas.

Planteamiento del problema

Al 2016, el departamento de TIC del Gobierno autónomo descentralizado de la provincia de Esmeraldas, no cuenta con los controles adecuados, ni con un plan de tratamiento de riesgos para la gestión de seguridad de la información.

Carencia de políticas de seguridad, falta de un controles, pérdida de información, ausencia de un manual de funciones y procedimientos, inexistencia de planes de capacitación, falta de continuidad en los planes de crecimiento y carencia de un Sistema Integral de Seguridad de la Información en el departamento de TIC del Gobierno autónomo descentralizado de la provincia de Esmeraldas son algunas de los factores que agudizan la inseguridad de la información.

En el caso específico, al no contar el departamento de TIC del Gobierno autónomo descentralizado de la provincia de Esmeraldas con un Sistema de Gestión de la Seguridad de Información o de un plan de tratamiento de riesgos se han visto retrasados los objetivos organizacionales de la institución y ha conllevado a niveles de ineficiencia en la labor interna de la institución, una vez detectada la necesidad que tiene el departamento de TIC y con el ánimo de aportar al mejoramiento de los servicios brindados por esta institución, se plantea desarrollar el proyecto con tema:

“PLANES Y CONTROLES DE TRATAMIENTO DE RIESGOS TECNOLÓGICOS PARA LA GESTIÓN DE INFORMACIÓN BASADO EN NORMAS DE SEGURIDAD: CASO GADPE”

Justificación

Una de las acciones planteadas por toda organización pública o privada radica en la introducción de estrategias que estén dirigidas a optimizar los procesos de seguridad de la información con el propósito salvaguardar lo considerado mundialmente como el activo más importante LA INFORMACIÓN.

Esta investigación aportará con la aplicación de los enfoques teóricos relacionados con la gestión de seguridad de la información, aplicando las normas de seguridad ISO/IEC 27001.

La ejecución de este proyecto beneficiara de manera objetiva al funcionamiento interno del departamento de TIC del Gobierno autónomo descentralizado de la provincia de Esmeraldas, el personal deberá asumir cambios en la manera de acceder a la información y seguir rigurosos controles para evitar la errónea administración de los datos.

La institución se verá beneficiada con la propuesta y posterior aplicación si lo considera pertinente de las políticas y el plan de tratamiento de riesgos, las políticas proporcionaran una seguridad de alto nivel, sin causar fugas de la información.

Al elaborar el plan de tratamiento de riesgos el departamento de TIC obtendrá un grado de reconocimiento en comparación con las demás instituciones al contar con información segura, a nivel práctico, esta investigación constituirá una oportunidad importante para el Gobierno autónomo descentralizado de la provincia de Esmeraldas, abordará con precisión cuáles son los problemas que se presentan al momento de acceder a la información y corregirlos sin causar fuga de la misma.

Objetivos

Objetivo general

Minimizar los riesgos y amenazas a los que se ve fuertemente expuesta la información de la unidad informática del Gobierno autónomo descentralizado de la provincia de Esmeraldas (GADPE) mediante la propuesta de políticas y el plan de tratamiento de riesgos basado en normas de seguridad.

Objetivos específicos

- Conocer la situación actual de la empresa con respecto a la seguridad de la información.
- Describir las políticas de Seguridad de la Información que permitan una rápida detección y respuesta a los incidentes de seguridad.
- Diseñar un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Elaborar el Plan de tratamiento de riesgos a través de la implementación de controles y procedimientos de monitorización para la detección a tiempo de posibles incidentes.

CAPÍTULO I

1. MARCO DE REFERENCIA

1.1. Antecedentes

La alta incidencia de la información en el cumplimiento de los objetivos institucionales de una organización y su crecimiento, han llevado a las organizaciones a la utilización de diversas medidas de protección y aseguramiento de la información. Así, esta tendencia se ha venido incrementando a lo largo de los años.

Estudios previos se enfocan en la importancia de una buena gestión de seguridad de la información para el cumplimiento de cada uno de los objetivos organizacionales de cualquier institución, además de una descripción de los fundamentos de la norma de seguridad ISO 27001, dando solución posteriormente a cada una de las falencias de seguridad a las que se ve expuesta la información de una empresa (Ladino, Villa, y López, 2011).

En posteriores estudios ligados a la gestión seguridad de la información se han analizado las principales debilidades empresariales incluyendo las referentes a la seguridad de la información a través de una investigación descriptiva para obtener una mejora considerable en la efectividad del trabajo de organización en general al lograr mitigar las debilidades antes encontradas (Arévalo, Bayona, y Rico, 2015).

A nivel nacional instituciones como la empresa MEGADATOS de Quito y la Corporación Metropolitana de Salud forman parte del conjunto de instituciones que han optado por una significativa mejora en el manejo y gestión de la información a través de la metodología plan, do, check y act (PDCA) o ciclo de mejora continua definida por la ISO 27001 para disminuir el número de amenazas a los que se ve expuesta información y reducir el impacto de dichas amenazas al explotar cualquier vulnerabilidad encontrada durante el análisis y elaboración

de la matriz de riesgos, obteniendo así a través de la implantación de un plan de tratamiento de riesgos un incremento de la integridad, disponibilidad y confidencialidad de la información. (Alvarez y García, 2007; Flores, Jiménez y Hidalgo, 2010) .

El enfoqué de los estudios dedicados a la protección del activo más importante de una organización (la información) es el mismo en todos los casos, las variantes entre uno y otro están determinadas por los activos de la institución y sus falencias o necesidades de controles para su protección, ninguna organización es idéntica en cuanto a los riesgos y amenazas a los que está expuesta la información pero el objetivo de todas es la preservación de la confidencialidad, integridad y disponibilidad de este activo tan importante.

La presente investigación pretende al igual que los estudios previos antes mencionados, la mitigación de las amenazas y vulnerabilidades a los que está expuesta la información del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas garantizando la disponibilidad, integridad y accesibilidad de esta.

1.2. Bases teóricas científicas

1.2.1. Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas

1.2.1.1. Ubicación geográfica.

El Gobierno Autónomo Descentralizado de la provincia de Esmeraldas se encuentra estratégicamente ubicado en la calle 10 de Agosto entre Bolívar y Pedro Vicente Maldonado cerca al parque Central 20 de Marzo justo en el centro de la ciudad, y repartiendo desde allí su labor a toda la ciudadanía.

1.2.1.2. Visión

El Gobierno Autónomo Descentralizado de la provincia de Esmeraldas se ha propuesto alcanzar la visión de liderar los procesos enfocados al desarrollo de la provincia a través de la ejecución eficiente de sus competencias, con un enfoque de total responsabilidad social, respeto y pluriculturalidad dentro de su territorio (Prefectura de Esmeraldas, 2014). Esta sirve como fuente de inspiración para la institución representando así la esencia que guía la iniciativa de cada uno de los trabajadores.

1.2.1.3. Misión

La misión en particular de tan emblemática institución pública de la ciudad de Esmeraldas es promover el desarrollo económico y social proporcionando servicios de calidad y la colaboración con liderazgo, solidaridad y transparencia de todas las autoridades pertinentes, departamentos y pobladores para asegurar una alta calidad de vida, conservar las riquezas naturales de la provincia y convertirse en referente a nivel nacional (Prefectura de Esmeraldas, 2014), Dejando en claro el compromiso de la institución con la comunidad.

1.2.1.4. Objetivos estratégicos

Los objetivos del Gobierno Autónomo descentralizado de la provincia de Esmeraldas están dirigidos al fortalecimiento, crecimiento y fortalecimiento están de la provincia, de acuerdo al estatuto Prefectura de Esmeraldas, 2014 son los siguientes:

- Promover el fortalecimiento de la institución y la mejora de sus capacidades administrativas, operativas y financieras a través de procesos periódicos.
- Elaborar una Agenda Territorial establecida entre las tres provincias hermanas de la zona 1 del Ecuador, Esmeraldas y otros actores.
- Fortalecer los procesos de participación ciudadana y de control social.

1.2.1.5. Plan Estratégico Informática

Dentro de la institución (GADPE) y su estructura organizacional la dirección de tecnólogas de la información está posicionada de manera que se le permite ejecutar las actividades tanto de apoyo como asesoría a las unidades usuarias y la alta dirección de la institución; cuenta con plena participación en la generación de cambios de mejora tecnológica y toma de decisiones, Conjuntamente certifica su autonomía con respecto a los espacios de los usuarias y garantiza la cobertura de servicios a todas las unidades de la organización (Prefectura de Esmeraldas, 2014).

1.2.1.6. Disposiciones Legales

De acuerdo la norma de control interno 410-03, establecida por entidad de control y vigilancia de gastos públicos o contraloría: El Plan Informático Estratégico de Tecnología deberá contar con un nivel de detalle que permita la definición adecuada de los planes operativos de tecnología de la información y determina claramente cuál es el aporte a los objetivos estratégicos de la institución; contiene propuestas de mejora con la colaboración de todos los departamentos de la institución y un estudio situacional. (Prefectura de Esmeraldas, 2014).

1.2.1.7. Misión de la dirección de TIC

Dentro de la institución y su estructura organizacional la dirección de TIC es una unidad ya posicionada que brinda asesoría y apoyo a todos los departamentos de la institución y a sus máximas autoridades, que participa en la toma de decisiones, que genera cambios de mejora tecnológica; que garantiza su independencia y asegura la cobertura de servicios a todas las unidades de la entidad (Prefectura de Esmeraldas, 2014).

1.2.1.8. Visión de la dirección de TIC

La dirección de TIC cuenta con el objetivo de posicionarse a través del Gobierno Electrónico como un referente de calidad a nivel nacional y mejora continua, creación de valor y conocimiento de la información para toma de decisiones y apoyar la gestión de la organización (Prefectura de Esmeraldas, 2014).

1.2.2. Tecnología de la Información y Comunicaciones (TIC's)

1.2.2.1. Definición

Según Gil (2002), las TIC se definen como todos los elementos ligados estrechamente a la digitalización de señales analógicas, sonidos, textos e imágenes, manejables en tiempo real como aplicaciones, sistemas, herramientas, técnicas y metodologías. Por su parte, Ochoa y Cordero (2002), consideran a las TIC como el conjunto de elementos relacionados al almacenamiento, procesamiento y la transmisión digitalizada de la información tales como el conjunto de productos y procesos derivados de las nuevas herramientas tanto de hardware como de software, soportes y canales de comunicación (Montiel, 2008).

Asimismo, Thompson y Strickland, (2004) han definido a las tecnologías de la información como cada uno de los elementos tales como herramientas, dispositivos, equipos y componentes electrónicos consignados a controlar, manejar y manipular toda la información de la cual depende el crecimiento económico de cualquier organización.

Es importante comprender que solo las organizaciones capaces de utilizar todos los medios a su alcance y saquen provecho a las oportunidades de su mercado visualizando en todo momento las amenazas, cumplirán con sus objetivos de éxito, teniendo en consideración el ambiente tan complejo que actualmente deben enfrentar (Montiel, 2008).

1.2.2.2. Las tecnologías

Actualmente la tecnología ocupa un puesto de privilegio en el desarrollo de las actividades diarias, se ha convertido para muchos en algo fundamental para la subsistencia diaria (Montiel, 2008).

Los puntos citados anteriormente enmarcan un mismo concepto principal definiendo a la tecnología como el conjunto de herramientas, procedimientos, instrucciones y conocimiento científico. Que ayudan a buscar la perfección y así satisfacer las necesidades del ser humano.

1.2.2.3. Papel de las TIC's en las empresas

Para encaminarse al éxito, crecer de manera ágil y rápida y cumplir con sus objetivos estratégicos institucionales muchas son las empresas que han optado por las tecnologías de la información y la comunicación o en sus siglas TIC, las instituciones económicas surgieron en una época de capacidades computacionales muy limitadas y de altos costos en comunicaciones; las tecnologías de la información y comunicación poseen la capacidad de minimizar los costos en procesamiento de información, coordinación y comunicación, no es sorpresa que tal reducción en costos tanto en computación como en comunicación generase un cambio estructural significativo de la economía (Brynjolfsson y Hitt, 2000).

En América del Sur el uso de la web o internet en las diferentes empresas ha tenido un aumento favorable, pero no se compara con Europa o América del Norte que son las grandes potencias mundiales en uso de las TIC's.

A pesar de ser cada vez mayor la implementación y uso de la informática en las instituciones, su valía en proceso de las actividades productivas no depende de las capacidades computacionales sino del nivel de productividad y destreza de los jefes de bloque departamental para enlazarla a la estructuración de procesos nuevos, estructura organizacional y procedimientos, es decir, determinar a la inversión tecnológica como punto clave para el crecimiento organizacional (Alderete, 2012).

La brecha digital que actualmente afrontan las Pymes, es debido a la falta de conocimientos adecuados, capacitaciones y educación a los empleados, y no tanto a la falta de tecnologías y su infraestructura. Como afirman Chen y Wellman (2003) existen muchas brechas digitales y no solo una. Por lo que, es apropiado definir que la brecha digital es multifacética dentro y entre las instituciones (Alderete, 2012).

1.2.3. Gestión de la Seguridad de la información

1.2.3.1. Definición

La seguridad de la información se define como el aseguramiento del uso adecuado y correcto de los recursos del sistema de información; que el uso de la información sea el idóneo, que el acceso a esta se encuentre contenida, que exista controles para que la modificación solo sea posible para usuarios autorizados (SGSI, 2015). En pocas palabras la seguridad de la información garantiza la preservación de la confidencialidad, integridad y disponibilidad de la información.

1.2.3.2. Planificación

Actualmente las organizaciones deben acoger un conglomerado mínimo de controles de seguridad debido a la rápida evolución de la infraestructura tecnológica requerida, para proteger tanto a los sistemas como los activos de información. El plan de seguridad tiene como objetivo proporcionar una visión general de sus requisitos en cuanto a su seguridad y describir los controles para cumplir dichos requisitos, determinar tanto los comportamientos como responsabilidades que se espera de cada ente que ingresa al sistema, delinear el aporte de cada individuo que accede al sistema (Galindo, 2014, pág. 107).

El sistema de seguridad en el proceso de planificación debe ser entendido por el personal de seguridad, los administradores de programas y los propietarios del sistema; el tratamiento de los controles de seguridad a aplicarse en los sistemas es responsabilidad de los encargados de la gestión y ejecución de los sistemas de información. (Galindo, 2014, pág. 108).

Es de vital importancia elaborar un plan de respuesta a incidentes, mantener un soporte en la institución y probarlo con regularidad; un plan bien elaborado y que cumpla con los estándares necesarios, además de reducir los efectos de una transgresión a la información también minimiza la mala publicidad (Galindo, 2014, pág. 108).

Son 4 las faces en la que puede ser dividido el plan de respuestas a incidentes:

- Gestión para la detección y/o minimización de los incidentes.
- Evaluar e investigar el incidente
- Empezar con la reposición de cada uno de los recursos que fueron afectados por el incidente.
- Informar del incidente oportunamente a los responsables.

Cabe recalcar que para una correcta gestión de incidentes la respuesta debe ser rápida y oportuna. Los requerimientos del plan incluyen:

- Apoyo económico por parte de la institución
- Contar con plan de acción eficaz
- Personal capacitado y experto en emergencias computacionales
- Contar con estrategias aprobadas
- Contar con recursos de hardware (recursos físicos)

1.2.3.3. Análisis y evaluación de Riesgos

Cualquier metodología conocida sirve de acogida para el análisis y evaluación de riesgos, pero la exigencia de la norma de seguridad de la información es que la metodología acogida arroje resultados comparables y reproducibles (Aranda, 2009).

Se recomienda para el cálculo de riesgos un método cualitativo debido a que se podrá abarcar con mayor facilidad todos los activos. Un método cuantitativo exigiría llevar a los activos a un valor monetario lo que en muchos casos se torna en una tarea complicada o tarda

demasiado, debido a que implica tanto el valor como la afectación que puede tener en su entorno. (Aranda, 2009).

La metodología identifica todas las amenazas existentes para cada activo, la posibilidad de ocurrencia de estas amenazas, las vulnerabilidades que pueden hacer que dicha amenaza se materialice y la posibilidad que dicha amenaza penetre tal vulnerabilidad. "El valor del riesgo está dado por el producto matemático del valor del activo, encontrado en la tasación, por el valor de la mayor de posibilidad de amenaza" (Aranda, 2009).

La escala para calcular las posibilidades es de 1 al 5, siendo 5 las de mayor posibilidad. De la misma forma como en la tasación de activos se puede descartar las de menor valor para enfocarse en las verdaderamente importantes, el valor del umbral es decisión del grupo taller (Aranda, 2009).

1.2.3.4. Selección de Controles

Los controles son las contramedidas o salvaguardas especificadas en el anexo A de la Norma ISO 27001:2005, enfocados a los 11 dominios de cobertura de la norma. Dichos 11 Dominios incluyen la adecuada gestión de activos, operaciones, comunicaciones, incidentes, continuidad del negocio y de los sistemas de información especificamente al mantenimiento, adquisición y desarrollo de dichos sistemas, además de las políticas para la seguridad, organización de la seguridad de la información, controles para el acceso, cumplimiento y seguridad tanto ambiental como física y de recursos humanos.

Los controles que se deben implementar en la organización se lo realizan en tres fuentes:

- Del tratamiento del riesgo, orientados a eliminar vulnerabilidades o minimizar el impactos.
- Los requerimientos legales (implementación no es discutible).
- Producto de las operaciones en el negocio de la compañía (Aranda, 2009).

Para tener una mayor información sobre las diferentes prácticas que se deben utilizar para poder implementar los controles se puede tomar como referencia la ISO 17799:2005. La organización tiene la posibilidad de crear controles propios siempre y cuando los que se encuentran en la norma no sean del beneficio de la organización. (Aranda, 2009).

1.2.3.5. Tratamiento de Riesgos

Para controlar los riesgos que pueda tener un activo o bien inmerso en la seguridad en la información debe realizarse una clasificación de las alternativas para poder manejarlos dentro de los procesos de la organización. Dicha clasificación se denomina tratamiento de Riesgos, el cual trae consigo una estructura que tiene un control adecuado luego de haber identificado, priorizado identificado los riesgos mediante acciones factibles y efectivas. (Galindo, 2014, pág. 110).

La planificación de la seguridad por muy buena que sea, será inútil si todas sus medidas no se cumplen a cabalidad (ITIL Foundation, 2011). De igual manera afirmar que los riesgos serán eliminados es un desacierto debido a que los riesgos pueden ser reducidos y controlados pero no eliminados.

1.2.3.6. Técnicas de manejo de riesgos

1.2.2.6.1. Evitar

Tratar de evadir el riesgo tomando ciertas medidas para evitar que se materialicen. Es siempre la primera alternativa a considerar y se cumple cuando en el interior de los procesos se observan cambios importantes por diferentes razones como: mejoramiento, rediseño o eliminación, resultado de cada una de las acciones y controles promovidos. Por ejemplo: manejo de recursos, controles de calidad, mantenimiento preventivo de los equipos, desarrollo tecnológico, entre otros (Rodríguez, 2011).

1.2.2.6.2. Reducir

Reducir implica llevar a un nivel bajo la probabilidad de riesgo y para eso se debe tomar medidas o acciones que guíen a la organización a disminuir esto y de igual manera al impacto. Este método es el más sencillo y económico para, previo a la aplicación de medidas posiblemente costosas y complicadas superar cualquier debilidad (Rodríguez, 2011).

1.2.2.6.3. Asumir

Al asumir un riesgo se debe tener en cuenta lo que es un riesgo residual, que no es más que el resultado de un riesgo luego de haber sido reducido o transferido, este riesgo de mantenerse es el gerente del proceso quien se hace cargo de la perdida residual y crea planes de contingencia para su control. (Rodríguez, 2011).

1.2.2.6.4. Transferir

Reducir el riesgo también se puede reducir el efecto mediante herencia de pérdidas a otras organizaciones, un ejemplo claro es que la información considerada de vital importancia puede ser respaldada y almacenada en una ubicación segura y aislada a la institución (Rodríguez, 2011).

1.2.3.7. Objetivo del tratamiento de riesgos

Este plan, se crea para detectar la acción correcta de gestión, recursos, responsabilidades y prioridades para poder controlar los riesgos de seguridad de la información. Las acciones que se deben contemplar en el plan de tratamiento de riesgos según UNAD Universidad Nacional abierta y a distancia de Colombia, 2013 son:

- Utilizar y aplicar los controles adecuados para marcar limites a los riesgos y disminuir sus consecuencias.

- Mientras las políticas y criterios organizacionales para la aceptación de los riesgos sea satisfechos, aceptar con total objetividad y conocimiento los riesgos.
- Evadir los riesgos sobre la seguridad de la información.
- Trasladar los riesgos ligados a la institución.

El tratamiento de riesgos se basa en seleccionar y aplicar las acciones más adecuadas para poder modificar el riesgo y de acuerdo a eso trata de sacar provecho de las ventajas que se reportan. Todos los sistemas de tratamientos de riesgos deben asegurar tres puntos según la Comunidad de Madrid, 2012:

- Efectividad y eficiencia de la organización en cuanto a su funcionamiento
- Contar con un nivel alto de efectividad con respecto a los controles internos
- Consentimiento absoluto de todo el personal acerca las leyes y reglamentos vigentes.

1.2.3.8. Medios de transmisión de ataques

Los medios de transmisión de ataques son aquellas herramientas informáticas que se utilizan por actores que tienden a amenazar la seguridad para así vulnerar los sistemas con el único objetivo de obtener, alterar o eliminar la información almacenada. Las herramientas de transmisión de ataques más utilizadas son:

- Spam
- Malware
- Botnets
- Phishing

La probabilidad de acceder a los recursos en la actualidad es muy amplia, y como consecuencia de este hecho es que los delitos informáticos han incrementado, entre ellos los fraudes, falsificaciones y ventas de información.

1.2.3.9. Actores que amenazan la seguridad

Estos actores buscan ingresar anónimamente mediante cualquier medio de transmisión de ataque y causar daños en el sistema, dentro de los actores de este tipo existen:

- Hackers: Es cualquier individuo que posea grandes conocimientos en tecnología, informática, electrónica o comunicaciones, se actualiza en cuanto a sus conocimientos constante y periódicamente, cuenta con un conocimientos absoluto de todo lo referente a programación y sistemas complejos; su motivación es el conocimiento relacionado a tener accesos a cualquier compendio de información segura, en conjunto su conocimiento y habilidad le proporcionan la facilidad de vulnerar sistemas con todo tipo de seguridades sin ser detectado (Galindo, 2014, pág. 114).

- Cracker: Son individuos con altos conocimientos de Software, hardware y programación enfocados a la creación de programas capaces de vulnerar servidores a través de métodos de infección del software; son de comportamiento compulsivo y se enorgullecen de sus capacidades (Galindo, 2014, pág. 115).

- Lamer: Es todo individuo que bajo de uso de software de fácil manejo creado por un hacker intentan vulnerar sistemas (Galindo, 2014, pág. 115).

1.2.4. Tecnologías de la Seguridad

Son las herramientas que junto al mejoramiento de los controles de acceso a la información, se utilizan para precautelar la información y a su vez mitigar la posibilidad de ingreso por cualquier medio de transmisión de ataques.

Dicha tecnología no es suficiente para mantener un equilibrio entre el acceso y la seguridad, considerando la premisa de que la fortaleza de todo sistema está definida por su eslabón más débil, es decir el recurso humano, la parte humana. En sí, puede ser utilizada en base a una metodología clara para la optimización de los procesos de seguridad (ISACA, 2014).

Las tecnologías principales concernientes a la seguridad de la información se encuentran desde los métodos más conocidos como antivirus, cortafuegos, gestión de cuentas de usuarios y tecnologías de monitoreo hasta los métodos más robustos como cifrado, firmas digitales, métodos de privacidad, detección de intrusos, prevención de intrusos, accesos remotos informática forense, redes VPNs entre otros.

1.2.5. Familia ISO 27000

1.2.5.1. ISO/IEC 27000

En jerarquía es considerada como la raíz de todos las demás normas que la conforman, ofrece una definición general de todas las demás delimitándolas cuanto a su propósito y alcance.

Establece la importancia de un sistema de gestión de seguridad de información (SGSI) y además brinda una descripción general de los pasos para su implantación y mejora (ISO 27000.es, 2015).

1.2.5.2. ISO/IEC 27001

Esta norma contiene los requisitos del SGSI y es considerada como la norma principal de la familia de estos estándares, brinda la información de cada uno de los controles definidos en la norma ISO 27002 y los objetivos de control previstos para ser escogidos por institución en la implantación del sistema de gestión de seguridad (ISO 27000.es, 2015).

La aplicación y cumplimiento en la norma ISO 27001 darán como resultados fuertes controles relacionados con las TI, que también proporcionaran ayuda a satisfacer las necesidades de muchas de las normas de la institución. La profundidad a la que la norma ISO 27001 puede ayudar a lograr el cumplimiento de otras normas de regulación depende de que los controles correctos se seleccionen y cómo implementar esos controles.

1.2.5.2.1. Objetivo de la Norma

En búsqueda de proteger la información es importante implementar, mantener y mejorar las medidas de seguridad establecidas para que la organización consiga sus objetivos y garantice la legislación.

La norma ISO27001 referente al Sistema de Gestión de Seguridad de la Información plantea que para poder evaluar los riegos esta norma es la solución de mejora más apropiada y además establecer una serie de estrategias y controles oportunos para asegurar la protección y defender la información; el análisis y gestión de riesgos en base a los procesos, evaluando y controlando a la institución en cuanto a los riesgos a los que está expuesta la información es el objetivo principal de esta norma (SGSI , 2015).

1.2.5.2.2. Controles del anexo A de la norma

Punto 5.2: Este punto delimita que cada una de las políticas de seguridad de la información deben regularmente ser revisadas para garantizar que bajo posibles cambios conserven su efectividad, idoneidad y adecuación como puntos claves para su correcto funcionamiento (ISO 27000.es, 2013).

Punto 6.2: Este punto define las tareas y áreas de responsabilidad que se deben asignar para confrontar los conflictos de interés con el objetivo de minimizar la posibilidad de que usuarios no autorizados modifiquen o den un mal uso a los activos de la institución (ISO 27000.es, 2013).

Punto 7.1.2: Este punto delimita los compromisos y obligaciones tanto de los empleados, contratistas y usuarios terceros como de la organización con respecto a la seguridad de la información los cuales deben ser conocidos, aceptados y firmados en el contrato de trabajo (ISO 27000.es, 2013).

Punto 8.1.3: Para garantizar el aceptable y adecuado uso de los activos, las normas reguladoras del uso de la información deben ser identificadas, implantadas y documentadas, de la misma forma para los activos asociados a recursos de tratamiento de la información (ISO 27000.es, 2013).

Punto 9.1.1: Puntualiza la importancia de las políticas de control su implantación, revisión y documentación correspondientes a cada necesidad de seguridad de la institución (ISO 27000.es, 2013).

Punto 12.1.1: Define la necesidad e importancia de la documentación de todos los procedimientos y políticas operativas y su disponibilidad para todos los usuarios que necesiten dicha información documentada (ISO 27000.es, 2013).

Punto 13.2.4: Delimita la importancia de los acuerdos de confidencialidad de los empleados con la institución, exige una identificación, revisión y documentación de dichos acuerdos de manera periódica para garantizar la protección de la información y su no divulgación (ISO 27000.es, 2013).

Punto 14.2.5: Los diferentes tipos de labor de implementación en el sistema de información necesitan del establecimiento de los principios de seguridad, de su mantenimiento regular y documentación (ISO 27000.es, 2013).

Punto 15.1.1: Para minimizar el riesgo de accesos indebidos por para de usuarios terceros, ajenos a la institución o proveedores, se establecen y documentan los requerimientos de seguridad de la información necesarios para cada activo de la institución (ISO 27000.es, 2013).

Punto 16.1.5: Respuesta a los incidentes de seguridad, Este punto permite dar una respuesta oportuna a los fallos que puedan suceder en temas referentes a la seguridad de la información con procedimientos previamente documentados. (ISO 27000.es, 2013).

Punto 17.1.2: Implantación de la continuidad de la seguridad de la información, Es de vital importancia que la institución tenga previamente establecidos, debidamente documentados, correctamente implantados y sobre todo sostener los procesos, procedimientos y controles para de esta manera certificar el mantenimiento que otorga este punto de control en el cumplimiento del nivel necesario de seguridad de la información cuando se presenten incidentes (ISO 27000.es, 2013).

Punto 18.1.1: Identificación de la legislación aplicable, Es necesario realizar la correcta identificación, documentación y tener actualizados de una forma precisa para cada uno de los sistemas de información y la institución en general los requerimientos estatutarios, normativos y contractuales legislativos que vallan de la mana con los lineamientos de la institución para cumplir con todos los requisitos mencionados (ISO 27000.es, 2013).

1.2.5.3. ISO/IEC 27002

Sirve de pauta o guía para utilizar de manera adecuada los objetivos de control y controles debido a que los describe de manera perfecta y es recomendable porque dichos controles y objetivos están basados en seguridad de la información. La utilización de controles no garantiza obtener una certificación de seguridad, está compuesto por 39 objeticos de control aparte de los 133 controles que están claramente agrupados en 11 dominios. La normativa ISO 27001 cuenta con el Anexo A donde están descritos cada uno de los controles (ISO 27000.es, 2015).

1.2.5.4. ISO/IEC 27003

Este apartado se encargar de tratar los puntos más relevantes o críticos que son determinantes durante la implantación exitosa de un Sistema de Información de la Seguridad en concordancia con la ISO/IEC 27001:2005. Explica de una manera específica los pasos a seguir para obtener un perfecto proceso de especificación y diseño que abarca temas que van desde el inicio hasta que se coloca a trabajar los planes de implementación, de la misma

manera realiza el estudio con el proceso que tendrá como resultado la aprobación del plan por la alta gerencia de la empresa. (ISO 27000.es, 2015).

1.2.5.5. ISO/IEC 27004

Sirve de apoyo fundamental para dar inicio al desarrollo, utilización de criterios y técnica de medición, que serán puestas en marcha para de esta lograr de medir de manera documentada la eficacia de un Sistema de Seguridad de la Información y a su vez obtener datos precisos de los controles o las agrupaciones de los mismos que se implementaron según la normativa que se está aplicando. (ISO 27000.es, 2015).

1.2.5.6. ISO/IEC 27005

Brinda criterios específicos que se centran en la correcta gestión de riesgos basados en la seguridad de la información, basa todos sus lineamientos, criterios y definiciones generales en la normativa aplicada. El diseño de esta normativa a su vez permite la correcta aplicación de la seguridad de la información previa a la obtención de la gestión de riesgo. (ISO 27000.es, 2015).

1.2.5.7. ISO/IEC 27006

Determina los requerimientos necesarios para obtener la acreditación de organizaciones tanto de certificación como auditoria de SGSI; en otras palabra es la encargada de colaborar a la correcta interpretación de los Es decir, ayuda a interpretar los criterios necesarios para la certificación ISO/IEC 17021 aplicada a organizaciones de acreditación ISO 27001 (ISO 27000.es, 2015).

1.2.5.8. Certificación

Con el pasar del tiempo es notable como se observado el crecimiento considerables que las certificaciones han tenido, todas basadas en un objetivo en general el cual es brindar

protección a la información que actualmente es el activo más importante de cualquier empresa, todo esto con el fin global de conservar y crear la estructura empresarial en los diferentes países (ISO 27000.es, 2013).

Para obtener la certificación de un Sistema de Seguridad de la Información, se debe pasar por un riguroso proceso que será aplicado por una organización externa especializada en este tipo de certificaciones que tomara el SGSI y lo someterá a pruebas que determinaran el grado de implantación en el que se encuentra y la eficacia con que está trabajando, después de todo el proceso de análisis y evaluación si los requisitos son cumplidos a cabalidad la certificación correspondiente será emitida. (CEEISEC, 2012).

1.2.6. CICLO DE DEMING

1.2.6.1. ¿Qué es el ciclo de DEMING?

Es ciclo de DEMING llamado así en honor al estadista norteamericano Edwards Deming o PDCA por sus siglas es una metodología sistemática que basa su estructura en 4 pasos esenciales que deben ser ejecutados para tener como resultado la mejora continua del proceso acción al cual sea aplicado, aumentando de manera considerable el mejoramiento o crecimiento de la calidad de procesos esto implica una disminución de las fallas y un aumento en la eficiencia, eficacia, donde se podrá observar la solución óptima de problemas y disminución de riesgos potenciales.

El método de trabajo del ciclo de DEMING es cíclico donde las etapas depende de que una sea finalizada antes de dar paso a la siguiente etapa, donde una vez se finaliza el ciclo su continuidad hace que vuelva al inicio y de esta manera se retoma el proceso, obteniendo como resulta la evaluación de las actividades en cada una de las vueltas que da el ciclo y así implementar las mejoras necesarias o nuevos procesos y actividades de ser necesario. (Bernal, 2013).

1.2.6.2. Definición de las etapas del ciclo de DEMING

1.2.6.2.1. Planificar (Plan)

En esta etapa que es la primera del ciclo se realiza un exhaustivo análisis de las actividades y procesos para encontrar la más vulnerable y de esta manera trazar los objetivos que se quieren lograr. Este análisis requiere de la participación de la alta gerencia y de los empleados asociados a los procesos para obtener datos de mayor precisión. (Bernal, 2013).

1.2.6.2.2. Hacer (Do)

Con los datos obtenidos en el primer paso se aplican los cambios necesarios para obtener resultados con la mejora propuesta, regularmente se recomienda realizar por etapas o partes para evaluar el desempeño antes de aplicar el cambio total. (Bernal, 2013).

1.2.6.2.3. Controlar o Verificar (Check)

Luego de la implementación de la mejora es prudente esperar un tiempo donde se verificara el correcto funcionamiento de los cambios implementados, si dichos cambios no logran corregir las falencias u objetivos planteados es necesario volver al paso uno y replantear el proceso de análisis y aplicación de los cambios (Bernal, 2013).

1.2.6.2.4. Actuar (Act)

Cuando el periodo de prueba llegue a su final se tomaran los datos arrojados como resultado y se realiza la comparativa funcional con los procesos y actividades que estaban funcionando antes de que la mejora fuera aplicada. Cuando los resultados estén alineados a los objetivos planteados se entenderá que la mejora aplicada cumplió su función con éxito y se implantada de forma definitiva de no ser así se volverá a iniciar el ciclo analizando los errores encontrados, con la finalización de la cuarta etapa se debe volver a la primera para que se cumpla de esta manera la mejora continua (Bernal, 2013).

1.2.6.3. Aplicación del ciclo de DEMING en la norma ISO 27001

La normativa ISO 27001 tiene como resultado a la aplicación del ciclo de DEMING la implantación del Sistema de Gestión de Seguridad de la Información, que corrobora el correcto desempeño en gestión y protección de la información, cumpliendo así el objetivo que propone la norma.

1.2.6.3.1. Definición de un SGSI

Sus siglas significan Sistema de Gestión de la Seguridad de la Información (SGSI)y a su vez tiene su nomenclatura en ingles ISMS que significa Information Security Management System (ISO 27000.es, 2014).

Definimos a la información como una colección de datos organizados de manera entendible y que tengan una representación o un valor, sin importar la manera de almacenamiento o reproducción de la misma a partir de su creación sin tomar en cuenta que sea generada interna o externamente en la institución (ISO 27000.es, 2014).

De la misma manera se define el concepto de seguridad de información como la prevención de la confidencialidad, integridad y disponibilidad de la información, así como también los diferentes sistemas implicados en su trato (ISO 27000.es, 2014).

1.2.6.3.2. Fundamentos

Cuando se cumple el objetivo que propone la normativa se garantiza que se cumplan los principios más básicos de la seguridad de la información que de acuerdo a Baldecchi Q, 2014 son los siguientes:

- Confidencialidad: Se define como el principio que garantiza que la información no esté disponible para usuarios no autorizados sino por el contrario
- Integridad: Garantiza que la información no sea alterada o modificada de manera no autorizada manteniendo su valor y precisión.

- Disponibilidad: Su finalidad es que todo usuario autorizado pueda acceder y utilizar la información en cuanto la solicite.

Pueden ser adheridos algunos requisitos Autenticación, Responsabilidad, no repudio y fiabilidad.

1.2.6.3.3. ¿Para qué sirve un SGSI?

La actualidad muestra como las instituciones de todo el mundo y sus diferentes sistemas de información son vulnerados a diario debido al aumento significativo de amenazas y vulnerabilidades que de coincidir ambas pueden causar un daño critico a los activos de información de la empresa impidiendo así el correcto funcionamiento, algunos otros ejemplos son los ataques de intrusión al sistema y denegación de servicios, virus, o cualquiera de los métodos de hacking existentes, pero sin duda no solo existen amenazas externas como las antes mencionadas por lo que la información debe estar protegida en contra de los incidentes accidentales o no accidentales causados dentro de la propia institución. (ISO 27000.es, 2014).

Un Sistema de Gestión de Seguridad de la Información basa su funcionamiento en algunos puntos fundamentales para su correcto desempeño enfocados a la protección y cumplimiento de los objetivos de la institución y su crecimiento tales como ajuste a las variables del ambiente, legalidad etc., estos puntos sirven de gran apoyo para una herramienta de mucha utilidad y que garantiza un correcto funcionamiento y gestión de las empresas.

La seguridad si no logra alcanzar un nivel adecuado con las herramientas que dispone llega a ser improductivo y causar daño a sí mismo, la alta gerencia debe tener una participación protagonista para logra obtener una efectiva y eficiente gestión de la seguridad para proceder a la toma de decisiones importantes, apoyándose también los empleados, clientes y demás personas u organizaciones que estén ligados con los objetivos propios de la Institución. (ISO 27000.es, 2014).

1.3. Marco Legal

Cualquier institución que requiera la implementación de un SGSI o el grupo de controles de gestión de información y plan de tratamiento de riesgos está obligada a cumplir con toda ley, norma o decreto que pueda ser aplicada al desarrollo de sus actividades.

Como punto fundamental en cuanto a las leyes específicas del control de la información partimos de la "LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA" que estipulan los derechos que tiene la ciudadanía a acceder a cualquier fuente de información definida como pública para ejercer la participación democrática respecto a la rendición de cuentas a los que está expuesto cada empleado público, esta ley contiene un conjunto de artículos definidos que establecen dichos derechos y sus límites.

La constitución ecuatoriana en su capítulo tercero Garantías jurisdiccionales, sección cuarta Acción de acceso a la información pública, señala que cuando el acceso a la información de carácter público ha sido negado o cuando dicha información no sea fidedigna o completa se garantice el acceso a esta, incluso si la negación se sustenta en el carácter de reservado, secreto o confidencial, puesto que estas clasificaciones de información deben ser estipulados junto con la creación de dicha información y no después de que ha sido solicitada por ser de carácter público.

La sección quinta o acción de hábeas data en su artículo 92 estipula los derechos de toda persona a acceder a su información de carácter personal, así mismo la constitución del Ecuador a través de la ley de "COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS" delimita las leyes en cuanto a la información privada su seguridad, acceso y manipulación solo por usuarios autorizados y castiga la intrusión no autorizada a cualquier sistema de información.

CAPITULO II

2. METODOLOGÍA

2.1. Descripción y caracterización del lugar

El Gobierno Autónomo Descentralizado de la provincia de Esmeraldas se encuentra estratégicamente ubicado en la calle 10 de Agosto entre Bolívar y Pedro Vicente Maldonado cerca al parque Central 20 de Marzo justo en el centro de la ciudad, y repartiendo desde allí su labor a toda la ciudadanía.

Es una entidad pública identificada por los esmeraldeños como la prefectura o GADPE; su principal objetivo es el desarrollo de la provincia a través de la ejecución eficiente de sus competencias, con un enfoque de total responsabilidad social, respeto y pluriculturalidad dentro de su territorio.

El GADPE como cualquier institución se encuentra dividida en departamentos enfocados todos a un solo fin colectivo, los esmeraldeños. Entre dichos departamentos se encuentra la dirección de Tecnologías de la información y la comunicación la cual está encargada de 4 áreas dentro de la institución, Redes y Comunicaciones, Desarrollo e Integración de Aplicaciones, Soporte he Infraestructura Tecnológica y Proyectos y Servicios Web en cada una de estas áreas hay un responsable o jefe de área y un ayudante, constituyéndose así que cada área es responsabilidad de dos personas y todas son responsabilidad del jefe del departamento.

2.2. Tipo de investigación

2.2.1. Descriptiva

El presente proyecto utilizó este tipo de investigación puesto que permitió realizar una comprobación específica de las necesidades de la institución de forma progresiva y sistemática.

2.2.2. Explicativa

Se utilizó la investigación explicativa puesto que por medio de un análisis situacional de la entidad quedaron claramente expuestas las causas de las falencias actuales y la necesidad de una normalización de controles de seguridad de la información.

2.2.3. De Campo

La investigación es de campo puesto que la recolección de información depende de técnicas como entrevistas y observación además del asesoramiento necesario para la correcta ejecución.

2.3. Métodos y técnicas

2.3.1 Métodos

MÉTODO INDUCTIVO

El método inductivo, permitió observar y analizar la situación actual de la Unidad Informática del Patronato Municipal de Esmeraldas y luego identificar los instrumentos necesarios para solucionar el problema planteado.

MÉTODO ANALÍTICO-SINTÉTICO

El método analítico sintético fue de importancia en este proyecto de investigación, al permitir que los resultados obtenidos mediante las investigaciones documentales y de campo sean analizados para entenderlos y describirlos, utilizando juicio de valor; es decir que este método servirá de apoyo para la elaboración del diagnóstico del problema planteado.

2.3.2. Técnicas

Entrevista

Mientras se desarrolló la investigación se aplicaron entrevistas estructuradas y no estructuradas a directivos, administrativos y miembros de la Unidad Informática, con el objetivo de obtener información de primera mano acerca del funcionamiento del departamento de informática en la Institución y las actividades que realiza.

2.4. Población y muestra de estudio (técnicas de muestreo)

2.4.1. Población

La población total del proyecto es de 9 personas, que corresponden a todo el personal del departamento y sus áreas Redes y Comunicaciones, Desarrollo e Integración de Aplicaciones, Soporte he Infraestructura Tecnológica y Proyectos y Servicios Web.

2.4.2. Muestra

Por ser la población tan pequeña la muestra es igual a la totalidad de esta, es decir la muestra es igual a 9 personas.

2.5. Descripción del instrumento

2.5.1. Entrevista

Se elaboraron tres entrevistas dirigidas al jefe de departamento de TIC en el primer trimestre del 2017 con el fin de obtener información de diagnóstico de la situación actual de la institución, dichas entrevistas se pueden apreciar en los anexos 1, 2 y 3 respectivamente.

2.6. Técnicas de procesamiento y análisis de datos

Una vez obtenida información a través de la técnica propuesta se procedió a almacenar los resultados obtenidos de manera digital en un formato legible y respetando la integridad de las respuestas obtenidas, se analizaron los resultados obtenidos y con la aprobación de los dueños de los procesos antes evaluados se obtuvo la información necesaria para proceder al desarrollo de los objetivos de la presente investigación.

2.7. Normas éticas

Cada una de las entrevistas aplicadas se las hizo respetando los derechos del participante, cumpliendo con las pautas de informarlo previo a la entrevista acerca del propósito y consecuencias de la investigación, por lo cual el entrevistado esta consiente del porque y para que de dicha técnica; se respetó el derecho a negarse a dar información considerada por el entrevistado como confidencial. Así mismo se respetó su deseo de abandonar en algún momento entrevista, para continuar después o darla por terminada; durante todo el proceso se mantuvo el respeto con el entrevistado y cabe recalcar que todo el proceso fue con el consentimiento y aprobación absoluto.

CAPITULO III

3. RESULTADOS

3.1. Análisis e interpretación de resultados

ENTREVISTA DIRIGIDA AL JEFE DEL DEPARTAMENTO DE TIC (Anexo 1)

OBJETIVO: **Descubrir la arquitectura y tecnologías de seguridad.**

Análisis

En cuanto a si el departamento cuenta con un inventario de activos actualizados, se corroboró que sí cuentan con los inventarios de activos existentes, con respecto a su almacenamiento según palabras del jefe del departamento existen dos copias, una la posee él y la otra el Analista de sistemas quien es justamente el responsable de dicho inventario, además existen copias de respaldo debidamente almacenadas.

Referente a la existencia de un inventario de procesos actualizado se confirmó que el departamento sí cuenta con los inventarios antes mencionados; con respecto a las metodologías para el control de procesos referentes a la seguridad de la información y la existencia de un documento de declaración de aplicabilidad se obtuvieron respuestas negativa y describen esta carencia como una de falencias en el control y manejo de la información.

El departamento trabaja de manera eficiente en cuanto al manejo de activos de información y procesos, pero requiere que a partir de esta documentación se elaboren metodologías de control de procesos y el documento de declaración de aplicabilidad ligado al conjunto de políticas de seguridad; los resultados reflejaron dicha necesidad pero a su vez reflejó también que el departamento trabaja bien y va por buen camino en busca de un máximo nivel de seguridad de la información que sin duda será alcanzado.

ENTREVISTA DIRIGIDA AL JEFE DEL DEPARTAMENTO DE TIC (Anexo 2)

OBJETIVO: **Identificar la arquitectura organizativa de la seguridad de la Información.**

Análisis

Con respecto a la política global de seguridad de la información existente, se determinó que la política consiste en el respaldo y resguardo de la información crítica e importante; concerniente a la existencia de políticas de seguridad de la información se corroboró que el departamento no cuenta con dichas políticas, pero si cuenta con informes de evaluación de riesgos; como último punto en cuanto a la existencia de un plan de capacitación de seguridad de la información al personal se determinó que forma parte de sus planes a futuro.

Los resultados reflejaron una clara necesidad de políticas de seguridad, la cual será ampliamente cumplida con la creación de un documento de políticas de seguridad de la información dirigido exclusivamente a los procesos más críticos del departamento reduciendo así las amenazas a la seguridad de la información y su posible consecuencia, junto con las políticas se debería capacitar a los miembros del departamento acerca de cada una de estas.

ENTREVISTA DIRIGIDA AL JEFE DEL DEPARTAMENTO DE TIC (Anexo 3)

OBJETIVO: **Conocer la situación actual de la empresa con respecto a la seguridad de la información.**

Análisis:

En respuesta a la pregunta acerca de la documentación con la que cuenta el departamento con respecto a la seguridad de la información se confirmó que la institución cuenta con algunas políticas de seguridad pero estas no están basadas en las necesidades actuales ni procesos críticos del departamento.

La situación de la empresa en cuanto a ciertos procesos es crítica, por lo cual las falencias mencionadas deben ser solucionas, la documentación que maneja actualmente la empresa en cuanto a activos y procesos además del conocimiento respecto al tema de los involucrados

son puntos de partida sumamente necesarios para elaboración de políticas y métricas de seguridad de la información.

CAPITULO IV

4. PROPUESTA

Con el fin de minimizar los riesgos y amenazas a los que se ve expuesta la información del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas (GADPE) se elaboraron el conjunto de políticas de seguridad de la información necesarias para el control, contención y respuesta oportuna ante dichos riesgos.

Se definieron el conjunto de métricas necesarias por política que determinarán la eficacia de cada uno de los controles establecidos, además se redactará la declaración de aplicabilidad basada en la normativa ISO 27002 (Anexo A).

4.1. Políticas de seguridad de la información

La información sin lugar a dudas es el activo de mayor importancia en una organización, y para una institución como el GADPE la protección de esta es una de sus mayores prioridades; las políticas de seguridad servirán de guía para la protección de la información a una amplia gama de amenazas, reduciendo los riesgos, probabilidades de pérdidas, daños y fuga de información garantizando el cumplimiento de los objetivos institucionales.

El GADPE cuenta con el compromiso de los altos directivos y todos los involucrados del departamento de TIC en la seguridad de información para su salvaguarda; las presentes políticas están basadas y aplicadas según los resultados obtenidos en la matriz de riesgos (Ver Anexo B) elaborada por el Ing. Jonathan Cedeño para el GADPE.

Objetivos

Proteger tanto la información como la tecnología utilizada para su procesamiento y almacenamiento frente a amenazas externas o internas, no intencionadas y deliberadas con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información.
Asegurar que sean implementadas las políticas de seguridad que comprenden este documento identificando la finalidad y responsables de cada una.

Mantener siempre actualizadas las políticas de seguridad con el fin de asegurar su eficacia y vigencia.

Alcance

La política de seguridad es aplicada en el departamento de TIC, a sus activos y procesos; en dicho departamento se realizan las actividades de control y almacenamiento de información, así como el manejo de los procesos y activos.

Responsabilidad de la dirección

- La dirección de TIC es la responsable de la aplicación de las políticas de seguridad de la información.
- La aplicación de la política de seguridad de la información es obligatoria para el personal del departamento.
- La Dirección aprueba y se responsabiliza de estas políticas y su modificación a futuro.

Aspectos Generales

Las pautas específicas de seguridad de la información que conforman esta política incluyen lo siguiente:

Seguridad ligada a los recursos humanos

Orientado a garantizar las capacidades y responsabilidades de los empleados en función al rol que cumplen o cumplirán en la organización, y que tanto contratistas como usuarios terceros entiendan sus responsabilidades para reducir los riesgos de robo, fraude y mal uso tanto de los medios como de las instalaciones.

Gestión de activos

Establecido para mantener un correcto inventario de activos proporcionándoles la protección debida., la política actual pretende que el departamento tenga pleno conocimiento de los activos que posee siendo esta información parte importante de una buena gestión de riesgos.

Control de accesos

Propuesto para controlar el acceso a la información y los activos a través de restricciones, implantando un procedimiento para el control de asignación de los derechos de usuario a cada activo de información

Cifrado

Definido para que a través de las políticas de cifrado se logre proteger la información de vital importancia para el departamento de TIC y la empresa en general utilizando técnicas y herramientas de criptografía.

Seguridad física y ambiental

Dirigido a mantener el control ante factores externos o ambientales a los que están expuestos los dispositivos por los que circula la información, además de impedir accesos no autorizados.

Seguridad en la operativa

Contempla el control a código malicioso para evitar contagios en los equipos de la institución, la instalación del software necesario en los sistemas de producción para el cumplimiento ágil de las funciones departamentales, las debidas restricciones de instalación, auditorias para el control de los sistemas de información y las respectivas copias de seguridad de la información.

Seguridad en las telecomunicaciones

Destinado a establecer los controles de red necesarios para su protección, el acuerdo y políticas intercambio de información.

Adquisición, desarrollo y mantenimiento de los sistemas de información

El objetivo de este apartado es Mantener la seguridad del software del sistema de aplicaciones y la información y garantizar que la seguridad es parte integral de los sistemas de información.

Relaciones con Suministradores

Se deberán implementar acuerdos, ejecutar procesos de monitoreo que garanticen su cumplimiento y aseguren que los servicios se entreguen de manera eficiente y que satisfagan los requerimientos solicitados por terceras personas.

Gestión de incidentes en la seguridad de la información

La gestión de incidentes pretende garantizar que cualquier eventualidad negativa a la que se encuentren expuestos los activos de información, sea detectada, tratada, mitigada de manera eficiente y documentada para prevenir futuros incidentes.

Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Con la finalidad de garantizar la continuidad del negocio se incluirán dentro de los procesos críticos del departamento los requisitos de seguridad de la información necesarios fijados para mejorar y asegurar la efectiva operatividad del departamento.

Cumplimiento

Todas las operaciones ejecutadas en los sistemas de información se encuentran bajo la regulación de las disposiciones contractuales y legales establecidos por la dirección, los cuales están debidamente documentados y respaldados.

Sanciones previstas por incumplimiento

Al incumplir con alguna de las políticas el infractor se expone a una sanción proporcional a la falta incurrida, será impartida por el responsable del proceso y a su vez las sanciones estarán previstas en el apartado de las políticas de Cumplimento.

4.1.1. Seguridad ligada a los recursos humanos

Generalidades

La presente política pretende dar garantías del correcto manejo de la información por parte del personal, además de controlar y asegurar las responsabilidades asignadas al personal de acuerdo a sus roles dentro del departamento para reducir los riesgos de mal uso de las instalaciones, robo de información y fraude; la presente política está asociada a las pautas establecidas en el punto 4 del EGSI (Esquema Gubernamental de Seguridad de la Información), referente a la seguridad de los recursos humanos.

Objetivos

- Garantizar que el personal del departamento entienda sus responsabilidades y sean competentes de acuerdo al rol que desempeñan.
- Asegurar la definición de cada una de las responsabilidades de seguridad previamente a la contratación del personal

4.1.1.1. Antes de la contratación

Previo a la contratación laboral se deberán detallar las responsabilidades del aspirante en cuanto a la seguridad de la información describiendo adecuadamente el trabajo que desempeñara, sus términos y condiciones aplicando el siguiente proceso:

- El departamento de TI conjuntamente al de recursos humanos de la institución deberá pasar a cada aspirante por un proceso de verificación de antecedentes.
- La selección de cualquier empleado, contratistas y usuarios de terceras partes deberá ser seleccionado de manera adecuada acorde a la necesidad del departamento y las aptitudes, actitudes, preparación y conocimientos del aspirante.
- El personal entrante (empleados, contratistas y usuarios de terceras partes) ligado a los servicios de procesamiento y manejo de información deberá firmar un acuerdo de confidencialidad que garantice su toral responsabilidad durante la ejecución de sus funciones con relación a la seguridad de la información.
- Informar al personal entrante de las sanciones previstas por incumplimiento de las políticas de seguridad.

4.1.1.1.1. Investigación de antecedentes

El proceso de investigación de antecedentes debe ser realizado en concordancia con la ética, requerimientos y regulaciones del departamento, tomando en cuenta estos parámetros, se filtrarán los aspirantes que cumplan tanto con los requerimientos legales y éticos como con

los conocimientos necesarios para las actividades requeridas, este proceso será responsabilidad tanto del departamento de TIC como del departamento de Recursos Humanos.

4.1.1.1.2. Términos y condiciones de contratación

Las obligaciones respecto al cumplimiento de las políticas de seguridad de la información deberán ser firmadas por el o los aspirante dentro de los términos y condiciones de contratación.

El aspirante debe tener conocimiento absoluto de cuáles serán sus responsabilidades dentro del departamento y las consecuencias y sanciones por el incumplimiento de las políticas de seguridad de la información.

Métricas: Porcentaje de los aspirantes que hayan sido aprobados después de la verificación y tengan pleno conocimiento de las políticas de seguridad de la información y las consecuencias por su incumplimiento además de los conocimientos y preparación necesarios podrán empezar a trabajar en el área solicitada.

Porcentaje de aspirantes aptos= PorcentAp

Aspirantes aceptados = ASPa

Aspirantes que cumplen las expectativas = ASPc

$$PorcentAp = ASPc \times 100 / ASPa$$

4.1.1.2. Durante la Contratación

- Con la finalidad de garantizar que la seguridad de la información es aplicada en cada uno de los puestos de trabajo deben ser definidas las responsabilidades de la dirección.
- El personal entero del departamento debe ser capacitado y concientizado con respecto a los procesos y políticas de seguridad de la información y el uso correcto de las instalaciones y medios institucionales.

- La gestión de las posibles brechas de seguridad estará definido por el proceso disciplinario previamente establecido por el departamento de TIC.

4.1.1.2.1. Responsabilidades de Gestión

Cada una de las gestiones en cumplimiento de sus actividades profesionales dentro del departamento por parte de los empleados o contratistas deben ser ejecutadas en función a las políticas y procedimientos de seguridad de la información.

4.1.1.2.2. Concienciación, educación y capacitación en seguridad de la información

El proceso de capacitación, educación y concienciación con respecto a las políticas de seguridad de la información debe ser prioridad dentro del departamento y debe ser aplicado a todos los empleados, dicho proceso se deberá actualizarse con regularidad en concordancia a las actualizaciones de las políticas.

Métricas: Total mensual de respuestas a las iniciativas de concienciación de seguridad de la información y cada una de las actividades de capacitación propuestas por el departamento.

4.1.2. Gestión de activos

Generalidades

La administración de riesgos es un punto vital para el correcto funcionamiento de las actividades del departamento, la política actual pretende que el departamento tenga pleno conocimiento de los activos que posee siendo esta información parte importante de una buena gestión de riesgos; la presente política está asociada a las pautas establecidas en el punto 3 del EGSI (Esquema Gubernamental de Seguridad de la Información), referente a la Gestión de los activos.

Objetivos

- Identificar los activos y su respectivo responsable con el fin de garantizar una protección adecuada.
- Minimizar los riesgos a los que se ven expuestos cada uno de los activos de la organización.

4.1.2.1. Responsabilidades sobre los activos

- Se debe justificar cada activo y asignarle un propietario con las respectivas responsabilidades de mantenimiento y control.
- El propietario del activo puede delegar las responsabilidades de control a terceras personas dentro del departamento, pero seguirá siendo el responsable directo de dicho activo.
- Se debe utilizar métodos de identificación como registro de códigos de barra para facilitar la elaboración del inventario de activos con respecto a los equipos del departamento, y poder registrar la salida y devolución de los equipos al departamento.

4.1.2.1.1. Inventario de activos

El inventario y responsable de cada activo está especificado en la matriz de riesgos inherentes que la institución posee, en caso de existir la necesidad de consulta, revisar dicho documento.

Métricas: Número y porcentaje de activos de información claves que han visto mitigados los riesgos de seguridad de la información a los que estaban expuestos.

Porcentaje de activos con riesgos mitigados = PorcAct

Activos en riesgos = AtcRies

Riesgos mitigados = RiesgMit

$$PorcAct = RiesgMit \times 100 / AtcRies$$

4.1.3. Control de accesos

Generalidades

El fin del presente política es controlar el acceso a la información y los activos a través de restricciones, implantando un procedimiento para el control de asignación de los derechos de usuario a cada activo de información; el proceso comprende el registro de usuarios nuevos con sus respectivos permisos y restricciones de acceso y la eliminación de dichos permisos en caso de ser necesario, la presente política está asociada a las pautas establecidas en el punto 7 del EGSI (Esquema Gubernamental de Seguridad de la Información), referente a Control de acceso.

Objetivos

- Mantener el control del acceso a la información, medios e instalaciones del departamento.
- Dar garantías de acceso a la información y bases de datos a usuarios autorizados.
- Impedir el acceso a la información, bases de datos y activos a usuarios no autorizados

Para garantizar el cumplimiento de los objeticos de la política el responsable de la información debe definir los procedimientos y normas para la correcta gestión de accesos a los sistemas de gestión de información, solicitudes de acceso a internet, bases de datos, monitoreo y uso del equipo e instalaciones dedicado al procesamiento y almacenamiento de información y elaborar un reporte periódico de los incidentes con el objetivo de actualizar, o añadir nuevas normas y procedimientos de control.

4.1.3.1. Requisitos del negocio para el control de accesos

Tomando en cuenta las necesidades del departamento se tomaran las medidas para el control de acceso a la información, los sistemas de tratamiento de información y procesos; cada propietario de activo es el responsable ante la dirección del departamento de la protección

del activo por lo cual definirán o aprobarán los controles de acceso, además de las sanciones en caso de posibles accesos no autorizados.

4.1.3.1.1. Política de control de acceso

Las políticas de control de acceso existente deberán ser revisadas, mejoradas y actualizadas en base a las necesidades del departamento en cuanto a la seguridad y a los reportes de las posibles incidencias ocurridas, definiendo claramente los perfiles de acceso a los usuarios de acuerdo a su puesto de trabajo y los permisos que posee.

4.1.3.1.2. Control de acceso a redes y servicios asociados

Se deben asignar los permisos y restricciones de acceso a las redes y servicios de red usados en el departamento reconociendo todos los tipos de conexiones disponibles.

Métricas: Porcentaje de sistemas, aplicaciones y bases de datos a las cuales se ha obtenido acceso adecuado por parte de usuarios autorizados a través del proceso de identificación y verificación de permisos de acceso, el porcentaje no deberá ser menor a 100% en caso de no ser así se deberán reestructurar y mejorar los controles establecidos para evitar los accesos no autorizados.

Porcentaje de accesos correctos por usuarios autorizados = PorAC

Accesos totales en el mes = AccTM

Accesos por usuarios correctos = AccUC

$$PorAC=AccUC*100 / AccTM$$

4.1.3.2. Gestión de acceso de usuarios

Dentro de la gestión de acceso se desarrollarán las normas y procedimientos para la asignación de derechos y permisos de acceso a las bases de datos, servicios y sistemas de información.

4.1.3.2.1. Gestión de altas/bajas en el registro de usuarios

- El departamento de TIC ejecutará un proceso de asignación de usuarios y contraseñas únicas para el ingreso a los activos de información.
- El usuario deberá identificar de manera clara al funcionario al que se le asigno, registrando cada vez que este obtenga acceso al sistema, bases de datos e información en general detallando fecha, hora de acceso y a que activo de información obtuvo acceso.
- Los usuarios deberán estar limitados en su acceso de acuerdo a los permisos que tiene el funcionario dentro del departamento.
- Todas las actividades que lleve a cabo cualquier funcionario con sus claves de acceso será responsabilidad del mismo y cualquier infracción deberá ser sancionada acorde a las políticas del departamento.
- Todos los usuarios deberán ser validados y aprobados por el jefe del departamento y posteriormente registrados y dados de alta por el encargado asignado por la gerencia.
- En caso de solicitarse alguna modificación en los datos de usuario, deberá ser justificada por parte del funcionario solicitante y aprobada por el jefe del departamento.
- Se guardara un registro de todos los usuarios dados de alta.
- El jefe departamental podrá dar de baja a todos los usuarios que cometan alguna infracción o incumplan los términos y condiciones firmados durante el proceso de contratación.
- Una vez que el funcionario deja la institución, inmediatamente deberá ser dado de baja del sistema de usuarios y revocados todos sus permisos de acceso.

4.1.3.2.2. Gestión de los derechos de acceso con privilegios especiales

- Cada perfil de usuario deberá estar ligado al rol específico que definirá sus privilegios de acceso de acuerdo a sus funciones dentro del departamento, siendo el jefe del departamento la única persona con permisos totales de acceso a la información y cada uno de sus activos.

- Ningún funcionario podrá acceder a los datos de administración de usuarios y contraseñas de los funcionarios del departamento.
- Los privilegios de acceso serán otorgados a los funcionarios cuyo rol en el departamento los requiera.

4.1.3.2.3. Revisión de los derechos de acceso de los usuarios

Los propietarios de los activos de información seguirán un proceso de monitoreo y control de los derechos de usuario, documentando la información obtenida y sancionando a los usuarios infractores en caso de ser necesario.

Cada propietario de activos será responsable de hacer respetar las normas éticas y de confidencialidad a las cuales se rige cada funcionario una vez firmado su contrato de trabajo dentro de la institución.

El acceso al data center estará restringido al jefe del departamento y el responsable directo asignado por según su rol.

4.1.3.2.4. Retirada o adaptación de los derechos de acceso

Todos los derechos de acceso deberán ser revocados en caso de que el funcionario:

- Incumpla con las políticas de seguridad
- Incumpla con las normas de confidencialidad y ética laboral.
- Termine su periodo de contrato con la institución
- Cambie su rol dentro del departamento

Métricas: Promedio de tiempo que trascurre entre la solicitud de alta de usuarios nuevos y el cumplimiento de dicha solicitud.

Promedio tiempo de solicitudes Alta de usuarios = PromTAU

Hora de la solicitud = HsAU

Hora de cumplimiento = HcAU

Solicitudes al mes = SolMAU

$$PromTAU=\sum(HcAU - HsAU) / SolMAU$$

Promedio de tiempo que trascurre entre la solicitud de modificación de permisos a usuarios activos y el cumplimiento de dicha solicitud.

Promedio tiempo de solicitudes Modificación de permisos = PromMP

Hora de la solicitud = HsMP

Hora de cumplimiento = HcMP

Solicitudes al mes = SolMMP

$$PromTMP=\sum(HcMP - HsMP) / SolMMP$$

Promedio de tiempo que trascurre entre la solicitud de eliminación de permisos de accesos a usuarios que ya no pertenecen al departamento o ya no cuentan con ningún permiso de acceso el cumplimiento de dicha solicitud.

Promedio tiempo de solicitudes eliminación de usuarios = PromTEU

Hora de la solicitud = HsEU

Hora de cumplimiento = HcEU

Solicitudes al mes = SolMEU

$$PromTEU=\sum(HcEU - HsEU) / SolMEU$$

4.1.3.3. Control de acceso a sistemas y aplicación

Se llevara un registro de cada acceso a sistemas, aplicaciones e intranet identificando al funcionario que accedió, fecha de acceso, hora de acceso y medio utilizado, toda esta información será confidencial y únicamente podrá ser vista por el jefe de departamento y el funcionario responsable de dicho rol.

Se generarán los respectivos registros de auditoria e informes que contengan información de los eventos realizados, estos informes serán entregados al jefe del departamento para su respectiva evaluación.

Cada Registro o informe generado será archivado y respaldado; los empleados deberán conocer el alcance de cada recurso informático y cuales son objeto de monitoreo y control.

Con regularidad se debe llevar control del espacio de almacenamiento disponible en los discos de cada servidor en funcionamiento.

4.1.3.3.1. Restricción del acceso a la información

El acceso a la información estará restringido a los usuarios y personal cuyo rol no requiera de los permisos y privilegios de acceso, el acceso a la información será limitado de acuerdo a la función que ejecute y a las necesidades de su función.

4.1.3.3.2. Procedimientos seguros de inicio de sesión

El procedimiento seguro log-on será el método utilizado para el control de acceso a los servicios y bases de datos, en cuanto a la infraestructura y control de acceso a los servidores el control se efectuará utilizando un control de registros biométrico.

4.1.3.3.3. Gestión de contraseñas de usuarios

La gestión de contraseñas de usuarios serán aplicados de acuerdo a los procedimientos actuales de la institución**.**

Métricas: Porcentaje de respaldos efectuados durante el mes.

Porcentaje de respaldos al mes = PorR

Respaldos necesarios efectuados = REF

Respaldo Totales necesarios = RTN

$$PorR = REF * 100 / RTN$$

4.1.4. Cifrado

Generalidades

A través de las políticas de cifrado luego de haber realizado el análisis de riesgo correspondiente, se preténdete proteger la información de vital importancia para el departamento de TIC y la empresa en general ya sean documentos importantes, claves de acceso, proyectos en ejecución utilizando técnicas y herramientas de criptografía que permitirán otorgar niveles de seguridad apropiados para la información.

Objetivos

- Utilizar herramientas y técnicas de criptografía para la protección de la información.
- Aplicar el nivel de cifrado correcto a la información de acuerdo a su importancia.
- Proteger la información de la institución de manera que se pueda dar fe de su confidencialidad e integridad.

El responsable de esta política debe cumplir con estos objetivos y de esta manera poder garantizar la correcta gestión de la información, logrando así un nivel de seguridad en el cifrado elevado en el acceso a los sistemas de información.

4.1.4.1. Controles criptográficos

Con el fin de garantizar la integridad, disponibilidad y confidencialidad de la información se implementan controles criptográficos en los diferentes niveles de acceso ya sean controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada o para el resguardo de aquella información relevante todo esto basado en los resultados de la evaluación de riesgos realizada por el departamento de TIC.

4.1.4.1.1. Política de uso de los controles criptográficos

En caso de ser necesario se pueden desarrollar procedimientos y también asignar funciones que permitan una mejor administración de las claves de acceso a los sistemas de información y datos importantes que en caso de perdida y daño servirían para poder recuperar la información que se encuentra protegida mediante el cifrado.

4.1.4.1.2. Gestión de claves

Revisar periódicamente el funcionamiento de las claves acceso, revisar longitud mediante los algoritmos de criptografía y en caso de ser necesario actualizarlas para obtener así una mayor seguridad al momento de querer acceder a los sistemas de información.

Además de las claves de acceso a la información que se encuentra protegida, se pueden implementar firmas digitales que ayudan en el proceso de autenticación para acceder a los datos que se encuentra almacenados de manera digital y asegurar de esta manera la integridad de la información.

Métricas: Porcentaje trimestral de sistemas que alojan datos de importancia para el correcto funcionamiento y cumplimiento de los objetivos institucionales se encuentran asegurados bajo controles criptográficos adecuados.

Porcentaje de sistemas asegurados = PorSA

Sistemas totales que alojan datos de valor = SisDV

Sistemas asegurados criptográficamente = SisAC

$$PorSA = SisAC \times 100 / SisDV$$

4.1.5. Seguridad Física y ambiental

Generalidades

Buscando minimizar los riesgos por daños físicos e interferencias a los equipos de almacenamiento de información afectando a su vez las operaciones del departamento se establecen los parámetros de seguridad física y ambiental necesarios, la presente política está asociada a las pautas establecidas en el punto 5 del EGSI (Esquema Gubernamental de Seguridad de la Información), referente a Seguridad Física y del Entorno.

Objetivos

- Minimizar los riesgos por daños físicos e interferencias a los equipos de almacenamiento de información.
- Evitar comprometer la integridad de los activos, robo de información y daños a la infraestructura tecnológica.

4.1.5.1. Áreas seguras

La finalidad de este control es asegurar que la infraestructura tecnológica y los medios de procesamiento de información confidencial o crítica estén ubicados en áreas seguras que garanticen su funcionamiento correcto y sin interrupciones.

4.1.5.1.1. Controles físicos de entrada

Las áreas seguras del departamento específicamente el Data Center deberá estar protegido a través de protocolos de entrada seguros y adecuados para garantizar que únicamente los usuarios con autorización tengan acceso.

El departamento de TIC mantendrá el control de acceso a las áreas seguras a través de un sistema biométrico con claves de acceso personalizadas designadas únicamente a los usuarios con acceso autorizado.

Área	Nivel de protección	Controles de acceso físico
Data Center	Alta	Sistema biométrico de acceso por contraseña

Tabla 1 Área segura del departamento de TIC

4.1.5.1.2. Seguridad de oficinas, despachos y recursos

- Las áreas seguras deberán ser ubicadas en zonas a las cuales no pueda acceder ningún usuario no autorizados.
- Las áreas donde se ejecutan las actividades de procesamiento de información serán discretas y no permitirán el uso de equipos y medios a usuarios no autorizados.
- El acceso al departamento será restringido a usuarios terceros no autorizados y se definirán parámetros para el acceso de personas particulares.
- Todo usuario particular no autorizado que requiera acceso al departamento o las zonas seguras de tratamiento de información deberá solicitar permiso al jefe departamental y será acompañado durante su visita por un responsable designado como responsable de la seguridad de las oficinas, despachos y recursos.

4.1.5.1.3. Protección contra las amenazas externas y ambientales

Los medios físicos de tratamiento de información se deberán proteger físicamente para evitar daños por desastres naturales, accidentes o ataques internos o externos a su integridad, para ello la zona segura donde está ubicado el Data Center y las estaciones de trabajo deberán contar con los procedimientos necesarios para su completa protección.

Métricas: Informe mensual de las inspecciones efectuadas a las instalaciones en cuanto a su seguridad física, anexando datos como estado actual de la seguridad, medidas correctivas necesarias a aplicar y medidas correctivas aplicadas previamente de acuerdo a informes anteriores.

4.1.5.2. Seguridad de los equipos

Todos los equipos y medios destinados al tratamiento de la información deberán ser protegidos físicamente evitando posibles daños por factores externos que pongan en peligro su integridad y la de los datos que almacena.

- Los equipos deberán estar a una temperatura adecuada para evitar el sobrecalentamiento.
- La ubicación de cada esquipo y hardware de tratamiento de información es clave, deberá proporcionar el espacio suficiente entre equipos y operadores para evitar golpes que pudiesen causar daños.
- Se deberá prohibir a cualquier visitante, empleado o personal del departamento manipular o trasladar equipo informático si no cuenta con una autorización respectiva del o los responsable de los activos.
- Todo equipo que bajo permiso de los responsable salga del departamento deberá ser registrado utilizando como referencia el código de barras.

4.1.5.2.1. Mantenimiento de los equipos

El mantenimiento de los medios que almacenan, procesan y gestionan la información es de vital importancia, el daño por falta de mantenimiento a estos podría ser catastrófico para el correcto cumplimiento de las actividades de la institución.

- El departamento de TIC garantizará, delegando a un responsable, el mantenimiento y revisión periódica a todos los equipos de cómputo del departamento.
- Todo el equipo de cómputo será sometido a procesos de mantenimiento preventivo de acuerdo a las recomendaciones previstas y autorización del responsable, dicho mantenimiento será documentado con fecha y hora de ejecución.
- El departamento deberá estar preparado para ejecutar el mantenimiento correctivo a los equipos en caso de ser necesario.

- Únicamente el responsable de los activos o un delegado de este podrá ejecutar las tareas de instalación, mantenimiento y configuración de los equipos; estará prohibida la manipulación y cambios en la configuración por parte de usuarios no autorizados.
- Cada falla encontrada en los equipos deberá ser documentada con los datos respectivos de serie del equipo, función, tratamiento de corrección a aplicar fecha de detección del daño, fecha de corrección del fallo y fecha de retorno a sus operaciones.

Métricas: Porcentaje semanal de equipos totalmente operativos y que cumplen con su función de manera correcta e informe del mantenimiento indicando cuáles y cuántos equipos presentan problemas especificando qué problema es y cuál es la solución ejecutada o por ejecutar por el técnico.

Porcentaje de equipos operativos = PorEO

Total de equipos = TotEq

Equipos totalmente operativos = EqTO

$$PorEO = EqTO \times 100 / TotEq$$

Informe de registros de equipos que salen del departamento bajo préstamo con datos como numero o identificador del equipo, fecha de salida, responsable del equipo (persona que lo solicitó), firma y fecha de entrada.

Inventario de equipos totales en posesión del departamento.

4.1.6. Seguridad en la operativa

Generalidades

Es fundamental contar los periodos de tiempo para restablecer las acciones y retomar las actividades en caso de que haya algún fallo de sistema, de la misma manera lograr aplicar un correctivo inmediato si la información queda expuesta por alguna falla ya sea humana o del sistema en sí. Monitorear el proceso de copias de resguardo de información, así como la prueba periódica de su restauración permite garantizar la restauración de las operaciones en

los tiempos de recuperación establecidos y acotar el periodo máximo de pérdida de información asumible para cada organización, la presente política está asociada a las pautas establecidas en el punto 6 del EGSI (Esquema Gubernamental de Seguridad de la Información), referente a Gestión de Comunicaciones y Operaciones.

Objetivos

- Controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada.
- Definir los tiempos de recuperación de sistemas y de vuelta a las actividades de la institución luego de sufrir algún fallo.
- Realizar la documentación de todas las actividades que se realicen para poder retomar el control de los sistemas en caso de falla.

Al cumplir con los procesos, controles y normas establecidas se puede tener claro los riesgos existentes y de esta manera poder dar una solución adecuada y de manera rápida al momento de presentarse alguno, mediante auditorías técnicas y registros de actividad de los sistemas se puede dar un seguimiento y de esta manera tener un análisis más exacto para saber la situación actual del departamento.

4.1.6.1. Protección contra código malicioso

Documentar la instalación de nuevo software y sistemas en la institución es muy importante ya que permite saber porque se instala ese programa, cuál será su función y además centrara con un responsable en caso de cause algún daño en el desarrollo de las actividades de la institución, también es necesario definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados a las redes de la organización.

4.1.6.1.1. Controles contra código malicioso

Es necesario definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados a las redes de la organización.

Métricas: Total mensual de amenazas o virus bloqueados o eliminados.

Total de amenazas bloqueadas o eliminadas = TotABE

Amenazas eliminadas = AmeE

Amenazas Bloqueadas = AmeB

$$TotABE = AmeE + AmeB$$

Porcentaje de amenazas bloqueadas o eliminadas.

Porcentaje de amenazas bloqueadas/eliminadas = PorABE

Amenazas detectadas = AmeD

$$PorABE = TotABE \times 100 / AmeD$$

4.1.6.2. Copias de seguridad

La correcta gestión de las copias de seguridad depende de un proceso elaborado y estructurado debe contar con la documentación correspondiente donde quede claro el responsable, la fecha en que se realizó la cantidad de información y a que área pertenece aplicando los controles de seguridad adecuados y el cifrado correspondiente de tal manera que la información respalda sea igual de confiable que la original.

4.1.6.2.1. Copias de seguridad de la información

La información que sea respaldada debe contar con altos nivel de criptografía para de esta manera asegurar que no sea alterada, la documentación de la misma también debe tener bien explicito quien hizo el respaldo, la hora y la cantidad de información y a que bloque pertenece.

Métricas: Numero semanal de backups de información sensible realizados.

Backups semanales = BckS

Porcentaje mensual de recuperación de información exitosos (Un porcentaje menor a 100% representaría la necesidad de revisar y restructurar los procedimientos seguidos para respaldar la información).

Porcentaje exitoso de datos recuperados = PorcExi

Recuperaciones de datos exitosa = RecExi

Intentos de recuperación ejecutados = IntRecEje

$$PorcExi = RecExi \times 100 / IntRecEje$$

4.1.6.3. Control del software en explotación

Con el fin de evitar potenciales amenazas a la seguridad al sistema o a los servicios del usuario, es necesario monitorear permanentemente el acceso y modificaciones a los diferentes sistemas de información y softwares del departamento de TIC, mediante procedimientos de control de cambios; todos los cambios efectuados a los sistemas deberán ser realizados por el personal capacitado, cumpliendo los procedimientos de seguridad y control.

Posteriormente a la ejecución de algún cambio en los sistemas se deberá proceder a actualizar la documentación del sistema con los cambios efectuados e informar a las áreas usuarias acerca de dichos cambios.

4.1.6.3.1. Instalación del software en sistemas en producción

Es sumamente necesario tener una separación de entornos de desarrollo, prueba y producción, estos entornos deben permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional y evitar de esta manera algún bug en los sistemas o la caída de los mismos, para ello se deberán implementar los debidos procedimientos para el control en la instalación de softwares en los sistemas.

Métricas: Numero mensual de instalaciones correctas de softwares en los sistemas versus el total de instalaciones fallidas o incorrectas.

4.1.6.4. Gestión de la vulnerabilidad técnica

Se debe monitorear y ajustar el uso de los recursos con el objetivo de garantizar el rendimiento adecuado en los sistemas, mediante técnicas de precisión que permiten encontrar las vulnerabilidades y tratarles de forma inmediata.

4.1.6.4.1. Restricciones en la instalación de software

Antes de realizar cualquier instalación o cambio de software se debe documentar el proceso y revisar que el nuevo software a instalarse en el departamento cumpla con las políticas de seguridad asignadas, para evitar que este cause algún daño y pérdida en los equipos de la institución.

Métricas: Porcentaje mensual de softwares instalados que no presentan efectos negativos en las actividades realizadas y que mantienen o mejoran el nivel de eficiencia con la que se lleva a cabo las labores para las cuales estas dispuestos. Esta métrica deberá ser aplicada pasada una semana de la instalación del último software del mes.

PorSw = Porcentaje de software instalado correctamente

SwInst = Softwares instalados

SwWoPr = Software instalados sin problemas en su funcionamiento y eficiencia

PorSw = SwWoPr * 100 / SwInst

4.1.6.5. Consideraciones de las auditorias de los sistemas de información

Mediante el proceso de las auditorías de los sistemas de información deben existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría. Estos procesos de auditoria deben estar correctamente documentados para de esta manera encontrar las soluciones a los problemas hallados, además los recursos de TI tienen que estar claramente identificados para agilizar el proceso de auditoría.

4.1.6.5.1. Controles de auditoria de los sistemas de información

Planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales, permite realizar el proceso de manear clara obteniendo resultados confiables y de esta manera minimizar las interrupciones en los procesos que se llevan a cabo en el departamento de TIC y en la institución en general

Métricas: Porcentaje de problemas referentes a la seguridad de la información hallados durante la auditoria que has sido resueltos.

ProPAR = Porcentaje de problemas resueltos

ProEnc = Problemas encontrados

ProRes = Problemas resueltos

ProPAR = ProRes * 100 / ProEnn

4.1.7. Seguridad en las telecomunicaciones

Generalidades

La seguridad en las telecomunicaciones pretende gestionar de manera segura las redes mediante el cuidadoso control del flujo de datos, monitoreo y protección considerando las implicaciones legales respectivas.

El departamento deberá establecer los respectivos controles y políticas de intercambio de información, cumpliendo los lineamientos establecidos en la legislación relevante.

Objetivos

- Asegurar que la información que se intercambia a través de redes telemáticas sea protegida.
- Evitar interferencias y daños a la información durante las comunicaciones telemáticas y evitar el acceso físico no autorizado.
- Garantizar la integridad y seguridad de la información que se transfiere a entidades externas.

4.1.7.1. Gestión de seguridad en las redes

A través de la políticas de monitoreo de redes de la institución se garantizaran las óptimas condiciones de operación de la red institucional y la prohibición de acceso a usuarios ajenos a la institución o no autorizados.

4.1.7.1.1. Controles de red

- Se ejecutarán procesos de monitoreo y control constantes a las redes de voz y datos de la institución por parte de él o los responsables designados por la dirección.
- Se establecerán los respectivos procedimientos de seguridad y cableado estructurado en caso de efectuarse cualquier proceso de trabajo en las redes.

- Periódicamente se verificará la operatividad de las redes institucionales para garantizar su disponibilidad durante los procesos del departamento.
- De ser necesaria la adaptación de nuevos puntos de red, deberán ser solicitados por escrito a la dirección del departamento de TIC para ser aprobados y posteriormente aprobados y ejecutados por parte del responsable de redes.
- Únicamente el responsable directo designado por la dirección de TIC podrá ejecutar los trabajos de infraestructura de redes y solo dicho responsable tendrá accesos a las zonas seguras de control de la red institucional.
- Todos los procesos ejecutados deberán ser documentados.

Métricas: Total mensual de incidentes de red identificados y categorizados de acuerdo a su importancia o afectación sobre los procesos y actividades institucionales (Leve / Grave).

4.1.7.2. Intercambio de información con partes externas

El intercambio de información con partes externas será permitido únicamente siguiendo rigurosas políticas que cumplan la legislación establecida por la institución, garantizando la protección de la información que entra y sale de la institución.

4.1.7.2.1. Políticas y procedimientos de intercambio de información

- Se deberán estudiar y verificar los canales de transmisión de información para evitar fuga y robo de los datos que entran y salen.
- Se establecerán los procedimientos a seguir en caso de alguna filtración y las sanciones que se ejecutarán en caso de verificarse que la filtración o falla en el intercambio fue producto de sabotaje por parte de algún funcionario de manera voluntaria o involuntaria.
- Los medios de intercambio de información a utilizar deberán siempre dar las garantías de confiabilidad necesarias conservando la integridad de la información.
- En caso de fallo o interrupción durante el intercambio se deberá evaluar el medio utilizado para conocer las causas del o los errores en el intercambio y evaluar las soluciones a los problemas hallados.

4.1.7.2.2. Acuerdos de intercambio

- Tanto el emisor como el receptor de la información deberán estar de acuerdo con las normas de confidencialidad que establecerán previo al intercambio.
- Las normas que establecerán ambas partes antes del intercambio deberán contener las sanciones o consecuencias por incumplimiento de alguna de las partes.
- Las sanciones podrán incurrir en acciones legales en caso de que la filtración de alguna de las partes sea de información vital o crítica.

Métricas: Porcentaje mensual de conexiones o enlaces con terceros en los cuales los requisitos de seguridad de la información fueron implementados correcta y satisfactoriamente.

PorcEn = Porcentaje de enlaces satisfactorios

TotEnl = Total de enlaces

EnlSat = Enlaces satisfactorios

$$PorcEn = EnlSat * 100 / TotEnl$$

4.1.8. Adquisición desarrollo y mantenimiento de los sistemas de información

Generalidades

La presente política pretende asegurar el buen control y monitoreo en el desarrollo y adquisición de sistemas para el manejo y gestión de la información; se incluirán los procedimientos y se documentarán las normas necesarias para el cumplimiento de la norma, la presente política está asociada a las pautas establecidas en el punto 8 del EGSI (Esquema Gubernamental de Seguridad de la Información), referente a la Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.

Objetivos

- Asegurar que todo proceso de desarrollo y adquisición de sistemas de información se ejecute bajo controles de seguridad y validación de datos previamente establecidos.

- Garantizar que la información y su seguridad sean parte integral de todos los sistemas de información en todo su ciclo de vida.
- Certificar que dentro del ciclo de vida de desarrollo de los sistemas de gestión de información se implemente la seguridad de la información.

4.1.8.1. Requisitos de seguridad de los sistemas de información

Se garantizará que todos los sistemas de información cuenten con los controles necesarios para cumplir con la con la confiabilidad y seguridad, se manejarán los accesos a los sistemas a través de niveles que identificaran el alcance de permisos por parte del solicitante.

4.1.8.1.1. Análisis y especificación de los requisitos de seguridad

Los requisitos de seguridad deberán contemplar a sistemas nuevos creados según la necesidad institucional y las posibles mejoras o modificaciones a sistemas ya existentes adquiridos o desarrollados cumpliendo con los controles establecidos para el desarrollo e integración de sistemas del departamento.

4.1.8.1.2. Seguridad de las comunicaciones en servicios accesibles por redes públicas

Los sistemas cuyo funcionamiento requiera el uso de redes públicas deberán ser protegidos para prevenir actividades fraudulentas que concluya en robos y manipulación de la información.

Todo sistema desarrollado o adquirido pasará por un periodo de prueba y verificación para garantizar su fiabilidad en el desarrollo de los procesos.

Una vez puesto en marcha algún sistema efectuara el monitoreo respectivo y en caso de hallar fallos no descubiertos en el periodo de prueba se procederá a buscar solución o darlo de baja.

4.1.8.1.3. Protección de las transacciones por redes telemáticas

Todo proceso de intercambio de información por redes telemáticas deberá cumplir con los respectivos controles asociados a las políticas de seguridad en las telecomunicaciones y sus apartados correspondientes; se deberá garantizar un control adecuado y evitar filtraciones, daños e interferencias.

Métricas: Porcentaje mensual de accesos a sistemas y aplicaciones cumpliendo con la identificación del usuario, aceptación de responsabilidades y cumpliendo con las normas de control de accesos (Control por roles).

PorAcc = Porcentaje de accesos por usuarios adecuados

AccSis = Accesos al sistema

AccCor = Accesos correctos

$$PorAcc = AccCor * 100 / AccSis$$

Informe Mensual de incidentes.

4.1.8.2. Seguridad en los procesos de desarrollo y soporte

El control en los procesos de desarrollo y soporte deberá ser estricto, se deberán determinar responsables de la seguridad de dichos procesos desde la dirección del departamento que garanticen la ejecución correcta de los procesos, la incorporación de la seguridad en su ciclo de vida y su finalización en el tiempo adecuado.

Se deberá desarrollar la documentación necesaria posterior al desarrollo de sistemas para usuarios y administradores que faciliten el uso y soporte.

4.1.8.2.1. Política de desarrollo seguro de software

Se deberán implantar y ejecutar los controles que garanticen el desarrollo seguro de software cumpliendo con las normativas legales.

- Todo software desarrollado deberá cumplir con las normas de seguridad de la información.
- Cada software desarrollado deberá cumplir con su función de manera eficiente, por lo que previo a su implantación final pasara por rigurosas pruebas para asegurar que su funcionamiento es efectivo y cumple con los estándares de seguridad necesarios.
- La función de todo software desarrollado deberá aportar a la mejora de las funciones ejecutadas en el departamento y mitigar falencias previas existentes antes de su implementación.

4.1.8.2.2. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Es de vital importancia cumplir con los procesos de revisión de las aplicaciones y sistemas críticos para el correcto funcionamiento de los procesos claves del departamento después de cualquier proceso de mantenimiento o actualización de sistemas, para garantizar que no existan efectos adversos en el funcionamiento correcto de las aplicaciones.

En caso de existir algún cambio adverso el responsable asignado deberá procurar solucionar lo antes posible el inconveniente.

4.1.8.2.3. Seguridad en entornos de desarrollo

Los entornos de desarrollo utilizados por la institución deberán estar protegidos bajo la responsabilidad del o los encargados del desarrollo de aplicaciones para el departamento.

Métricas: Informe mensual del estado de seguridad de los procesos de desarrollo de software detallando vulnerabilidades conocidas, probabilidad de que explote dicha vulnerabilidad y sus posibles efectos.

4.1.9. Relaciones con suministradores

Generalidades

Se deberán implementar acuerdos, ejecutar procesos de monitoreo que garanticen su cumplimiento y aseguren que los servicios se entreguen de manera eficiente y que satisfagan los requerimientos solicitados por terceras personas.

Garantizar que todos los activos de la organización a los que los proveedores tienen acceso estén debidamente protegidos.

Objetivos

- Protección de los activos de la institución a los que los proveedores tienen acceso
- Garantizar la seguridad de la información y entrega de servicios solicitados por terceros, de igual manera dar las mismas garantías de seguridad para servicios y productos externos solicitados por la institución a proveedores externos.

4.1.9.1. Seguridad de la información en relaciones con suministradores

La política actual pretende garantizar que los niveles de seguridad de la información no deben verse reducidos por la inserción de algún producto o servicio externo ni afectar los medios de procesamiento de datos.

El acceso de terceros a cualquiera de los medios de tratamiento de información del departamento deberá ser restringido; en caso de ser estrictamente necesario su acceso deberán evaluarse las posibles afectaciones a la seguridad, tomar las medidas de control pertinentes y deberá hacerse bajo el debido control del responsable asignado por la dirección.

4.1.9.1.1. Política de seguridad de la información para suministradores

- Se deberán firmar acuerdos de confidencialidad con los suministradores para evitar la filtración de información.

- Se evitara cualquier acceso de usuarios terceros a los medios de procesamiento de información.
- Se documentaran los accesos al departamento adjuntando fecha, razón de la visita y horas de ingreso y salida.

4.1.9.1.2. Tratamiento del riesgo dentro de acuerdos de suministradores

Todos los proveedores deberán tener pleno conocimiento de los requisitos de seguridad establecidos dentro del departamento; en caso de que se requiera que algún proveedor acceda, almacene, procese o proporcione algún elemento de hardware e infraestructura para el departamento este deberá conocer los lineamientos de seguridad de la información que deberá obligatoriamente respetar, en caso de no hacerlo el departamento tomará las medidas pertinentes.

4.1.9.1.3. Cadena de suministro en tecnologías de la información y comunicación

Dentro de los acuerdos con los proveedores deberán estar claramente expuestos los lineamientos de seguridad de la información, además de especificar los riesgos de SI enlazados a la cadena de suministros en TIC.

Métricas: Porcentaje mensual de conexiones identificadas, evaluadas y categorizadas como seguras.

PorCS = Porcentaje de conexiones seguras

ConSol = Conexiones solicitadas

ConSE = Conexiones seguras ejecutadas sin novedades de seguridad

$$PorCS = ConSE * 100 / ConSol$$

4.1.10. Gestión de incidentes en la seguridad de la información

Generalidades

La gestión de incidentes pretende garantizar que cualquier eventualidad negativa a la que se encuentren expuestos los activos de información, sea detectada, tratada, mitigada de manera eficiente y documentada para prevenir futuros incidentes la presente política está asociada a las pautas establecidas en el punto 9 del EGSI (Esquema Gubernamental de Seguridad de la Información), referente a la Gestión de Incidentes de seguridad de la información.

Objetivos

- Procurar que cualquier incidente asociado a los activos de información sea detectados a tiempo.
- Garantizar que cualquier debilidad y evento de seguridad de la información encontrado, asociado a los sistemas de información sea comunicado para que se ejecuten las debidas acciones de corrección necesarias
- Contar con una gestión de incidentes de seguridad de la información totalmente eficaz.

4.1.10.1. Gestión de incidentes de seguridad de la información y mejoras

Se establecerán los procedimientos para el control efectivo de incidentes y manejo de debilidades que afecten a los activos de información una vez que sean comunicados a los responsables dentro del departamento.

A través de procesos de mejora continua, se buscara mejorar la gestión de incidentes con el transcurso del tiempo; toda eventualidad encontrada deberá ser documentada, registrada y almacenada debidamente.

Los activos y medios de procesamiento de información afectados por alguna incidencia serán evaluados posteriormente de la ejecución de los controles correctivos para garantizar la eficacia de dichos controles.

4.1.10.1.1. Notificación de puntos débiles de la seguridad

Toda vulnerabilidad a la seguridad de la información detectada deberá ser informada inmediatamente a los responsables, es obligación de todo funcionario del departamento dar aviso de dicha eventualidad.

4.1.10.1.2. Respuesta a los incidentes de seguridad

Una vez informada la debilidad o vulnerabilidad de seguridad de la información encontrada se procederá a ejecutar las acciones acordes al incidente para dar solución y mitigar la amenaza de seguridad.

Métricas: Informe mensual de incidentes detectados categorizados por nivel de gravedad, documentación de los resultados de la evaluación de costos por posibles daños y acciones de reparación.

Coste mensual total por encima del umbral aceptable provocado por daños por incidentes de seguridad no detectados, la dirección definirá el coste límite aceptable.

4.1.11. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio

Generalidades

Con la finalidad de garantizar la continuidad del negocio se incluirán dentro de los procesos críticos del departamento los requisitos de seguridad de la información necesarios fijados para mejorar y asegurar la efectiva operatividad del departamento la presente política está asociada a las pautas establecidas en el punto 10 del EGSI (Esquema Gubernamental de Seguridad de la Información), referente a la Gestión de continuidad del negocio.

Objetivos

- Garantizar que la seguridad de la información sean preservados durante la ejecución de todas las funciones del departamento para el correcto funcionamiento y continuidad del negocio.
- Mantener la seguridad en todas las gestiones y procesos de continuidad del negocio.
- Asegurar para el proceso de la información la disponibilidad de las instalaciones necesarias.

4.1.11.1. Continuidad de la seguridad de la información

Se deberán ejecutar procesos y cambios de implementación para garantizar la continuidad de la seguridad de la información, los cuales a su vez deberán ser documentados; toda medida de continuidad de seguridad de la información deberá ser verificada en cuanto a su efectividad y validez.

4.1.11.1.1. Implantación de la continuidad de la seguridad de la información

En caso de situaciones adversas que afecten los procesos de tratamiento y la seguridad de la información, el departamento deberá establecer, documentar e implementar los controles previamente establecidos que garanticen la continuidad y ejecución de los procesos normales del departamento.

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

Los controles de continuidad del negocio establecidos deberán pasar regularmente por un proceso de verificación, revisión y evaluación para asegurar que ante situaciones adversas su ejecución sea eficaz.

4.1.11.2. Redundancias

El control de redundancias deberá garantizar que las instalaciones cuentan con el equipo disponible para el procesamiento de la información, y en caso de verificarse de que no es así informar a la dirección solicitando el equipo necesario justificando las razones y como afecta en las operaciones del negocio no contar con él.

4.1.11.2.1. Disponibilidad de instalaciones para el procesamiento de la información

Un encargado departamental deberá verificar que los equipos actuales son suficientes para la ejecución correcta de los procesos de manejo y gestión de información, presentar un informe, una vez recibido el informe la dirección deberá decidir la factibilidad de adquirir nuevos equipos en caso de ser necesario.

Métricas: Tiempo medio entre fallos del sistema asumiendo su reparación inmediata (MTBF), tiempo medio entre fallos asumiendo que el sistema no se ha reparado (MTTF) y nivel de fiabilidad de un sistema (MTTF/MTBF).

4.1.12. Cumplimiento

Generalidades

Todas las operaciones ejecutadas en los sistemas de información se encuentran bajo la regulación de las disposiciones contractuales y legales establecidos por la dirección, los cuales están debidamente documentados y respaldados, la presente política está asociada a las pautas establecidas en el punto 11 del EGSI (Esquema Gubernamental de Seguridad de la Información), referente a Cumplimiento.

Objetivos

- Cumplir con cada una de las disposiciones legales y contractuales para evitar la ejecución de sanciones que de acuerdo a la gravedad de la infracción podría incurrir en casos civiles o penales.

4.1.12.1. Revisiones de la seguridad de la información

El presente control pretende dar garantías de que todas las operaciones del departamento se ejecutan de acuerdo a las políticas de seguridad de la información y procedimientos de la organización.

4.1.12.1.1. Cumplimiento de las políticas y normas de seguridad

El jefe departamental deberá periódicamente verificar que se cumpla con todas las normativas de seguridad de la información en todas las áreas de trabajo dentro del departamento, y en caso de encontrar irregularidades tomas las acciones pertinentes de acuerdo a las políticas y normas de la organización.

Métricas: Porcentaje mensual de incumplimientos no sustanciales de seguridad de la información detectados posteriores a la revisión de cumplimiento de SI.

PorIn = Porcentaje de incumplimiento

IncNSDet = Incumplimientos no sustanciales detectados

IncDet = Incumplimientos detectados

$$PorIn = IncNSDet * 100 / IncDet$$

4.1.13. Control del documento e historia de cambios

El presente documento de políticas de seguridad versión 1.0 dirigido al departamento de TIC del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas fue elaborado por

David Cedeño el 03 de febrero del 2017 con la aprobación del jefe del departamento el Mgt. David Rodríguez.

4.2. Plan para la implementación de políticas

El presente plan está basado en la en las normativas de control ISO 27002 (ver Anexo A), los controles que son relevantes y aplicables para la organización y al mismo.

Fecha de elaboración: 13/02/2017					
Actividad					
Sección	Controles ISO 27002	Salvaguardas planeadas	Observación	Responsable	Plazo de inicio y finalización
7	Seguridad ligada a los recursos humanos				
7.1	Antes de la contratación				
7.1.1	Investigación de antecedentes	Revisar las políticas de seguridad de la información punto 4.1.1.1.1	El departamento de RR.HH. ejecuta procesos de investigación de antecedentes a postulantes.	Departamento de RR.HH.	Anual
7.1.2	Términos y condiciones de contratación	Revisar las políticas de seguridad de la información punto 4.1.1.1.2	Los contratados firman aceptando los términos y condiciones de contratación	Departamento de RR.HH.	Anual
7.2	Durante la contratación				

7.2.1	Responsabilidades de gestión	Revisar las políticas de seguridad de la información punto 4.1.1.2.1	Existes políticas de responsabilidad	Jefe de TIC	Anual
7.2.2	Concienciación, educación y capacitación en SI	Revisar las políticas de seguridad de la información punto 4.1.1.2.2		Jefe de TIC	Anual
8	Gestión de activos				
8.1	Responsabilidad sobre los activos				
8.1.1	Inventario de activos	Revisar las políticas de seguridad de la información punto 4.1.2.1.1	Cuentan con una matriz de activos y responsables. (Matriz de riesgo inherente)	Analista de Sistemas	Anual
9	Control de accesos				
9.1	Requisitos del negocio para el control de accesos				
9.1.1	Política de control de accesos	Revisar las políticas de seguridad de la información punto 4.1.3.1.1	Los accesos a la información están cedidos por niveles y de acuerdo al cargo ocupado	Analista de Redes	Anual
9.1.2	Control de acceso a las redes	Revisar las políticas de seguridad de la información punto 4.1.3.1.2	Existen políticas de control de redes	Analista de Redes	Anual

9.2	Gestión de accesos de usuarios				
9.2.1	Gestión de altas/bajas en el registro de usuarios	Revisar las políticas de seguridad de la información punto 4.1.3.2.1	Se efectúan los procesos de altas y bajas en el sistema	Analista de Redes	Anual
9.2.3	Gestión de derechos de acceso con privilegios especiales	Revisar las políticas de seguridad de la información punto 4.1.3.2.2	Privilegios limitados únicamente al jefe departamental	Analista de Redes	Anual
9.2.5	Revisión de los derechos de acceso de los usuarios	Revisar las políticas de seguridad de la información punto 4.1.3.2.3		Analista de Redes	Anual
9.2.6	Retirada o adaptación de los derechos de acceso	Revisar las políticas de seguridad de la información punto 4.1.3.2.4		Analista de Redes	Anual
9.4	Control de acceso a sistemas y aplicaciones				
9.4.1	Restricción de acceso a la información	Revisar las políticas de seguridad de la información punto 4.1.3.3.1		Analista de Redes	Anual
9.4.2	Procedimientos seguros de inicio de sesión	Revisar las políticas de seguridad de la información punto 4.1.3.3.2	Procedimientos de Log-on	Analista de Redes	Anual

9.4.3	Gestión de contraseñas de usuario	Revisar las políticas de seguridad de la información punto 4.1.3.3.3	Restablecimiento de contraseñas	Analista de Redes	Anual
10	Cifrado				
10.1	Controles criptográficos				
10.1.1	Política de uso de los controles criptográficos	Revisar las políticas de seguridad de la información punto 4.1.4.1.1	Equipos asegurados con contraseñas	Analista de Redes	Anual
10.1.2	Gestión de claves	Revisar las políticas de seguridad de la información punto 4.1.4.1.2		Analista de Redes	Anual
11	Seguridad física y ambiental				
11.1	Áreas seguras				
11.1.2	Controles físicos de entrada	Revisar las políticas de seguridad de la información punto 4.1.5.1.1		Analista de Redes	Anual
11.1.3	Seguridad de oficinas, despachos y recursos	Revisar las políticas de seguridad de la información punto 4.1.5.1.2	Sistema biométrico en el DATA CENTER	Analista de Redes	Anual

11.1.4	Protección contra amenazas externas y ambientales	Revisar las políticas de seguridad de la información punto 4.1.5.1.3	Políticas de protección al data center	Analista de Redes	Anual
11.2	Seguridad de los equipos				
11.2.4	Mantenimiento de los equipos	Revisar las políticas de seguridad de la información punto 4.1.5.2.1	Existen responsables del mantenimiento	Analista de Sistemas	Anual
12	Seguridad en la operativa				
12.2	Protección contra código malicioso				
12.2.1	Controles contra código malicioso	Revisar las políticas de seguridad de la información punto 4.1.6.1.1	Antivirus	Analista de Sistemas	Anual
12.3	Copias de seguridad				
12.3.1	Copias de seguridad de la información	Revisar las políticas de seguridad de la información punto 4.1.6.2.1	Respaldo de la información crítica	Analista de Sistemas	Anual
12.5	Control del software en explotación				

12.5.1	Instalación del software en sistemas en producción	Revisar las políticas de seguridad de la información punto 4.1.6.3.1		Analista de Sistemas	Anual
12.6	Gestión de la vulnerabilidad técnica				
12.6.2	Restricciones en la instalación de software	Revisar las políticas de seguridad de la información punto 4.1.6.4.1		Analista de Sistemas	Anual
12.7	Consideraciones de las auditorias de los sistemas de información				
12.7.1	Controles de auditoria de los sistemas de información	Revisar las políticas de seguridad de la información punto 4.1.6.5.1		Analista de Sistemas	Anual
13	Seguridad en las telecomunicaciones				
13.1	Gestión de la seguridad en las redes				
13.1.1	Controles de red	Revisar las políticas de seguridad de la información punto 4.1.7.1.1	Existen políticas para el control de redes	Analista de Redes	Anual

13.2	Intercambio de información con partes externas				
13.2.1	Políticas y procedimientos de intercambio de información	Revisar las políticas de seguridad de la información punto 4.1.7.2.1		Analista de Redes	Anual
13.2.2	Acuerdos de intercambio	Revisar las políticas de seguridad de la información punto 4.1.7.2.2		Analista de Redes	Anual
14	Adquisición, desarrollo y mantenimiento de los sistemas de información				
14.1	Requisitos de seguridad de los sistemas de información				
14.1.1	Análisis y especificación de los requisitos de seguridad	Revisar las políticas de seguridad de la información punto 4.1.8.1.1	Cuentan con políticas de seguridad de la información	Analista de Redes	Anual
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	Revisar las políticas de seguridad de la información punto 4.1.8.1.2		Analista de Redes	Anual

14.1.3	Protección de las transacciones por redes telemáticas	Revisar las políticas de seguridad de la información punto 4.1.8.1.3		Analista de Redes	Anual
14.2	Seguridad en los procesos de desarrollo y soporte				
14.2.1	Política de desarrollo seguro de software	Revisar las políticas de seguridad de la información punto 4.1.8.2.1		Analista de Redes	Anual
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Revisar las políticas de seguridad de la información punto 4.1.8.2.2		Analista de Redes	Anual
14.2.6	Seguridad en entornos de desarrollo	Revisar las políticas de seguridad de la información punto 4.1.8.2.3		Analista de Redes	Anual
15	Relaciones con suministradores				
15.1	Seguridad de la información en relaciones con los suministradores				
15.1.1	Política de seguridad de la información para suministradores	Revisar las políticas de seguridad de la información punto 4.1.9.1.1		Analista de Sistemas	Anual

15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	Revisar las políticas de seguridad de la información punto 4.1.9.1.2		Analista de Sistemas	Anual
15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	Revisar las políticas de seguridad de la información punto 4.1.9.1.3		Analista de Sistemas	Anual
16	Gestión de incidentes en la seguridad de la información				
16.1	Gestión de incidentes en la seguridad de la información y mejoras				
16.1.3	Notificación de puntos débiles en la seguridad	Revisar las políticas de seguridad de la información punto 4.1.10.1.1	Cuentan con políticas para la notificación de vulnerabilidades	Analista de Sistemas	Anual
16.1.5	Respuesta a los incidentes de seguridad	Revisar las políticas de seguridad de la información punto 4.1.10.1.2		Analista de Sistemas	Anual
17	Aspectos de la seguridad de la información en la gestión de la continuidad del negocio				

17.1	Continuidad de la seguridad de la información				
17.1.2	Implantación de la continuidad de la seguridad de la información	Revisar las políticas de seguridad de la información punto 4.1.11.1.1	Dentro de sus políticas contempla en parte la continuidad del negocio	Analista de Sistemas – Jefe de TIC	Anual
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Revisar las políticas de seguridad de la información punto 4.1.11.1.2		Jefe de TIC	Anual
17.2	Redundancias				
17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	Revisar las políticas de seguridad de la información punto 4.1.11.2.1		Analista de Sistemas	Anual
18	Cumplimiento				
18.2	Revisiones de la seguridad de la información				
18.2.2	Cumplimiento de las políticas y normas de seguridad	Revisar las políticas de seguridad de la información punto 4.1.12.1.1	Cuenta con políticas y normas de seguridad	Jefe de TIC	Anual

Tabla 2 Plan para la implementación de políticas

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- El buen uso y aplicación de las políticas de seguridad de la información propuestas reducirá la probabilidad de que cualquier amenaza existente vulnere los sistemas poniendo en juego la integridad de los activos de información.
- La normativa utilizada cuenta con un conjunto de controles para el correcto tratamiento de la información de la institución garantizando su disponibilidad, integridad y confiabilidad.
- Las políticas de seguridad cuentan con el conjunto de herramientas de control necesario para la detección temprana de amenazas y mitigación de vulnerabilidades.
- Las métricas definidas permitirán llevar el control de efectividad de las políticas para garantizar que su funcionamiento es correcto.

5.2. Recomendaciones

- La alta dirigencia departamental y el personal deben estar comprometidos a participar de la aplicación de las políticas de seguridad en cada uno de los procesos y etapas pertinentes.
- El personal debe estar capacitado acerca de las políticas de seguridad implantadas y tener plena conciencia de la importancia de su aplicación y las consecuencias o sanciones por incumplimiento
- Se deberán mantener actualizadas las políticas de acuerdo a la adaptación de nuevos procesos o modificación de procesos existentes para garantizar la perduración de su efectividad dentro de los procesos de tratamiento de información.

REFERENCIAS

- Alderete, M. V. (2012). EL DEBATE: ¿Las TIC reducen la distancia entre las empresas? Revista Iberoamérica de ciencia, tecnología y sociedad. Obtenido de http://www.revistacts.net/elforo/484-el-debate-ilas-tic-reducen-la-distancia-entre-las-empresas
- Álvarez Zurita, F. M., & García Guzmán, P. A. (Octubre de 2007). bibdigital-repositorio digital EPN. Obtenido de bibdigital-repositorio digital EPN: http://bibdigital.epn.edu.ec/bitstream/15000/565/1/CD-1077.pdf
- Aranda Segovia, J. (2009). IMPLEMENTACION DEL PRIMER SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION, EN EL ECUADOR, CERTIFICADO . Guayaquil-Ecuador. Obtenido de https://www.dspace.espol.edu.ec/bitstream/123456789/8080/1/Implementaci%C3%B3n%20del%20primer%20Sistema%20de%20Gesti%C3%B3n%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf
- Arévalo Acanio, J. G., Bayona Trillos, R. A., & Rico Bautista, D. W. (2015). Implantación de un sistema de gestión de seguridad de la información bajo la ISO 27001:análisis de riesgo de la información. Tecnura, 123-134.
- Bernal, J. J. (23 de 08 de 2013). PDCA Home. Obtenido de PDCA Home: http://www.pdcahome.com/5202/ciclo-pdca/
- Brynjolfsson, E., & Hitt, L. (2000). Beyond Computation: Information. Journal of Economic Perspectives, 14(4). Obtenido de The MIT center for digital business: http://ebusiness.mit.edu/erik/Beyond%20Computation%20-%20JEP.pdf
- Cedeño Tenorio, J. O. (2017). EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL DEPARTAMENTO DE TIC DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE ESMERALDAS (GADPE) BASADO EN LA NORMA DE SEGURIDAD ISO 27001. Esmeraldas: PUCESE.
- CEEISEC. (2012). CEEISEC. Obtenido de CEEISEC: http://www.ceeisec.com/nuevaweb/doc/ISO27001.pdf

- Flores Estévez, F. P., Jiménez Núñes, D. C., & Hidalgo Lascano, P. W. (27 de Septiembre de 2010). bibdigital-repositorio digital EPN. Obtenido de bibdigital-repositorio digital EPN: http://bibdigital.epn.edu.ec/bitstream/15000/2414/1/CD-3144.pdf
- Galindo López, C. M. (2014). Introducción a la informática y la seguridad. Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica, 351. Obtenido de https://books.google.com.ec/books?id=xKkYBgAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- ISACA. (2014). Acortando la brecha entre el acceso y la seguridad en grandes conjuntos de datos. ISACA JOURNAL, 6. Obtenido de http://www.isaca.org/Journal/archives/2014/Volume-6/Documents/Bridging-the-Gap-Between-Access-and-Security-in-Big-Data_joa_Spa_1114.pdf
- ISO 27000.es. (2013). El portal de la ISO 27001. Obtenido de El portal de la ISO 27001: http://www.iso27000.es/certificacion.html
- ISO 27000.es. (2013). el portal de la ISO 27002. Obtenido del portal de la ISO 27002: http://iso27000.es/iso27002_9.html
- ISO 27000.es. (2013). El portal de la ISO 27002. Obtenido de El portal de la ISO 27002: http://iso27000.es/iso27002_5.html
- ISO 27000.es. (2013). El portal de la ISO 27002. Obtenido de El portal de la ISO 27002: http://iso27000.es/iso27002_6.html
- ISO 27000.es. (2013). El portal de la ISO 27002. Obtenido de El portal de la ISO 27002: http://iso27000.es/iso27002_7.html
- ISO 27000.es. (2013). El portal de la ISO 27002. Obtenido de El portal de la ISO 27002: http://iso27000.es/iso27002_8.html
- ISO 27000.es. (2013). El portal de la ISO 27002. Obtenido de El portal de la ISO 27002: http://iso27000.es/iso27002_12.html
- ISO 27000.es. (2013). El portal de la ISO 27002. Obtenido de El portal de la ISO 27002: http://iso27000.es/iso27002_13.html
- ISO 27000.es. (2013). El portal de la ISO 27002. Obtenido de El portal de la ISO 27002: http://iso27000.es/iso27002_14.html

- ISO 27000.es. (2013). El portal de la ISO 27002. Obtenido de El portal de la ISO 27002: http://iso27000.es/iso27002_15.html
- ISO 27000.es. (2013). El portal de la ISO 27002. Obtenido de El portal de la ISO 27002: http://iso27000.es/iso27002_17.html
- ISO 27000.es. (2013). El portal de la ISO 27002. Obtenido de El portal de la ISO 27002: http://iso27000.es/iso27002_18.html
- ISO 27000.es. (2014). El portal de la ISO 27001. Obtenido de El portal de la ISO 27001: http://www.iso27000.es/sgsi.html
- ISO 27000.es. (2015). El portal de la ISO 27001. Obtenido de El portal de la ISO 27001: http://www.iso27000.es/iso27000.html
- ITIL Foundation. (2011). ITIL Foundation. Obtenido de ITIL Foundation: http://itilv3.osiatis.es/diseno_servicios_TI/gestion_seguridad_informacion/aplicacion_medidas_seguridad.php
- Ladino, M., Villa, P. A., & López, A. M. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. Scientia Et Technica, 334-339.
- Montiel, N. D. (2008). TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN PARA LAS ORGANIZACIONES DEL SIGLO XXI. (N. De Vita Montiel, Ed.) CICAG, 5(1). Obtenido de CICAG: http://www.urbe.edu/publicaciones/cicag/pdf/7-tecnologias-de-informacion.pdf
- Prefectura de Esmeraldas. (2014). Prefectura de Esmeraldas. Obtenido de Prefectura de Esmeraldas: http://www.prefecturadeesmeraldas.gob.ec/images/pdf/PEI%20GADPE.pdf
- Rodríguez Portes, D. (2014). Prefectura de Esmeraldas. Recuperado el 25 de 07 de 2015, de Prefectura de Esmeraldas: http://www.prefecturadeesmeraldas.gob.ec/files/PIE-GADPE-2012-214.pdf
- Rodríguez Taylor, E. (09 de 2011). Departamento Administrativo de la función pública de Colombia. Obtenido de Departamento Administrativo de la función pública de Colombia: http://portal.dafp.gov.co/portal/pls/portal/formularios.retrive_publicaciones?no=1592

- SGSI . (23 de 04 de 2015). SGSI Blog especializado en Sistemas de Gestión. Obtenido de SGSI Blog especializado en Sistemas de Gestión: http://www.pmg-ssi.com/2015/04/la-importancia-de-la-norma-iso-27001/
- SGSI. (21 de 05 de 2015). SGSI Blog especializado en Sistemas de Gestión. Obtenido de SGSI Blog especializado en Sistemas de Gestión: http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

ANEXOS

Anexo 1

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

ENTREVISTA DIRIGIDA AL JEFE DEL DEPARTAMENTO DE TIC´s

OBJETIVO: **Descubrir la arquitectura y tecnologías de seguridad.**

1. **¿Cuenta el departamento con un inventario de activos de información actualizado hasta la fecha?**

2. **¿Dónde están guardados los inventarios de activos de información?**

3. **¿Quién es el responsable de los inventarios de activos de información?**

4. **¿Cuenta el departamento con un inventario de procesos actualizado hasta la fecha?**

5. **¿Existe un documento de metodologías para el control de procesos de seguridad de la información?**

6. **¿Cuáles son las metodologías que utiliza para el control de procesos?**

7. **¿El departamento cuenta con el documento de declaración de aplicabilidad (SoA)?**

Anexo 2

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

ENTREVISTA DIRIGIDA AL JEFE DEL DEPARTAMENTO DE TIC´s

OBJETIVO: **Identificar la arquitectura organizativa de la seguridad de la Información.**

6. **¿Cuál es la política global de seguridad de la información bajo la cual se manejan actualmente?**

7. **¿Cuenta el departamento con un conjunto de políticas específicas de seguridad de la información?**

8. **¿Cuentan con un informe de evaluación de riesgos?**

9. **¿Existe un plan de capacitación de seguridad de la información para** el personal del departamento**?**

Anexo 3

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

ENTREVISTA DIRIGIDA AL JEFE DEL DEPARTAMENTO DE TIC´s

OBJETIVO: **Conocer la situación actual de la empresa con respecto a la seguridad de la información.**

1. **¿Actualmente con que documentación cuenta el departamento con respecto a la seguridad de la información?**

2. **¿Cuánto es el monto hasta la fecha que la institución ha invertido en seguridad de la información?**

3. **¿El personal nuevo tiene conocimiento de las políticas actuales para la seguridad de la información?**

4. **¿Existen métricas para la obtención de resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles?**

5. **¿Se hace un seguimiento de los indicadores de los procesos documentados?**

6. **¿Quién es el encargado del seguimiento de los indicadores de los procesos?**

7. **¿Qué medidas son tomadas cuando no se cumple el indicador?**

Anexo A ISO/IEC 27002

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

GES | CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

iso27000.es: Documento sólo para uso didáctico. La norma oficial debe adquirirse en las entidades autorizadas para su venta.

Octubre-2013

Ilustración 1 Controles ISO/IEC 27002

Anexo B Matriz de Riesgo Inherente

TIPIFICACIÓN RIESGO	PROCESO	ACTIVO DE INFORMACIÓN	PROPIETARIO DEL ACTIVO	AMENAZA	VULNERABILIDAD	PROPIETARIO DEL RIESGO	OBJETIVO DE CONTROL	CONTROL
R1	**Competencias tecnológicas**	Computador Personal-Lenovo	**Director de Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
				Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	16.1	16.1.3 16.1.5
				Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	8.1 12.6	8.1.1 12.6.2
				Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	9.2	9.2.1 9.2.3 9.2.6
R2		Programa Anual		Espionaje industrial	Inadecuada supervisión del trabajo de los empleados	**Analista de Sistemas**	7.1	7.1.1 7.1.2
R3		Reporte Mensual		Interceptación de información	Información disponible para personas no autorizadas	**Analista de Sistemas**	16.1	16.1.1
R4	**Modelo de Información**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1

R5	**Organizacional**	Servidor-Panasonic		Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	12.1	12.1.1
R6		Data Center – Libert		Acceso no autorizado al sistema de información	Contraseñas inseguras	**Analista de Redes**	9.1 9.4 10.1	9.1.1 9.1.2 9.4.2 10.1.2
R7		modelo organizacional		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	11.1	11.1.2
R8		diccionario de datos		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	13.1	13.1.1
R9		esquema		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	7.2	7.2.1 7.2.2
R10		Base de Datos		Destrucción de registros	Sesiones activas después del horario laboral	**Analista de Redes**	9.2	9.2.1 9.2.5 9.2.6
				Espionaje industrial	Mantenimiento inadecuado	**Analista de Redes**	7.1	7.1.1 7.1.2
				Falsificación de registros	Inadecuados derechos de usuario	**Analista de Redes**	9.1 9.4	9.1.1 9.4.1 9.4.2

								9.4.3
R11	**Garantizar la seguridad de los sistemas de intranet**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
R12		Servidor-Panasonic		Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	12.5 12.7	12.5.1 12.7.1
R13		Base de Datos		Acceso no autorizado al sistema de información	Contraseñas inseguras	**Analista de Redes**	9.1 9.4	9.1.1 9.4.1
R14		Data Center – Libert		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	11.1	11.1.2
R15		Datos del Usuario		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	13.1	13.1.1
				Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	7.2	7.2.1 7.2.2
R16		Notificación de alta		Modificación no autorizada de registros	Bases de datos con protección desactualizada contra códigos maliciosos	**Analista de Redes**	12.2	12.2.1

R17		Reporte Mensual		Sustracción de información	Nivel de confidencialidad no definido con claridad	**Analista de Redes**	9.2	9.2.2 9.2.3 9.2.4 9.2.5 9.2.6
R18	**Políticas de Seguridad de Tecnologías de Información**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
				Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	16.1	16.1.3 16.1.5
				Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	8.1 12.6	8.1.1 12.6.2
				Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	9.2	9.2.1 9.2.3 9.2.6
R19		Modelo de datos		Fuga o revelación de información	Falta de control en datos de entrada y salida	**Analista de Sistemas**	12.4	12.4.1 12.4.2 12.4.3
R20		diccionario de datos		Fuga o revelación de información	Falta de control en datos de entrada y salida	**Analista de Sistemas**	12.4	12.4.1 12.4.2 12.4.3
R21		Esquema de datos		Fuga o revelación de información	Falta de control en datos de entrada y salida	**Analista de Sistemas**	12.4	12.4.1 12.4.2 12.4.3
R22	**Gestión de Riesgo Informático**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1

				Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	16.1	16.1.3 16.1.5
R23		Matriz de riesgo		Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	8.1 12,6	8.1.1 12,6,2
R24		Activos GADPE		Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	9.2	9.2.1 9.2.3 9.2.6
R25	**Continuidad de los Servicios**	Solicitud de nuevo servicio	**Analista Tic**	Incumplimiento de leyes	Inadecuada capacidad de gestión	**Analista Tic**	17.1 17.2 18.1	17.1 .2 17.1.2 17.1.3 17.2.1 18.1.1
R26	**Monitoreo de Redes y Comunicaciones**	Servidor-Panasonic	**Analista de Redes**	Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	12.1	12.1.1
R27		Base de Datos		Acceso no autorizado al sistema de información	Contraseñas inseguras	**Analista de Redes**	9.1 9.4 10.1	9.1.1 9.1.2 9.4.2 10.1.2
R28		Data Center - Libert		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	11.1	11.1.2
R29		Servidor tipo Blade-IBM		Acceso no autorizado a la red	Redes accesibles a	**Analista de Redes**	13.1	13.1.1

					personas no autorizadas			
R30		Redes de datos		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	7.2	7.2.1 7.2.2
R31		Contrato de Redes y Telecomunicaciones		Incumplimiento de relaciones contractuales	Inadecuada capacidad de gestión	**Analista de Redes**	7.1	7.1.1
R32		Reporte de Trafico de Red		Incumplimiento de leyes	Inadecuado nivel de conocimiento y/o concienciación de empleados	**Analista de Redes**	7.2 18.2	7.2.1 7.2.2 18.2.2
				Interceptación de información	Inadecuada gestión de redes	**Analista de Redes**	13.1 13.2	13.1.1 13.2.1 13.2.2
R33	**Resguardo de la información**	Servidor-Panasonic	**Alasita de Sistemas Activos**	Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	12.1	12.1.1
R34		Data Center - Libert		Acceso no autorizado al sistema de información	Contraseñas inseguras	**Analista de Redes**	9.1 9.4 10.1	9.1.1 9.1.2 9.4.2 10.1.2

R35		Base de Datos		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	11.1	11.1.2
R36		Servidor tipo Blade-IBM		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	13.1	13.1.1
R37		Redes de datos		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	7.2	7.2.1 7.2.2
R38		Computador personal HP		Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
R39		computador personal LENOVO		Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	16.1	16.1.3 16.1.5
R40		Computador HP		Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	8.1 12,6	8.1.1 12,6,2
R41		Computador COMPAQ		Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	9.2	9.2.1 9.2.3 9.2.6
R42		Computador Apple		Uso no autorizado de software	Sesiones activas después del horario laboral	**Analista de Sistemas**	10.1 11.1 11.2	10.1.2 11.1.2 11.2.4

R43		Computador Portátil Toshiba		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R44		Computador Aditk		Error de usuario	Eliminación de soportes de almacenamiento sin borrado de datos	**Analista de Sistemas**		
R45		Computador Altek		Modificación no autorizada de registros	Claves criptográficas accesibles a personas no autorizadas	**Analista de Sistemas**	10.1	10.1.1 10.1.2
R46		SISTEMA PROGRAMA DE CONTABILIDAD-Olimpo		Daños provocados por actividades de terceros	Redes accesibles a personas no autorizadas	**Analista de Sistemas**	15.1	15.1.1 15,1,2 15,1,3
R47		LICENCIA WINDOWS-Server 2003		Daños ocasionados durante pruebas de intrusión	Bases de datos con protección desactualizada contra códigos maliciosos	**Analista de Sistemas**	12.2	12.2.1
R48		SISTEMA INF. DE CONT. Y FISCAL. DE OBRAS		Destrucción de registros	Sistemas desprotegidos ante acceso no autorizado	**Analista de Sistemas**	9.4 11.1	9.4.1 9.4.2 9.4.3 11.2 11.3

R49		SIST. CAPTURA DATOS CONTROL ACTIVOS-Symbol		Uso erróneo de herramientas de auditoría	Inadecuado nivel de conocimiento y/o concienciación de empleados	**Analista de Sistemas**	7.1 12.7	7.1.1 7.1.2 12.7.1
R50		SISTEMA DE AUTOMATIZACIÓN DE TEMPERATURA		Modificación no autorizada de registros	Falta de desactivación de cuentas de usuario luego de finalizado el empleo	**Analista de Sistemas**	9.2	9.2.1 9.2.6
R51		PAQUETE TÉCNICO DE CALCULO		Sustracción de información	Copiado sin control	**Analista de Sistemas**	7.1 11.1 12.3	7.1.1 7.1.2 11.1.1 11.1.4 12.3.1
R52		PROGRAMA DE ROLES DE PAGO SYSPAGO V30		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R53		PROGRAMA DE CONTABILIDAD SIA XP		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R54		PROGRAMA DE CONTABILIDAD ALFA G		Modificación accidental de datos del	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3

				sistema de información				
R55		Solicitud de Respaldo		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R56		Información Respaldada		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R57		SOFTWARE DE INFORM. GEOGRÁFICA		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R58	**Instalación y Actualización de Software**	computador personal HP	**analista de sistemas**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
R59		computador personal LENOVO		Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	16.1	16.1.3 16.1.5
R60		Computador HP		Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	8.1 12,6	8.1.1 12,6,2
R61		Computador COMPAQ		Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	9.2	9.2.1 9.2.3 9.2.6

R62		Computador Apple		Uso no autorizado de software	Sesiones activas después del horario laboral	**Analista de Sistemas**	10.1 11.1 11.2	10.1.2 11.1.2 11.2.4
R63		Computador Portátil Toshiba		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R64		Computador Aditk		Daños provocados por actividades de terceros	Eliminación de Registros y datos de funcionamiento de la información	**Analista de Sistemas**		
R65		Computador Altek		Errores de mantenimiento	Inadecuado control de cambios	**Analista de Sistemas**		
R66		SISTEMA PROGRAMA DE CONTABILIDAD-Olimpo		Robo	Inadecuada gestión del empleador	**Analista de Sistemas**	7.1	7.1.1 7.1.2
R67		LICENCIA WINDOWS-Server 2003		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R68		SISTEMA INF. DE CONT. Y FISCAL. DE OBRAS		Modificación accidental de datos del	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3

				sistema de información				
R69		SIST. CAPTURA DATOS CONTROL ACTIVOS-Symbol		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R70		SISTEMA DE AUTOMATIZACIÓN DE TEMPERATURA		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R71		PAQUETE TÉCNICO DE CALCULO		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R72		SOFTWARE DE INFORM. GEOGRÁFICA		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R73	**Administración de intranet, internet y correo electrónico**	Servidor-Panasonic	**analista de sistemas activos**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
R74		Data Center - Libert		Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	16.1	16.1.3 16.1.5

R75				Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	8.1 12.6	8.1.1 12.6.2
R76				Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	9.2	9.2.1 9.2.3 9.2.6
R77				Uso no autorizado de software	Sesiones activas después del horario laboral	**Analista de Sistemas**	10.1 11.1 11.2	10.1.2 11.1.2 11.2.4
R78				Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R79				Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	12.1	12.1.1
R80		Base de Datos		Acceso no autorizado al sistema de información	Contraseñas inseguras	**Analista de Redes**	9.1 9.4 10.1	9.1.1 9.1.2 9.4.2 10.1.2
R81		Servidor tipo Blade-IBM		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	11.1	11.1.2

R82		Redes de datos		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	13.1	13.1.1
R83		Contrato de Redes y Telecomunicaciones		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	16.1	16.1.1
R84	**Desarrollo e Integración de Sistema**	Aplicaciones Desarrolladas	**analista de sistemas activos**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
R85		Servidor-Panasonic		Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	16.1	16.1.3 16.1.5
R86		base de Datos		Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	8.1 12.6	8.1.1 12.6.2
R87		Servidor tipo Blade-IBM		Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	9.2	9.2.1 9.2.3 9.2.6
R88		Redes de datos		Uso no autorizado de software	Sesiones activas después del horario laboral	**Analista de Sistemas**	10.1 11.1 11.2	10.1.2 11.1.2 11.2.4
R89		Data Center - Libert		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3

R90				Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**		
R91		Manual de usuario		Mala utilización de la aplicación	Mala redacción del manual	**Analista de Redes**	9.1 9.4 10.1	9.1.1 9.1.2 9.4.2 10.1.2
R92		Manual de Instalación de Sistema		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	11.1	11.1.2
R93		Cronograma de Trabajo		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	13.1	13.1.1
R94		Acta de entrega del Sistema		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	14.1 14.2	14.1.1 14.1.2 14.1.3 14.2.1 14.2.3 14.2.6
R95		Código Fuente		Plagio	Falta de control de desarrollo			
				Mala utilización de la aplicación	Mala redacción del manual		14.2	14.2.1

Tabla 3 Matriz de Riesgo (Cedeño, 2017)