PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE EN ESMERALDAS

ESCUELA:

INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

TÍTULO:

Evaluación del Sistema de Gestión de Seguridad de la Información del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas (GADPE)

PREVIO:

A la obtención del Título de Ingeniera en Sistemas y Computación

AUTORA:

DIANA LISSETTE ANDRADE ESPAÑA

ASESOR:

MSC. Ing. David Rodríguez Portes.

JUNIO 2016.

"Trabajo de tesis aprobado luego de haber dado cumplimiento a los requisitos exigidos por el reglamento de Grado de la PUCESE previo a la obtención del título de Ingeniero de Sistemas y Computación".

…….

PRESIDENTE TRIBUNAL DE GRADUACIÓN

…….

LECTOR 1

…….

LECTOR 2

…….

DECANO DE LA FACULTAD/DIRECTOR DE ESCUELA

…….

DIRECTOR DE TESIS

AUTORÍA

"Yo, DIANA LISSETTE ANDRADE ESPAÑA, declaro que la presente investigación enmarcada en el actual trabajo de tesis es absolutamente original, auténtica y personal".

En virtud que el contenido de ésta investigación es de exclusiva responsabilidad legal y académica del autor y de la PUCESE.

DIANA LISSETTE ANDRADE ESPAÑA
1721483095

DEDICATORIA

Al creador de todas las cosas, el que me ha dado fortaleza para continuar cuando he estado a punto de caer, por permitirme llegar a este momento tan especial en mi vida, por los triunfos y los momentos difíciles que me han enseñado a valorar su infinito amor cada día, por ello le dedico este proyecto de tesis a Dios.

A mis amados padres Kléber Andrade y Yiya España, pilares fundamentales en mi vida, sin ellos jamás hubiese podido conseguir lo que hasta ahora, su tenacidad y su lucha incansable han hecho de ellos el gran ejemplo a seguir y destacar, no solo para mí, sino para mis hermanas y familia en general.

A mi preciosa hija Valentina, que ha sido el motor que me ha impulsado para conseguir este logro tan importante, y por motivarme cada día a seguir adelante.

A mi esposo amado Fabricio, compañero inseparable de mi vida, por motivarme cada día y creer en mi sin dudar de mis habilidades.

Diana Lissette Andrade España

AGRADECIMIENTO

En primer lugar a Dios por protegerme durante todo mi camino y ayudarme a superar obstáculos y dificultades a lo largo de toda mi vida.

A mis padres, Kléber y Yiya por su apoyo incondicional y porque han sabido formarme con buenos sentimientos, hábitos y valores, por sus sabios consejos que me han ayudado a salir adelante en los momentos difíciles y disfrutar de los momentos felices.

A mí querida Valentina porque con cada sonrisa me ha motivado a afrontar cada reto que se me presenta.

Agradezco también a mi esposo Fabricio, por la confianza y apoyo moral brindado, por compartir momentos de alegrías, tristeza y demostrarme que siempre podré contar con él.

A mis hermanas Mayra y Carolina, que a pesar de la distancia física entre nosotros, siempre han estado demostrándome su apoyo incondicional y su amor.

Al Ing. David Rodríguez, asesor de tesis, por su valiosa guía y asesoramiento para la realización de este proyecto.

Diana Lissette Andrade España

CONTENIDO

CONTENIDO DE TABLAS

CONTENIDO DE FIGURAS

RESUMEN

La presente investigación tuvo como objetivo central, evaluar el sistema de gestión de seguridad de la información del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas (GADPE), identificando las vulnerabilidades y oportunidades de mejora del mismo. Aplicando como metodología de evaluación, la norma ISO 27001:2013, con la cual a través de los métodos deductivo e inductivo, se procesó la información obtenida de las entrevistas, encuestas y observación a la población objeto de estudio en lo relacionado a los riesgos de seguridad de la información y la aplicación de los controles respectivos. También se tomó como referencia al estándar COBIT para la elaboración del instrumento de evaluación del sistema de gestión seguridad de la información. Esta investigación describe la situación actual en la que se encuentra la institución en lo referente al riesgo informático y la seguridad de la información; se establecen las causas y efectos en cada parámetro normado; se describen los principales impactos a nivel tecnológico, administrativo, legal, social, ético, organizacional obtenidos como resultado de la aplicación de este trabajo; y por último se realizan las debidas recomendaciones, que en conclusión garantiza la continuidad de los servicios y permite gestionar el riesgo informático y llegar así al cumplimiento de los objetivos institucionales en beneficio del desarrollo provincial

Palabras clave: *Evaluación, sistema, gestión, información, seguridad, normas ISO, COBIT.*

ABSTRACT

This research had as its central objective, to assess the safety management system of information Decentralized Autonomous Government of the Province of Esmeraldas (GADPE), identifying vulnerabilities and opportunities for improvement. Applying as evaluation methodology, ISO 27001: 2013, this through deductive and inductive method, the information obtained from interviews, surveys and observation to study population was processed in relation to the risks of information security and implementation of the respective controls. He also made reference to COBIT standard for the development of the assessment tool management system information security. This research describes the current situation in which is the institution in relation to IT risk and information security; the causes and effects in each regulated parameter set; the main impacts, administrative, legal, social, ethical, organizational technological level obtained as a result of the application of this work are described; and finally appropriate recommendations, in conclusion guarantees continuity of services and can manage IT risk and reach the fulfillment of institutional objectives for the benefit of provincial development realized

Keywords: *Evaluation, system management, information security, ISO, COBIT standards.*

INTRODUCCIÓN

Los activos informáticos son fundamentales para el normal desarrollo de las actividades en una organización, por este motivo deben ser protegidos, así como también la información de acuerdo con los principios de integridad, confidencialidad y disponibilidad de la misma.

Un sistema de gestión de seguridad de la información de una institución no gestiona propiamente a la institución pero ayuda a la toma de decisiones de las autoridades de la misma por eso sus normas y estándares deben estar sometidos a controles.

El Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas, es una entidad pública cuyo objetivo es brindar servicios a la colectividad, liderando proyectos de desarrollo mediante su eficiente ejecución; por este motivo es necesario que el sistema de gestión de seguridad de la información se encuentre bien definido y sea actualizado constantemente, estableciendo condiciones adecuadas para la seguridad informática.

La información es uno de los activos informáticos más importantes que posee la institución, por lo tanto se deben desarrollar mecanismos que permitan asegurar las características de la misma, ya que se encuentra sujeta amenazas tanto internas como externas.

En el primer capítulo se estructuró una fundamentación teórica sobre los aspectos más relevantes de los sistemas de gestión de seguridad definidos bajo estándares internacionales utilizados para el gobierno de las tecnologías de información.

En el segundo capítulo se realizó el diagnóstico del problema existente mediante la aplicación de los métodos inductivo y deductivo, que permitieron analizar los resultados obtenidos con la aplicación de los instrumentos (entrevista, encuesta y observación) para su procesamiento mediante tablas y gráficos que facilitaron el entendimiento del problema y la interpretación de los resultados

En el tercer capítulo se elaboró el informe de resultados de la evaluación realizada al sistema de gestión de seguridad de información del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas mediante la aplicación de la norma ISO 27001:2013, donde se especifican los 14 dominios, sus controles y sus respectivos objetivos de control. También se tomó como referencia el estándar COBIT para el

diseño de los instrumentos de evaluación que permitieron la sistematización de cada dominio y la cuantificación de cada uno de los controles.

En el cuarto capítulo se estableció el análisis de impactos a nivel tecnológico, organizacional, ético, social y económico; de manera que a través de la cuantificación de cada uno de los indicadores definidos se describa el beneficio general que esta investigación permite obtener no solo al departamento de Tecnología de Información y Comunicación sino al GADPE como institución.

Por último, se determinaron las conclusiones y recomendaciones basadas en los objetivos planteados, contrastando las teorías revisadas y los resultados tanto del diagnóstico de la problemática como de la evaluación de cada dominio del sistema de gestión de seguridad de información a nivel institucional; todo esto, para mejorar los controles existentes, implantar otros que son necesarios, así mismo procedimientos informáticos, la elaboración y documentación de políticas para la seguridad de la información.

CAPÍTULO I: FUNDAMENTOS TEÓRICOS

1.1. Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas (GADPE)

1.1.1. Historia

Según López (2002) señala que:

> Los Consejos Provinciales aparecen en el año 1928 – 1929, cuando en la Constitución Política del Estado se crean oficialmente dichos organismos seccionales en el Art. 139 de la Carta Magna y es en cumplimiento de este mandato constitucional que se organizan en el Ecuador los Consejos Provinciales en representación y administración del Estado a nivel del Gobierno subnacional intermedio. Decimos entonces que los Consejos Provinciales desde hace 74 años, existen cumpliendo la misión estatal a nivel provincial y atendiendo prioritariamente los sectores menos favorecidos de la sociedad ecuatoriana. En la Constitución Política No. 18 de la República, Registro Oficial No 1 del 11 de Agosto del año 1998 se constituye el Gobierno Provincial como la entidad estatal que a nombre del Estado, en la Provincia, ejerce su gobierno, la representación y administración política, articula y ejerce la intermediación de las acciones de los gobiernos nacionales y municipalidades.
>
> En Julio de 1984 es electo por votación popular prefecto de Esmeraldas, Don Jorge Chiriboga Guerrero. Luego es electo en 1988 por segunda ocasión como Prefecto Francisco Mejía Villa. Su período lo termina en 1992 el señor David Medina Rojas. A partir de 1992 a 1996 es electo por votación popular don Carlos Saúd Saúd. Para el periodo de 1996 al 2000, el pueblo se pronuncia democráticamente en su gran mayoría por el candidato populista don René Marcelo Rhor Valenzuela. Entre el sábado 10 de Agosto y el lunes 12 de Agosto se produce un hecho sin precedentes en la historia del Consejo Provincial. Al acudir a comenzar las labores el prefecto y la planta administrativa del organismo se encuentran con los indicios de llamas. Manos criminales al parecer el domingo al amanecer habían prendido fuego a muchos valiosos documentos de la anterior administración y de otras, y lo que es más deplorable de este acto vandálico es que las llamas consumen dos voluminosos libros de actas que

guardaban gran parte de la historia de la administración del H. Consejo Provincial de Esmeraldas.4 En el período 2000 – 2004 ocupa la Prefectura don Homero Horacio López Saúd, y desde el 2005 hasta la fecha, cumpliendo ahora su segunda administración, fue re-electa como Prefecta la Ing. Lucía de Lourdes Sosa Robinzón de Pimentel. (López, 2002)

1.1.2. Misión y visión

Según la (Prefectura de Esmeraldas, 2014) la misión es: Fomentar el desarrollo socio-económico de la provincia a través de servicios de calidad, la participación activa de todas sus autoridades, entidades y pobladores, con liderazgo, transparencia, y solidaridad; para mejorar la calidad de vida de sus habitantes, superar las inequidades, conservar la riqueza natural y ser un referente a nivel regional y nacional, para lo cual también define hacia el 2019 que el Gobierno Autónomo Descentralizado Provincial de Esmeraldas es la entidad que lidera los procesos de desarrollo de la provincia, mediante la eficiente ejecución de sus competencias, con un amplio sentido de responsabilidad social y de respeto a la biodiversidad y pluriculturalidad presentes en su territorio.

1.1.3. Gestión de Tecnologías de Información y Comunicación (TIC)

Según GADPE (2015) la Dirección de TIC del GADPE es la encargada de planificar, organizar, ejecutar y evaluar los sistemas, servicios e infraestructura de tecnología de información y comunicación de que requieren las diferentes instancias; Para lo cual define cuatro subprocesos:

- **Infraestructura Tecnológica:** Garantizar la operación, funcionamiento continuo, y uso eficiente de la Infraestructura Tecnológica utilizada, para alcanzar los objetivos del plan informático de la Institución; a fin de optimizar la utilización de los recursos informáticos puestos a disposición del personal del Gobierno Provincial.
- **Redes y Comunicaciones:** Planificar, organizar y controlar la red, los equipos de hardware y el software utilizado en el Gobierno Provincial para optimizar su uso en los procesos y actividades laborales, garantizando confiabilidad, oportunidad y seguridad en la información y la comunicación.

- **Sistemas y Aplicaciones:** Desarrollar e integrar sistemas, programas y aplicaciones informáticas definidas para las diferentes unidades administrativas, documentar los procesos de desarrollo y/o integración, adiestrar en el manejo a los usuarios del sistema; a fin de lograr la integración y eficiencia de los procesos automatizados de datos del Gobierno Provincial.
- **Proyectos y Servicios Web:** Administrar proyectos de tecnología y proveer servicios de internet, intranet, correo electrónico y sitio web de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos.

1.2. Información

La información es un conjunto de datos organizados acerca de algún evento o suceso, que tiene un significado explicito, que tiene como finalidad llegar al conocimiento de algo.

Según (Chiavetano, 2006) afirma que "En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones" (p. 73).

1.2.1. Tipos de información

Según (Laudon, Laudon, 2004) se establecen algunos tipos de información:

- **Información Privilegiada:** este tipo de información es aquella a la cual puede acceder un grupo de personas; por consiguiente esta información no es pública ya que su conocimiento es restringido.
- **Información Pública:** es aquella que es de fácil acceso para todo público, por lo tanto cualquier persona puede acceder a la misma debido a que se encuentra abierta es decir sin restricciones.
- **Información Confidencial:** como su nombre lo indica, se trata de información secreta que no se encuentra dirigida al público en general, por lo tanto solo un circulo muy cerrado de personas puede acceder a ella.

- **Información Externa:** esta tipo de información es aquella que se hace pública según ciertos parámetros de construcción ya que se encuentra creada con un fin específico.
- **Información Interna**: es aquella información que se maneja al interior de un grupo de personas, no es un tipo de información especial, sino que generalmente solo le interesa a esas personas.
- **Información Personal:** como su nombre lo indica es un tipo de información que nos indica los datos personales de una persona en particular.

1.2.2. Seguridad de la Información

En su artículo de revista López (2014) considera que la seguridad de la información "Es un conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma" (p. 100).

No se debe confundir el concepto de seguridad de la información con seguridad informática ya que este último se refiere a la seguridad en cuanto a los medios tecnológicos, pero la información puede estar en distintos medios o formas en el entorno organizativo, y no solo en medio informático. (Aranda & García, 2013)

Es importante conocer que el manejo de la seguridad de la información se basa en la tecnología, en una organización la información está centralizada por lo tanto su valor es muy significativo; ya que si no hay una seguridad en la misma dicha información puede ser mal utilizada, divulgada, robada, eliminada o saboteada. Lo que afectaría su disponibilidad, integridad y confidencialidad poniéndola en riesgo.

La información está clasificada de la siguiente manera según las posibilidades estratégicas para acceder a la misma:

- **Critica:** es el pilar fundamental para la operación de la organización.
- **Valiosa:** es un activo de la empresa y de muy alto valor.
- **Sensible:** solo el personal autorizado debe tener acceso a ella.

Godoy (2014) afirma que “el riesgo es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como también el impacto negativo que ocasione a las operaciones de negocio y seguridad es una forma de protección contra los riesgos”(p 101). La concepción de la seguridad de la información se da principalmente debido a que se encuentra basada en la tecnología y que la información que se maneja en las organización se encuentra centralizada y es de un alto valor ya que puede ser confidencial.

1.2.3. Aspectos fundamentales de la seguridad de la información

Confidencialidad.- Se entiende por confidencialidad el servicio de seguridad, condición, que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados.

Sánchez, Chalmeta, Coltell, Monfort, y Campos (2003) aseguran que: “La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él”

La confidencialidad es muy importante en una organización porque es la protección de los daos o información que pueden ser divulgados a personas no autorizados, información que es de vital importancia para la toma de decisiones en una institución.(Aguilera, 2010)

Integridad.- es el servicio de seguridad, que garantiza que la información es modificada, incluyendo su creación y borrado, solo por el personal autorizado. Suelen integrarse varios conceptos análogos en este segundo aspecto de la seguridad: precisión, integridad y autenticidad (Sanchez, 2003).

Es decir este aspecto de la información asegura que la información o los datos de la organización solo puede ser modificada por personal autorizado de una forma controlada.

Disponibilidad.- Asegura que el acceso a los datos o a los recursos de información por personal autorizado se produce correctamente y en tiempo. Es decir, la disponibilidad garantiza que los sistemas funcionan cuando se les necesita (Luna, 2004).

La disponibilidad de la información es un aspecto importante en una organización ya que si se necesitare una información en el instante esta debe estar a disposición de quienes la solicitaren con el fin de acceder a ella, sin ningún inconveniente.

1.2.4. Tipos de seguridad

La seguridad activa se caracteriza por comprender un conjunto de defensas o medidas donde su objetivo primordial es evitar o disminuir los riesgos que amenazan al sistema. Por otra parte tenemos la seguridad pasiva que se encuentran constituidas por medidas que se implantan, para que una vez ocurrido el incidente de seguridad se logre minimizar su repercusión y facilitar la recuperación del sistema. **(Godoy, 2014)**

1.2.5. Seguridad en sistemas

La seguridad se puede analizar desde dos enfoques: la seguridad externa y la seguridad interna.

Corrales, Beltrán y Guzmán (2006) afirman que "La seguridad externa son todos los mecanismos dirigidos a asegurar el sistema informático sin que le propio sistema intervenga"

A la seguridad externa podemos dividirlas en dos tipos las cuales son seguridad física y seguridad en administración:

Corrales, Beltrán y Guzmán (2006) dicen que:

> La seguridad física engloba los mecanismos que impiden a los agentes físicos entrar al sistema informático podemos establecer dos formas:

- Protección contra desastres: elementos de prevención, detección y eliminación de agentes tales como fuego, humo, inundaciones, etc.
- Protección contra intrusos: elementos que no permitan el acceso físico de las personas no autorizadas.

Según Corrales (2006) la seguridad de administración engloba los mecanismos más usuales para impedir el acceso lógico de personas físicas al sistema. Podemos dividir esto como:

- Protección de acceso: mecanismo que permite conectare a los usuarios autorizados y no permitir la entrada a los intrusos.
- Seguridad funcional: engloba aspectos relativos al funcionamiento del sistema ya la seguridad de las instalaciones.

Corrales, Beltrán y Guzmán (2006) afirman que la seguridad interna son todos los mecanismos dirigidos a asegurar el sistema informático, siendo el propio sistema el que controla dichos mecanismos, se engloban en lo que podemos denominar seguridad interna como por ejemplo el sistema de control de acceso y autenticación o el acceso a recursos compartidos.

1.3. Sistemas de información

La palabra sistema proviene del latín systema, y es un módulo ordenado de elementos que están interrelacionados y que interactúan entre sí, es decir es un conjunto de partes que se encuentran relacionados para llegar a un objetivo determinado.

López Hermoso et al (2000) afirma que por "Sistema se entiende un conjunto de elementos en interacción dinámica organizados para la consecución de un objetivo"

Un sistema de información dentro de una organización es de gran importancia, ya que sirve para llegar a los objetivos que se desean y facilita la toma de decisiones de los directivos. (Lopez J. , 2010).

El sistema de información dentro una organización debe ser de gran eficacia si facilita la información que necesita la institución para realizar sus actividades diarias, y también debe ser eficiente aprovechando con menores recursos posibles de la empresa ya sean tecnológicos, económicos, y así mismo el talento humano.

Bermúdez, Vargas y Rivera (2010) aseguran que un sistema de información realiza cuatro actividades básicas:

- Entrada de Información: Es el proceso mediante el cual el Sistema de Información toma los datos que requiere para procesar la información de Información toma los datos que requiere para procesar la información. Las entradas pueden ser manuales o automáticas. Las manuales son aquellas que se proporcionan en forma directa por el usuario, mientras que las automáticas son datos o información que provienen o son tomados de otros sistemas o módulos.
- Almacenamiento de Información: El almacenamiento es una de las actividades o capacidades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardada en la sección o proceso anterior. Esta información suele ser almacenada en estructuras de información denominadas archivos.
- Procesamiento de Información: Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida. Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados.
- Salida de Información: La salida es la capacidad de un Sistema de Información para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, terminales, cintas magnéticas y los plotters, entre otros.(Bermudez, 2010)

1.3.1. Sistema informático

Gallegos & Folgado (2011) asegura que: “Un sistema informático es un conjunto de partes que funcionan relacionándose entre sí para conseguir un objetivo preciso” (p. 236).

Según Laudon & Laudon (2012) las partes que componen un sistema informático son las siguientes:

- **Hardware:** es parte tangible del sistema, es decir son los dispositivos informáticos como mouse, teclado, cpu, pantalla etc.
- **Software:** es la parte intangible del sistema, como son los sistemas operativos, programas, aplicaciones etc.
- **Recursos humanos:** es el personal que se relacionan con el sistema ya sea desarrollando software, o en el tratamiento de los equipos para que esa interacción sea posible.
- **Documentación:** son los manuales, o instrucciones en donde se encuentre por escrito detalladamente el uso del sistema informático.

1.3.2. Sistema de Gestión

Según Ogalla (2005) sostiene que "El Sistema de Gestión es la herramienta que permite dar coherencia a todas las actividades que se realizan, y en todos los niveles, para alcanzar el propósito de la organización" (p. 3).
Un sistema de gestión debe tener una estructura determinada que debe estar adaptado al tipo de características de la organización tomando siempre en cuenta los elementos que sean más apropiados.

Se debe definir claramente la estructura organizativa, haciendo referencia a las funciones, responsabilidades y jerarquías en la institución, también tomar en cuenta los resultados a los que se quiere llegar, los procesos que deben realizarse para llegar a los resultados deseados, los procedimientos mediante los cuales se ejecutan actividades y tareas, y por ultimo tener presente los recursos de los que dispone la organización para lograr sus objetivos planteados.

1.4. Sistema de gestión de seguridad de la información

La gestión de seguridad de la información abarca todas actividades que se encuentren relacionadas con la dirección y control de la seguridad de los activos de información.

> Un sistema de gestión de seguridad de la información (SGSI) es parte del sistema de gestión global, basado en el enfoque en los riesgos del negocio y que

> establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. El sistema de gestión incluye la estructura organizacional, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. Por tanto, este concepto hace referencia a los esfuerzos sistemáticos y organizados destinados a perseverar la seguridad de la información en las organizaciones. (Areitio, 2008)

Un SGSI dentro de un ciclo comienza previniendo las amenazas que aparezcan en el sistema o que puedan afectar al mismo, se reducen los peligros que puedan existir y la contención de los probables incidentes.

1.4.1. Ciclo PDCA

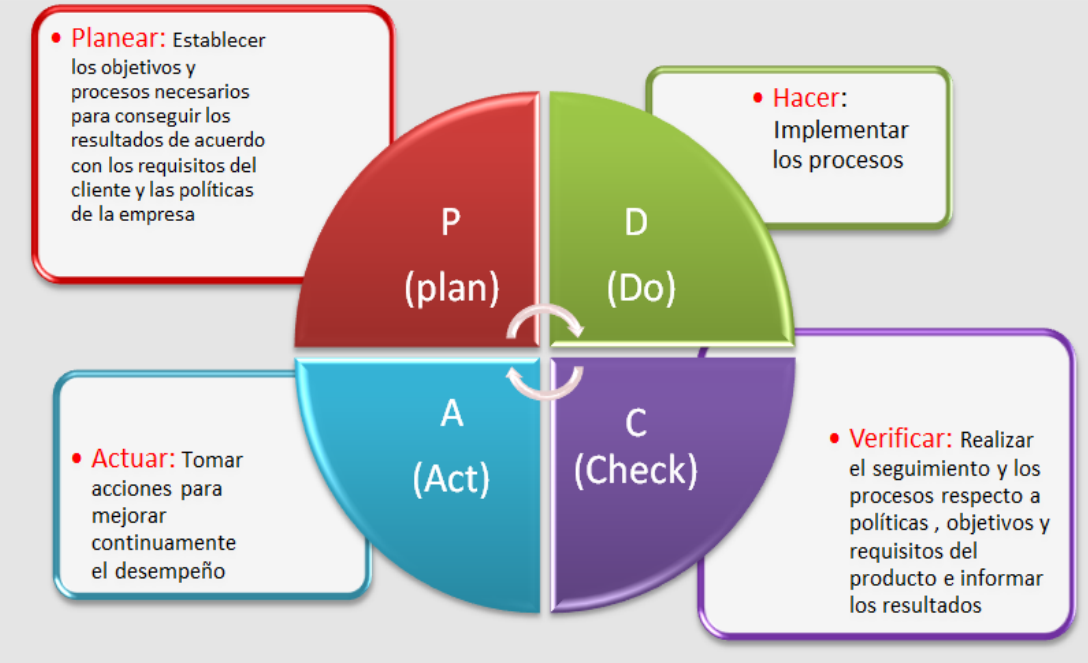
> Se trata de una estrategia de mejora continua difundida por Edwards Deming en la década de 1950, con base en las definiciones hechas por Walter A. Shewart en los años 30, y que describe cuatro pasos básicos para lograr la mejora: Plan, Do, Check y Act. La idea subyacente es que, más que lograr cambios radicales en el corto plazo, lo cual resulta costoso y poco efectivo casi siempre, debiera aplicarse un ciclo infinito de mejora continua en la que se realizan una y otra vez los cuatro pasos. Si esto se hace así, dice la teoría, se conseguirá una maduración gradual, eficiente y bien sustentada de los mecanismos – el sistema – para establecer las metas y definir las actividades que llevarán a las mismas.(Juarez, 2011)

El ciclo PDCA, ciclo de Deming o ciclo de mejora continua es una metodología que describe los cuatro pasos esenciales que se deben ejecutar de manera sistemática para llegar al mejoramiento de la calidad, estas cuatro etapas se deben ejecutar de manera cíclica de tal forma que cuando se haya finalizado la etapa final se vuelve a repetir la primera etapa del nuevo ciclo de forma que las actividades son nuevamente evaluadas para incorporar nuevas mejoras.

A continuación se detalla en qué consiste cada etapa según Juárez (2011):

- **Plan (planear o planificar).-** En este primer paso lo primero que debe realizarse es la identificación de todo aquello que se quiere mejorar, se reúnen e investigan los datos iniciales, se determinan los objetivos esperados y se planifican las actividades que se van a ejecutar.
- **Do (hacer o ejecutar).-** Lo siguiente es poner en marcha las actividades del plan hecho en el primer paso y documentar los resultados.
- **Check (verificar).-** Se procede con la comparación de los resultados obtenidos versus los resultados esperados, que se definieron en el en la planificación.
- **Act (actuar).-** por último se efectúan los ajustes necesarios para que se logren, los objetivos planeados; se revisan las lecciones aprendidas y se reinicia el ciclo completo.

Figura 1. Ciclo de Deming



1.5. Conceptos básicos importantes

Para continuar con el desarrollo de este capítulo es importante definir conceptos básicos que son de gran importancia para el desarrollo de esta investigación y que van a servir para fijar el rumbo de la misma.

1.5.1. Vulnerabilidad en los sistemas de información

Se puede definir a la vulnerabilidad como cualquier tipo de debilidad que tiene un sistema mismo que pueda comprometer los activos informáticos de una organización. Gutiérrez y Tena (2003) definen a la vulnerabilidad como "La posibilidad de ocurrencia de la materialización de una amenaza sobre un activo" (p. 38).

1.5.1.1. Tipos de Vulnerabilidad

- **Física:** se encuentra relacionado con el acceso físico a las instalaciones y a los activos informáticos de una organización.
- **Natural:** son desastres naturales que pueden ocurrir y causar daño al sistema.
- **Hardware:** esta vulnerabilidad representa la probabilidad que la parte tangible del sistema de información falle o pueda ser usado por terceras personas para atentar contra el sistema.
- **Software:** este puede ser usado como un medio para atacar al sistema de una organización debido a errores de programación.
- **Red:** mediante la red se puede penetrar a los equipos de cómputo y atacar a la red entera del sistema.
- **Factor humano:** son la parte más vulnerable del sistema ya que por la falta de capacitaciones y concienciación puede dar lugar al incumplimiento de las políticas para la falta de seguridad de la información. (Gutierrez J. , 2003)

1.5.2. Riesgo en los sistemas de información

Es un conjunto de elementos que ponen en peligro al sistema de información, y que pueden verse afectados en su operatividad, integridad o privacidad.

Aguilera (2010) define al riesgo como lo siguiente "Se denomina riesgo a la probabilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad"

1.5.2.1. Tipos de riesgos

Aguilera (2010) señala los siguientes tipos de riesgos:

- Integridad: son todos aquellos asociados a la autorización y procesamiento de las aplicaciones que son utilizadas en una organización.
- De Relación: son aquellos riesgos que se encuentran relacionados directamente con la toma de decisiones, ya que esta información es generada por las aplicaciones de la organización.
- De Acceso: son aquellos riesgos que están basados en el acceso inadecuado al sistema de la organización, a la información y sus datos.
- De Infraestructura: son aquellos riesgos que tienen que ver con la infraestructura tecnológica de la organización, misma que no podría estar funcionando de manera efectiva.
- De Seguridad General: estos riesgos tiene que ver con el diseño general y conexiones de la infraestructura tecnológica, como pueden ser un nivel de alto voltaje, materiales inflamables, niveles que inadecuados de energía, inestabilidad en las piezas eléctricas, ondas de ruido etc.

1.5.3. Amenazas en el sistema de información

En su libro Aguilera (2010) afirma que una amenaza es "la presencia de uno o más factores de diversa índole (personas, maquinas o sucesos) que –de tener oportunidad- atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad"; Es decir que una amenaza es la posibilidad que pueda ocurrir algún evento o se realice una acción que produzca un daño sobre los elementos del sistema de información.

1.5.3.1. Tipos de Amenazas

Los tipos de amenazas según Aguilera (2010) puede ser:

- Criminalidad: es toda acción que se efectúe con el fin de causar daños el sistema, originadas por la intervención de un factor humano, y que son penadas por la ley.
- Sucesos de Origen físico: son todos aquellos incidentes causados por la naturaleza o de orden técnico o por descuido del factor humano.
- Negligencia y decisiones institucionales: son todas aquellas decisiones tomadas por parte de los directivos que dirigen una organización y que influencia en el sistema.

1.6. Evaluación

Evaluación es un proceso que tiene por objeto determinar en qué medida se han logrado los objetivos previamente establecidos que supone un juicio de valor sobre la programación establecida, y que se emite al contrastar esa información con dichos objetivos (Aguilera, 2010).

1.6.1. Métodos de evaluación

Existen dos métodos para realizar una evaluación: subjetivamente u objetivamente.

- **Evaluación objetiva:** en esta evaluación es necesaria la medición, ya que no es suficiente que la investigación se encuentre basada en opiniones personales, se elabora en base a un análisis y a un diagnostico realiza sobre el hecho o fenómeno a evaluar. Cuando se efectúa la medición es necesario asignar números para cuantificar el objeto o hecho que se está investigando.

- **Evaluación subjetiva:** ésta por el contrario, se encuentra basada en opiniones de personas sobre un hecho o fenómeno, pero que carece de fundamento por la tanto no puede ser certificado.

1.6.2. Evaluación de sistemas

Según Rincón y Alonso (2000) con varios autores más exponen que la evaluación de los sistemas permite conocer el diagnostico existente de una organización en cuanto a la disponibilidad de recursos materiales y técnicos, cuando hablamos de evaluación de sistemas no solo abarcamos lo que son los activos informáticos sino que también al talento humano que labora dentro de la institución y de las personas de afuera, sus intenciones, sus fines, sus deseos.

Los progresos realizados en un sistema dentro de una institución deben ser aprobados, evaluados y monitoreados para conocer falencias, problemas o mejoras del mismo, es importante tomar en cuenta que la evaluación de cualquier tecnología debe ir acompañada de un conjunto de medidas, estándares o buenas prácticas ya definidas.

1.6.3. Proceso para realizar una evaluación

Los progresos o retrasos que se evidencian en un sistema deben ser medidos o evaluados para realizar mejoras o a su vez conocer cuáles son deficiencias que éste tiene.

Según Blásquez (2012), para llegar al cumplimiento de los objetivos planteados, la evaluación de cualquier sistema debe seguir ciertos pasos fundamentales:

- **Medir la consecución de los objetivos previamente establecidos**: Se determina si se cumple la evaluación con los factores de eficacia, eficiencia o factor de impacto de un servicio o sistema de información.
- **Disponer de un instrumento para diagnosticar los puntos débiles en el funcionamiento:** El instrumento puede ser el propio sistema de información o metodología específica para la medición de factores o indicadores de actividad, calidad, servicio, producción, etc.
- **Facilitar el proceso de la toma de decisiones:** Utilizando información objetiva, no basadas en opiniones o suposiciones.
- **Permitir la comparación entre sistemas mediante la construcción de estándares de referencia:** Evaluar la unidad de información y documentación en función de trabajos de evaluación de otras bibliotecas, centros de documentación o archivos. Por lo tanto se fijan unos indicadores comunes por los que determinar la eficiencia y eficacia de los servicios y procesos. Éste método también ha sido denominado evaluación exógena.
- **Justificar la existencia de los servicios y sistemas de información**: Evaluar para justificar el buen funcionamiento y mantenimiento de un servicio en función de su rendimiento económico, difusión o alcance, resultados operativos, calidad de servicio y respuesta al usuario. Todo ello implica como resultado la satisfacción del usuario. (Blásquez, 2012)

1.7. Métricas para evaluar la seguridad de la información

En su publicación (Laborde, 2013) afirma que métrica "Es una metodología de planificación, desarrollo y mantenimiento de sistemas de información. Son un

conjunto de medidas que se le aplica a la información para mantenerla precisa y segura de cualquier agente externo que pudiera ponerla en peligro".

Es decir que una métrica define como un conjunto de reglas y mandatos, que son fundamentales para poder medir de manera la realidad existente de una organización en cuanto a la seguridad de la información.

En su publicación (Gutierrez C. , 2013) basada en el documento publicado por OWASP Application Security, Guide for CISO's, indica que existen las siguientes métricas para evaluar la seguridad de la información:

- **Métricas de procesos de seguridad:** El objetivo de las métricas de procesos es determinar qué tan bien los procesos de seguridad en la organización cumplen con los requisitos definidos por las políticas de seguridad y las normas técnicas seguidas por la empresa.
- **Métricas de riesgos de seguridad:** Como parte de las métricas es muy importante conocer la eficacia de las medidas tanto preventivas como correctivas que se implementan en la empresa como parte de la gestión de la seguridad. Por ejemplo, tener medidos los tiempos de respuesta a incidentes productos las pruebas de los Planes de Continuidad del Negocio. También tener un inventario de los problemas de seguridad que han sido explotados y relacionarlos con los análisis de vulnerabilidad realizados y las acciones correctivas implementadas, de esta forma se puede conocer la eficacia de las medidas de control.
- **Seguridad en el ciclo de vida de desarrollo de las aplicaciones:** Un aspecto a menudo descuidado es el gasto en seguridad que se hace sobre las aplicaciones antes de que salgan a producción. En este sentido si se hiciera inversión en pruebas para determinar la seguridad de las aplicaciones, los costos de las correcciones serían menores a hacerlo cuando ya están en producción. Algo que puede sonar tan obvio muchas veces no es aplicado buscando la agilidad en los procesos de desarrollo. En este sentido tener un control sobre el cumplimiento de los tiempos de desarrollo, puede ayudar a que no se limiten los tiempos de prueba con el propósito de cumplir con la implementación.(Gutierrez C. , 2013).

1.8. Estándares y normas para la seguridad de la información

Un estándar es un documento que se ha determinado por la aprobación de una institución reconocida a nivel mundial, y que ofrece guías, reglas o características determinadas para que se usen repetidamente dentro de una organización.

A continuación se presentan los estándares más reconocidos para la seguridad de la información:

Cobit, acrónimo de "Control Objectives for Information and related Technology" (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por la Information Systems Audit and Control Foundation (ISACA), la cual fue fundada en 1969 en EE.UU., y que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TIC. Actualmente tiene más de 60.000 miembros en alrededor de 100 países. Por otra parte también existe Itil, Acrónimo de "Information Technology Infrastructure Library", ITIL es una norma de mejores prácticas para la administración de servicios de Tecnología de Información (TI), desarrollada a finales del año 1980 por entidades públicas y privadas con el fin de considerar las mejores prácticas a nivel mundial. La normativa COSO, acrónimo de The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework, está principalmente orientada al control de la administración financiera y contable de las organizaciones. En síntesis, el Informe COSO es un documento que contiene directivas e indicaciones para la implantación, gestión y control de un sistema de Control Interno, con alcances al área informática. A semejanza de otras normas ISO, la 27000 es una serie de estándares, que incluye (o incluirá, pues algunas partes aún están en desarrollo), definiciones de vocabulario (ISO 27000), requisitos para sistemas de gestión de seguridad de la información (ISO 27001), guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información (ISO 27002), una guía de implementación de SGSI (Sistema de Gestión en Seguridad de la Información) junto a información de uso del esquema PDCA (Plan, Do, Check, Act) [6] (ISO 27003), especificación de métricas para determinar la eficacia de SGSI (ISO 27004), una guía de técnicas de gestión de riesgo (ISO 27005), especificación de requisitos para acreditación de entidades de auditoría y

> certificación de SGSI (ISO 27006), una guía de auditoría de SGSI (ISO 27007), una guía de gestión de seguridad de la información para telecomunicaciones (ISO 27011), una guía de continuidad de negocio en cuanto a TIC (ISO 27031), una guía de ciber-seguridad (ISO 27032), una guía de seguridad en redes (ISO 27033), una guía de seguridad en aplicaciones (ISO 27034), y una guía de seguridad de la información en el sector sanitario (ISO 27799).(Burgos, 2010)

La ISO 27001:2013 es una norma internacional formulada por la Organización Internacional de Estandarización, y refiere como realizar la gestión de la seguridad de la información en una organización, ya sea de tipo gubernamental, organizaciones sin fines de lucro, comerciales etc.

Esta norma esta direccionada a aspectos netamente organizativos, ya que establece una serie de acciones para establecer la implementación, monitorización, operación, revisión y mantenimiento de un sistema de gestión de seguridad de la información. (Bustos , Chávez, & González, 2009)

Esta norma se ha convertido en la principal a nivel mundial para la seguridad de la información y muchas organizaciones han certificado su cumplimiento.

Lo primordial para este estándar es proteger la confidencialidad, integridad y disponibilidad de la información de una organización, realizando una investigación exhaustiva de cuáles son los problemas que podrían afectar de manera especial a la información, y luego plantear soluciones para estas anomalías.

Kosutic, Osca y Leal (2010) afirman que:

> Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.(Kosutic, 2015)

Según ISACA (2015) COBIT ayuda a las organizaciones a crear valor óptimo de la Tecnología de Información, manteniendo un balance entre los beneficios, riesgos y recursos, sirve para administrar y gobernar la información y tecnología relacionada en toda la organización, también permite que la tecnología sea gobernada y gestionada de una manera integral para toda la empresa.

1.9. Cuadro comparativo entre estándares

Tabla 1. Comparación entre estándares

ESTANDAR	FUNCIONES	AREAS	CREADOR	¿Para qué se implementa?	¿Quiénes evalúan?
COBIT	Mapeo de Procesos	4 Procesos y 34 Dominios	ISACA	Auditoria de Sistemas de Información	Compañías de consultoría IT, Compañías de Contabilidad, Organizaciones en general que posean S.I.
ITIL	Mapeo de la Gestión de Niveles de Servicios de IT	9 procesos	OGC	Gestión de Niveles de Servicio	Compañía de Consultoría de IT
ISO 27000	Marco de referencia de seguridad de la información	10 Dominios	ISO International Organization for Standarization	Cumplimiento del estándar de seguridad	Empresas que posean o quieran definir su SGSI. Compañías de Consultoría de IT, Empresas de Seguridad, Consultores de seguridad en la información
COSO	Control interno	5 componentes	Comité de Organizaciones Patrocinadoras de la Comisión Treadway	Contiene directivas e indicaciones para la implantación, gestión y control de un sistema de Control Interno, con alcances al área informática.	Organizaciones en general que deseen evaluar su sistema de control interno

1.10. Dominios de la ISO 27001-2013

Los dominios de la Norma ISO 27001:2013 se encuentra comprendida por 14 cláusulas de controles de seguridad de la información, 34 controles y 114 objetivos de control, varios controles han sido borrados, muchos han sido fusionados otros revisados y actualizados, comparado con la ISO 27001-2005.

En el Anexo C se presenta la tabla que indica de una forma más clara como se encuentran divididos dichos dominios con sus respectivos controles y estos a su vez en objetivos de control.

1.8. Investigaciones realizadas

Se han realizado investigaciones que tienen como base evaluar el SGSI de una institución o empresa, como es el proyecto realizado en la Escuela Politécnica del Ejercito del Ecuador elaborado por Guagalango y Moscoso (2011) sobre el uso de los controles de la Norma ISO 2700, dedicada a especificar requerimientos necesarios para establecer, mantener y mejorar un Sistema de Gestión de Seguridad de la información.

Para efectuar ésta investigación los autores realizaron la evaluación utilizando la herramienta MAGERIT que principalmente se utiliza para recomendar medidas para controlar los riesgos, misma que complementaron con un software denominado PILAR que realiza el análisis de los riesgos de la seguridad informática.

Otra investigación se ha efectuado por Villegas (2008) elaborado en la Universidad Simón Bolívar y que tiene como título Modelos de Madurez para la Gestión y Administración de la Seguridad Informática en las Universidades donde afirma que:

> El objetivo de esta investigación fue el de diseñar un Modelo de Madurez Organizacional con respecto a la Administración y Gestión de la Seguridad de la Información para Universidades Venezolanas ubicadas en la Región Capital. La metodología utilizada para el logro de este objetivo es una investigación de campo, de carácter explorativo; además se aplico el método Delphi para validar el modelo de madures construido a través de entrevistas realizadas a personal experto y consultores en Seguridad de la Información.(Vilegas, 2008)

En ésta investigación la autora diseño un instrumento de medición con la finalidad de determina el nivel de madurez organizacional con respecto a la administración y gestión de la seguridad de la información.

La investigación de Ramírez (2014) que su proyecto titulado *Actualización del sistema de Gestión de Seguridad de la Información de una empresa a la norma ISO/IEC 27001:2013* donde dice que "Este proyecto aborda realizar la transición del sistema de gestión de seguridad de la información de una empresa dedicada al transporte de energía basado en ISO 7IEC 27001:2005 al nuevo estándar ISO/IEC 27001:2013"(Ramirez, 2014).

CAPITULO II: DIAGNÓSTICO

2.1. Antecedentes diagnósticos

Esta investigación se realizó en el segundo semestre del año 2015 en la ciudad de Esmeraldas, en las instalaciones del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas.

Se aplicaron entrevistas a los 8 funcionarios incluyendo al director del departamento de Tecnología de Información y Comunicación, los cuales al principio de la investigación mostraron cierta incomodidad con relación a las preguntas que se les realizaba, pero mientras más se profundizaba en el tema según los dominios de la norma ISO 27001:2013, lograron entender que es necesario realizar esta evaluación para así poder determinar cuál es la realidad actual en torno a la seguridad de la información en la institución, se abarcaron así todas las áreas que conforman la dirección las cuales son: Desarrollo e Integración de Sistemas; Soporte e Infraestructura Tecnológica; Redes y Comunicaciones: y Servicios Web.

Se tomó la muestra de los 128 usuarios a quienes se les aplicó la técnica de la encuesta, los cuales mostraron apertura al realizar el proceso, de donde se pudo obtener más información.

La técnica de la observación (Ver Anexo E) y la recopilación documental son técnicas de investigación que también fueron aplicadas de manera objetiva para analizar la información seleccionada y que fue de gran validez para esta investigación.

2.2. Objetivos diagnóstico

A continuación se puntualizan los objetivos que determinaron el camino de ésta investigación:

- Conocer los procesos y procedimientos del manejo del sistema de gestión de seguridad de la información por el personal que labora en el departamento de tecnología de la información y comunicación del GADPE.

- Efectuar una valoración de la infraestructura tecnológica (hardware y software) existente en el GADPE.
- Analizar la estructura departamental de la dirección de TIC del GADPE, realizando la respectiva investigación de la segregación de funciones del talento humano que labora en dicho departamento.
- Evaluar los procesos de la dirección de TIC mediante los dominios de la norma ISO 27001:2013 que se ajustan a la realidad existente en el departamento.

2.3. VARIABLES DEL DIAGNÓSTICO

2.3.1 Procesos y Procedimientos

Esta investigación permitió conocer si los procedimientos se efectuaron de una forma eficaz y eficiente para realizar la planificación, operación y control de los procesos del SGSI del GADPE.

2.3.2. Infraestructura Tecnológica

Al realizar la respectiva evaluación de la infraestructura tecnológica se determinó cuántos y cuáles fueron los recursos de TI, en qué estado fueron colocados en producción y en qué estado se encuentran. (Ver Anexo I)

2.3.3. Estructura Departamental

Mediante ésta investigación se conoció la estructura interna de la dirección de Tic, cual es la función del talento humano que labora dentro del departamento, es decir, descubrir y evaluar los conocimientos, habilidades, destrezas y comportamientos del funcionario.

2.3.4. Dominios de la norma ISO 27001:2013

Se efectuó el análisis de los dominios con los que se procedió a evaluar el departamento de tecnologías de la información y comunicación del GADPE, apoyado en un instrumento de evaluación elaborado por la Contraloría General del Estado basado en COBIT.

2.4. INDICADORES O SUBASPECTOS

2.4.1. Tratamientos de incidentes relacionados en el marco de seguridad y privacidad de la información.- mediante la técnica de la observación (Ver Anexo E) se pudo identificar que este indicador permitió medir la eficiencia y eficacia en el tratamiento de incidentes relacionados en el marco de seguridad y privacidad de la información, ya que los incidentes fueron reportados por los usuarios del sistema.

2.4.2. Control de accesos a los equipos de cómputo y a los sistemas.- Este indicador permitió identificar la existencia de lineamientos para el control de accesos por parte del personal hacia los equipos de cómputo y a los sistemas, ya que de ésta manera se verificaría la existencia o no de algún tipo de barrera física y lógica respectivamente evitando así la intrusión de personas no autorizadas a los mismos. (Ver Anexo E)

2.4.3. Políticas confidencialidad, integridad y disponibilidad de la información.- Mediante este indicador se logró conocer la existencia de implementación de políticas de seguridad de la información en la institución.

2.4.4. Detección de anomalías en la prestación de servicios del departamento de TIC.- Mediante este indicador se determinó la existencia o no de algún mecanismo que permita detectar si hay algún tipo de irregularidad en los servicios que presta el departamento de TIC de la institución. (Ver Anexo E)

2.4.5. Porcentaje de implementación de controles.- Este indicador buscó identificar el grado de avance en la implementación de controles de seguridad en la institución. (Ver Anexo E)

2.4.6. Alcance del sistema de gestión de seguridad de la información en cuanto a activos de información.- El indicador logró determinar y realizar un seguimiento en cuanto a los activos críticos de información de la entidad y la existencia de controles aplicados para la protección de los mismos.(Ver Anexo E)

2.4.7. Identificación de activos informáticos.- Este indicador permitió la realización de inventarios de los activos informáticos para luego proceder a realizar la

respectiva clasificación del activo informático, tratamiento, características de cada activo, análisis de capacidad y desempeño con los que fueron colocados en producción y evaluación del riesgo sobre el activo. (Ver Anexo E)

2.4.8. Organización de la seguridad de la información.- El talento humano ocupa un rol muy importante dentro de la entidad, por lo que mediante este indicador se realizó un seguimiento al compromiso del departamento de TIC, en cuanto a la asignación de personas y responsabilidades en lo relacionado a la seguridad de la información al interior del GADPE. (Ver Anexo D)

2.4.9. Evaluación del desempeño del funcionario.- Mediante este indicador se logró identificar si se han efectuado las evaluaciones del desempeño del funcionario, cuáles han sido sus calificaciones y si han existido planes de mejoras en cuanto a su rendimiento en el desempeño de su cargo y el cumplimiento de sus funciones.

2.4.10. Verificación del perfil profesional del funcionario.- Buscó realizar un análisis del organigrama y de las funciones por cargo de cada trabajador del departamento de TIC. (Ver Anexo C).

2.4.11. Aplicación de dominios de la norma ISO 27001-2013.- Mediante este indicador se evaluó el sistema de gestión de seguridad de la información mediante los dominios de la norma ISO 27100-2013 que fueron aplicados.

2.5. MATRIZ DIAGNOSTICA

Esta matriz tiene como objetivo extraer información del entorno y de la institución misma, para de esta manera determinar las técnicas de investigación que se van a realizar de acuerdo al indicador y al objetivo diagnostico planteado, como también cuáles fueron las fuente de información de donde se obtuvieron los datos para realizar el análisis respectivo.

Tabla 2. Matriz Diagnóstica

Objetivos	**Variables**	**Indicadores**	**Técnicas**	**Fuente de información**
Conocer los procesos y procedimientos del manejo del sistema de gestión de seguridad de la información por el personal que labora en el departamento de tecnología de la información y comunicación del GADPE.	Procesos y Procedimientos	Tratamientos de incidentes Control de accesos Políticas Detección de anomalías % implementación de controles.	Documental Entrevista Entrevista Entrevista Encuesta	Director de TIC Responsable de la seguridad de la información Personal de TIC Usuarios
Efectuar una valoración de la infraestructura tecnológica (hardware y software) existente en el GADPE.	Infraestructura Tecnológica	Alcance del sistema de gestión de seguridad de la información Identificación de activos informáticos.	Entrevista Observación	Responsable de la infraestructura tecnológica Departamento de TIC
Analizar la estructura departamental de la dirección de TIC del GADPE, realizando la respectiva investigación de la segregación de funciones del talento humano que labora en dicho departamento.	Estructura Departamental	Perfil profesional del funcionario. Evaluación del desempeño Organización de la seguridad de la información.	Observación Entrevista Documental	Director de TIC
Evaluar los procesos de la dirección de TIC mediante los dominios de la norma ISO 27001:2013 que se ajustan a la realidad existente en el departamento.	Dominios ISO 27001-2013	Aplicación de dominios de la norma ISO 27001-2013.	Observación Documental	Departamento de Tic

2.6. MECÁNICA OPERATIVA

2.6.1. Población o Universo

Para el desarrollo de esta investigación se ha estimado una población de 200 usuarios, de los cuales 8 laboran dentro del departamento de Tecnología de Información y Comunicación a quienes se les aplicó la técnica de la entrevista; lo que significa que la población a la que se le aplicará la técnica de la encuesta, para determinar la muestra es de 192 usuarios, que están conformados por trabajadores y empleados del GADPE.

2.6.2. Muestra

Para el análisis de la información recopilada se usó las técnicas estadísticas para así visualizar cada fase e interpretar los resultados. Debido a que la población de funcionarios, es finita se utilizó la técnica del muestreo aleatorio simple sin reposición, según Warnberg (2014) cuya fórmula es la siguiente:

$$\boldsymbol{n} = \frac{Z^2 PQN}{Z^2 \mathrm{PQ} + \mathrm{Ne}^2}$$

En donde,

n =	Tamaño de la muestra	
Z=	Nivel de Confiabilidad	1.96
P=	Probabilidad de ocurrencia	0.50
Q=	Probabilidad de no ocurrencia	0.50
N =	Población	192.00
e =	Error de Muestreo	0,05

$$\boldsymbol{n} = \frac{(1.96)^2 * 0.50 * 0.50 * 192}{(1.96)^2 * 0.50 * 0.50 + 192 * (0.05)^2}$$

$$\boldsymbol{n} = \frac{184{,}39}{1.44}$$

$$\boldsymbol{n} = 128{,}01$$

Por lo tanto la muestra es de 128 personas

2.6.3. Fuente de información primaria

2.6.3.1. Observación

Se aplicó la técnica de la observación directa; ya que por medio de ella se logró determinar el desarrollo y el contexto de las actividades en la institución, si existe la aplicación de barreras, y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se observó cada uno de los departamentos de la institución para donde se logró conocer la infraestructura tecnológica que poseen. Este proceso se realizó mediante la aplicación de una ficha de observación (Ver Anexo E) para llevar constancia de lo observado en los desarrollos de las labores diarias durante el mes de Diciembre del 2015.

2.6.3.2. Encuesta

La encuesta fue la otra técnica que permitió captar la información, tabularla, graficarla y analizarla, para ello a mediados del mes de noviembre del 2016, se realizó un cuestionario con varias preguntas entre cerradas y abiertas, el cual tuvo como finalidad examinar el interés que hay en los funcionarios con la evaluación del sistema de gestión de seguridad de la información del GADPE. (Ver Anexo F).

2.6.3.3. Entrevistas

La técnica de la entrevista permitió diseñar entrevistas para captar la información de los funcionarios que trabajan en el departamento de TIC del GADPE en lo que concierne a sus responsabilidades según su cargo y qué inconvenientes han presentado con respecto a la infraestructura tecnológica, y en cuanto al desarrollo de sus actividades como departamento. Estas entrevistas se realizaron los primeros días de mes de diciembre del 2015.

2.6.3.4 Recopilación Documental

Mediante esta técnica se elaboró un marco teórico conceptual donde se logró formar un cuerpo de ideas sobre el sistema de gestión de seguridad de la información, con el propósito de elegir los instrumentos para la recopilación de información basados en fuentes de información de información confiables.

2.6.4. Fuente información secundaria

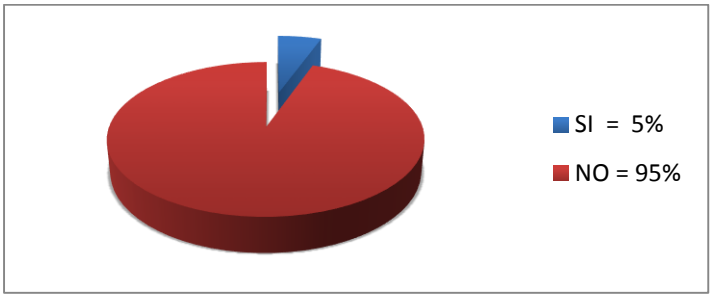
La información secundaria se recopiló a través de revistas físicas como PC World y revistas online que informan sobre la seguridad informática de las empresas y lo importante que es detectar las amenazas que inundan el sistema identificarlas es el primer paso, conocer qué y cómo ponen en riesgo la información y los procesos en las instituciones.

2.7. TABULACIÓN Y ANÁLISIS DE LA INFORMACIÓN

2.7.1. Encuesta dirigida a funcionarios del GADPE

Pregunta No.1: ¿Conoce usted si en la institución existen políticas de seguridad de la información? ¿Si su respuesta es negativa indique el porque?

Figura 2. Relación pregunta 1 para funcionarios

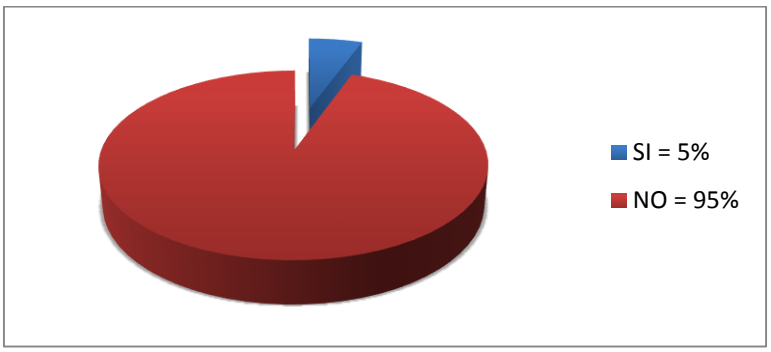


ANÁLISIS

Como se puede observar en la Figura 2 de los funcionarios que fueron encuestados, el 5% conoce que existen políticas de seguridad de la información por el contrario, el 95% tiene desconocimiento de la existencia de las mismas, según algunos señalaron la razón es que no ha existido una socialización correcta de las políticas para que todo el personal de la institución se empape del tema.

Pregunta N°2: ¿Ha recibido algún tipo de información sobre las normas y procedimientos relativos a la seguridad de la información? ¿porque?

Figura 3. Relación pregunta 2 para funcionario

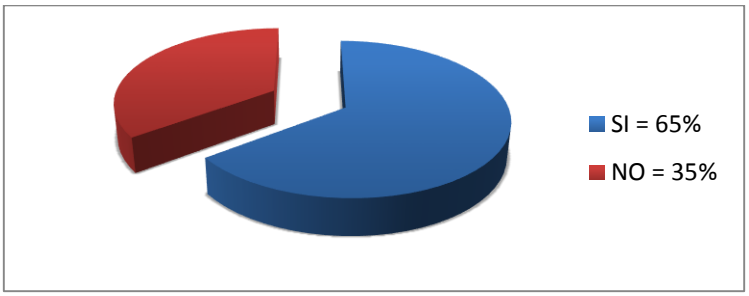


ANALISIS

En la Figura 3 se puede observar que un 95% de los encuestados no ha recibido ningun tipo de informacion de las normas y procedimientos entorno a la seguridad de la informacion, ya que los encuestados manifestaron que no existe algún tipo de mecanismo de publicación o comunicación de las mismas hacia los usuarios.

Pregunta N°3: ¿Cumple su contraseña con requisitos mínimos de seguridad como son caracteres alfanuméricos, combinados, caracteres especiales etc.? ¿Por qué?

Figura 4. Relación pregunta 3 para funcionarios

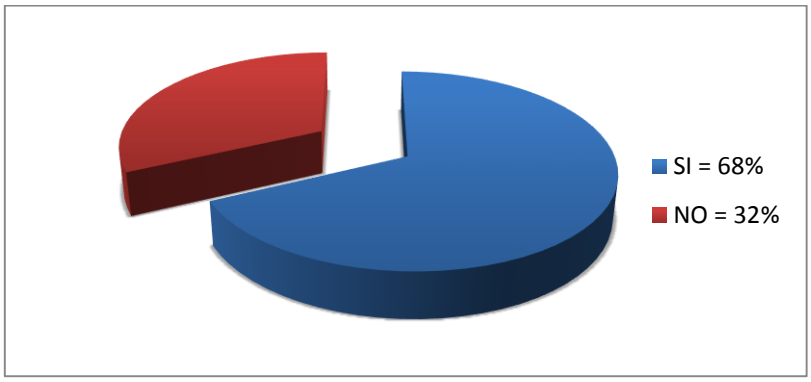


ANÁLISIS

Como se puede observar en la Figura 4 el 65% de los encuestados tiene conocimiento de la importancia te colocar una contraseña segura y la posee, según opinaron los encuestados que mientras más segura sea la contraseña más protegida se encontrará la información de las amenazas; mientras que el 35% dijeron que no utilizan contraseña con dichos requisitos mínimos indicados ya que no les parece de mayor relevancia.

Pregunta N°4: ¿Cree usted que la información dentro de la institución está segura? ¿Por qué?

Figura 5. Relación pregunta 4 para funcionarios

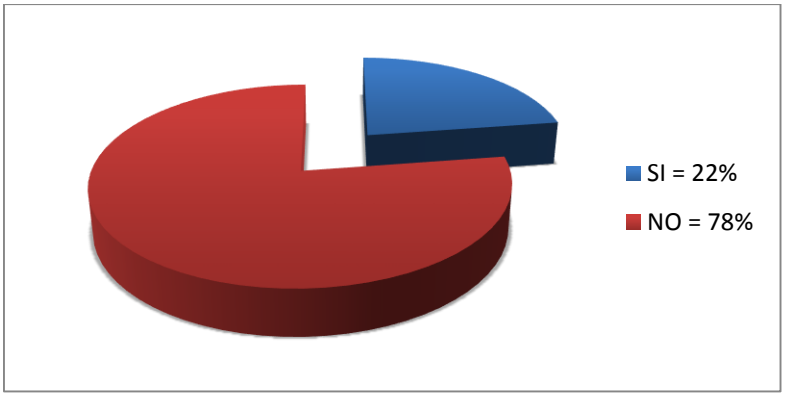


ANALISIS

En la Figura 5 se puede observar el 68% de los usuarios considera que la información se encuentra segura dentro de la institucion, ya que los funcionarios señalaron que jamás ha existido un fraude electrónico ni atentado.

Pregunta N°5: ¿Ha recibido usted algún tipo de capacitación para reconocer la criticidad de la información?

Figura 6. Relación pregunta 5 para funcionarios



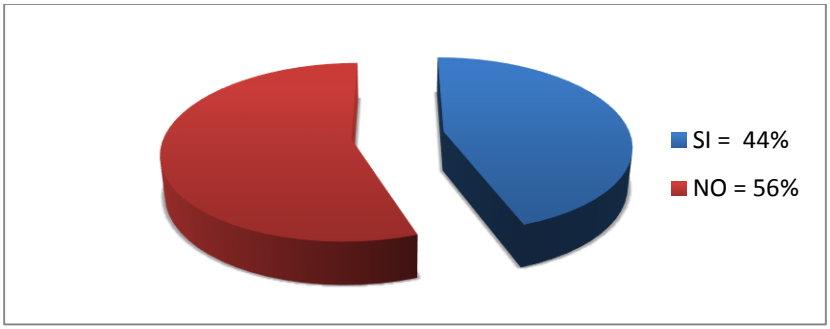
ANÁLISIS

Elaborando el análisis respectivo de la pregunta N°5 se puede evidenciar claramente que no se ha dado ningún tipo de capacitación a los usuarios, ya que el 78% de los

encuestados ha respondido que no han recibido ningún tipo de preparación para reconocer la criticidad de la información.

Pregunta N° 6: ¿Separa usted la información dependiendo de su importancia? ¿Por qué?

Figura 7. Relación pregunta 6 para funcionarios

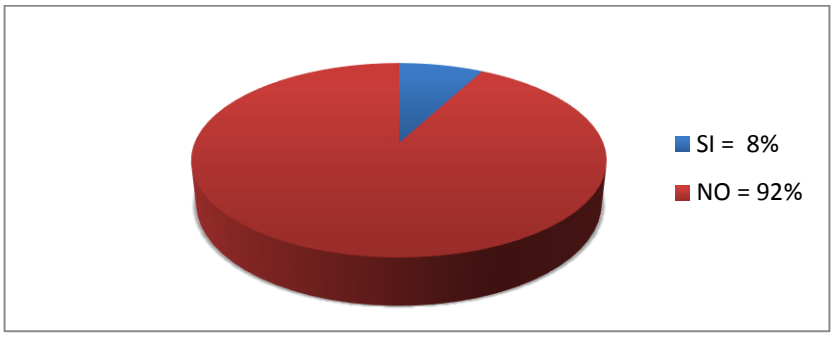


ANÁLISIS

Mediante la Figura 7 se ilustra que un 56% de los encuestados no separa la información dependiendo de su importancia ya que los mismos manifestaron que no les parece tener mayor relevancia porque ellos conocen en donde se encuentra cada información que manejan, por el contrario un 44% respondió positivamente donde indicaron que separando la información es más fácil organizar la misma.

Pregunta N° 7: ¿Se le ha hecho conocer si existe algún procedimiento o manual que ayude al manejo de la información privada o restringida? ¿Por qué?

Figura 8. Relación pregunta 7 para funcionarios



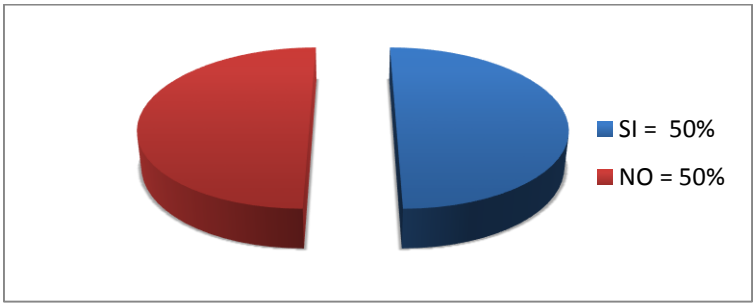
ANÁLISIS

Elaborando el respectivo análisis de la Figura 8 que corresponde a la pregunta N° 7 de la encuesta se puede evidenciar que el 75% de los encuestados responde de manera

negativa, ya que supieron indicar que no conocen sobre ningún tipo de procedimiento en que se les haya capacitado, y que no se les ha dado ningún tipo de manual en el cual ellos puedan apoyarse para el manejo de la información privada y restringida.

Pregunta N° 8: ¿Realiza respaldos de su información? ¿Por qué?

Figura 9. Relación pregunta 8 para funcionarios

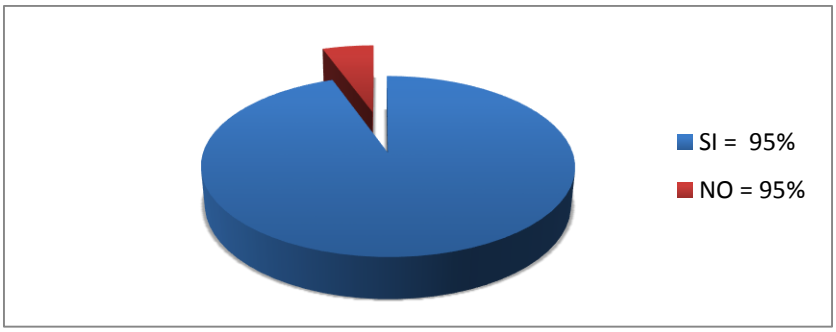


ANÁLISIS

Mediante la Figura 9 se puede evidenciar que la mitad de los usuarios realizan este proceso como señalaron que ésta es de mucho valor para la institución y para su desempeño como trabajador, la otra mitad de los encuestados no realizan respaldos de la información ya que consideran que es un proceso que le concierne netamente al departamento de TIC.

Pregunta N° 9: ¿Ha insertado un flash memory en su puesto de trabajo? ¿Para qué?

Figura 10. Relación pregunta 9 para funcionarios



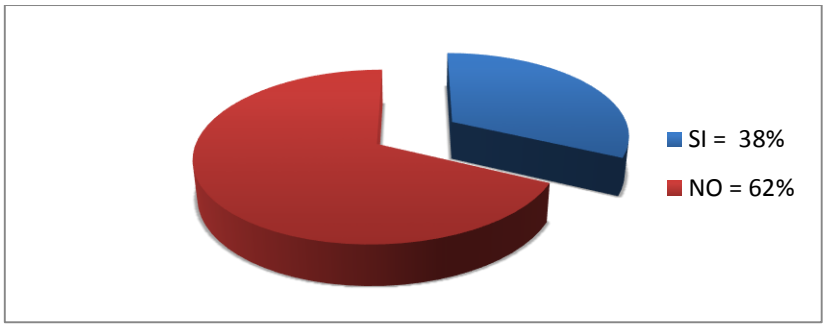
ANÁLISIS

En el Figura 10 se puede observar que un porcentaje mayoritario de un 95% ha insertado un flash memory en su ordenador, ya que supieron indicar que le es de mucha

importancia debido a que en algunos departamentos no se encuentran en buen estado las impresoras y ellos deben de trasladarse a otros departamentos para poder imprimir información inherente a su trabajo.

Pregunta N° 10: ¿Alguna vez se le ha perdido algún dispositivo de almacenamiento con información de la institución? ¿Por qué?

Figura 11. Relación pregunta 10 para funcionarios

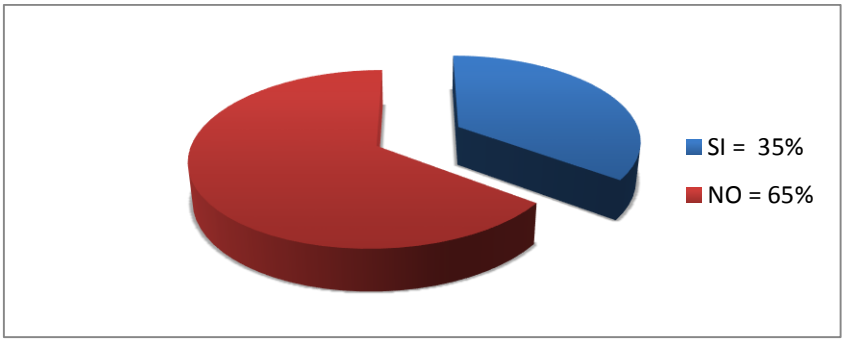


ANÁLISIS

Realizando el respectivo analisis dela Figura 11, se logra observar que el 62% de los funcionarios encuestados no ha sufrido de perdidas de informacion en dispositivos de almacenamiento, ya que manifestaron que los dispositivos de almacenamiento que contienen informacion importante de la institucion los dejan en su puesto de trabajo con las respectivas seguridades (bajo llave), por otraparte el 38% de los encuestados dijeron que se le ha perdido dispositivos de almacenamiento con informacion de la institucion porque las han trasladado fuera de la institucion, y en ese proceso se han extraviado.

Pregunta N° 11: ¿Ha instalado cualquier tipo de programa en su puesto de trabajo? ¿Por qué?

Figura 12. Relación pregunta 11 para funcionarios

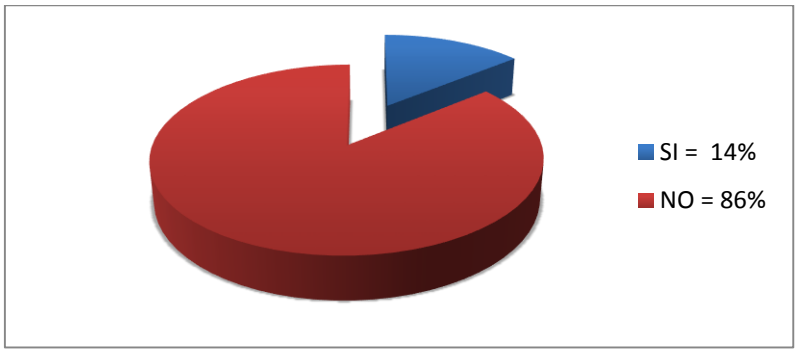


ANÁLISIS

Existe una política institucional la cual indica que no se debe instalar programas o aplicaciones en los equipos de cómputo un 35% de los encuestados que es una minoría ha hecho caso omiso a dicha política y ha procedido a instalar programas o aplicaciones en su puesto de trabajo, ya que indicaron que lo han realizo porque no les parecía que fuese de importancia la instalación de los mismos debido a que son programas inofensivos según su criterio. (Programas para bajar música, juegos, aplicaciones etc.)

Pregunta N° 12: ¿Ha tratado de ingresar a documentos o archivos y se le ha denegado el acceso? ¿Por qué?

Figura 13. Relación pregunta 12 para funcionarios

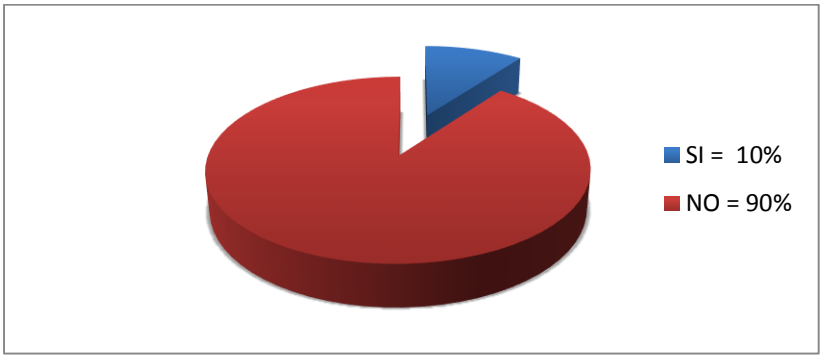


ANÁLISIS

El 86% de los encuestados indican que no han intentado ingresar a ningún tipo de documento o archivo ya que supieron indicar que no utilizan la red, ni tampoco las carpetas compartidas.

Pregunta N° 13: ¿Ha ingresado a otras cuentas de usuario? ¿Por qué?

Figura 14. Relación pregunta 13 para funcionarios

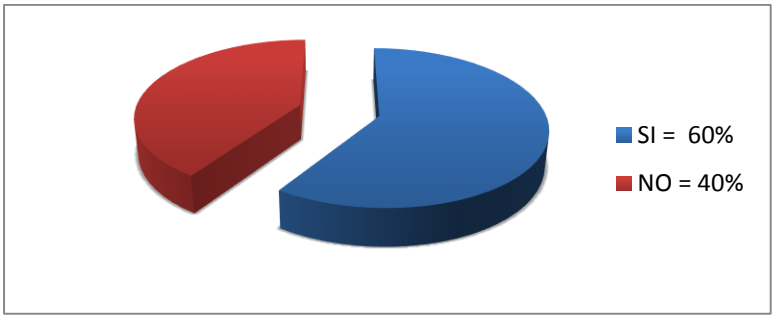


ANÁLISIS

En la Figura 14 se logra observar que los funcionarios en su gran mayoría responde de forma negativa ya que el 90% de ellos ha respondido que no ha ingresado a otras cuentas de usuario porque señalaron que cada funcionario posee su nombre de usuario y su respectiva contraseña, para acceder tanto a aplicaciones, sistemas, y sistemas operativos.

Pregunta N° 14: ¿Se le ha hecho firmar algún acuerdo de confidencialidad en la institución?

Figura 15. Relación pregunta 14 para funcionarios

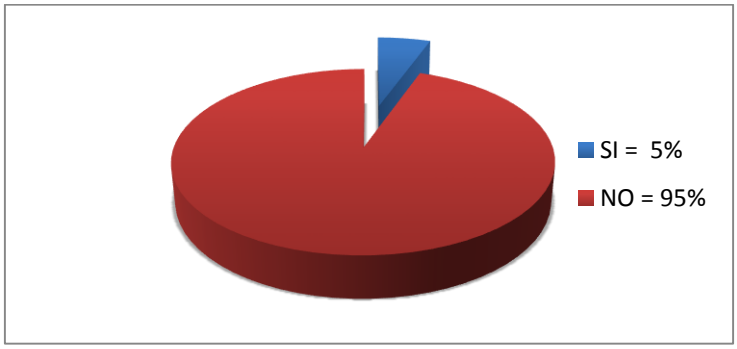


ANÁLISIS

Al observar la Figura 15 el 60% de los funcionarios asegura haber firmado un acuerdo de confidencialidad de la información, ya indicaron tener conocimientos de estos acuerdos en donde se comparte información pero se restringe su uso público.

Pregunta N° 15: ¿Se le ha comunicado de las vulnerabilidades observadas o sospechadas en la institución? ¿Por qué?

Figura 16. Relación pregunta 15 para funcionarios

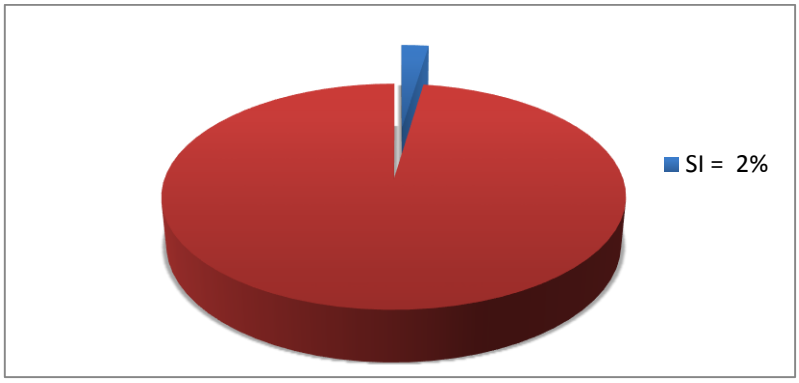


ANÁLISIS

Como se puede observar en la Figura 16 el 95% de los encuestados indicaron que las vulnerabilidades de la institución se mantienen en total reserva ya que los funcionarios desconocen de las mismas, no han recibido ningún tipo de comunicación sobre este tema.

Pregunta N° 16: ¿Se le ha comunicado que bajo ningún motivo usted debe probar estas vulnerabilidades? ¿Por qué?

Figura 17. Relación pregunta 16 para funcionarios

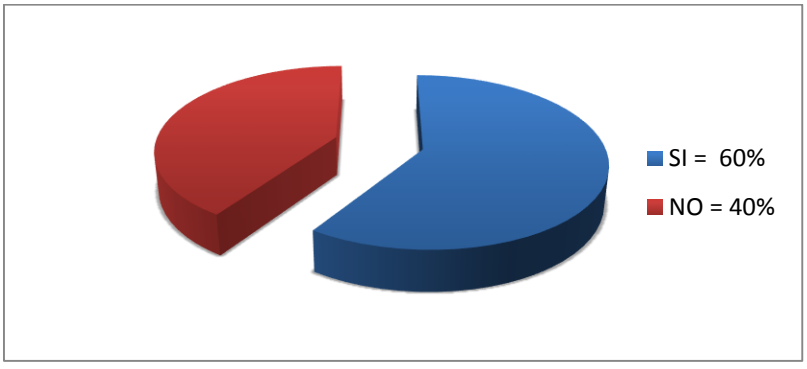


ANÁLISIS

El 98% de los encuestados como se observa en la Figura 17 desconocen de las vulnerabilidades lo que supieron indicar es no se le han comunicado de las mismas por lo tanto no pueden ser probadas.

Pregunta N° 17: ¿Cuándo se instala un nuevo programa lo capacitan para el manejo del mismo? ¿Por qué?

Figura 18. Relación pregunta 17 para funcionarios

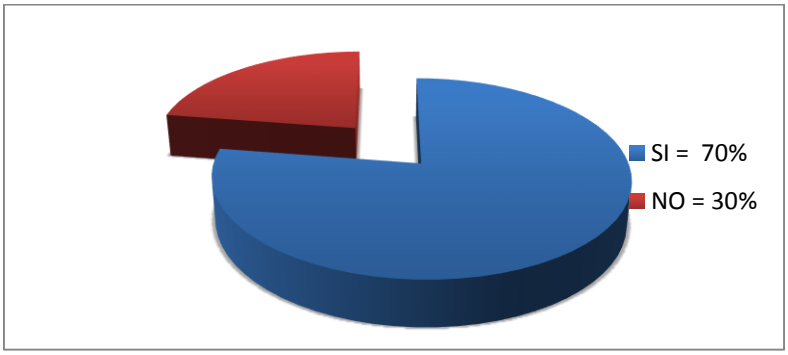


ANÁLISIS

En la Figura 18 se puede evidenciar que un 60% de los usuarios han sido capacitados cuando se ha instalado un nuevo programa por lo que ellos mismos manifestaron.

Pregunta N° 18: ¿Se le ha instalado algún antivirus en su estación de trabajo?

Figura 19. Relación pregunta 18 para funcionarios

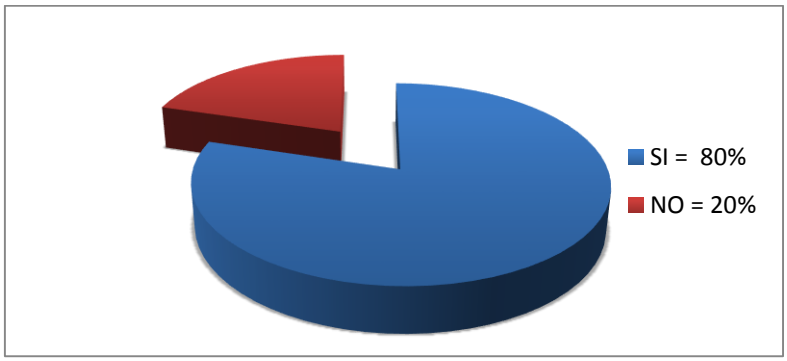


ANÁLISIS

Realizando el respectivo análisis de la Figura 19 el 70% de los funcionarios ha manifestado que se le ha instalado el antivirus y se les ha indicado que se debe estar alerta para saber si está realizando las funciones que se le han encomendado.

Pregunta N° 19: ¿Ha notificado al departamento de TIC por algún mensaje de error de alguna aplicación en su computador? ¿Por qué?

Figura 20. Relación pregunta 19 para funcionarios



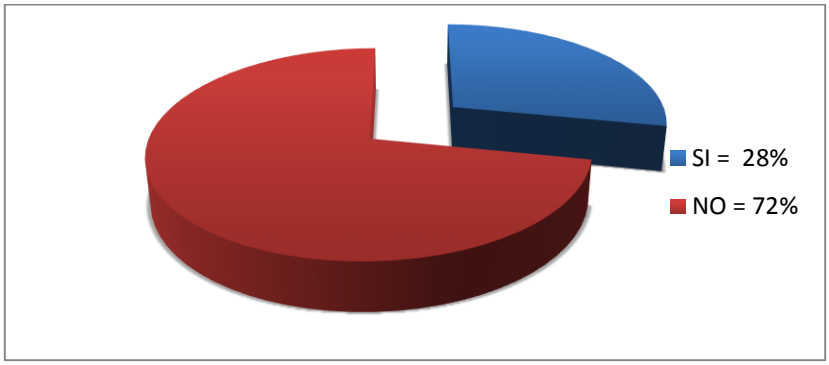
ANÁLISIS

Al realizar el respectivo análisis a la pregunta N° 19 se puede denotar en la Figura 20 que los funcionarios en un 80% comunican de los errores que se le presentan en alguna

aplicación al departamento de Tic ya que indicaron que les da un poco de temor que se les puedan borrar archivos importantes de la computadora.

Pregunta N° 20: ¿Ha encontrado archivos o información en su computador que no correspondan a su puesto de trabajo?

Figura 21. Relación pregunta 20 para funcionarios



ANÁLISIS

En la Figura 24 se puede observar que un 72% de las personas encuestadas no ha encontrado información que no pertenezca a las funciones que desempeña dentro de la institución ya que nos supieron indicar que se han dado cuenta que se realiza mantenimiento preventivo y correctivo a las maquinas.

2.7.2. Análisis de la entrevista realizada al Director de Tecnologías de Información y Comunicación

Realizando el respectivo análisis a dicha entrevista donde se hace referencia específicamente a seis dominios y controles con sus respectivos objetivos de control se recopiló la información que se presenta en el Anexo G.

Se pudo conocer que existen políticas de seguridad de la información en el GADPE, pero dichas políticas no han sido socializadas con el personal que ahí labora son conocidas por el personal del departamento de TIC; algunas se encuentran debidamente documentadas pero existen otras que se encuentran determinadas de manera informal. No hay un responsable de documentar dichas políticas ni de realizar la debida actualización de las mismas cuando es necesario, por lo que tampoco se realizan

controles periódico para verificar el cumplimiento de las mismas. La segregación de funcionarios del departamento de TIC se encuentra perfectamente definida. Por otra parte el acceso de los usuarios al sistema está debidamente validado y cada acceso queda registrado en el sistema. En otro ámbito cuando ocurre algún tipo de incidente el usuario se comunica de inmediato con el departamento de TIC, se le da solución al mismo y se realiza un reporte del evento que se ha presentado. En cuanto a la gestión de continuidad del negocio no se han elaborado planes de contingencias, ya que no tiene una política definida para esto ni se ha realizado un análisis de impacto en caso de ocurrencia de una crisis.

2.7.3. Análisis de la entrevista realizada al Analista de Desarrollo e Integración de Aplicaciones

En esta entrevista se pudo determinar que para realizar una adquisición de software se consideran requerimientos básicos así como también para desarrollar los mismos, pero la entidad no cuenta con una política determinada para ello, se realiza la revisión técnica pero no hay un manual o guía para realizar este procedimiento. Existen procedimientos para la etapa de análisis que determina la especificación de los requisitos de seguridad de los sistemas de información. Por otra parte no se cuenta con algún programa para proteger los datos que utilizan para pruebas en los sistemas de información.

2.7.4. Análisis de la entrevista realizada al Asistente de Desarrollo e Integración de Aplicaciones

Elaborando el respectivo análisis a esta entrevista se pudo denotar que existe un inventario físico y digital de los activos informáticos que posee la institución mismo que se actualiza de acuerdo a la adquisición que se realice; estos activos informáticos son asignados a un propietario mismo que es responsable del uso y abuso del mismo. Así mismo poseen procedimientos para el clasificado de la información pero no tiene una guía para el manejo de activos. Por otra parte para el manejo de medios removibles se documenta la asignación de este medio físico pero cuando se realiza una transferencia esta no es documentada. En cuanto a los recursos humanos se pudo denotar que sus funciones y responsabilidades se encuentran claramente definidas en contrato de

trabajo, pero no se efectúan capacitaciones constantes a los funcionarios en cuanto a las medidas de seguridad que se deben tomar en cuanto a la información que manejan.

2.7.5. Análisis de la entrevista realizada al Analista de Soporte e Infraestructura Tecnológica.

Al realizar el análisis a esta entrevista se pudo denotar que la mitad de los procedimientos operacionales en el sistema informático de la institución se documentan, los otros son realizados de manera empírica sin elaborar un informe de los mismos, la infraestructura tecnológica es controlada periódicamente. Existen controles contra códigos maliciosos de prevención y detección debido al antivirus que se encuentra instalado en los equipos informáticos mismo que se encuentra dentro de una consola de administración principal que se actualiza en cascada, es decir no se actualiza en los computadores mediante el internet, este antivirus demuestra un alto nivel de usabilidad y gran efectividad mantiene protegido los equipos contra virus. Las copias de respaldo se realizan periódicamente pero no hay un manual para realizar este procedimiento, el mismo depende del criterio del técnico. Existe una política que no permite la instalación de software en los sistemas operativos pero muchas veces no es cumplida. Se lleva un registro técnico de las vulnerabilidades que presenta el sistema, pero no se han efectuado ningún tipo de auditoría a los sistemas de información.

2.7.6. Análisis de la entrevista realizada al Asistente de Soporte e Infraestructura Tecnológica

Realizando el respectivo análisis a dicha entrevista donde se hace referencia a la seguridad física y del entorno se logró denotar que las barreras físicas para el acceso a las áreas restringidas son aplicadas, existe servicio de guardianía y se procede al registro en bitácoras el acceso de alguien ajeno a la institución, así mismo el acceso de los empleados es registrado en el reloj biométrico, aunque no existe mayor control en el acceso físico a los departamentos. Por otra lado los equipos informáticos se encuentran en áreas seguras protegidas contra el acceso no autorizado, se realiza un mantenimiento periódico a los equipos informáticos, mismos que se encuentran protegidos contra fallas de energía y control térmico y también cuentan con una política de escritorio limpio y pantalla limpia.

2.7.7. Análisis de la entrevista realizada al Analista de Redes y Comunicaciones.

Después de elaborar el análisis a esta entrevista se ha llegado a la conclusión que no tiene una política documentada para la gestión de seguridad de la redes, la misma es de carácter informal, las características de la red se encuentran debidamente definidas, pero no poseen un plan que indique cual es el control que se debe realizar en las redes.
No tiene un manual para realizar el procedimiento de la transferencia de la información, pero se han firmado acuerdos de confidencialidad de la información mismos que son actualizados según sea el caso.

2.7.8. Análisis de la entrevista realizada al Asistente de Redes y Comunicaciones.

Realizando el respectivo análisis a dicha entrevista donde se hace referencia a los requisitos del negocio se pudo obtener información de que hay una política de control de acceso a las redes, solo algunos empleados dependiendo de sus funciones pueden acceder a ella. El acceso de los usuarios a la red se encuentra registrado, así mismo cuando un usuario cambia de funciones también se realiza el cambio en sus privilegios dentro del sistema, la autenticación secreta de los usuarios se efectúa pero no tiene una documentación de este proceso. Los usuarios poseen claves seguras mismas que son cambiadas periódicamente, el acceso seguro de los usuarios al sistema es controlado y queda registrado en el sistema cada accedo. En cuanto a los programas utilitarios se lleva un control de cuantos son pero no en que puestos de trabajo han sido instalados.

2.7.9. Análisis de la entrevista realizada al Analista de Proyectos y Servicios Web.

Realizando el respectivo análisis a dicha entrevista a la analista de Proyectos y Servicios Web donde se establece como una de sus funciones el proveer servicios de internet, intranet, correo electrónico y sitio web de la entidad, a base de las disposiciones legales, normativas y los requerimientos de los usuarios internos y externos definió que se elaboran normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio web de la

entidad. Mientras que también se logra administrar y hacer seguimiento de los proyectos informáticos que ejecuten las áreas técnicas que conforman la Dirección. Adicionalmente realiza la administración de los usuarios de la intranet, internet y correo electrónico garantizando el acceso del usuario a los recursos informáticos compartido o a otra máquina de la red, a través del uso de un servidor de dominio, controlando el correcto funcionamiento de los servidores que están bajo la administración de la unidad.

2.7.10. Análisis de la entrevista realizada al Asistente de Proyectos y Servicios Web.

Realizando el respectivo análisis a la entrevista al asistente de Proyectos y Servicios Web se resume que dentro de sus funciones está la de mantener la página web institucional actualizada y funcional, que permita la publicación de contenidos de todas las unidades usuarias de la institución de manera ágil, segura, y oportuna, cumpliendo con las normas establecidas por la Ley de Transparencia, mediante la actualización y disponibilidad permanente hacia el público en general y autoridades pertinentes, desarrollando entornos que interactúen como enlaces a la Intranet local u otros servicios de manera segura documentando cada procesos e incluyendo programación personalizada.

2.8. FODA

2.8.1. Fortalezas

F1. Excelente infraestructura informática.
F2. Soporte a los usuarios del sistema.
F3. Segregación de funciones bien definidas.
F4. Apoyo por parte de la máxima autoridad a los proyectos del departamento.

2.8.2. Debilidades

D1. Falta de capacitación a los usuarios en cuanto a la seguridad de la información.
D2. Insuficiencia de políticas de seguridad de la información que regulen las actividades con tecnología de información y comunicación.

D3. Carencia de un responsable que se encargue de verificar si las normas son cumplidas.

D4. Poca comunicación con los distintos departamentos.

2.8.3. Oportunidades

O1. La existencia de varias normas o estándares certificados y reconocidos a nivel mundial, que pueden ser aplicadas en la institución para asegurar el buen funcionamiento del Sistema de Gestión de Seguridad de la Información.

O2. Conocimiento de herramientas que se encargan a la evaluación y seguimiento de los procesos de la institución con la finalidad de establecer y fortalecer un buen SGSI.

O3. Aplicación normas a nivel nacional como es la 410-01 de la Contraloría General del Estado que ayudan al crecimiento de la organización en cuanto a la seguridad de la información.

2.8.4. Amenazas

A1. Riesgo de robo, daño o corrupción de la información.

A2. Accesos no autorizados físicos y lógicos.

A3. Robo de equipos informáticos.

A4. Paralización de las actividades de la institución.

A5. Siniestros naturales.

2.9. ESTRATEGIAS FA, FO, DO, DA

Tabla 3. Estrategias FO, FA DO, DA.

	FORTALEZAS	**DEBILIDADES**
OPORTUNIDADES	Administrar la seguridad de la información dentro de la institución estableciendo un marco referencial para iniciar y controlar la implementación de políticas de seguridad de la información para la distribución de funciones y responsabilidades en los funcionarios, mediante la evaluación y seguimiento de los procesos. (F4, F3, O2, O1).	Definir un responsable de verificar el cumplimiento de las políticas de seguridad de la información, aprobando y acordando metodologías para procesos específicos, manteniendo la confidencialidad, disponibilidad e integridad de la información.(O3, D3, D4)
AMENAZAS	Garantizar la aplicación de barreras de seguridad adecuadas, tanto física como lógica, para evitar el acceso no autorizado de terceros a los activos informáticos de la institución. (F1,A3, A2, A5)	Coordinar la capacitación que se les dé a los funcionarios sobre la importancia de la seguridad de la información, verificando el fiel cumplimiento de las políticas de seguridad para el eficiente servicio del GADPE a la colectividad. (D1,D2, A4)

2.10. DETERMINACIÓN DEL PROBLEMA DIAGNOSTICO

Analizando las encuestas, las entrevistas, y las fichas de observación se logró detectar que los funcionarios del GADPE no se encuentran al tanto de las políticas de seguridad de la información, debido a que algunas no se encuentran bien definidas, y otras no se encuentran elaboradas, muchos de los procedimientos que se realizan, se los hace de forma empírica, y este es uno de los problemas que entre otros problemas diagnósticos se producen por varias causas.

La concientización y capacitación a los funcionarios en cuanto al tratamiento que se le debe dar a la información dependiendo de su criticidad es casi nula según los datos estadísticos que arrojo el instrumento de evaluación; es importante recalcar que la capacitación y la concientización sobre el manejo de la información a los empleados es

de vital importancia para el buen desempeño de la organización, misma que debe ser constante y expresarlas de forma clara y concisa.

Se pudo identificar que la documentación de políticas y procedimientos para la seguridad de la información no ha sido elaborada en su mayoría. Muchos de los controles que se realizan no son debidamente documentados; ya esto es de gran relevancia para el departamento de TIC porque se debería llevar un registro de los incidentes que se han presentado, como se ha solucionado y cuál ha sido el control implementado para el mismo, lo cual haría entrar a la institución en un proceso continuo de revisión y mejora del sistema.

CAPITULO III: RESULTADOS DE LA EVALUACIÓN REALIZADA AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL GADPE.

3.1. INTRODUCCIÓN

La Evaluación del Sistema de Gestión de Seguridad de la Información del Gobierno Autónomo Descentralizado de la provincia de Esmeraldas, aplicando la norma estándar ISO 27001:2013, apoyada en un instrumento de evaluación basado en COBIT (Ver Anexo H).

El objetivo principal de este informe técnico es lograr evidenciar las necesidades puntuales que presenta la institución acerca del sistema de gestión de seguridad de la información, por lo cual mediante el análisis del mismo se logró de manera concreta puntualizar la situación en la que se encuentra la institución, los riesgos que mantiene y por ultimo elaborar las respectivas recomendaciones que permitan resguardar y proteger los activos informáticos de la organización.

Después de realizar el debido análisis en el capítulo 1 (Tabla 1), sobre las funciones de cada uno de los estándares utilizados a nivel mundial, para aplicación de buenas prácticas de TI, se decidió tomar como referencia la norma ISO 27001:2013 ya que es la que más se ajusta a la naturaleza de esta investigación, y también por motivos de vigencia tecnológica. Así mismo para elaborar el instrumento de evaluación se escogió al estándar COBIT ya que se encuentra dirigida al control supervisión de Tecnología de Información.

Este estándar está compuesto por catorce dominios, cada dominio o sección principal se divide en objetivos de control, los cuales se dividen en controles para la gestión de seguridad de la información, mismos que se cuantifican de manera ponderada sobre cien, lo que permitió elaborar las recomendaciones que aquí se presentan. (Ver Anexo C).

Es de suma importancia elaborar un análisis exhaustivo de la situación actual de institución, y los riesgos a los que se enfrentan, para que sean entendidos y asimilados

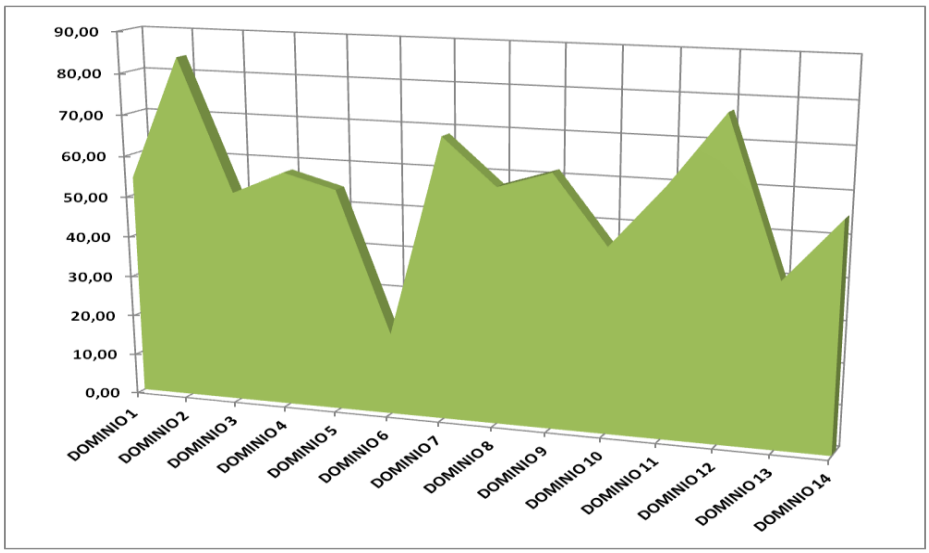
por la institución y sus actores. Así mismo tomar en cuenta las recomendaciones que se realizan las cuales mitigarían los riesgos de daño y asegurarían el cumplimiento de manera eficiente de los objetivos que percibe la entidad pública.

3.2. RESULTADOS DE LA EVALUACIÓN

Tabla 4. Resumen de la Evaluación al SGSI

RESUMEN DE EVALUACIÓN DE RIESGO Y CONFIANZA DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION DEL GADPE		
Norma	**Confianza**	**Nivel de riesgo**
Dominio 1	54,29	Moderado
Dominio 2	84,00	Bajo
Dominio 3	52,00	Moderado
Dominio 4	57,71	Moderado
Dominio 5	54,31	Moderado
Dominio 6	20,00	Alto
Dominio 7	68,45	Moderado
Dominio 8	57,38	Moderado
Dominio 9	61,50	Moderado
Dominio 10	45,09	Alto
Dominio 11	60,00	Moderado
Dominio 12	77,14	Bajo
Dominio 13	40,00	Alto
Dominio 14	55,00	Moderado
Nivel de confianza	**56,21**	**Moderado**

Figura 22. Resultado de la evaluación al SGSI del GADPE



3.3. Propuesta para el SGSI por Dominio

1) Dominio: Política de Seguridad de la Información

Controles

- Orientación de la dirección para la gestión de la seguridad de la información.

Situación

- Falta de documentación de políticas de seguridad de la información.
- No existen normativas, procedimientos y controles de las políticas.
- No hay un responsable que se encargue de elaborar las políticas y realizar el respectivo control para hacer que se cumplan en la Prefectura de Esmeraldas.
- De las políticas que se han efectuado no se ha hecho socialización de las mismas al personal que labora en la institución.

Riesgos

- Existe un riesgo evidente frente a las amenazas antes descritas al no tener debidamente documentadas las políticas de seguridad.

Recomendaciones

- Todas las políticas de seguridad de la información una vez desarrolladas deben ser aprobadas por la máxima autoridad del GADPE.
- Se debe realizar una socialización de las políticas de seguridad de la información con los funcionarios del GADPE, de una forma interactiva para llegar a la comprensión de las mismas.
- Concientizar a los usuarios que manejan información, cualquiera que sea su nivel de criticidad, sobre la importancia de cumplir las políticas.
- Conseguir que los funcionarios del GADPE cumplan las políticas de seguridad de la información.
- Realizar los respectivos controles para verificar que se estén cumpliendo las políticas.
- Realizar las respectivas actualizaciones de las políticas.
- Suprimir dichas políticas si ya han quedado en desuso.

2) Dominio: Organización de la seguridad de la información

Controles

- Organización interna.

- Dispositivos móviles y teletrabajo.

Situación

- De acuerdo con la documentación revisada que se encuentra debidamente anexada en este trabajo de investigación (Ver Anexo C) se pudo verificar que existen roles y responsabilidades bien definidos para las personas que trabajan en el departamento de TIC de la prefectura.
- Existe una segregación de funciones de los empleados, de acuerdo con la información verificada.
- El contacto con las autoridades se lo realiza de manera formal.
- El contacto con grupo de interés es de manera informal.
- No tienen una estructura determinada para la gestión de seguridad de la información en cuanto a proyectos de acuerdo con las observaciones realizadas.
- No tienen políticas documentadas.

Riesgos

- La política del acceso con dispositivos móviles al no encontrarse documentada ni socializada con los usuarios del GADPE, percibe un gran riesgo debido a que el usuario podría atentar ya sea accidentalmente o deliberadamente contra el sistema de información mediante códigos móviles maliciosos, ya que podría haber la descarga de virus que cesarían el funcionamiento del sistema de información.
- Al no existir un contacto de manera formal con estos grupos de interés especial, el GADPE se arriesga frente a cualquier amenaza, al no poseer la documentación correspondiente de los temas que se han tratado con dichos grupos, ya que no existe un plan definido para cada área de contacto. En cuanto a los proyectos que se elaboran dentro de la institución al no tener una estructura determinada los proyectos no tienen procedimientos definidos a seguir.

Recomendaciones

- Se debe continuar con las reuniones formales con los organismos reguladores del GADPE y proponer nuevos planes para implementarse en torno a la seguridad de la información.

- Los contactos con el grupo de interés especial debe ser de carácter formal, ya que las políticas de seguridad de la información tienen un ciclo de vida y en su fase de implementación implica la comunicación de las mismas, es importante llevar a cabo estas reuniones para que cada jefe de área ponga énfasis en sus grupo de trabajo de cómo debe de ser el tratamiento de la información que manejan en el GADPE.
- Se debe nombrar a un responsable de elaborar, actualizar, controlar, y verificar que sean cumplidas las políticas de seguridad de la información en GADPE.
- Las responsabilidades en torno a la seguridad de la información, de cada funcionario que labora dentro del departamento de TIC, deben ser medibles y gestionables.

3) Dominio: Seguridad de los recursos humanos.

Controles

- Antes de asumir el empleo.
- Durante la ejecución del empleo.
- Terminación y cambio de empleo.

Situación

- No se da mucha relevancia a la seguridad de la información en la fase de selección del personal.
- No se han realizado capacitaciones al personal que labora en el GADPE en cuanto a seguridad de la información.
- Existe un reglamento interno donde se indican las sanciones disciplinarias que se aplicarán en caso de que el funcionario incurra en una falta.
- No existe un precedente de que se haya aplicado una sanción disciplinaria a funcionarios del GADPE que hayan incurrido en algún evento donde se haya visto comprometida la disponibilidad, integridad y confidencialidad de la información.

Riesgos

- La falta de capacitación al recurso humano en cuanto a la seguridad de la información puede conllevar al fracaso de los proyectos de la institución.
- Robo, pérdida y fuga de la información.

- Corrupción de los datos.
- Falta de disponibilidad de la información.

Recomendaciones

- Establecer responsabilidades de seguridad de la información a todos los usuarios que manejan los sistemas de información.
- Realizar capacitaciones y concienciaciones permanentes a los usuarios del sistema y a las personas que se van a contratar en temas de seguridad de la información.
- Llevar un registro tanto físico como digital de las bajas que se dan a los usuarios en el sistema y los cambios de privilegios que se hacen a los funcionarios del GADPE que adquieren nuevas responsabilidades en su cargo.

4) Dominio: Gestión de activos

Controles

- Responsabilidad por los activos.
- Clasificación de la información.
- Manejo de medios.

Situación

- Poseen inventario físico y digital actualizado de las adquisiciones que se realizan en cuanto a infraestructura de TI.
- La concesión de los activos informáticos se encuentran debidamente documentados y registrados así como también la devolución del mismo.
- La clasificación de la información se realiza según las necesidades de la institución no así el etiquetado de la misma que es realizada de manera empírica.
- No existe estandarización, ni procedimiento documentados para el tratamiento de los medios removibles.

Riesgos

- Se puede ver comprometida la información ya que no se le da un tratamiento adecuado a los medios removibles.
- Extracción, modificación o pérdida de información confidencial.

- Accesos no autorizados a la información crítica o sensible que contenga el medio removible.
- Extravío de los medios removibles.
- No se lleva un registro de equipos ajenos al GADPE que ingresan a la institución.

Recomendaciones

- Se debe llevar un control de autorización y supervisión del responsable del activo fuera del horario normal de labores del GADPE.
- Deben existir normas y procedimientos específicos documentados en cuanto a la clasificación y etiquetado de la información.
- Los medios removibles deben encontrarse almacenados en un ambiente limpio, seguro y resguardado según la clasificación de la información.
- Se deberá aplicar un borrado seguro a los medios removibles que serán reutilizados.
- Si una información crítica o sensible de la institución tiene un tiempo de duración mayor al tiempo de vida del medio en donde se encuentra almacenada, deberá ser respaldada en otro medio para evitar la pérdida de la misma.
- El usuario debe darle el uso más correcto al medio removible e informar al departamento de TIC sobre cualquier deterioro del mismo.

5) Dominio: Control de acceso.

Controles

- Requisitos del negocio para control de acceso.
- Gestión de acceso de usuarios.
- Responsabilidades de los usuarios.
- Control de acceso a sistemas y aplicaciones.

Situación

- Políticas de control de acceso no socializadas.
- Falta de manual de procedimientos para el registro y cancelación de usuarios.
- No hay evidencia física de los procedimientos para la gestión de acceso a los usuarios.

- Política interna no documentada de la responsabilidad de cada usuario.
- Controles de accesos fallidos y exitosos de los usuarios mediante un registro.
- Actualización periódica de las contraseñas.
- Contraseñas con buena encriptación.
- Control informal del acceso a programas utilitarios.

Riesgos

- Accesos no autorizados.
- Corrupción de la información.
- Pérdida total o parcial de la información.
- Posibles amenazas que puedan llevarse a cabo y no poseer procedimientos de respuesta ante dicho evento.
- Descargas de virus en equipos informáticos.

Recomendaciones

- Designar a un responsable que verifique que se cumplan las políticas de seguridad de la información en el GADPE.
- Socializar y verificar que se cumplan las políticas de control de accesos.
- Documentar las políticas de gestión de accesos de usuarios del sistema de información.
- Verificar periódicamente los derechos de accesos de los usuarios y notificarle por escrito de los mismos.
- Documentar la cancelación y otorgamiento de nuevos privilegios asignados a los funcionarios con nuevos roles y responsabilidades, y comunicar a los mismos por escrito.
- Los puestos de diagnostico remoto deben encontrarse debidamente protegidos.

6) Dominio: Criptografía

Controles

- Controles criptográficos.

Situación

- No existen controles criptográficos.
- No hay ninguna documentación sobre políticas de controles criptográficos.

Riesgos

- Se puede comprometer información personal o de la institución.
- Daño total o parcial de los sistemas de información.
- Pérdida total o parcial de la información sensible de la organización.

Recomendaciones

- Investigar sobre técnicas criptográficas para el desarrollo de políticas sobre controles criptográficos.
- Elaborar políticas para el uso de controles criptográficos en el GADPE.
- Documentar dichas políticas y hacer la respectiva socialización de las mismas.
- Se debe establecer una gestión de claves criptográficas acorde con las técnicas investigadas.

7) Dominio: Seguridad física y del entorno

Controles

- Áreas seguras.
- Equipos.

Situación

- Existe un perímetro de seguridad física definido para la infraestructura tecnológica para los accesos físicos.
- Existen guardias de seguridad contratados 24/7.
- Se realiza un control de los equipos que entran y salen de la institución.
- No existe mayor control de acceso a los equipos informáticos en los departamentos del GADPE.
- No existe mayor protección para los equipos contra las amenazas ambientales.
- No existen políticas definidas para el trabajo en áreas seguras.
- No existe normativa para el uso de equipos informáticos fuera de la institución.
- Existe un buen suministro eléctrico y cableado estructurado.
- Hay una política de escritorio limpio e imagen corporativa del GADPE en la pantalla.

Riesgos

- Ingreso no autorizado al centro de procesamiento de datos.
- Daños e intrusiones en las instalaciones de la institución.
- Intercepciones o daños en el cableado estructurado.
- Pérdida o robo de equipos informáticos.
- Pérdida total o parcial por amenazas climatológicas.

Recomendaciones

- Poseer sistemas de seguridad que rijan a la institución contra intrusos y amenazas ambientales.
- Elaborar un plan de contingencia para ejecutarlo en caso de que se presenten incidentes que afecten a la infraestructura tecnológica, y por ende paralicen las actividades de la institución.
- Desarrollar políticas para el trabajo en áreas seguras y socializarlo con los funcionarios del GADPE
- Documentar las políticas de disposición segura y reutilización de equipos.

8) Dominio: Seguridad de las operaciones

Controles

- Procedimientos operacionales y responsabilidades.
- Protección contra códigos maliciosos.
- Copias de respaldo.
- Registro y seguimiento.
- Control de software operacional.
- Gestión de la vulnerabilidad técnica.
- Consideraciones sobre auditorias de sistemas de información.

Situación

- Existe parcialmente documentación sobre los procedimientos de operación.
- Se realiza el debido proceso de gestión de cambios.
- Se controla de manera constante el rendimiento de la infraestructura tecnológica del GADPE.
- No existen planes para la gestión de capacidad.

- Existe el debido control contra código malicioso mediante el antivirus ESET.
- No existe una política definida para sacar las copias de respaldo.
- No hay un control en cuanto a la sincronización de relojes.
- Se controlan periódicamente los registros de evento, del administrador y operador.
- Desarrollar y documentar la gestión de vulnerabilidades técnicas.
- No existe ningún tipo de control de auditoría de sistemas de información.

Riesgos

- El funcionamiento de los sistemas críticos del GADPE podrían verse afectados.
- Mal uso del sistema de información.
- Ejecución de códigos móviles que puedan alterar las actividades diarias de la institución.
- Uso deliberado de la información.

Recomendaciones

- Documentar todos los procedimientos operativos de la institución.
- Implementar medidas de seguridad para preservar la confidencialidad, integridad y disponibilidad de la información.
- Realizar seguimiento constante de las actualizaciones y parches que son instalados en los equipos informáticos del GADPE.
- Realizar el debido control sobre las actualizaciones de software y hardware.
- Evaluar el impacto potencial del cambio en cuanto a servicios e integridad de los datos.
- Elaborar planes para gestionar la capacidad de las operaciones.

9) Dominio: Seguridad de las comunicaciones.

Controles

- Gestión de la seguridad de las redes.
- Transferencia de información.

Situación

- No existe un plan detallado de cómo se debe controlar y gestionar las redes, del GAPDE, solo existe la evidencia de la impresión de un informe.
- Se realizan los controles debidos a los servicios de red.
- No existe una política para la separación de las redes.
- No existen políticas sobre transferencia de información se lo realiza mediante un procedimiento informal.
- No existe evidencia sobre acuerdos de transferencia de la información entre la institución y partes externas.
- Si tienen control sobre la mensajería electrónica.
- Existen acuerdos de confidencialidad de la información los cuales son revisados periódicamente, y actualizados si es necesario.

Riesgos

- Daños en las redes de la institución.
- Pérdida total o parcial de la información.
- Corrupción de la información.
- Cese de funciones de la institución.

Recomendaciones

- Elaborar un plan detallado de control y gestión de redes del GADPE.
- Realizar monitoreo de las necesidades de capacidad de los sistemas que se encuentran en operación, para lo cual se debe tener en cuenta los nuevos requerimientos de los sistemas, tendencias actuales en el procesamiento de la información de la institución.
- Elaborar y firmar acuerdos de transferencia de información entre la institución y partes externas.
- Elaborar, documentar y aplicar la política de separación de redes.
- Elaborar un manual en donde se describa el procedimiento que se debe realizar para la transferencia de información bajo un estándar determinado.

10) Dominio: Adquisición, desarrollo y mantenimiento de sistemas

Controles

- Requisitos de seguridad de los sistemas de información.
- Seguridad en los procesos de desarrollo y soporte.
- Datos de prueba.

Situación

- No existe, normas o políticas documentadas para el análisis o especificación de requisitos de la seguridad de la información del GADPE
- Falta de comunicación en torno a la seguridad de servicios de a aplicaciones en redes públicas.
- Existe documentación de los privilegios que tienen los usuarios en torno a la protección de transacciones de los servicios de las aplicaciones.
- No hay política o normativa que sea aplicada a los sistemas y aplicaciones desarrollados en la institución.
- Se realizan procedimientos de control de cambio en los sistemas pero no están documentados.
- Carecen de manual o plan en donde se detalle la revisión técnica de las aplicaciones después de cambios en la plataforma de operación, pero si se realiza el procedimiento de manera informal.
- Se mantienen principios de construcción de los sistemas protegiendo los ambientes de desarrollo, realizando las respectivas restricciones en los cambios de paquetes de software.
- No poseen ningún programa de pruebas de aceptación de sistemas.
- No tiene un plan que realice el procedimiento de protección de los datos de prueba.

Riesgos

- Fallas humanas que puedan incurrir en el cese de las actividades de la institución.
- Uso negligente o mala utilización de los sistemas de información.
- Compromiso o daño total o parcial de los recursos informáticos.
- Corrupción de la información crítica del GADPE.
- Accesos no autorizados a los sistemas de información.

Recomendaciones

- Realizar los debidos controles de los programas que se encuentran en desarrollo, protegiendo los datos de prueba y el acceso al código fuente.
- Elaborar y documentar políticas que implique la adquisición, desarrollo y mantenimiento de los sistemas.

- Realizar el respectivo análisis y especificación de los requerimientos que exigen a los sistemas de información en torno a la seguridad para cumplir con las necesidades de las actividades del GADPE.
- Realizar la validación de la entrada de datos, implementación de controles internos, para poder detectar si existe una corrupción de la información en las aplicaciones ya sea si se hayan realizado de manera intencional o accidentalmente y por ultimo validar la salida de los datos para verificar si estos requerimientos son de acuerdo a la aplicación, elaborar el plan que con lleva este proceso y documentarlo.

11) Dominio: Relaciones con los proveedores

Controles

- Seguridad de la información en las relaciones con los proveedores.
- Gestión de la prestación de servicios de proveedores.

Situación

- No existe una política documentada sobre la información que debe compartirse con los proveedores, pero esta información es limitada.
- Existen acuerdos firmados con los proveedores que tienen acceso y almacenan cualquier recurso informático.
- No se audita la prestación de servicios de los proveedores ni se hace seguimiento.
- No existen políticas de cambios de servicios de los proveedores por ende no hay una regulación de las mismas.

Riesgos

- La falta de control en el seguimiento de los servicios de los proveedores podría causar que las actividades de la empresa podrían paralizarse o retrasarse del plazo que se tiene establecido en la planificación que tiene la institución en una determinada obra lo que puede generar deficiencias en el sistema de la institución.
- El riesgo al no tener políticas documentadas sino de manera informal es que no quede plasmadas ni socializadas las normativas de la institución con la relación con los proveedores, podría haber un mal uso de la información manejada por parte de estos.

Recomendaciones

- Se debe elaborar un modelo base para la firma de acuerdos de confidencialidad, requisitos de seguridad, e intercambio de la información que deben firmar los proveedores, el mismo que debe ser divulgado a todos los jefes departamentales del GADPE, para que sean socializados para todos aquellos funcionarios sean responsables o adquieran recursos informáticos.
- Se deben evaluar y aprobar los accesos que han tenido los proveedores a la información de la institución.
- Definir las condiciones de conexión de los equipos de cómputo ocupados por terceras partes a la red del GAPDE.
- Mitigar los riesgos relacionados con seguridad de la información que estén relaciones con proveedores que tengan acceso a los sistemas de información.

12) Dominio: Gestión de seguridad de la información

Controles

- Gestión de incidentes y mejoras en la seguridad de la información.

Situación

- Cada funcionario del GADPE es responsable de la información que maneja.
- Existen reportes de los eventos de seguridad que se han dado en la institución.
- Existen reportes que han realizado los funcionarios del GAPDE en torno a debilidades en la seguridad de la información.
- Se realiza la clasificación de los eventos de seguridad que se han reportado y se da seguimiento a los mismos, pero esta política no está documentada, solo se realiza la impresión de los informes que da respuesta a los eventos.

Riesgos

- Así como existen evento de menor alcance podrían ocurrir incidentes de gran magnitud y si no existe un precedente de los mismos de forma física o digital y de cómo se solucionó el anterior es probable que los responsables pierdan tiempo averiguando que solución encontrar para el mismo.
- Violentarían de regulación estatutaria, y a cualquier requerimiento de la seguridad.
- Robo de información critica de la institución.

- Daño o corrupción de la información.
- Mal uso de los sistemas de información.

Recomendaciones

- Los funcionarios que manejan información del GADPE deben informar al departamento TIC sobre los incidentes de seguridad que identifiquen o reconozcan la posible materialización de los mismos.
- El departamento de TIC debe elaborar y documentar políticas en donde se establezcan procedimientos que aseguren dar una respuesta eficaz y eficiente frente a los incidentes de seguridad de la información que se presenten.
- Se debe designar un personal que se encuentre debidamente calificado para investigar los incidentes de seguridad que han reportado los funcionarios de la institución, proporcionando soluciones y previniendo que estas vuelvan a ocurrir.
- Los funcionarios deben notificar de manera inmediata si se conoce de alguna divulgación o uso de información restringida o sensible del GADPE al departamento de TIC para que se realice la gestión correspondiente y proceder con el respectivo procedimiento.

13) Dominio: Aspectos de seguridad de la información de la gestión de continuidad del negocio.

Controles

- Continuidad de seguridad de la información.
- Redundancias.

Situación

- No hay ningún plan de donde se definan los requisitos para la continuidad de la seguridad de la información.
- Existen procedimientos para situaciones adversas pero no hay una política de la misma.
- Los controles de seguridad se realizan periódicamente en el GADPE.
- No hay una política ni normativa de disponibilidad de instituciones de procedimiento de información.
- No tienen un plan de contingencia contra los desastres naturales.

Riesgos

- Todo procedimiento que se realiza debe documentarse ya que se podría dar el mal uso a las instalaciones de procesamiento de información.
- Si no se tiene un plan para la continuidad de la seguridad de la información el personal podría no responsabilizarse por el mal uso de la información o peor aún la perdida de la misma.
- Los procedimientos que se efectúan en la organización para realizar una actividad no siempre se recuerdan a menudo, la mente humana es frágil, es ahí donde radica la importancia de tener un plan de continuidad del negocio ya si no es así los procedimientos pueden fallar en la realización de pruebas, o cambios en los equipos informáticos o en el recurso humano, lo cual afectaría a la institución en el desarrollo de sus actividades.
- Sabotaje de la información crítica de la institución.
- Infiltraciones.
- Mal manejo de equipos y sistemas de información.

Recomendaciones

- Las autoridades reguladoras del GADPE junto con el departamento de TIC deben hacer reuniones para que se determine las amenazas naturales que podrían sobrevenir, como afectaría esto a la institución y la solución a esta amenaza.
- Elaborar un análisis de impacto al negocio y los riesgos de continuidad, para realizar propuestas sobre las estrategias más convenientes para la institución de recuperación ante cualquier desastre natural.
- Realizar pruebas de recuperación ante desastres y notificar el resultado de la misma a la máxima autoridad del GADPE.
- Documentar y probar todos los procedimientos de continuidad que podrían ser utilizados en caso de algún incidente que atente en contra de la seguridad de la información para verificar que sean efectivos.
- Documentar políticas de disponibilidad de instalaciones de procesamiento de información.
- Analizar y determinar los requerimientos de redundancias para los sistemas de información del GADPE así mismo para la infraestructura tecnológica que le da apoyo.

- Evaluar las soluciones de redundancia tecnológica, probar dichas soluciones y escoger la solución cuyos requerimientos sean cumplidos.

14) Dominio: Cumplimiento

Controles

- Cumplimiento de requisitos legales y contractuales.
- Revisiones de seguridad de la información.

Situación

- No hay documentación sobre derechos de propiedad intelectual.
- Todo software en la institución se encuentra debidamente patentado o con licencia.
- No hay controles criptográficos.
- No se realizan revisiones independientes de todos los controles en cuanto a la seguridad de la información sino se lo realiza de manera global.
- El cumplimiento de las normas dentro del departamento de TIC se lo realiza eventualmente.
- Se realizan controles periódicos del cumplimiento técnico.

Riesgos

- El no tener políticas de seguridad de la información bien definidas y documentadas, socializadas y puestas en práctica afecta a este dominio del cumplimiento de los requisitos legales ya que puede haber violaciones a la ley, regulaciones contractuales y en si a cualquier requerimiento del sistema de gestión de seguridad de la información de la institución.

Recomendaciones

- Identificar y documentar los requisitos legales, reglamentarios y contractuales relacionados a la seguridad de la información y que pueden ser aplicables al GADPE.
- Actualizar los requisitos legales periódicamente para evitar posibles amenazas que impidan ejecutar el cumplimiento de los mismos.
- Elaborar un inventario del software que se encuentra en cada estación de trabajo de la institución para el normal desarrollo de sus labores, mismos que deben está debidamente protegidos por derechos de autor o requiera licencia o su vez si es software de libre distribución.

CAPITULO IV: ANALISIS DE IMPACTOS

4.1. ANTECEDENTES

Después de haber desarrollado la evaluación del sistema de gestión de seguridad de la información del GADPE, se elaboró el análisis de impactos de forma prospectiva, donde se definieron impactos tanto positivos como negativos.

Para una mejor interpretación de los impactos se ha elaborado un breve análisis de cada uno de ellos como son tecnológicos, organizacionales, éticos, económicos y sociales.

En la siguiente matriz se clasifican numéricamente los niveles de impacto que se le otorgara a cada indicador en las matrices respectivas:

IMPACTO NUMERICO	DESCRIPCION
-3	Impacto alto negativo
-2	Impacto medio negativo
-1	Impacto bajo negativo
0	No hay impacto
1	Impacto bajo positivo
2	Impacto medio positivo
3	Impacto alto positivo

- A cada indicador se asignó un valor numérico de nivel de impacto en la respectiva matriz.
- Se efectúa una sumatoria de los niveles de impactos en cada matriz y se divide este valor para cada número de indicadores obtenidos, de este modo se obtuvo el promedio de área o ámbito.
- Hay que señalar que bajo cada matriz se incluye el análisis y argumento de las razones y las circunstancias por las que se asigna el valor.

4.2. Impacto Tecnológico

Niveles de Impacto Indicadores	-3	-2	-1	0	1	2	3
1. Salvaguardar los sistemas de información: Confidencialidad, integridad y disponibilidad.							x
2. Cumplimiento de políticas de seguridad de la información.							x
3. Detección y solución de incidentes de seguridad							x
TOTAL	9						
Nivel de Impactos: ∑/ número de indicadores = $\frac{9}{3}$ = 3							
Nivel de impacto: Impacto Alto Positivo.							

Análisis

1. Se considera como impacto ***alto positivo*** a la elaboración de esta investigación ya que por medio de la misma se logró identificar los activos de información de la institución que poseen un valor para la entidad, los mismos que hoy en día necesitan estar protegidos ante cualquier ataque.

2. Esta investigación planteó que las políticas de seguridad de información sean bien elaboradas, documentadas y socializadas para poder dar cumplimiento a las mismas, que deben estar conformadas por normativas y patrones que deben seguirse en las diferentes instancias en las que los activos de información se vean comprometidos por eso este indicador se ha considerado como ***alto positivo.***

3. ***Alto positivo,*** ya que aplicando las respectivas políticas se pudo detectar y resolver de manera eficiente los incidentes de seguridad que se presentan en la institución, ya que se pudo tomar medidas encaminadas a reducir circunstancialmente los riesgos a los que la entidad enfrente.

4.3. Impacto Organizacional

Niveles de Impacto Indicadores	-3	-2	-1	0	1	2	3
1. Gestión de productividad en los procesos en torno a la seguridad de la información en todos los departamentos						x	
2. Control de inventario de activos informáticos							x
3. Toma de decisiones							x
TOTAL	8						
Nivel de Impactos: ∑/ número de indicadores = $\frac{8}{3}$ = 2.66=3							
Nivel de impacto: Alto Positivo.							

Análisis

1. La seguridad de la información es de vital importancia para la correcta administración de la institución, por lo que este indicador tiene un impacto ***medio positivo*** ya que mediante la socialización de dichas políticas propuso el conocimiento de las mismas por parte de los funcionarios y con su control se verificará su respectivo cumplimiento.

2. ***Alto positivo,*** mediante la aplicación de las respectivas políticas de gestión de activos se pudo determinar quién es el responsable de cada activo, en qué condiciones se puso en producción dicho activo, en qué condiciones se entregan y de esta manera se previene la pérdida o el daño del mismo sin tener un responsable a su cargo.

3. ***Alto positivo,*** esta investigación propuso una toma de decisiones en base a información integra, sobre el estado de los sistemas de información para llegar al cumplimiento de los objetivos de la institución, de modo que la máxima autoridad de la entidad pudo apoyar estas decisiones de manera consciente y responsable.

4.3. Impacto Ético

Niveles de Impacto Indicadores	-3	-2	-1	0	1	2	3
1. Concientización del personal						x	
2. Capacitación de los funcionarios en el tema de seguridad de la información.							x
3. Estrategias de seguridad de la información en torno a la organización.							x
TOTAL	8						
Nivel de Impactos: ∑/ número de indicadores = $\frac{8}{3}$ = 2.66=3							
Nivel de impacto: Alto Positivo.							

Análisis

1. Se definió al indicador como ***medio positivo*** ya que mediante la debida concientización al personal en cuanto a la importancia de proteger la información que manejan.

2. ***Alto positivo,*** este indicador se definió de esta manera ya que se debe elaborar y ejecutar un plan de manera permanente con el objetivo de apoyar la protección adecuada de la información para así poder contar con un personal calificado en cuanto al tratamiento que se le debe dar a la información

3. Este indicador se determinó como ***alto positivo,*** ya que mediante la identificación de los riesgos que presenta la institución se pueden elaborar estrategias para la gestión coordinada de la seguridad de la información de la organización.

4.4. Impacto Social

Niveles de Impacto Indicadores	-3	-2	-1	0	1	2	3
1. Eficiencia y mejora de los procesos internos							x
2. Mejor despliegue de servicios por parte del GADPE hacia la colectividad.							x
3. Mejora de la competitividad como entidad publica							x
TOTAL	9						
Nivel de Impactos: ∑/ número de indicadores = $\frac{9}{3}$ =3							
Nivel de impacto: Alto Positivo.							

Análisis

1. Este indicador tiene un nivel de impacto ***alto positivo*** debido a que el GADPE lidera los procesos de desarrollo de la provincia y con esta investigación donde se recomienda aplicar los debidos correctivos se dará una eficiente ejecución de sus competencias donde se beneficiará sociedad esmeraldeña.

2. Se cuantificó como ***alto positivo***, debido a que se efectuará un mejor despliegue de los servicios de calidad por parte de la institución hacia la colectividad mejorando cada uno de los procesos que efectúan con la participación activa del departamento de TIC, agilitando todos los procesos.

3. Se definió con un nivel de impacto ***alto positivo*** a este proyecto porque por medio de la evaluación al SGSI porque mejora la gestión de la organización la hace más competentes para desarrollar procesos que van en pro de la mejoramiento de la provincia.

4.5. Impacto Económico

Niveles de Impacto Indicadores	-3	-2	-1	0	1	2	3
1. Evitar costosos incidentes de seguridad de la información.						x	
2. Impedir robos o daños a los activos informáticos que suponen un alto coste.						x	
3. Productividad de la institución							x
TOTAL	7						
Nivel de Impactos: ∑/ número de indicadores = $\frac{7}{3}$ =2							
Nivel de impacto: Alto Positivo.							

Análisis

1. Este indicador incide directamente sobre la gestión que realiza el GADPE, ya que se puede observar cómo se pueden evitar varias situaciones que supone un alto costo para la institución por eso este indicador se lo ha determinado como ***medio positivo***.

2. Los activos informáticos son de suma importancia para el desempeño de las actividades de la institución, por ende deben ser cuidados y protegidos para que desempeñen la función para la cual están destinados, por esto mismo este indicador se determinó como ***medio positivo.***

3. Las decisiones que se tomarán en la institución serán en base a un sistema de gestión de seguridad de la información fiable y seguridad por lo tanto la productividad de la misma va a tener mayor alcance, por este motivo este indicador se lo ha definido como ***alto positivo.***

4.6. Matriz General

Niveles de Impacto Indicadores	-3	-2	-1	0	1	2	3
1. Impacto Tecnológico							x
2. Impacto Organizacional							x
3. Impacto Ético							x
4. Impacto Social							x
5. Impacto Económico						x	
TOTAL	13						
Nivel de Impactos: ∑/ número de indicadores = $\frac{13}{5}$ =2.6= 3							
Nivel de impacto: Alto Positivo.							

Análisis

1. El nivel de Impacto Tecnológico que se ha generado es ***Alto Positivo*** ya que al tener un sistema de gestión de seguridad de la información fiable, íntegro y protegido se evitarán interrupciones en el flujo normal de actividades de la institución, ya que se mantendrán protegidos los activos informáticos de la institución, para ofrecer un mejor servicio a la colectividad, ya que el GADPE es una entidad pública que lidera los procesos de desarrollo de la provincia con un alto sentido de responsabilidad social.
2. Por otro parta el nivel de impacto Organizacional, Ético y Social también se han determinado como ***Alto Positivo***, ya que la investigación presenta varios beneficios para la institución donde se observa la realidad existente en el GADPE en cuanto al sistema de gestión de seguridad de la información y se elaboran recomendaciones evitar los riesgos que la evaluación presenta.
3. El impacto Económico que presenta esta investigación es ***Medio Positivo*** ya que se garantiza la continuidad del negocio ya que estas prácticas revalorizan las actividades de la institución y mejorarían su desempeño como entidad pública dedicada a fomentar el desarrollo socio-económico de la Provincia de Esmeraldas.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Los activos informáticos dentro de una organización, deben encontrarse protegidos y resguardados debidamente; mismos que se encuentran expuestos a riesgos que puedan materializarse causando daños a los mismos. Aplicando las correspondientes salvaguardas y estrategias de alto nivel que permitan realizar un control adecuado y la administración efectiva de los recursos informáticos.
- El sistema de gestión de seguridad de la información de toda entidad tanto pública como privada, debe identificar los riesgos a los que su información se enfrenta, los mismos que deben ser asumidos, mitigados y controlados de una forma sistemática y definida.
- Mediante la verificación y el cumplimiento de las políticas de seguridad de la información luego de haber sido elaboradas, definidas, documentadas y socializadas dentro de la institución, ayudarán a la preservación y aseguramiento de la confidencialidad, integridad y disponibilidad de la información.
- El talento humano forma una parte fundamental dentro de toda organización. Por ese motivo deben realizarse contantes capacitaciones en cuanto a la seguridad de la información y el tratamiento que se le debe dar a la misma. Deben tener asociados los perfiles de usuario y sus privilegios según las funciones que desempeñe.
- La norma ISO 27001:2013 es un estándar internacional permite conocer de forma general la realidad existente del GADPE en términos de seguridad de la información, obteniendo así resultados mediante la evaluación al sistema de gestión de seguridad de la información.
- El instrumento de evaluación basado en COBIT, ha ayudado a cuantificar los niveles de riesgo y confianza que tiene el Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas.

5.2. RECOMENDACIONES

- Elaborar, definir y documentar políticas de seguridad de la información, las mismas que permitirán conseguir el cumplimiento de los objetivos institucionales mediante la aplicación de controles de seguridad, pero gestionar un nivel de riesgo aceptable, con lo que se logrará garantizar un alto desempeño de las actividades de la institución, obteniendo requisitos de seguridad cuyo fin es impedir infracciones y violaciones de seguridad en la institución.

- Concientizar y capacitar continuamente a los funcionarios de la institución sobre la importancia que tiene proteger la información, de una forma interactiva mediante un programa efectivo, ya que uno de los factores de éxito en una organización es la comunicación entre las áreas que la conforman.

- Definir un responsable cuyas funciones sean claramente definidas, que se encargue de verificar que las políticas de seguridad de la información sean cumplidas por los funcionarios de la institución, cuya finalidad sea la de cumplir y soportar las actividades de seguridad de la información.

- Desarrollar un plan de seguridad informático tomando en cuenta las recomendaciones que se han realizado mediante esta evaluación, para proteger los activos informáticos de la institución, mitigando riesgos y enfrentando las amenazas.

Referencias bibliográficas

Aceituno, V. (2001). *Seguridad de la informacion* . Mexico : Copyright.

Aguilera, P. (2010). *Seguridad Informatica.* Madrid: Editex.

Anónimo. (23 de 10 de 2012). *Ucml*. Obtenido de Ucml: Evaluación https://www.uclm.es/profesorado/ricardo/Practicum/Relieve/evaluacion.htm

Aranda, R., & García, A. (2013). *Sistema de seguridad de informática integral.* Cantabria: Universidad Cantábrica.

Areitio, J. (2008). *Seguridad de la Informacion* . Madrid : Paraninfo.

Bermudez, M. (2010). *Sistema de Informacion para el archivo historico del departamento nacional de planeacion.* Buenos Aires: Corporacion universitaria minuto de Dios. Obtenido de CORPORACION UNIVERSITARIA MINUTO DE DIOS: http://repository.uniminuto.edu:8080/jspui/bitstream/10656/1733/1/TTI_VargasIzquierdoAngelaLuisa_2010.pdf

Blásquez, M. (7 de 2 de 2012). *Evaluacion de Sistemas de Información y Usuarios*. Obtenido de Evaluacion de Sistemas de Información y Usuarios: http://ccdoc-evaluacionsistemasinformacion.blogspot.com/2011/02/03-que-es-la-evaluacion.html

Burgos, J. (10 de 09 de 2010). *Ceur.Modelo para la Seguridad de Informacion en TIC* Obtenido de Ceur: http://ceur-ws.org/Vol-488/paper13.pdf

Bustos , F., Chávez, C., & González, N. (2009). *Metodología para evaluar y calificar la seguridad física de un centro de procesamiento de datos.* México: Instituto Poliotécnico Nacional de México.

Chiavetano, I. (2006). Introduccion a la teoria general de la administración. En I. Chiavetano, *Introduccion a la teoria general de la administración* (pág. 110). Nicaragua: McGraw-Hill Interamericana.

Contraloria, G. d. (16 de 11 de 2009). *Normas de Control interno para las entidades y organismos.* Recuperado el 23 de 10 de 2015, de Normas de Control interno para las entidades y organismos: http://www.contraloria.gob.ec/documentos/normatividad/ACUERDO%20039%20CG%202009%205%20Normas%20de%20Control%20Interno.pdf

Corletti, A. (2011). *Seguridad por niveles* . Madrid: Learnin Consulting .

Corrales, L. (2006). *Diseño e implementacion de arquitecturas informaticas seguras. Una aproximacion practica.* Estados Unidos: Dykinson.

Daltabuit, E. (2016). *Seguridad de la Informacion consideraciones sobre la identidad* . Oaxaca: Create Space.

Delgado, X. (205). *Auditoria Informatica.* California: EUNED .

Diaz, A. (2009). *La seguridad y la informacion de Estado.* California : Taller de Escuela de Artes Graficas .

Diaz, G. (2014). *Procesos y Herramientas para la seguridad en redes.* Madrid: Universidad nacional de educacion a Distancia.

Direccion de Tecnologias de la Informacion y Comunicacion-Gadpe. (s.f.). *GADPE-TIC*. Obtenido de http://www.prefecturadeesmeraldas.gob.ec/index.php/en/direcciones/tics

Fisher, R. P. (1988). *Seguridad en los sistemas informaticos* . Madrid : Diaz de Santos.

Freidas, V. d. (2012). *Sistema de Gestion de Seguridad de la Informacion* . Madrid: EAE .

GADPE. (2014). *Antecedentes para la seguridad de la información.* Esmeraldas.

Galindo Lopez, Celvin Manolo. (2014). La firma electronica avanzada y su certificacion . *Seguridad de la informacion* , 102.

GallegosyFolgado. (2011). *Montaje y mantenimiento de equipos.* Madrid: Editex.

Garcia, A. (2011). *Seguridad Informatica* . Madrid: Parainfo.

Giner, F. (2004). *Los sistemas de informacion en la sociedad del conocimiento* . Madrid: ESIC.

Godoy, R. (2014). Seguridad de la informacion. *Seguridad de la Informacion*, 163.

Guagalango, R. (11 de 08 de 2011). *Repositorio ESPE.* Evaluacion Tecnica de la Seguridad Informatica del Data Center de la Escuela Politecnica del Ejercito Obtenido de Repositorio ESPE: http://repositorio.espe.edu.ec/xmlui/handle/21000/176/browse?value=Guagalango+Vega%2C+Ricardo+Napole%EF%BF%BD&type=author

Gutierrez, C. (26 de 11 de 2013). *We Life Security*. Obtenido de We Life Security: http://www.welivesecurity.com/la-es/2013/11/26/que-tener-cuenta-metricas-seguridad-informacion-owasp/

Gutierrez, J. (2003). *Protocolos Criptograficos y Seguridad en REdes.* España: Servicio deEdiciones de la Universidad de Cantabria.

Juarez, H. A. (08 de 11 de 2011). *Magazcitum.* Obtenido de Magazcitum: http://www.magazcitum.com.mx/?p=1574#.Vr4kKPLhDIU

Kosutic, D. (2015). *Advisera.* Obtenido de Advisera: http://advisera.com/27001academy/es/que-es-iso-27001/

Laborde, C. (20 de 08 de 2013). *Auditoria informatica y metricas de seguridad informatica* . Obtenido de Auditoria informatica y metricas de seguridad informatica : https://prezi.com/hlutc0jk_ja4/auditoria-informatica-y-metricas-de-seguridad-informatica/

Langefors, B. (1976). *Teoria de los sistemas de informacion* . Buenos Aires : El Ateneo Laudon, Laudon. (2004). *Sistemas de informacion gerencial* . New York : Pearson.

López Estupiñan, Luis. (2007). *El consejo provincial de Esmeraldas.* Esmeraldas: Casa de la Cultura Ecuatoriana. Recuperado el 27 de enero de 2016, de https://www.google.com.ec

Lopez, G. (2014). La firma electronica avanzada y su certificacion. *Seguridad de la informacion: Segunda Cohorte del doctorado en Seguridad Estrategica*, 100.

Lopez, J. (2010). *Informatica aplicada a la gestion de empresas.* Madrid: Esic.

López, L. (2002). Gobierno Provincial de Esmeraldas. En L. E. Luis, *Gobierno Provincial de Esmeraldas* (pág. 6). Esmeraldas.

Luna, I. (20 de 10 de 2004). *Belt Iberica S.A.* Obtenido de Belt Iberica S.A.: http://www.belt.es/expertos/experto.asp?id=2245

Mauricio Bermudez, Vargas Angela, Karol Rivera. (2010). *Sistema de informacion para el archivo historico del departamento nacional de planeacion.* Corporacion universitaria minuto de dios. Obtenido de corporacion universitaria minuto de dios: http://repository.uniminuto.edu:8080/jspui/bitstream/10656/1733/1/TTI_VargasIzquierdoAngelaLuisa_2010.pdf

Medina, S. (2006). *Direccion y gestion de los sitemas de informacion en la empresa* . Madrid: ESIC.

Mora Díaz, E. &. (2008). *Políticas de seguridad, plan de contingencia GAD* . Cuenca: Universidad Politécnica Salesiana de Cuenca.

Moscoso, P. (Abril de 2010). Manual de Politicas de Seguriad de la Informacion *ESPE.* Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/4279/3/T-ESPE-032634-A.pdf

Ochando, D. M. (s.f.). *Evaluacion de Sistemas de Informacion y usuarios.* Obtenido de http://ccdoc-evaluacionsistemasinformacion.blogspot.com/2011/02/03-que-es-la-evaluacion.html

Ogalla, F. (2005). *Sistema de Gestión* . España: Diaz de Santos.

Pallas, G. (diciembre de 2009). Metodologia de Implantacion de un SGSI en un grupo empresarial jerarquico *FING.* Obtenido de http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

Posso, M. (2011). *Proyectos, Tesis y marco logico.* Quito: Nocion.

Prefectura de Esmeraldas. (7 de Noviembre de 2014). Plan Estratégico del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas 2014-2019. Esmeraldas, Esmeraldas, Ecuador.

Ramirez, A. (10 de 5 de 2014). *Open Access.* Obtenido de Open Access: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/36241/6/aramirezcasTFM0514memoria.pdf

Ramos, B. (2004). *Avances en Criptologia y Seguridad de la Informacion* . Madrid: Diaz de santos .

Rivera Pitti, E. (2005). *Planes de contingencia y respaldo.* México: Prince-Hall.

Royer, J. (2004). *Seguirdad de la Informatica en empresa.* Barcelona : ENI.

Royer, J. M. (2004). *Sefuridad en la informatica de la empresa.* Ediciones Eni.

Sanchez, J. S. (2003). *Ingenieria de Proyectos Informaticos.* Mexico: Universitat Jaume I.

Sistemas integrados de Gestion. (22 de 10 de 2015). *Implementacion SIG*. Obtenido de Implementacion SIG: http://www.implementacionsig.com/index.php/23-noticiac/28-que-es-un-sistema-de-gestion

Tamayo, A. (2001). *Auditoria de Sitemas* . Colombia: Universidad de Colombia .

Tecnologico, O. (2012). *Observatorio Tecnologico.*

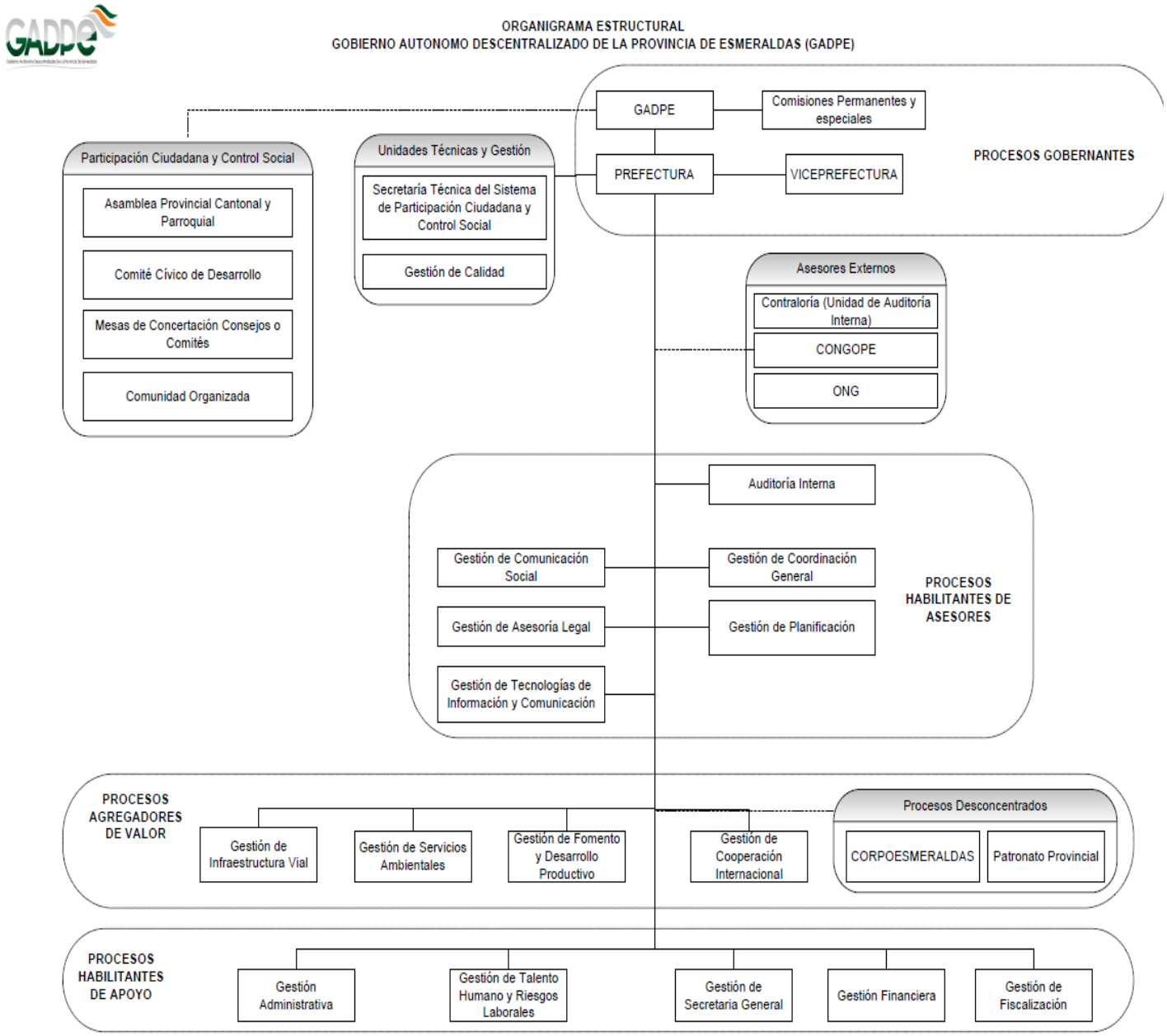
Thompson, I. (2008). Que Es La Informacion. *Promonegocios*.

Universidad Auitónoma de Santo Domingo. (2006). *Tipos de ataque en la red.* Santo Domingo: UASD.

Vilegas, M. (09 de 10 de 2008). *Mendillo.* Obtenido de Mendillo: http://mendillo.info/seguridad/tesis/Villegas2.pdf

ANEXOS

ANEXO A: Organigrama estructural del gobierno autónomo descentralizado de la provincia de esmeraldas



ANEXO B: Organigrama departamental de la dirección de tecnología de información y comunicación del GADPE

ANEXO C: Estructura de la norma ISO 27001-2013

DOMINIO	CONTROL	OBJETIVO DE CONTROL
Políticas de Seguridad de la Información	Orientación de la dirección para la gestión de la seguridad de la información	Políticas para la seguridad de la información
		Revisión de las políticas para la seguridad de la información
Organización de la Seguridad de la Información	Organización Interna	Roles y responsabilidades para la seguridad de la información
		Separación de deberes
		Contacto con las autoridades
		Contacto con grupos de interés especial
		Seguridad de información en la gestión de proyectos
	Dispositivos móviles y teletrabajo	Política para dispositivos móviles
		Teletrabajo
Seguridad de los Recursos Humanos	Antes de asumir el empleo	Selección
		Términos y condiciones del empleo
	Durante la ejecución del empleo	Responsabilidades de la dirección
		Toma de conciencia, educación y formación en la seguridad de la información
		Proceso disciplinario
Gestión de Activos	Responsabilidad por los activos	Inventario de activos
		Propiedad de los activos
		Uso aceptable de los activos
		Devolución de activos
	Clasificación de la información	Clasificación de la información
		Etiquetado de la información
		Manejo de Activos
	Manejo de medios	Gestión de medios removibles
		Disposición de los medios
		Transferencia de medios físicos
Control de Acceso	Requisitos del negocio	Política del control de acceso
		Acceso a redes y a servicios de red
	Gestión de acceso a usuarios	Registro y cancelación de registro de usuario
		Suministro de acceso de usuarios
		Gestión de derechos de acceso privilegiado
		Gestión de información de autenticación secreta de usuarios
		Revisión de los derechos de acceso de los usuarios
		Retiro o ajuste de los derechos de acceso
	Responsabilidades de los usuarios	Uso de información de autenticación secreta
	Control de acceso a sistemas y aplicaciones	Restricción de acceso a la información
		Procedimientos de ingreso seguro
		Sistema de gestión de contraseña
		Uso de programas utilitarios privilegiados
		Control de acceso a códigos fuente de programas
Criptografía	Controles criptográficos	Política sobre el uso de controles criptográficos
		Gestión de llaves
Seguridad Física y del Entorno	Aéreas Seguras	Perímetro de Seguridad
		Controles de acceso físico

		Seguridad en oficinas, recintos e instalaciones
		Protección contra amenazas externas y ambientales
		Trabajo en áreas seguras
		Aéreas de despacho y carga
	Equipos	Ubicación y protección de los equipos
		Servicios de suministro
		Seguridad del cableado
		Mantenimiento de equipos
		Retiro de activos
		Seguridad de equipos y activos fuera de las instalaciones
		Disposición segura o reutilización de equipos
		Equipos de usuarios desatendidos
		Política de escritorio limpio y pantalla limpia
Seguridad de las operaciones	Procedimientos operacionales y responsabilidades	Procedimientos de operación documentados
		Gestión de cambios
		Gestión de capacidad
		Separación de los ambientes desarrollados, pruebas y operación
	Protección contra códigos maliciosos	Controles contra códigos maliciosos
	Copias de respaldo	Respaldo de información
	Registro y seguimiento	Registro de eventos
		Protección de la información
		Registros del administrador y del operador
		Sincronización de relojes
	Control de software operacional	Instalación de software en sistemas operativos
	Gestión de vulnerabilidad técnica	Gestión de las vulnerabilidades técnicas
		Restricciones sobre la instalación de software
	Consideraciones sobre auditorias de sistemas de información	Controles de auditorías de sistemas de información
Seguridad de las comunicaciones	Gestión de seguridad de las redes	Controles de redes
		Seguridad de los servicios de red
		Separación en las redes
	Transferencia de información	Políticas y procedimientos de transferencia de información
		Acuerdos sobre transferencia de información
		Mensajería electrónica
		Acuerdos de confidencialidad o de no divulgación
Adquisición, desarrollo y mantenimiento de sistemas	Requisitos de seguridad de los sistemas de información	Análisis y especificación de requisitos de seguridad de la información
		Seguridad de servicios de las aplicaciones en redes publicas
		Protección de transacciones de los servicios de las aplicaciones
	Seguridad en los procesos de desarrollo y soporte	Política de desarrollo seguro
		Procedimientos de control de cambios en sistemas
		Revisión técnica de las aplicaciones después de cambios en la plataforma de operación
		Restricciones en los cambios a los paquetes de software
		Principios de construcción e los sistemas seguros

		Ambiente de desarrollo seguro
		Desarrollo contratado externamente
		Pruebas de seguridad de sistemas
		Pruebas de aceptación de sistemas
	Datos de prueba	Protección de los datos de prueba
Relaciones con los proveedores	Seguridad de la información en las relaciones con los proveedores	Política de seguridad de la información para las relaciones con los proveedores
		Tratamiento de seguridad dentro de los acuerdos con proveedores
		Cadena de suministro de tecnología de información y comunicación
	Gestión de la prestación de servicios de proveedores	Seguimiento y revisión de los servicios de los proveedores
		Gestión de cambios en los servicios de los proveedores
Gestión de incidentes de seguridad de la información	Gestión de incidentes y mejoras en la seguridad de la información	Responsabilidades y procedimientos
		Reporte de eventos de seguridad de la información
		Reporte de debilidades de seguridad de la información
		Evaluación de eventos de seguridad de la información y decisiones sobre ellos
		Respuesta a incidentes de seguridad de la información
		Aprendizaje obtenido de los incidentes de seguridad de la información
		Recolección de evidencia
Aspectos de seguridad de la información de la gestión de continuidad del negocio	Aspectos de seguridad de la información de la gestión de continuidad del negocio	Planificación de la continuidad de la seguridad de la información
		Implementación de la continuidad de la seguridad de la información
		Verificación, revisión y evaluación de la continuidad de la seguridad de la información
	Redundancias	Disponibilidad de instalaciones de procesamiento de la información
Cumplimiento	Cumplimiento de requisitos legales y contractuales	Identificación de la legalización aplicable y de los requisitos contractuales
		Derechos de propiedad intelectual
		Protección de registros
		Privacidad y protección de información de datos personales
		Reglamentación de controles criptográficos
	Revisiones de seguridad de la información	Revisión independiente de seguridad de la información
		Cumplimiento con las políticas y normas de seguridad
		Revisión del cumplimiento técnico

ANEXO D: Funciones por cargo del departamento de TIC del GADPE

Denominación del Puesto	Analista Provincial 1
Procesos de trabajo	Infraestructura Tecnológica
Área Funcional	Dirección de Gestión TIC
Cantidad necesaria	01

MISIÓN:

Ejecutar labores de diseño, mejoramiento y programación especializada de la infraestructura tecnológica y sistemas de procesamiento automáticos de datos y orientar a usuarios de los sistemas informáticos del GADPE; a fin implementar el gobierno electrónico institucional; de acuerdo con las capacidades de equipamiento, enlaces de los sistemas y el Plan Informático.

RESP**ONSABILIDADES PRINCIPALES:**

- Implementar el Gobierno por resultados mediante plataformas tecnológicas de punta, de manera documentada y con el respectivo levantamiento de procesos.
- Adiestrar en el manejo a los usuarios del sistema de Gobierno por resultados a fin de lograr la integración y eficiencia de los procesos automatizados de datos
- Ajustar los procedimientos y operaciones de la Institución e incorporar los medios técnicos necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos.
- Diseñar, implementar y mantener un sistema de información y comunicación eficiente, que permita registrar, procesar, resumir e informar sobre las operaciones técnicas, administrativas y financieras de la entidad facilitando el monitoreo y evaluación de los indicadores de gestión de la entidad para la toma de decisiones de la máxima autoridad.
- Elaborar reportes e informes sobre especificaciones técnicas de equipamiento informático que se prevea adquirir en coordinación con los requirientes.
- Planificar y administrar la asignación de recursos para el desarrollo, mantenimiento y operación de la red.
- Dirigir las actividades de integración y mantenimiento cumpliendo con las especificaciones de seguridad y estándares de cableado estructurado.
- Desarrollar políticas, estándares y normas de seguridad lógica y física para la protección de la red.
- Establecer un cronograma en la asignación de recursos y las prioridades involucradas en los proyectos de desarrollo, expansión y cambios de la red.
- Mantener un Plan de Contingencia para recuperación y funcionamiento de los servidores y redes luego de un siniestro.
- Reportar a la Dirección los avances logrados en los proyectos e implantaciones a su cargo.
- Administrar la base de datos institucionales y velar por la seguridad de la información.
- Desarrollar y documentar procedimientos de administración, control y seguridad de toda la infraestructura de redes de datos de la institución.

Denominación del Puesto	Asistente Provincial 2
Procesos de trabajo	Infraestructura Tecnológica
Área Funcional	Dirección de Gestión TIC
Cantidad necesaria	01

MISIÓN:

Garantizar la operación, funcionamiento continuo, y uso eficiente de la infraestructura tecnológica utilizada, para alcanzar los objetivos del plan informático de la institución; a fin de optimizar la utilización de los recursos informáticos puestos a disposición de los servidores del Gobierno Autónomo Descentralizado Provincial.

RESPONSABILIDADES PRINCIPALES:

- Establecer mecanismos que protejan y salvaguarden contra perdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.
- Coordinar con la Dirección Administrativa la asignación de equipos de cómputo en función de los requerimientos, necesidades de los usuarios y especificaciones técnicas.
- Diseñar y ejecutar programas de mantenimiento preventivo y correctivo de los bienes informáticos de larga duración a fin de no afectar la gestión operativa de la entidad.
- Administrar la operación, planificar e implementar el crecimiento del Data Center, las redes de computadoras, para el suministro de servicios a los usuarios locales y remotos.
- Planificar, supervisar las actividades de mantenimientos del hardware a su cargo.
- Asesorar y supervisar a los ayudantes y/o pasantes (Si los hubiera) en el uso, instalación, configuración y mantenimiento de equipos y programas.
- Dar soporte técnico a los usuarios en actividades relacionadas al buen funcionamiento del hardware, software base (Sistema Operativo) y los recursos de comunicación, redes e internet.
- Elaborar reportes e informes sobre especificaciones técnicas del equipamiento informático que se necesite adquirir, en coordinación con las Direcciones solicitantes.
- Administrar los recursos destinados para prestar el servicio de internet.
- Optimizar el uso de recursos materiales de la institución en su área de labores.
- Presentar informes, que dentro de la naturaleza de sus funciones, solicitasen sus jefes inmediatos y demás autoridades en la institución.
- Cumplir con cualquier actividad que dentro de la naturaleza de su cargo solicitasen su jefe inmediato.

Denominación del Puesto	Analista Provincial 2
Procesos de trabajo	Sistemas y Aplicaciones
Área Funcional	Dirección de Gestión TIC
Cantidad necesaria	01

MISIÓN:
Desarrollar e integrar sistemas, programas y aplicaciones informáticas definidas para las diferentes unidades administrativas, documentar los procesos de desarrollo y/o

integración, adiestrar en el manejo a los usuarios del sistema; a fin de lograr la integración y eficiencia de los procesos automatizados de datos del Gobierno Autónomo descentralizado Provincial.

RESPONSABILIDADES PRINCIPALES:

- Codificar, programar, desarrollar e implementar los sistemas de información en base a los estándares definidos para el desarrollo de sistemas.
- Realizar el mantenimiento y las actualizaciones de los sistemas existentes.
- Diseñar el flujo lógico de cada programa ajustándolo a las especificaciones y los estándares recomendados.
- Instalar las herramientas y lenguajes de programación necesarios para la ejecución de actividades de desarrollo e implementación.
- Planificar los recursos necesarios para el desarrollo de los sistemas y programas.
- Diseñar y administrar la base de datos para el desarrollo de los sistemas y/o aplicaciones en coordinación con el administrador de sistemas.
- Establecer la visión y alcance de los sistemas a desarrollar, planificar las actividades y repostar el avance de las tareas hasta la finalización del proyecto.
- Realizar las pruebas y depuración de programas que sean necesarios antes de entregarlos.
- Documentar los desarrollos con los respectivos manuales: del sistema, de operación, y del usuario; de acuerdo a estándares establecidos a nivel nacional y/o internacional.
- Garantizar el correcto funcionamiento de las aplicaciones desarrolladas, mediante monitoreo y medición de la satisfacción de los usuarios.
- Desarrollar aplicaciones móviles y/o de acceso remoto para los funcionarios.
- Asistir en la capacitación y/o entrenamiento de los usuarios de los sistemas.
- Presentar informes, que dentro de la naturaleza de sus funciones, solicitasen sus jefes inmediatos y demás autoridades en la institución.
- Cumplir con cualquier actividad que dentro de la naturaleza de su cargo solicitasen su jefe inmediato.

Denominación del Puesto	**Asistente Provincial 1**
Procesos de trabajo	Aplicaciones y Sistemas
Área Funcional	Dirección de Gestión TIC
Cantidad necesaria	01

MISIÓN:

Desarrollar sistemas, programas y aplicaciones informáticas definidas para las diferentes unidades administrativas, documentar los procesos de desarrollo y/o integración, adiestrar en el manejo a los usuarios del sistema; a fin de lograr la integración y eficiencia de los procesos automatizados de datos del Gobierno Autónomo Descentralizado Provincial.

RESPONSABILIDADES PRINCIPALES

- Codificar, programar, desarrollar e implementar los sistemas de información en base a los estándares definidos para el desarrollo de sistemas.

- Realizar el mantenimiento y las actualizaciones de los sistemas existentes.
- Instalar las herramientas y lenguajes de programación necesarios para la ejecución de actividades de desarrollo e implementación.
- Diseñar y administrar la base de datos para el desarrollo de los sistemas y/o aplicaciones en coordinación con el administrador de sistemas.
- Realizar las pruebas y depuración de programas que sean necesarios antes de entregarlos.
- Documentar los desarrollos con los respectivos manuales: del sistema, de operación, y del usuario; de acuerdo a estándares establecidos a nivel nacional y/o internacional.
- Garantizar el correcto funcionamiento de las aplicaciones desarrolladas, mediante monitoreo y medición de la satisfacción de los usuarios.
- Desarrollar aplicaciones móviles y/o de acceso remoto para los funcionarios.
- Asistir en la capacitación y/o entrenamiento de los usuarios de los sistemas.
- Presentar informes, que dentro de la naturaleza de sus funciones, solicitasen sus jefes inmediatos y demás autoridades en la institución.
- Cumplir con cualquier actividad que dentro de la naturaleza de su cargo solicitasen su jefe inmediato.

Denominación del Puesto	Analista Provincial 1
Procesos de trabajo	Proyectos y Servicios Web
Área Funcional	Dirección de Gestión TIC
Cantidad necesaria	01

MISIÓN:

Proveer servicios de internet, intranet, correo electrónico y sitio web de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios internos y externos.

RESPONSABILIDADES PRINCIPALES:

- Elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio web de la entidad.
- Incorporar el uso de la firma electrónica en los procesos de la institución de conformidad con la ley de comercio electrónico, firmas y mensajes de datos y sus reglamentos.
- Administrar y hacer seguimiento de los proyectos informáticos que ejecuten las áreas técnicas que conforman la Dirección.
- Asistir a los usuarios en todas las actividades de administración y soporte de las aplicaciones web y recursos de internet.
- Administrar los usuarios de la intranet, internet y correo electrónico.
- Garantizar el acceso del usuario a los recursos informáticos compartido o a otra máquina de la red, a través del uso de un servidor de dominio.
- Garantizar el correcto funcionamiento de los servidores que están bajo la administración de la unidad.

- Capacitar a los usuarios de los servicios de la intranet, internet y aplicaciones de la institución.
- Instalar y configurar una plataforma virtual y/o de participación para la capacitación y formación continua de los usuarios internos y externos.
- Desarrollar instrumentos electrónicos para el monitoreo de la satisfacción de los servicios prestados por la Dirección de TIC.
- Presentar informes, que dentro de la naturaleza de sus funciones, solicitasen sus jefes inmediatos y demás autoridades en la institución.
- Cumplir con cualquier actividad que dentro de la naturaleza de su cargo solicitasen su jefe inmediato.

Denominación del Puesto	Asistente Provincial 1
Procesos de trabajo	Proyectos y Servicios Web
Área Funcional	Dirección de Gestión TIC
Cantidad necesaria	01

MISIÓN:

Mantener la página web institucional actualizada y funcional, que permita la publicación de contenidos de todas las unidades usuarias de la institución de manera ágil, segura, y oportuna.

RESPONSABILIDADES PRINCIPALES

- Mantener el correcto funcionamiento del sitio web y sus servicios en todo momento.
- Cumplir con las normas establecidas por la Ley de Transparencia, mediante la actualización y disponibilidad permanente hacia el público en general y autoridades pertinentes.
- Mantener la comunicación y coordinación directa con la Dirección de Relaciones Públicas semanalmente, para la actualización de boletines, noticias u otros eventos de intereses que la Institución lleve a cabo mediante cualquiera de sus demás direcciones que la conforman.
- Diseñar, elaborar, corregir entornos del Sitio Web tanto en su forma como en su fondo.
- Desarrollar entornos que interactúen como enlaces a la Intranet local u otros servicios que incluyan la programación personalizada.
- Innovar el uso de nuevas herramientas informáticas que se adapten al Sitio Web de la institución mejorando tiempos de respuesta a los usuarios.

Denominación del Puesto	Asistente Provincial 1
Procesos de trabajo	Redes y comunicaciones
Área Funcional	Dirección de Gestión TIC
Cantidad necesaria	01

MISIÓN: Atender órdenes de trabajo de asistencia técnica generadas por el sistema de HELP DESK (mesa de ayuda) que guarden relación al área de redes y comunicaciones

de voz y de datos (cableado estructurado, mantenimiento de equipos de comunicación, impresoras y copiadoras con red, internet, intranet, correo electrónico, servidores, respaldos de información, cámaras de monitoreo, data center, etc.).

RESPONSABILIDADES PRINCIPALES:

- Atender y cerrar las órdenes de trabajo generadas por el sistema de Gestión de Incidencias (Help Desk/Mesa de ayuda)
- Brindar el servicio de soporte técnico a los usuarios de la institución en el uso de la red y servicios de red.
- Dar soporte técnico a los usuarios en actividades relacionadas al buen funcionamiento de la intranet y del sistema de incidencias.
- Llevar un control del mantenimiento preventivo, correctivo y proactivo de la red local y de los equipos de comunicación.
- Elaborar toda clase de documentos de tramitación general de la unidad donde presta los servicios, buscar información y documentar los trámites administrativos que se realizan en la misma.
- Preparar informes técnicos y dar respuestas a pedidos de personas u organismos públicos o privados; a fin de mantener en custodia la documentación de respaldo de los trámites administrativos realizados en la respectiva unidad de trabajo.

Denominación del Puesto	Analista Provincial 2
Procesos de trabajo	Redes y comunicaciones
Área Funcional	Dirección de Gestión TIC
Cantidad necesaria	01

MISIÓN:

Recibir y atender solicitudes de servicio y asistencia técnica vía telefónica, intranet, correo electrónico, y comunicación escrita o verbal de los usuarios internos y externos, sobre diversos aspectos tecnológicos, proporcionando una solución en línea, o canalizando sus requerimientos a las áreas de especialización técnica para su atención a fin de facilitar el control, registro y suministro de información de datos reales y oportunos, necesarios para el tratamiento de la información de uso interno y externo del GADPE, de acuerdo con las normas legales y procedimientos correspondientes.

RESPONSABILIDADES PRINCIPALES:

- Mantener actualizado el sistema de Gestión de Incidencias.
- Brindar el servicio de soporte remoto a los usuarios de la institución en el uso de aplicaciones y sistemas.
- Dar soporte técnico a los usuarios en actividades relacionadas al buen funcionamiento de la intranet y del sistema de incidencias.
- Llevar un control del mantenimiento preventivo, correctivo y proactivo del equipamiento informático.
- Elaborar toda clase de documentos de tramitación general de la unidad donde presta los servicios, buscar información y documentar los trámites administrativos

que se realizan en la misma; a fin de presentar asistencia secretarial a los directivos de la unidad.

- Elaborar cuadros estadísticos especiales, efectuar liquidaciones, rectificaciones y realizar trámites para pagos por servicios prestados y adquisiciones, control de garantías.
- Preparar informes y dar respuestas a pedidos de personas u organismos públicos o privados; a fin de mantener en custodia la documentación de respaldo de los trámites administrativos realizados en la respectiva unidad de trabajo.
- Orientar a los empleados del Gobierno Provincial, funcionarios y público en general, sobre los trámites administrativos y otros que deben realizar las mismas para la obtención de los servicios o productos que entrega la Dirección de TIC.

ANEXO E

Fichas de observación 1

INSTITUCION:	GOBIERNO AUTONOMO DESCENTRALIZADO DE LA PROVINCIA DE ESMERALDAS	**FICHA N°:**	1
DIRECCION:	BOLIVAR Y 10 DE AGOSTO	**Hora inicial:**	09:40
FECHA:	6/10/2015	**Hora final:**	12:00
OBSERVADOR:	DIANA LISSETTE ANDRADE ESPAÑA		

ASPECTOS	**CALIFICATIVOS**	
	SI	**NO**
¿La infraestructura que procesa y almacena la información está en área segura?		
¿Existe algún control que impida el acceso físico a las instalaciones de la institución de las personas externas?		
¿Existe algún control que impida el acceso físico al data center de personal no autorizado?		
¿El centro de datos se encuentra en un área segura, cerrada, aislada y protegida contra eventos naturales?		
¿La institución cuenta con vigilancia privada?		
¿Cuenta la institución con cámaras de vigilancia?		
¿Dispone el GADPE de alarmas?		
¿Existen medidas de prevención contra incendios?		
¿La institución dispone de medidas de prevención contra altas temperaturas?		
¿Existen protecciones frente a los fallos en la alimentación eléctrica?		

Fichas de observación 2

INSTITUCION:	GOBIERNO AUTONOMO DESCENTRALIZADO DE LA PROVINCIA DE ESMERALDAS	**FICHA N°:**	2
DIRECCION:	BOLIVAR Y 10 DE AGOSTO	**Hora inicial:**	13:00
FECHA:	22/10/2015	**Hora final:**	16:00
OBSERVADOR:	DIANA LISSETTE ANDRADE ESPAÑA		

ASPECTOS	**CALIFICATIVOS**	
	SI	**NO**
¿Existen estabilizadores eléctricos en la red de suministro a los equipos?		
¿Hay seguridad en el cableado del centro de datos frente a daños e intercepciones no deseadas?		
¿Los accesos a los patch panel son restringidos?		
¿Existen controles en la institución para los accesos a los recursos informáticos?		
¿Existen controles si se ingresa algún equipo informático que no sea de la institución?		
¿Los visitantes externos a la institución poseen algún tipo de identificación visible?		
¿Los funcionarios poseen algún tipo de identificación?		
¿Existe algún mecanismo para autenticar usuarios como tarjeta biométrica, voz, etc.?		
¿La institución cuenta con un cronograma de mantenimiento de equipos informáticos?		
¿Se realiza dicho mantenimiento a los equipos informáticos?		

Ficha de observación 3

FECHA:	**HORA:**	**LUGAR:**
OBJETIVO		
FUENTE DE INFORMACION		
DESCRIPCION DE LO OBSERVADO		
OBSERVACIONES ADICIONALES		

ANEXO F

Encuesta a los funcionarios de la institución

PREGUNTAS	SI	NO	DESCRIBA
1.- ¿Conoce usted si en la institución existen políticas de seguridad de la información? Si su respuesta es negativa indique el ¿Por qué'			
2.- ¿Ha recibido alguna información sobre cuáles son las normas y procedimientos relativos a la seguridad de la información? Si su respuesta es negativa indique el ¿Por qué?			
3.- ¿Cumple su contraseña con requisitos mínimos de seguridad como son caracteres alfanuméricos, máximo 8 caracteres, login diferente al password, etc.? ¿Por qué?			
4.- ¿Cree usted que la información dentro de la institución está segura? ¿Por qué?			
5.- ¿Ha recibido usted algún tipo de capacitación para reconocer la criticidad de la información? ¿Por qué?			
6.- ¿Separa usted la información dependiendo de su importancia? ¿Por qué?			
7.- ¿Se le ha hecho conocer si existe en la institución algún procedimiento o manual que ayude al manejo de la información privada o restringida? ¿Por qué?			
8.- ¿Realiza respaldos de su información diariamente en dispositivos de almacenamiento? ¿Por qué?			
9.- ¿Ha insertado un flash memory en su puesto de trabajo? ¿Por qué?			
10.- ¿Alguna vez se le ha perdido algún dispositivo de almacenamiento con información de la institución? ¿Por qué?			
11.- ¿Ha instalado cualquier tipo de programa en su puesto de trabajo? ¿Por qué?			
12.- ¿Ha tratado usted ingresar a documentos o archivos y se le ha denegado el acceso? ¿Por qué?			
13.- ¿Ha ingresado a otras cuentas de usuario? ¿Por qué?			
14.- ¿Se le ha hecho firmar algún acuerdo de confidencialidad en la institución?			
15.- ¿Se le ha comunicado de las vulnerabilidades observadas o sospechadas en la institución? ¿Por qué?			
16.- ¿Se le ha comunicado que bajo ningún motivo usted debe probar estas vulnerabilidades? ¿Por qué?			
17.- ¿Cuándo se instala un nuevo programa lo capacitan para el manejo del mismo? ¿Por qué?			
18.- ¿Se le ha instalado antivirus en su puesto de trabajo? ¿Por qué?			
19.- ¿Ha notificado al departamento de TIC por algún mensaje de erros de alguna aplicación en su computador? ¿Por qué?			
20.- ¿Ha encontrado archivos o información en su computador que no correspondan a su puesto de trabajo?			

ANEXO G: Entrevista realizada a los funcionarios del departamento de TIC

DIRECTOR DE TIC

Dominio: Políticas de Seguridad de la Información.
Control: Orientación de la dirección para la gestión de la seguridad de la información.
Políticas para la seguridad de la información: la institución cuenta con políticas de seguridad de la información pero no se encuentran debidamente documentadas, la evidencia de los documentos físicos lo demuestran. Tampoco sido socializadas con los funcionarios que laboran dentro de la institución. No hay un responsable que se ocupe de elaborar y documentar cuidadosamente y de la manera más idónea dichas políticas, la evidencia que se tiene de esto es por las funciones que se desempeña por cargo según la estructura departamental de TIC.
Revisión de las políticas para la seguridad de la información: se realizan revisiones a las políticas de la seguridad de la información anualmente, pero no todo se modifica, las actualizaciones se hacen si ha existido alguna modificación en las políticas de la institución, no se tiene un control de las veces que se han realizado dichas actualizaciones o modificaciones.

Dominio: Organización de la seguridad de la información.
Control: Organización interna.
Roles y responsabilidades para la seguridad de la información: si existen estos roles y responsabilidades para la seguridad de la información que se encuentran definidos y estructurados en torno al sistema de gestión de seguridad de la información de la institución y cada una de sus competencias varían y cuyo objetivo es velar por la integridad de la información.
Separación de deberes: existe la segregación de funciones en las cuales están claramente establecidos los controles que se hacen; donde cada área hace monitoreo dependiendo de los procesos que tenga a su cargo.
Contacto con las autoridades: si existe un contacto con las autoridades donde se ha tratado disposiciones entorno a la seguridad de la información, ya que existe un protocolo de comunicación con respecto a cualquier evento que se presente ya sea de carácter normal o anormal.
Contactos con grupos de interés especial: el contacto con dichos grupos se realizan parcialmente, son de carácter informal, han existido conversaciones y acercamientos con los jefes departamentales, pero no se encuentran dentro de un plan integral para cada área donde se especifique los controles y las políticas en cuanto al manejo de la información se debe tener.
Seguridad de información en la gestión de proyectos: este objetivo se realiza de forma parcial ya que si a proyectos se refiere son realizados a menor escala en cuanto a desarrollo y planificación, no tienen una estructura determinada, pero se rigen bajo ciertos parámetros informales que no se encuentran documentados, en torno a la seguridad de información de los mismos.
Control: Dispositivos móviles y teletrabajo
Política para dispositivos móviles: poseen una política no documentada en cuanto al acceso a la información a través de los dispositivos móviles desde la red, el cual se encuentra totalmente restringido a los usuarios, según indica el director; solo ciertos servidores según las funciones de su cargo pueden acceder, las seguridades se encuentran debidamente validadas y cada ingreso se encuentra registrado. Por otra parte si los usuarios poseen datos móviles en sus celulares pueden acceder a la intranet la cual

también se encuentra con los controles mismos que validan el usuario que está realizando el acceso, así mismo queda debidamente registrado con cada acceso que realice el usuario.
Teletrabajo: este objetivo de control no se encuentra instituido para todos los departamentos de la institución ya que el departamento de Tecnología de la Información y Comunicación se encuentra realizando pruebas para que luego sea instaurado para los demás departamentos.

Dominio: Relaciones con los proveedores.
Control: Seguridad de la información en las relaciones con los proveedores.
Política de seguridad de la información para las relaciones con los proveedores: con respecto a la información que se comparte con los proveedores se encuentra totalmente limitada a lo que es estrictamente necesario compartir pero esta política existe de manera informal, es decir no hay documentación de la misma como respaldo.
Tratamiento de seguridad dentro de los acuerdos con proveedores: se han firmado acuerdos con todos aquellos proveedores que tienen acceso, almacenan y suministran cualquier recurso informático y sobre el tratamiento de la seguridad de la información,
Cadena de suministro de tecnología de información y comunicación: dentro de los acuerdos se deja también plasmado los riesgos que se podrían tener en este tratamiento de los suministros de tecnologías, se realiza una identificación y monitoreo de los riesgos relacionados con los servicios que prestan terceras partes.
Control: Gestión de la prestación de servicios de proveedores.
Seguimiento y revisión de los servicios de los proveedores: se realiza seguimiento, y se audita a la prestación de servicios de los proveedores, existe documentación sobre el seguimiento realizado
Gestión de cambios en los servicios de los proveedores: no se realiza ningún tipo de gestión sobre los cambios de los proveedores ni se regulan las políticas, ni se realizan mejoras, ya que dichas políticas no se encuentran elaboradas de manera formal.

Dominio: Gestión de incidentes de seguridad de la información.
Control: Gestión de incidentes y mejoras en la seguridad de la información.
Responsabilidades y procedimientos: las responsabilidades y procedimientos son asignadas a cada uno de los funcionarios de la institución, cada usuario es estrictamente responsable sobre la información que maneja, a pesar que no tienen una política documentada sobre esto, pero se encuentran definida en sus funciones.
Reporte de eventos de seguridad de la información: existen reporte de los eventos de seguridad de la información que se han dado dentro de la institución, los usuarios se comunican de forma inmediata con el departamento de TIC si han tenido algún evento fuera de lo normal en cuanto al manejo de la información dentro de sus funciones.
Reporte de debilidades de seguridad de la información: los usuarios de los sistemas de información realizan reportes al departamento de TIC en cuanto a alguna vulnerabilidad observada en los sistemas de información.
Evaluación de eventos de seguridad de la información y decisiones sobre ellos: se realiza la clasificación respectiva de los eventos de seguridad de la información en donde se determina si son incidentes realizando una evaluación de los mismos para poder tomar una decisión, dicho evento y clasificación del mismo queda plasmado en informe elaborado por el responsable de dicha evaluación.
Respuesta a incidentes de seguridad de la información: se da respuestas a los incidentes de seguridad de la información de manera inmediata pero este procedimiento.

Aprendizaje obtenido de los incidentes de seguridad de la información: se adquiere conocimiento sobres estos incidentes los cuales sirven de base para incidentes futuros que se van presentando.
Recolección de evidencia: la única evidencia que se tienen de los incidentes son los informes que hay cuando se realiza la clasificación de los incidentes.

Dominio: Aspectos de seguridad de la información de la gestión de continuidad del negocio.
Control: Continuidad de seguridad de la información.
Planificación de la continuidad de la seguridad de la información: no se ha elaborado un plan en donde existan los requisitos de la seguridad de la información y como se gestiona la misma en casos de crisis.
Implementación de la continuidad de la seguridad de la información: se mantienen los procesos y los procedimientos en situaciones adversas que presenta la institución pero no todas se encuentran documentadas e implementadas.
Verificación, revisión y evaluación de la continuidad de la seguridad de la información: los controles de la seguridad de la información se realizan periódicamente para constatar la efectividad de los mismos.
Control: Redundancias.
Disponibilidad de instalaciones de procesamiento de información: los requisitos de disponibilidad se cumplen en las instalaciones de procesamiento de la información pero de una manera informal.

Dominio: Cumplimiento.
Control: Cumplimiento de requisitos legales y contractuales.
Identificación de la legislación aplicable y de los requisitos contractuales: se verifican las reglamentaciones correspondientes y se actualizan para cada sistema de información en la institución.
Derechos de propiedad intelectual: existen procedimientos que aseguran el uso de software patentado, de manera informal pero no documentado.
Protección de registros: los registros se encuentran debidamente protegidos contra pérdidas, accesos no autorizados y falsificación pero no se tiene un documento donde se encuentre dicha información.
Privacidad y protección de información de datos personales: se garantiza la seguridad de la información de los datos personales de los usuarios de los sistemas de información, solicitando autorización por escrito para manipulación de los mismos; cumpliendo así con las normas de control interno.
Reglamentación de controles criptográficos: no existen controles criptográficos, por ende no hay una reglamentación que rija a los mismos.
Control: Revisiones de seguridad de la información.
Revisión independiente de seguridad de la información: no se realizan revisiones independientes de todos los controles, políticas, procesos y procedimientos en cuanto a la seguridad de la información de la institución sino se la elabora de una manera global.
Cumplimiento con las políticas y normas de seguridad: dentro del departamento de TIC se verifica el cumplimiento de las normas de seguridad de información eventualmente.
Revisión del cumplimiento técnico: los sistemas de información son periódicamente revisados, por el personal del departamento de TIC para encontrar falencias y realizar mejoras en los mismos.

ANALISTA DE DESARROLLO E INTEGRACION DE APLICACIONES

Dominio: Adquisición, desarrollo y mantenimiento de sistemas.
Control: Requisitos de seguridad de los sistemas de información.
Análisis y especificación de requisitos de seguridad de la información: se definen procedimientos que si bien es cierto se realizan para que en la etapa de análisis y diseño del sistema sean incorporados a los requerimientos, pero dichos procedimientos son de carácter informal, se elaboran informes de los mismos y pero poseen un manual de cómo se debe realizar este procesos. Se realizan pruebas con los usuarios en los sistemas de información.
Seguridad de servicios de las aplicaciones en redes públicas: se realiza un control informal sobre estos servicios, no se encuentra documentado.
Protección de transacciones de los servicios de las aplicaciones: existen usuarios con ciertos privilegios según sus funciones que se les ha permitido el acceso a ciertas transacciones en línea que les permite ejecutar sus tareas asignadas, se encuentran con los controles respectivos los cuales evitan algún fraude o malversación de fondos. Existe un informe sobre los registros y los privilegios de estos usuarios.
Control: Seguridad en los procesos de desarrollo y soporte.
Política de desarrollo seguro: no tienen ninguna norma o regla que se aplique para los sistemas y aplicaciones que se desarrollan dentro de la institución.
Procedimiento de control de cambios en sistemas: existen procedimientos informales que se realizan para el control de cambios en los sistemas dentro del ciclo de desarrollo, como son sistemas de control de versiones, se elaboran informes de estos procedimientos.
Revisión técnica de las aplicaciones después de cambios en la plataforma de operación: no tienen un plan o manual de cómo se debe realizar este proceso, pero se lo realiza de manera informal se revisan las aplicaciones cuando se cambian las plataformas de operación y se ponen a prueba para ver si se desarrollan de una forma correcta y que afecte su ejecución en las actividades de la institución.
Restricciones en los cambios a los paquetes de software: se realizan los cambios de software solo si son estrictamente necesarios los cuales son documentados.
Principios de construcción de los sistemas seguros: se mantienen y se aplican dichos principios los cuales son implementados en el desarrollo de cualquier sistema de información.
Ambiente de desarrollo seguro: se protegen de manera adecuada los ambientes de desarrollo seguro identificando requerimientos tanto internos como externos.
Desarrollo contratado externamente: la dirección de TIC realiza una supervisión y seguimiento de los servicios de desarrollo de software que son contratados externamente.
Pruebas de seguridad de sistemas: se realizan las respectivas pruebas de seguridad cuando se desarrollan los sistemas o aplicación antes de ponerlos en ejecución para cerciorarse de funcionalidad en torno a la seguridad que posee el mismo.
Pruebas de aceptación de sistemas: no tienen ningún programa de prueba para la aceptación de sistemas cuando se realizan actualizaciones del software a una nueva versión.
Control: Datos de prueba.

Protección de los datos de prueba: lo datos de pruebas se seleccionan y se controlan de una manera informal, no siguen un plan especifico para realizar este procedimiento.

ASISTENTE DE DESARROLLO E INTEGRACION DE APLICACIONES

Dominio: Seguridad de los recursos humanos.
Control: Antes de asumir el empleo.
Selección: en la etapa de selección del personal no se hace mayor énfasis en cuanto a la confidencialidad de la información, no existen mayores impedimentos o formalismos que cumplir, se les hace conocer de la ética y las leyes relevantes de la institución.
Términos y condiciones del empleo: si existe una cláusula en los contratos donde se establecen responsabilidades, se restringe la extracción de la información, se firman acuerdos de confidencialidad y tratamiento de la información para la seguridad de la misma.
Control: Durante la ejecución del empleo.
Responsabilidades de la dirección: se les comunica a los empleados de manera informal que en los procesos que cada uno realiza apliquen seguridad a la información que manipulan, como la no divulgación de la misma, es decir parámetros superficiales. No existe un mecanismo o documento que brinde mayor información a los servidores públicos que laboran en la institución sobre cuáles son las seguridades exactas que deben aplicarse, como debe ser el tratamiento de la información, la criticidad de la misma etc.
Toma de conciencia, educación y formación en la seguridad de la información: no se realizan capacitaciones a los funcionarios en cuanto a la seguridad de la información se refiere, tienen conocimiento de que la información no puede ser divulgada, pero aun así la información se filtra, no se realizan sesiones de concienciación a los empleados para que se implementen nuevas medidas de seguridad.
Proceso disciplinario: si existe un manual de ética y procedimientos disciplinarios en contra de los funcionarios que incurran en los malos hábitos que afecten a la seguridad de la información.
Control: Terminación y cambio de empleo.
Terminación o cambio de responsabilidades de empleo: informalmente existe una política interna, es decir no se encuentra documentada, donde se da de baja a los usuarios cuyas relaciones laborales han sido culminadas con la institución, así mismo se les asignan nuevos privilegios en el sistema a los funcionarios cuyas responsabilidades han sido cambiadas según la magnitud del proceso al cual han sido encargados

Dominio: Gestión de Activos.
Control: Responsabilidad por los activos.
Inventario de activos: si manejan un inventario físico y digital de los activos debidamente justificados, el mismo que es actualizado según las adquisiciones que se realicen tanto en software como hardware.
Propiedad de los activos: los activos se encuentran concedidos a un propietario y se les ha asignado responsabilidades a los mismos de dichos activos como así también la protección de los mismos. Este objetivo se encuentra debidamente documentado.
Uso aceptable de los activos: no existen regulaciones documentadas para el uso adecuado, abuso, riesgo y procedimientos en caso de incidencias de los activos informáticos.
Devolución de activos: cuando existe una terminación de contrato con un responsable de un activo informático no se procede a la devolución del activo mismo que no es registrado en algún tipo de documentación.
Control: Clasificación de la información.

Clasificación de la información: se clasifica la información según la necesidad de la institución, sus prioridades, el nivel de protección, sensibilidad y criticidad de la misma.
Etiquetado de la información: existen procedimientos para el tratamiento que se le debe dar a la información y el respectivo etiquetado de la misma que se encuentra acorde con la clasificación de la información.
Manejo de activos: existen procedimientos para la manipulación de activos pero los mismos se realizan de forma empírica, los cuales se encuentran estrictamente ligadas a la clasificación de la información y al etiquetado.
Control: Manejo de medios
Gestión de medios removibles: existe una política establecida para la gestión de medios removibles, es decir existe un procedimiento y hay una estandarización para el tratamiento de los medios removibles, depende el criterio del técnico que realiza el proceso.
Disposición de los medios: no existe una política formal de asignación de estos mismos medios pero se documenta la asignación de cada medio removible al propietario.
Transferencia de medios físicos: hay una estandarización para la transferencia de los medios físicos, pero este proceso no se encuentra documentado es decir no se realizan informes al realizar la transferencia de los mismos.

ANALISTA DE SOPORTE E INFRAESTRUCTURA TECOLOGICA

Dominio: Seguridad de las operaciones.
Control: Procedimientos operacionales y responsabilidades.
Procedimientos de operación documentados: hay procedimientos que se encuentran documentados, pero otros que tienen mayor relevancia para los usuarios no se encuentran debidamente documentados, y tampoco han sido socializados con los usuarios.
Gestión de cambios: se realiza el control de los cambios en los medios y también en los sistemas de procesamiento de la información. Los sistemas operacionales y el software de aplicación se encuentran sujetos a un estricto control gerencial del cambio.
Gestión de capacidad: se cubren las necesidades de los recursos informáticos, se controla de manera constante el rendimiento de la infraestructura tecnológica y se gestiona y racionaliza la demanda de los recursos de TI, todo esto se encuentra debidamente documentado, lo que no se desarrolla son planes de capacidad asociados a los niveles de servicio acordado.
Separación de los ambientes de desarrollo, pruebas y operación: los ambientes de desarrollo, pruebas y operación se encuentran debidamente separados evitando riesgos innecesarios en cuanto a cambios o accesos no autorizados.
Control: Protección contra códigos maliciosos.
Controles contra códigos maliciosos: se encuentran implementados los respectivos controles de prevención, detección y reparación de software contra códigos maliciosos, se realizan las revisiones regulares y actualizaciones del software correspondientes para la detección de códigos maliciosos. Los equipos informáticos se encuentran protegidos con el antivirus ESET dentro de una consola de administración principal que se actualiza en cascada, es decir no se actualiza en los computadores mediante el internet, este antivirus demuestra un alto nivel de usabilidad y gran efectividad mantiene protegido los equipos contra virus.
Control: Copias de respaldo.

Respaldo de la información: las copias de respaldo para la seguridad de la información se realizan mensualmente, no existe documentación sobre la misma, no tienen una política definida.
Control: Registro y seguimiento**.**
Registro de eventos: se elaboran y revisan regularmente los eventos importantes que realizan los usuarios del sistema, fallas y eventos de seguridad de la información.
Protección de la información de registro: la información en la institución se encuentra protegida contra alteraciones y acceso no autorizado, procesos que se realizan de manera informal.
Registros del administrador y del operador: se lleva un control de las actividades del administrador y del operador, en donde se registra la hora en que ocurre un evento, que procesos se encuentran involucrados, cual es el administrador y el operador que constan en las fallas y la información del evento.
Sincronización de relojes: no se lleva un control en cuanto a la sincronización de relojes, ya que se ha podido evidenciar que los relojes en todos los sistemas, y en la intranet se encuentran desfasados.
Control: Control de software operacional.
Instalación de software en sistemas operativos: existen políticas para instalación de software en sistemas operativos, mismos que son controlados por parte del personal de tecnología de información y comunicación.
Control: Gestión de la vulnerabilidad técnica.
Gestión de las vulnerabilidades técnicas: se realizan de manera informal, no se lleva un orden sistemático, ni poseen un método determinado, no documentan estas gestiones.
Restricciones sobre la instalación de software: los usuarios tienen prohibido instalar cualquier tipo de software en sus computadores.
Control: Consideraciones sobre auditorias de sistemas de información.
Controles de auditoría de sistemas de información: no existe ningún tipo de control de auditoría de sistemas de información porque no se realizado ninguna de auditoría al departamento de sistemas.

ASISTENTE DE SOPORTE E INFRAESTRUCTURA TECOLOGICA

Dominio: Seguridad Física y del Entorno
Control: Áreas Seguras
Perímetro de seguridad: se manejan restricciones de acceso físico aplicando barreras y controles de entrada, se ha definido un área segura para la infraestructura tecnológica y para la información.
Controles de acceso físico: existen guardias de seguridad ubicados en las partes estratégicas del edificio quienes trabajan las 24 horas del día los 7 días de la semana, son quienes llenan una bitácora según el acceso de las personas que ingresan a la institución, proceden a realizar los respectivos controles si entra o sale algún equipo informático registrándolo con número de serie, modelo y color.
Seguridad en oficinas, recintos e instalaciones: no existe mayor control de acceso a los equipos en algunos departamentos, lo que si hay son cámaras de vigilancia que se encuentra en constante monitoreo.
Protección contra amenazas externas y ambientales: no existe mayor protección física contra las amenazas ambientales como inundación, contra incendios si poseen extintores, y también poseen control térmico contra altas temperaturas.
Trabajo en áreas seguras: no existen procedimientos definidos, formales y documentados para trabajar en áreas seguras.

Áreas de despacho y carga: existe un espacio físico para el despacho y carga acorde para ingresar materiales de diferente naturaleza.
Control: Equipos
Ubicación y protección de los equipos: la ubicación del centro de datos se encuentra en un espacio físico de difícil acceso para el personal no autorizado, en algunas áreas no se protegen los equipos informáticos contra los accesos innecesarios.
Servicios de suministro: los equipos se encuentran protegidos contra fallas de energía e interrupciones eléctricas, existen puntos de red y toma corrientes necesarios para cada equipo en todas las áreas.
Seguridad del cableado: existe un cableado de alto nivel de seguridad, la red principal del edificio se encuentra estructurado con cable de categoría 6 el cual se está implementando poco a poco en los seis pisos de la institución, tres de los seis pisos se encuentran con cableado de categoría 6 y los otros tres con categoría 5.
Mantenimiento de equipos: el mantenimiento de los equipos se realiza cada seis meses ya que de esta manera les permite asegurar la integridad y la disponibilidad de los mismos.
Retiro de activos: no se realizan retiros de equipos si no existe una autorización previa por escrito por parte de la dirección del departamento de tecnología de información y comunicación, dicho proceso se lo realiza de manera formal con su respectivo documento de descargo.
Seguridad de equipos y activos fuera de las instalaciones: no existe una normativa para la utilización de los equipos fuera de las instalaciones, solo se procede con el llenado de la información en las bitácoras de cuál es el equipo que sale de la institución y su respectivo responsable.
Disposición segura o reutilización de equipos: existe un proceso para el retiro o borrado según sea el caso, de cualquier software o información sensible que contengan los medios de almacenamiento de cualquier equipo para ser reutilizado, lo cual no lo tienen documentado pero se realiza de manera informal. Poseen una política de manera informal de reciclaje de equipos, es decir de un equipo que ya no funciona, las partes del mismo que se encuentran en buen estado se lo reutiliza para otro equipo.
Equipos de usuarios desatendidos: no existe ninguna política sobre este objetivo de control, lo único que se logra observar es que si un equipo de usuario se encuentra desatendido después de 30 segundos el mismo procede a bloquearse.
Política de escritorio limpio y pantalla limpia: existe una política que se encuentra en socialización en donde se debe presentar la imagen corporativa de la institución en el escritorio del computador, donde la pantalla también debe encontrarse limpia.

ANALISTA DE REDES Y COMUNICACIONES

Dominio: Seguridad de las comunicaciones
Control: Gestión de seguridad de las redes
Controles de Redes: se realiza un procedimiento en donde se gestiona y se controla las redes pero es un tanto informal ya que solo se realiza la impresión de un informe, pero no existe un plan en donde se detalle el proceso paso a paso y como debe realizarse.
Seguridad de los servicios de red: los controles de los servicios de red se encuentran definidos e implementados, así como también los mecanismos de seguridad, para proteger la información contra el acceso no autorizado.
Separación en las redes: todos los servicios de información, usuarios, y sistemas de información se encuentran divididos en la red, cuya documentación se encuentra actualizada.

Control: Transferencia de información.
Políticas y procedimientos de transferencia de información: existen políticas pero de carácter informal se realizan respaldos del disco duro se transfiere la información a la máquina nueva y luego se formatea la máquina vieja. Pero no existe un manual de cómo se debe realizar el proceso.
Acuerdos sobre transferencia de información: no existe ningún acuerdo sobre la transferencia de información entre la institución y las partes externas.
Mensajería electrónica: se mantiene control sobre la mensajería electrónica como protección contra ataques como virus, protección a los archivos adjuntos y demás controles, pero no se encuentran documentadas estas normas y procedimientos, son de carácter informal.
Acuerdos de confidencialidad o de no divulgación: si tienen acuerdos de confidencialidad que se encuentran debidamente documentados se revisan periódicamente para ser actualizados según las necesidades de la institución.

ASISTENTE DE REDES Y COMUNICACIONES

Dominio: Control de Acceso
Control: Requisitos del negocio
Política del control de acceso: existe una política de control de acceso a la red y a la intranet de la institución pero no se encuentra documentada ni socializada con los usuarios.
Acceso a redes y a servicios en red: el acceso a las redes y los servicios en red se encuentran restringidos según los perfiles de usuarios.
Control: Gestión de accesos a usuarios
Registro y cancelación del registro de usuarios: se posibilita la asignación de accesos usuarios mediante un proceso determinado debidamente documentado donde se identifica el registro pero no hay informes sobre la cancelación del registro de usuarios.
Suministro de acceso de usuarios: para todos los sistemas y servicios se le autoriza y desautoriza los derechos a los usuarios según las funciones de su cargo mediante un proceso informal.
Gestión de derecho de acceso privilegiado: cuando los empleados asumen nuevas responsabilidades se realiza el cambio o cancelación de privilegios según su nuevo rol, no existe un manual o proceso documentado para esta gestión.
Gestión de información de autenticación secreta de usuarios: se realiza la gestión de la información de autenticación secreta mediante un proceso formal, es decir que se encuentra documentado.
Revisión de los derechos de acceso de los usuarios: existe un control de acceso a los datos y sistemas de información, pero este proceso no se encuentra debidamente justificado mediante la documentación correspondiente.
Retiro o ajuste de los derechos de acceso: se dan de baja a los usuarios que ya no tienen ningún tipo de vínculo laboral con la institución, y se reajustan los privilegios de los usuarios si sus responsabilidades han cambiado.
Control: Responsabilidades de los usuarios.
Uso de información de autenticación secreta: se realiza el registro de usuario, y se definen los roles de acceso del usuario según el perfil del usuario, mediante una política interna que no se encuentra documentada, se lo realiza de forma empírica.
Control: Control de acceso a sistemas y aplicaciones.
Restricción de acceso a la información: existe la restricción de acceso a la información tales como el acceso al computador, sistema operativo, sistemas de

información, y aplicaciones en general, así como también el acceso a la información del reloj biométrico.
Procedimiento de ingreso seguro: se mantiene un control eficaz del acceso a los datos y sistemas de información, se lleva un registro de los accesos exitosos y fallidos al sistema.
Sistema de gestión de contraseñas: las contraseñas son de alta calidad y buena encriptación, las mismas que son actualizadas periódicamente por personal del departamento de TIC se lleva un registro de las veces que han sido actualizadas dichas contraseñas.
Uso de programas utilitarios privilegiados: se lleva un control informal de todos los programas utilitarios que podrían tener la capacidad de inutilizar el sistema y las aplicaciones.
Control de acceso a códigos fuente de programas: se realizan los respectivos controles de acceso a códigos fuente de todos los programas que son desarrollado en la institución donde solo el administrador tiene acceso al código fuente de la aplicación.

Dominio: Criptografía
Control: Controles criptográficos.
Política sobre el uso de controles criptográficos: no existen políticas formales e informales sobres este objetivo de control.
Gestión de llaves: no hay evidencia de gestión de claves.

ANEXO H: EVALUACION DEL SGSI DEL GADPE

Dominio: Políticas de Seguridad de la Información						**54,29**
Control: Orientación de la dirección para la gestión de la seguridad de la información						**54,29**
Objetivo de control: Políticas para la seguridad de la información						
Objetivo de control: Revisión de las políticas para la seguridad de la información						
Período :		**DEL**		**AL**		

No.	**Preguntas**							**Evidencias**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	1	2	3	4	5		
		2,9	**5,7**	**8,6**	**11,4**	**14,3**	54,29	
1	¿Existen políticas de seguridad de la información en el Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas?				**X**		11,43	MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION
2	¿Las políticas de seguridad de la información del GADPE se encuentran debidamente documentadas?				**X**		11,43	MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION
3	¿Se han establecido procedimientos de comunicación, difusión y coordinación que permitan dar a conocer las políticas de seguridad de la información a los funcionarios de la institución?		**X**				5,71	NO HAY REGISTROS
4	¿Existe un responsable que se ocupe de documentar las políticas de seguridad de la información?		**X**				5,71	DOCUMENTO DE FUNCIONES POR CARGO DEL DEPARTAMENTO DE TIC
5	¿Se efectúan revisiones periódicas a las políticas de seguridad de la información en el Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas?				**X**		11,43	MANUAL DE POLITICA INSTITUCIONAL
6	¿Se realizan controles para verificar la efectividad de las políticas de seguridad de la información de la institución?		**X**				5,71	NO HAY REGISTROS
7	¿Se lleva un registro ya sea manual o digital de las veces que se han efectuado actualizaciones a las políticas de seguridad de la información?	**X**					2,86	NO HAY REGISTROS

Dominio: Organización de la Seguridad de la Información								**84,00**
Control: Organización Interna								**88,00**
Objetivo de Control: Roles y responsabilidades para la seguridad de la información								
Objetivo de Control: Separación de deberes								
Objetivo de Control: Contacto con las autoridades								
Objetivo de Control: Contacto con grupos de interés especial								
Objetivo de Control: Seguridad de información en la gestión de proyectos								
Período :		**DEL**			**AL**			
No.	**Preguntas**	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	**Evidencias**
	ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	1	2	3	4	5		
		4,0	**8,0**	**12,0**	**16,0**	**20,0**	88,00	
1	¿Las responsabilidades, actividades, procedimientos y roles del personal de tecnologías están claramente definidos y fueron formalmente comunicadas?					**X**	20,00	DOCUMENTACION
2	¿Se encuentran establecidas la respectiva segregación de funciones de los funcionarios de TIC?					**X**	20,00	DOCUMENTACION
3	¿Las políticas de seguridad de la información y procedimientos que permiten organizar apropiadamente el área de tecnología de información, fueron aprobadas formalmente por la máxima autoridad?					**X**	20,00	DOCUMENTACION
4	¿Las responsabilidades, actividades, y roles de los usuarios de los sistemas de información están claramente definidos y fueron formalmente comunicados?				**X**		16,00	DOCUMENTACION
5	¿Los proyectos que son elaborados en la institución tienen una estructura determinada en cuanto a la seguridad de la información que manejan los mismos?			**X**			12,00	DOCUMENTACION

Control: Dispositivos móviles y teletrabajo								**80,00**
Objetivo de Control: Política para dispositivos móviles								
Objetivo de Control: Teletrabajo								
No.	**Preguntas**	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	**Evidencias**
	DISPOSITIVOS MOVILES Y TELETRABAJO	1	2	3	4	5		

		3,3	**6,7**	**10,0**	**13,3**	**16,7**	80,00	
1	¿Existen políticas para acceder a la información de la institución mediante dispositivos móviles?		**X**				6,67	NO HAY DOCUMENTACION
2	¿Cualquier usuario del sistema de información de la institución puede acceder mediante los dispositivos móviles?					**X**	16,67	REPORTES DEL SISTEMA
3	¿Existe un registro del ingreso de los usuarios a la red?					**X**	16,67	REPORTES DEL SISTEMA
4	¿Se validan los ingresos de los usuarios?					**X**	16,67	REPORTES DEL SISTEMA
5	¿Se puede acceder a la intranet mediante el dispositivo móvil?				**X**		13,33	REPORTES DEL SISTEMA
6	¿Se encuentra disponible la función de teletrabajo para todos los funcionarios de la institución?			X			10,00	PRUEBAS TIC

Dominio: Seguridad de los Recursos Humanos								**52,00**
Control: Antes de asumir el empleo								**60,00**
Objetivo de Control: Selección								
Objetivo de Control: Términos y condiciones del empleo								
No.	**Preguntas**	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	**Evidencias**
	ANTES DE ASUMIR EL EMPLEO	1	2	3	4	5		
		10,0	**20,0**	**30,0**	**40,0**	**50,0**	60,00	
1	¿Existen algún tipo de comunicación en la etapa de selección del personal sobre las políticas de seguridad de la información?	**X**					10,00	
2	¿Las funciones, responsabilidades, actividades, y procedimientos del personal a contratar están claramente definidos en su contrato de trabajo y fueron formalmente comunicados?					**X**	50,00	CONTRATO LABORAL

Control: Durante la ejecución del empleo	**44,00**
Objetivo de Control: Responsabilidades de la dirección	
Objetivo de Control: Toma de conciencia, educación y formación en la seguridad de la información	

Objetivo de Control: Proceso disciplinario								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**Evidencias**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	DURANTE LA EJECUCION DEL EMPLEO	1	2	3	4	5		
		4,0	**8,0**	**12,0**	**16,0**	**20,0**	44,00	
1	¿Existe algún mecanismo de difusión por parte del departamento de tecnología, sobre cuáles son las seguridades que deben aplicar a la información que manejan para que la misma no sufra algún tipo de perdida, modificación o manipulación por terceros?		**X**				8,00	
2	¿Se efectúan capacitaciones constantes a los funcionarios sobre cuáles son las medidas de seguridad que deben aplicar a la información que manejan en la institución?	**X**					4,00	
3	¿Existe un plan de capacitación informática que contemple las actividades y eventos de capacitación relacionados con las responsabilidades, funciones o actividades que deben cumplir los servidores de acuerdo a su cargo?	**X**					4,00	
4	¿Se ha realizado supervisiones a los funcionarios sobre las seguridades que aplican a la información que manejan?		**X**				8,00	
5	¿Se efectúa algún proceso disciplinario en contra de los funcionarios que incurran en malos hábitos que atenten en contra de la seguridad de la información?					**X**	20,00	MANUAL DE ETICA Y PROCEDIMIENTOS DEL GADPE

Dominio: Gestión de Activos					**57,71**
Control: Responsabilidad por los activos					**57,14**
Objetivo de Control: Inventario de activos					
Objetivo de Control: Propiedad de los activos					
Objetivo de Control: Uso aceptable de los activos					
Objetivo de Control: Devolución de activos					
Período :		**DEL**		**AL**	

No.	Preguntas							Evidencias
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	RESPONSABILIDAD POR LOS ACTIVOS	1	2	3	4	5		
		2,9	**5,7**	**8,6**	**11,4**	**14,3**	57,14	
1	¿Existe un inventario de activos informáticos del GADPE?					**X**	14,29	INVENTARIO FISICO Y DIGITAL
2	¿Se actualiza el inventario de activos informáticos de la institución?					**X**	14,29	INVENTARIO FISICO Y DIGITAL
3	¿Se les asigna propietarios a los activos informáticos?					**X**	14,29	REGISTROS DIGITALES
4	¿Se les hace conocer formalmente cuales son las responsabilidades del propietario de cada activo informático?		**X**				5,71	
5	¿Manejan algún tipo de regulación para el uso de los activos informáticos?	**X**					2,86	
6	¿Se hace la respectiva devolución de los activos informáticos si el responsable del mismo cambia de función o termina el contrato?	**X**					2,86	
7	¿Se documenta cada devolución de un activo informático?	**X**					2,86	

Control: Clasificación de la información								**56,00**
Objetivo de Control: Clasificación de la información								
Objetivo de Control: Etiquetado de la información								
Objetivo de Control: Manejo de Activos								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**Evidencias**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	CLASIFICACION DE LA INFORMACION	1	2	3	4	5		
		4,0	**8,0**	**12,0**	**16,0**	**20,0**	56,00	
1	¿Existen procedimientos para clasificar la información?			**X**			12,00	REGISTROS DIGITALES
2	¿Existen procedimientos para el etiquetado de la información?			**X**			12,00	REGISTROS DIGITALES
3	¿Existen procedimientos para el manejo de activos?			**X**			12,00	REGISTROS DIGITALES
4	¿Existe alguna regla sobre el manejo de los activos?			**X**			12,00	REGISTROS DIGITALES
5	¿Hay alguna guía a seguir para el manejo de los activos?		**X**				8,00	

Control: Manejo de medios								**60,00**
Objetivo de Control: Gestión de medios removibles								
Objetivo de Control: Disposición de los medios								
Objetivo de Control: Transferencia de medios físicos								
Período :		**DEL**			**AL**			
No.	**Preguntas**	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	**Evidencias**
	MANEJO DE MEDIOS	1	2	3	4	5		
		4,0	**8,0**	**12,0**	**16,0**	**20,0**	60,00	
1	¿Existe una política sobre la gestión de medios removibles?			**X**			12,00	REGISTROS DIGITALES
2	¿Tienen un estándar para elaborar dicho procedimiento?			**X**			12,00	REGISTROS DIGITALES
3	¿Se documenta la asignación de cada medio removible a un propietario?					**X**	20,00	REGISTROS DIGITALES
4	¿Existe algún estándar para la transferencia de los medios físicos?			**X**			12,00	REGISTROS DIGITALES
5	¿Se documenta la transferencia de cada medio físico?	**X**					4,00	

Dominio: Control de Acceso								**54,31**
Control: Requisitos del negocio								**24,44**
Objetivo de Control: Política del control de acceso								
Objetivo de Control: Acceso a redes y a servicios de red								
Período :		**DEL**			**AL**			
No.	**Preguntas**	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	**Evidencias**
	REQUISITOS DEL NEGOCIO	**2,2**	**4,4**	**6,7**	**8,9**	**11,1**	24,44	
1	¿La entidad cuenta con una política de control de acceso a las redes informáticas?				**X**		8,89	ENTREVISTA
2	¿Existe algún mecanismo de difusión a los servidores de la institución de estas políticas?	**X**					2,22	NINGUNA
3	¿Dicha política se encuentra debidamente documentada?	**X**					2,22	NO HAY MANUAL
4	¿El acceso a los recursos de tecnología de información de la institución se encuentra restringido?					**X**	11,11	REGISTRO DE PERFILES DE USUARIO

Control: Gestión de acceso a usuarios					**62,22**
Objetivo de Control: Registro y cancelación de registro de usuario					
Objetivo de Control: Suministro de acceso de usuarios					
Objetivo de Control: Gestión de derechos de acceso privilegiado					
Objetivo de Control: Gestión de información de autenticación secreta de usuarios					
Objetivo de Control: Revisión de los derechos de acceso de los usuarios					
Objetivo de Control: Retiro o ajuste de los derechos de acceso					
Período :		**DEL**		**AL**	

No.	**Preguntas**							**Evidencias**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	GESTION DE ACCESO A USUARIOS	1	2	3	4	5		
		2,2	**4,4**	**6,7**	**8,9**	**11,1**	62,22	
1	¿Existe documentación de los registros que se realizan de cada usuario?					**X**	11,11	REGISTROS DIGITALES
2	¿Se expide un certificado de cancelación de registros de usuario cuando se ha dado por terminada la relación laboral con el funcionario?	**X**					2,22	
3	¿Cuándo un usuario ha cambiado de funciones se daba de baja a ese usuario y se le asigna otro con diferentes privilegios según su cargo?					**X**	11,11	REGISTROS DIGITALES
4	¿Se documenta el proceso de la pregunta 3?	**X**					2,22	
5	¿Se realiza un proceso formal para la gestión de información de autenticación secreta de usuarios?				**X**		8,89	REGISTROS DIGITALES
6	¿El proceso de autenticación de usuario se encuentra documentado?	**X**					2,22	
7	¿Se efectúa un cambio de clave cada cierto periodo de tiempo?					**X**	11,11	REGISTROS DIGITALES
8	¿Se efectúan revisiones periódicas al derecho de acceso de los usuarios?		**X**				4,44	
9	¿Se realiza una revisión periódica de la asignación de los privilegios?				**X**		8,89	REGISTROS DIGITALES

Control: Responsabilidades de los usuarios								**55,00**
Objetivo de Control: Uso de información de autenticación secreta								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**Evidencias**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	RESPONSABILIDADES DE LOS USUARIOS	1	2	3	4	5		
		5,0	**10,0**	**15,0**	**20,0**	**25,0**	55,00	
1	¿Existe una política sobre el uso de información de autenticación secreta?			**X**			15,00	
2	¿Los usuarios poseen contraseñas seguras?					**X**	25,00	REGISTRO DIGITAL
3	¿Se le asigna responsabilidades de seguridad de la información por escrito al funcionario con respecto a su perfil de usuario?		**X**				10,00	
4	¿Se efectúan revisiones periódicas sobre esta política?	**X**					5,00	

Control: Control de acceso a sistemas y aplicaciones								**75,56**
Objetivo de Control: Restricción de acceso a la información								
Objetivo de Control: Procedimientos de ingreso seguro								
Objetivo de Control: Sistema de gestión de contraseña								
Objetivo de Control: Uso de programas utilitarios privilegiados								
Objetivo de Control: Control de acceso a códigos fuente de programas								
No.	**Preguntas**							**Evidencias**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	1	2	3	4	5		
		2,5	**5,0**	**7,5**	**10,0**	**12,5**	75,56	
1	¿Se encuentran aplicados diferentes tipos de restricciones a la información según el perfil de usuario?					**X**	11,11	REGISTROS DIGITALES
2	¿Se controla el acceso seguro de los usuarios al sistema?					**X**	11,11	REGISTROS DIGITALES
3	¿Se lleva un control de cada acceso de los usuarios al sistema?				**X**		8,89	REGISTROS DIGITALES
4	¿Las contraseñas son de alta calidad?					**X**	11,11	

5	¿Las contraseñas son actualizadas periódicamente?					**X**	11,11	REGISTROS DIGITALES
6	¿Se lleva un control de los programas utilitarios?				**X**		8,89	REGISTROS DIGITALES
7	¿Se lleva un control de acceso al código fuente de programas?				**X**		8,89	REGISTROS DIGITALES
8	Haciendo referencia a la pregunta 7 ¿Este control se documenta?		**X**				4,44	

Dominio: Criptografía								**20,00**
Control: Controles criptográficos								**20,00**
Objetivo de Control: Política sobre el uso de controles criptográficos								
Objetivo de Control: Gestión de llaves								
Período :		**DEL**		**AL**				
Norma Técnica aplicada: 410-06								
No.	**Preguntas**	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	**EVIDENCIAS**
	CONTROLES CRIPTOGRAFICOS	**5,0**	**10,0**	**15,0**	**20,0**	**25,0**	20,00	
1	¿Existe una política de uso de las medidas criptográficas para proteger la información?	**X**					5,00	
2	¿El departamento de TIC cuenta con algún tipo de técnica criptográfica como medida de protección de la información?	**X**					5,00	
3	¿Se realiza un gestionamiento de claves criptográficas?	**X**					5,00	
4	¿En la entidad se efectúan controles criptográficos en cada departamento?	**X**					5,00	

Dominio: Seguridad Física y del Entorno	68,45
Control: Áreas Seguras	**70,91**
Objetivo de Control: Perímetro de Seguridad	
Objetivo de Control: Controles de acceso físico	
Objetivo de Control: Seguridad en oficinas, recintos e instalaciones	
Objetivo de Control: Protección contra amenazas externas y ambientales	
Objetivo de Control: Trabajo en áreas seguras	
Objetivo de Control: Áreas de despacho y carga	

Período :		DEL			AL			
No.	**Preguntas**	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	**Evidencias**
	AREAS SEGURAS	**1,8**	**3,6**	**5,5**	**7,3**	**9,1**	70,91	
1	¿Se han definido barreras físicas a áreas restringidas?				**X**		7,27	REGISTROS DE GUARDIANIA
2	¿La infraestructura tecnológica de la institución se encuentra en un área segura?				**X**		7,27	PLANOS DE LA ENTIDAD
3	¿En la entidad existen controles de acceso físico a la misma?				**X**		7,27	FICHAS DE OBSERVACION
4	¿Se lleva un registro de las personas que acceden a la institución?				**X**		7,27	BITACORA-REGISTROS RELOJ BIOMETRICO
5	¿Se documenta el acceso o salida de algún equipo informático?				**X**		7,27	DOCUMENTOS FISICOS
6	¿Existe control en el acceso físico a cada departamento?		**X**				3,64	FICHAS DE OBSERVACION
7	¿Existen cámaras de vigilancia en la institución monitoreadas constantemente?				**X**		7,27	FICHAS DE OBSERVACION
8	¿Hay protección física contra amenazas ambientales?			**X**			5,45	FICHAS DE OBSERVACION
9	¿Poseen control térmico?					**X**	9,09	FICHAS DE OBSERVACION
10	¿Existen procedimientos documentados para trabajar en áreas seguras?	**X**					1,82	
11	¿Poseen área de despacho y carga?				**X**		7,27	FICHAS DE OBSERVACION
Control: Equipos								**66,00**
Objetivo de Control: Ubicación y protección de los equipos								
Objetivo de Control: Servicios de suministro								
Objetivo de Control: Seguridad del cableado								
Objetivo de Control: Mantenimiento de equipos								
Objetivo de Control: Retiro de activos								
Objetivo de Control: Seguridad de equipos y activos fuera de las instalaciones								
Objetivo de Control: Disposición segura o reutilización de equipos								
Objetivo de Control: Equipos de usuarios desatendidos								
Objetivo de Control: Política de escritorio limpio y pantalla limpia								
No.	**Preguntas**	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	**Evidencias**
	EQUIPOS	1	2	3	4	5		
		2,0	**4,0**	**6,0**	**8,0**	**10,0**	66,00	
1	¿En la entidad la ubicación de los equipos				**X**		8,00	FICHAS DE OBSERVACION

	informáticos se encuentra en un área segura?							
2	¿Se protegen los equipos de los accesos de personal no autorizado?		X				4,00	FICHAS DE OBSERVACION
3	¿Existe protección de los equipos contra fallas de energía?					X	10,00	FICHAS DE OBSERVACION
4	¿El cableado que existe es de alto nivel de seguridad?					X	10,00	FICHAS DE OBSERVACION
5	¿Se realiza el mantenimiento de los equipos periódicamente?				X		8,00	REGISTRO DIGITAL
6	¿Cuándo se retiran los activos informáticos se registra algún tipo de documentación para la misma?					X	10,00	DOCUMENTOS FISICOS
7	¿Existe algún tipo de norma o regla para la seguridad de los activos que salen de la institución?		X				4,00	REGISTRO DIGITAL
8	¿Hay algún tipo de normativa para el borrado de información sensible que contengan medios de almacenamiento?	X					2,00	
9	¿Existe alguna normativa para los equipos de los usuarios desatendidos?	X					2,00	
10	¿La entidad cuenta con alguna política de escritorio limpio y pantalla limpia?				X		8,00	FICHAS DE OBSERVACION

Dominio: Seguridad de las operaciones								**57,38**
Control: Procedimientos operacionales y responsabilidades								**60,00**
Objetivo de Control: Procedimientos de operación documentados								
Objetivo de Control: Gestión de cambios								
Objetivo de Control: Gestión de capacidad								
Objetivo de Control: Separación de los ambientes desarrollados, pruebas y operación								
Período :		**DEL**			**AL**			
No.	**Preguntas**	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	**EVIDENCIAS**
	Procedimientos operacionales y responsabilidades	**4,0**	**8,0**	**12,0**	**16,0**	**20,0**	60,00	
1	¿Existe documentación sobre los procedimientos de operación?			X			12,00	DOCUMENTOS FISICOS
2	¿Han sido socializados los procedimientos de operación con el personal de la institución?	X					4,00	ENCUESTAS
3	¿Existe algún tipo de control en la gestión de cambios de los medios de procesamiento de la				X		16,00	REGISTROS DIGITALES

	información?							
4	¿Se controla periódicamente el rendimiento de la infraestructura informática?				**X**		16,00	REGISTROS DIGITALES
5	¿Existe una separación de ambientes de desarrolla, pruebas y operación?			**X**			12,00	REGISTROS DIGITALES
Control: Protección contra códigos maliciosos								**100,00**
Objetivo de Control: Controles contra códigos maliciosos								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**EVIDENCIAS**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	Protección contra códigos maliciosos	1	2	3	4	5		
		5,0	**10,0**	**15,0**	**20,0**	**25,0**	100,00	
1	¿Existe controles de prevención y detección contra códigos maliciosos?					**X**	25,00	REGISTROS DIGITALES
2	¿Se efectúan revisiones regulares para la prevención de código malicioso?					**X**	25,00	REGISTROS DIGITALES
3	¿Se realizan actualizaciones periódicas del software contra código malicioso?					**X**	25,00	REGISTROS DIGITALES
4	¿Los equipos informáticos se encuentran protegidos con antivirus?					**X**	25,00	REGISTROS DIGITALES
Control: Copias de respaldo								**45,00**
Objetivo de Control: Respaldo de información								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**EVIDENCIAS**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	Protección contra códigos maliciosos	1	2	3	4	5		
		6,7	**13,3**	**20,0**	**26,7**	**33,3**	45,00	
1	¿La entidad cuenta con una política definida para las copias de respaldo de la información?		**X**				10,00	
2	¿Se realizan periódicamente copias de respaldo de la información?					**X**	25,00	REGISTROS DIGITALES
3	¿Existe documentación sobre las copias de respaldo?		**X**				10,00	
Control: Registro y seguimiento								**70,00**
Objetivo de Control: Registro de eventos								
Objetivo de Control: Protección de la información								

Objetivo de Control: Registros del administrador y del operador								
Objetivo de Control: Sincronización de relojes								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**EVIDENCIAS**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	Registro y seguimiento	1	2	3	4	5		
		5,0	**10,0**	**15,0**	**20,0**	**25,0**	70,00	
1	¿Se lleva un control de los eventos que se han efectuado en el sistema?				**X**		20,00	REGISTROS DIGITALES
2	¿Existe protección de la información de registro de los usuarios del sistema?				**X**		20,00	REGISTROS DIGITALES
3	¿Se registra las actividades que realizan el administrador y operador del sistema?					**X**	25,00	REGISTROS DIGITALES
4	¿Los relojes de los equipos informáticos se encuentran en la misma hora simultáneamente?	**X**					5,00	FICHAS DE OBSERVACION
Control: Control de software operacional								**60,00**
Objetivo de Control: Instalación de software en sistemas operativos								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**EVIDENCIAS**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	Control de software operacional	1	2	3	4	5		
		6,7	**13,3**	**20,0**	**26,7**	**33,3**	60,00	
1	¿Existen políticas para la instalación de software en sistemas operativos?				**X**		13,33	MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION
2	¿Existe un control para la instalación de software en sistemas operativos?					**X**	33,33	REGISTROS DIGITALES
3	¿Se lleva un registro físico o digital del control que se realiza sobre la instalación de software?		**X**				13,33	
Control: Gestión de vulnerabilidad técnica								**46,67**
Objetivo de Control: Gestión de las vulnerabilidades técnicas								
Objetivo de Control: Restricciones sobre la instalación de software								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**EVIDENCIAS**

		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	Gestión de vulnerabilidad técnica	1	2	3	4	5		
		6,7	**13,3**	**20,0**	**26,7**	**33,3**	46,67	
1	¿Existe alguna política sobre las vulnerabilidades técnicas?	**X**					6,67	
2	¿Se lleva un registro de la gestión de vulnerabilidades del sistema?		**X**				13,33	
3	¿Existe una política sobre la restricción sobre la instalación de software en los puestos de trabajo?				**X**		26,67	REGISTROS DIGITALES
Control: Consideraciones sobre auditorias de sistemas de información								**20,00**
Objetivo de Control: Controles de auditorías de sistemas de información								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**EVIDENCIAS**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	Controles de auditorías de sistemas de información	1	2	3	4	5		
		6,7	**13,3**	**20,0**	**26,7**	**33,3**	20,00	
1	¿Se han efectuado auditorias de los sistemas de información?	**X**					6,67	
2	¿Se lleva un registro de estas auditorías?	**X**					6,67	
3	¿Se tiene documentación física de los controles que se han tomado después de las auditorias?	**X**					6,67	

Dominio: Seguridad de las comunicaciones								**61,50**
Control: Gestión de seguridad de las redes								**55,00**
Objetivo de Control: Controles de redes								
Objetivo de Control: Seguridad de los servicios de red								
Objetivo de Control: Separación en las redes								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**Evidencias**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	Gestión de Seguridad de las redes	**5,0**	**10,0**	**15,0**	**20,0**	**25,0**	55,00	

1	¿Existe una guía o plan en donde se indique cual debería ser el control de las redes?	**X**					5,00	
2	¿Existe documentación sobre el control de las redes?			**X**			15,00	INFORMES
3	¿Se encuentran definidas las características de la red?			**X**			15,00	DOCUMENTACION FISICA
4	¿Se encuentran separadas las redes en el rango determinado y sugerido?				**X**		20,00	DOCUMENTACION FISICA
Control: Transferencia de información								**68,00**
Objetivo de Control: Políticas y procedimientos de transferencia de información								
Objetivo de Control: Acuerdos sobre transferencia de información								
Objetivo de Control: Mensajería electrónica								
Objetivo de Control: Acuerdos de confidencialidad o de no divulgación								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**Evidencias**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	Políticas y procedimientos de transferencia de información	1	2	3	4	5		
		4,0	**8,0**	**12,0**	**16,0**	**20,0**	68,00	
1	¿Existe una política sobre la transferencia de información?			**X**			12,00	
2	¿Existe un manual para elaborar el procedimiento de la transferencia de la información?	**X**					4,00	
3	¿Se tiene un control sobre la mensajería instantánea dentro de la institución?			**X**			12,00	
4	¿Existen acuerdos de confidencialidad de la información?					**X**	20,00	DOCUMENTADOS FISICOS
5	¿Se realizan actualizaciones a dichos acuerdos de confidencialidad de la información?					**X**	20,00	DOCUMENTADOS FISICOS

Dominio: Adquisición, desarrollo y mantenimiento de sistemas								**45,09**
Control: Requisitos de seguridad de los sistemas de información								**76,00**
Objetivo de Control: Análisis y especificación de requisitos de seguridad de la información								
Objetivo de Control: Seguridad de servicios de las aplicaciones en redes publicas								
Objetivo de Control: Protección de transacciones de los servicios de las aplicaciones								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**Evidencias**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	Requisitos de seguridad de los sistemas de información	**4,0**	**8,0**	**12,0**	**16,0**	**20,0**	76,00	
1	¿Existen procedimientos que determinen la etapa de análisis y especificación de los requisitos de seguridad de la información?				**X**		16,00	REGISTROS DIGITALES
2	¿Estos procedimientos son debidamente documentados?	**X**					4,00	
3	¿Se aplica algún tipo de control en los servicios de las aplicaciones en redes públicas?				**X**		16,00	REGISTROS DIGITALES
4	¿Existen controles de las transacciones de los servicios de aplicaciones?					**X**	20,00	REPORTES DEL SISTEMA
5	¿Estos accesos se encuentran registrados?					**X**	20,00	DOCUMENTACION FISICA

Control: Seguridad en los procesos de desarrollo y soporte	**47,27**
Objetivo de Control: Política de desarrollo seguro	
Objetivo de Control: Procedimientos de control de cambios en sistemas	
Objetivo de Control: Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	
Objetivo de Control: Restricciones en los cambios a los paquetes de software	
Objetivo de Control: Principios de construcción e los sistemas seguros	
Objetivo de Control: Ambiente de desarrollo seguro	
Objetivo de Control: Desarrollo contratado externamente	

Objetivo de Control: Pruebas de seguridad de sistemas								
Objetivo de Control: Pruebas de aceptación de sistemas								
Período :		**DEL**			**AL**			
No.	**Preguntas**	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	**Evidencias**
	Seguridad en los procesos de desarrollo y soporte	**1,8**	**3,6**	**5,5**	**7,3**	**9,1**	47,27	
1	¿La entidad cuenta con una política para el desarrollo seguro de software?	**X**					1,82	
2	¿Se consideran requerimientos de seguridad para adquirir o desarrollar un software?				**X**		7,27	DOCUMENTOS FISICOS
3	¿Existe una metodología determinada para desarrollar el software?	**X**					1,82	
4	¿Existen procedimientos de control de cambios en el sistema?			**X**			5,45	REGISTROS DEL SISTEMA
5	¿Estos procedimientos de control de cambios en el sistema se encuentran documentados?	**X**					1,82	
6	¿Existe un manual o plan para el efectuar la revisión técnica de un software desarrollado?		**X**				3,64	
7	¿Se efectúan cambios de software?				**X**		7,27	REGISTROS DEL SISTEMA
8	¿Se documenta cada cambio de software?	**X**					1,82	
9	¿Existe algún protocolo para los aplicativos desarrollados?			**X**			5,45	
10	¿Se efectúan pruebas de seguridad de los sistemas contratados y desarrollados?					**X**	9,09	REGISTROS DEL SISTEMA
11	¿Cuentan con algún software para efectuar las pruebas de aceptación de sistemas?	**X**					1,82	

Control: Datos de prueba							**12,00**
Objetivo de Control: Protección de los datos de prueba							
Período :		**DEL**			**AL**		
No.	**Preguntas**	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	**Evidencias**

	Datos de prueba	6,7	13,3	20,0	26,7	33,3	12,00	
1	¿Existe una política para otorgar los datos de prueba para verificar la efectividad del sistema?	X					4,00	
2	¿La información que es entregada a los desarrolladores se encuentra enmascarada?	X					4,00	
3	¿Se realiza la eliminación de la información de prueba una vez que se haya concluido el procedimiento?	X					4,00	

Dominio: Relaciones con los proveedores							60,00
Control: Seguridad de la información en las relaciones con los proveedores							65,00
Objetivo de Control: Política de seguridad de la información para las relaciones con los proveedores							
Objetivo de Control: Tratamiento de seguridad dentro de los acuerdos con proveedores							
Objetivo de Control: Cadena de suministro de tecnología de información y comunicación							
Período :		DEL			AL		
No.	Preguntas	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	Evidencias
	Seguridad de la información en las relaciones con los proveedores	5,0	10,0	15,0	20,0	25,0	65,00	
1	¿Se han establecidos mecanismos de control en las relaciones con los proveedores?				X		20,00	DOCUMENTOS FISICOS
2	¿Se tiene una política con respecto a la información que se comparte a los proveedores?	X					5,00	
3	¿Se ha generado un modelo base para los acuerdos con los proveedores?				X		20,00	DOCUMENTOS FISICOS
4	¿Se monitorean los riesgos relacionados con los servicios provistos por los proveedores?				X		20,00	DOCUMENTOS FISICOS
Control: Gestión de la prestación de servicios de proveedores							55,00	
Objetivo de Control: Seguimiento y revisión de los servicios de los proveedores								
Objetivo de Control: Gestión de cambios en los servicios de los proveedores								

Período :		DEL			AL			
No.	Preguntas	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	Evidencias
	Gestión de la prestación de servicios de proveedores	**6,7**	**13,3**	**20,0**	**26,7**	**33,3**	55,00	
1	¿Se realiza un monitoreo a la prestación de los servicios que ofrecen los proveedores?					**X**	25,00	REGISTROS DIGITALES
2	¿Se realizan cambios en las políticas de la gestión de servicios de los proveedores?		**X**				10,00	
3	¿Se realiza el cumplimiento de las condiciones determinadas para prestación de servicios?				**X**		20,00	DOCUMENTACION FISICA

Dominio: Gestión de incidentes de seguridad de la información	**77,14**
Control: Gestión de incidentes y mejoras en la seguridad de la información	**77,14**
Objetivo de Control: Responsabilidades y procedimientos	
Objetivo de Control: Reporte de eventos de seguridad de la información	
Objetivo de Control: Reporte de debilidades de seguridad de la información	
Objetivo de Control: Evaluación de eventos de seguridad de la información y decisiones sobre ellos	
Objetivo de Control: Respuesta a incidentes de seguridad de la información	
Objetivo de Control: Aprendizaje obtenido de los incidentes de seguridad de la información	
Objetivo de Control: Recolección de evidencia	

Período :		DEL			AL			
No.	Preguntas	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	Evidencias
	Gestión de incidentes y mejoras en la seguridad de la información	**2,9**	**5,7**	**8,6**	**11,4**	**14,3**	77,14	
1	¿Se encuentran definidos las responsabilidades y procedimientos con respecto a los incidentes de seguridad de la información?				**X**		11,43	DOCUMENTOS FISICOS

2	¿Se realizan reportes en torno a los incidentes que se han presentado en la institución con respecto a la seguridad de la información?				**X**		11,43	DOCUMENTOS FISICOS
3	¿Se realizan evaluaciones de eventos de seguridad de la información?				**X**		11,43	DOCUMENTOS FISICOS
4	¿Se elaboran reportes sobre las evaluaciones realizadas de los eventos de seguridad de la información?			**X**			8,57	DOCUMENTOS FISICOS
5	¿Se asegura una rápida respuesta ante cualquier incidente de la seguridad de la información?				**X**		11,43	DOCUMENTOS FISICOS
6	¿Se lleva un registro de los incidentes que se han presentado con anterioridad?				**X**		11,43	DOCUMENTOS FISICOS
7	¿Existe alguna evidencia de los incidentes de seguridad de la información presentados?				**X**		11,43	DOCUMENTOS FISICOS

Dominio: Aspectos de seguridad de la información de la gestión de continuidad del negocio	**40,00**
Control: Continuidad de la seguridad de la información	**40,00**
Objetivo de Control: Planificación de la continuidad de la seguridad de la información	
Objetivo de Control: Implementación de la continuidad de la seguridad de la información	
Objetivo de Control: Verificación, revisión y evaluación de la continuidad de la seguridad de la información	

Período :		**DEL**		**AL**				
No.	**Preguntas**	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	**Evidencias**
	Continuidad de la seguridad de la información	**5,0**	**10,0**	**15,0**	**20,0**	**25,0**	40,00	
1	¿Se ha elaborado un plan de contingencia en donde se determine que procesos se deban realizar en caso de crisis?		**X**				10,00	
2	¿Se ha realizado un análisis de impacto en caso de que ocurra alguna catástrofe?		**X**				10,00	
3	¿Se han elaborado análisis de riesgos a los que se encuentran sometidos la institución en cuanto a su seguridad de la información?		**X**				10,00	
4	¿Se ha elaborado un plan de recuperación ante desastres para la institución?		**X**				10,00	

Control: Redundancias								**40,00**
Objetivo de Control: Disponibilidad de instalaciones de procesamiento de la información								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**Evidencias**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	Redundancias	1	2	3	4	5		
		6,7	**13,3**	**20,0**	**26,7**	**33,3**	40,00	
1	¿Se garantiza el nivel de disponibilidad requerido para las actividades de la institución?		**X**				13,33	
2	¿Se prueban los sistemas de información redundantes?		**X**				13,33	
3	¿Existe una política definida sobre las redundancias?		**X**				13,33	

Dominio: Cumplimiento								**55,00**
Control: Cumplimiento de requisitos legales y contractuales								**63,33**
Objetivo de Control: Identificación de la legalización aplicable y de los requisitos contractuales								
Objetivo de Control: Derechos de propiedad intelectual								
Objetivo de Control: Protección de registros								
Objetivo de Control: Privacidad y protección de información de datos personales								
Objetivo de Control: Reglamentación de controles criptográficos								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**Evidencias**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	Cumplimiento de requisitos legales y contractuales	**3,3**	**6,7**	**10,0**	**13,3**	**16,7**	63,33	

1	¿Se actualizan los requisitos legales de la entidad con respecto a la seguridad de la información?				**X**		13,33	DOCUMENTOS FISICOS
2	¿Existe un Inventario del software que se ejecuta en la institución?				**X**		13,33	DOCUMENTOS FISICOS
3	¿Se lleva un control, de que todo software que se ejecuta en la institución este debidamente licenciado o en suceso sea software libre?				**X**		13,33	DOCUMENTOS FISICOS
4	¿Se le ha hecho conocer al usuario que es ilegal duplicar software o documentación que se encuentre protegidos por derechos de autor sin la debida autorización del autor?	**X**					3,33	
5	¿Se pide autorización por escrito para manejar los datos de funcionarios, proveedores etc.?					**X**	16,67	DOCUMENTOS FISICOS
6	¿En la entidad existen controles criptográficos?	**X**					3,33	
Control: Revisiones de seguridad de la información								**46,67**
Objetivo de Control: Revisión independiente de seguridad de la información								
Objetivo de Control: Cumplimiento con las políticas y normas de seguridad								
Objetivo de Control: Revisión del cumplimiento técnico								
Período :		**DEL**			**AL**			
No.	**Preguntas**							**Evidencias**
		INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	TOTAL FACTOR	
	Revisiones de seguridad de la información	1	2	3	4	5		
		6,7	**13,3**	**20,0**	**26,7**	**33,3**	46,67	
1	¿Se realiza una revisión de forma independiente a los procesos de la seguridad de la información?		**X**				13,33	
2	¿Se verifica si se cumplen las normas de seguridad de la periódicamente?		**X**				13,33	
3	¿Se realiza un monitoreo de los sistemas de información periódicamente?			**X**			20,00	

ANEXO I: Activos Informáticos del GADPE