PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE ESMERALDAS

ESCUELA:

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

INFORME FINAL DE PROYECTO DE INVESTIGACIÓN

TEMA: EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL DEPARTAMENTO DE TIC DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE ESMERALDAS (GADPE) BASADO EN LA NORMA DE SEGURIDAD ISO 27001.

AUTOR: CEDEÑO TENORIO JONATHAN OSWALDO

LÍNEA DE INVESTIGACIÓN:

GOBIERNO Y ADMINISTRACIÓN DE TECNOLOGÍA DE INFORMACIÓN

ASESORA: ING. SUSANA PATIÑO

MES / AÑO: ENERO DEL 2017

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

_____

PRESIDENTE DEL TRIBUNAL DE GRADUACIÓN.

_____

Ing. Kléber Vera T.

LECTOR 1.

_____

Mgt. David Rodríguez

LECTOR 2.

_____

Ing. Susana Patiño

DIRECTOR DE TESIS.

_____

Mgt. Xavier Quiñonez Ku

DIRECTOR DE ESCUELA.

FECHA:……

AUTORÍA

Yo, Cedeño Tenorio Jonathan Oswaldo, portador de la cédula de ciudadanía Nº 080301105-5, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se ha respetado las diferentes fuentes de información realizando las citas correspondientes.

_____

Cedeño Tenorio Jonathan Oswaldo

AUTOR.

DEDICATORIA

Dedico el trabajo de grado a Dios, a mi madre, a mi padre, familiares y amigos.

A Dios, antes que todo por la vida y bendiciones que me ha dado en el trascurso de la misma.

A mi madre, por ser un puntal fundamental en mi formación profesional y personal.

A mi padre, por sus consejos y esfuerzos para sacarnos adelante dignamente.

A mis familiares, que siempre de una manera u otra han estado conmigo y ha contribuido para la realización de este logro.

A mi asesora, por su tiempo y dedicación para conmigo y mi proyecto.

A mi novia, por su entrega incondicional y su apoyo durante la realización de mi proyecto de grado.

A todos los que han velado por mi desarrollo personal y profesional desde el principio de mi carrera.

AGRADECIMIENTO

Mi agradecimiento es para todas aquellas personas que colaboraron para la finalización de este proyecto.

A mi madre y mi padre que siempre estuvieron presentes con palabras de ánimo y herramientas para mi formación profesional, agradezco también su esfuerzo para brindarme los estudios universitarios.

A la Ing. Susana Patiño, por su apoyo y comprensión al brindarme sugerencias claves para mejorar mi trabajo.

A los lectores que con cada consejo han sido una guía permanente para mejorar mi proyecto y así finalizarlo.

A la Pontificia Universidad Católica del Ecuador Sede Esmeraldas que me ha dado las herramientas para que pueda realizar mi trabajo de grado.

RESUMEN

El presente proyecto de investigación será de gran importancia para el Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas y el departamento de TIC debido a que el principal objetivo es corregir todas las falencias y riesgos encontrados en la seguridad de la información con la aplicación de los controles necesarios para que los errores sean corregidos de manera oportuna.

La adopción de la normativa de seguridad de información ISO 27001 ha sido utilizada a nivel mundial por las empresas más prestigiosas que ven como anualmente grandes cantidades de información son sustraídas sin permiso por piratas informáticos y aplicando la normativa buscan proteger sus activos, principalmente la información que es considera actualmente como el activo más importante dentro de cualquier institución.

Durante el desarrollo del proyecto el principal problema fue encontrar el responsable de cada proceso y activos asignados lo que significa un riesgo alto para cumplir los objetivos de la institución, con la implantación del Sistema de Seguridad de la Información, la institución obtuvo como beneficios la identificación y disminución de los riesgos en los activos de información pertenecientes a la institución, el correcto control e identificación de los procesos de manera que los recursos sean aprovechados de manera óptima manteniendo siempre la disponibilidad, integridad y confidencialidad de la información.

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

ABSTRACT

The present project of investigation will perform great importance for the Autonomous Government Decentralized of the Province of Esmeraldas and the department of TIC due to the fact that the main aim is correct all the failings and risks found in the safety of the information the application the necessary controls in order that the mistakes are corrected in an opportune way.

The adoption of the safety regulation of ISO information 27001 has been used worldwide by the most prestigious companies that they see as anually big quantities of information they are removed without permission by hackers and applying the regulation they seek to protect his assets, principally the information that is considers nowadays as the most important assets inside any institution.

During the development of the project the main problem was found the person in charge of every process and assigned assets what means a high risk to fulfill the aims of the institution, with the implantation of the System of Security of the Information, the institution obtained as benefits the identification and decrease of the risks in the assets of information belonging to the institution, the correct control and identification of the processes so that the resources are taken advantage in an ideal way supporting always the availability, integrity and confidentiality of the information.

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

Contenido

LISTA DE GRÁFICOS

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

INTRODUCCIÓN

Con el pasar del tiempo, se han desarrollado nuevas tecnologías que permiten el trato de la información y se relacionan directamente con los objetivos a cumplir de las instituciones, de la misma manera las amenazas y vulnerabilidades aumentan notablemente transformándose en una gran preocupación para las empresas, por lo que es sumamente necesario proteger los activos y uno de ellos, el más importante, la información, de tal manera que se pueda dar fe de la integridad de la misma, su disponibilidad y confidencialidad con que esta cuenta.

La amenazas a las cuales se enfrenta la información evolucionan de manera que perjudican directamente el correcto desarrollo de la institución: la fuga de información, ataques orquestados por piratas informáticos, mal uso de los recursos de la compañía, falta de capacidad de los empleados, podrían en un instante aparecer y dejar expuesta la información confidencial y logar de esta manera derrumbar la empresa, por lo que es importante que la institución cuente con una táctica que permita la continuidad de las actividades en el tiempo debido.

Una correcta gestión del riesgo es el proceso más óptimo a realizar para salvaguardar la integridad, disponibilidad y confidencialidad de los activos de información y de esta manera lograr identificar de manera precisa los elementos que se encuentran altamente expuestos y corregir de manera oportuna la falla.

Las tareas organizadas en procesos facilitan el funcionamiento de la empresa y ayudan al manejo correcto de los activos asignándolos a sus procesos correspondientes permitiendo así un control sobre el uso que se les está dando y evaluar el desempeño que tienen dentro de la empresa.

De esta manera se plantea recolectar toda la información importante para la implantación exitosa de un Sistema de Gestión de Seguridad de la Información que tiene como base la normativa ISO 27001, y de esta manera asegurar la protección de los activos de información y otorgar un ambiente de tranquilidad al departamento de TIC y

al Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas. Cabe recalcar que la norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

CAPITULO I: MARCO TEÓRICO

1.1 Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas

1.1.1 Ubicación geográfica.

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

1.1.2 Filosofía institucional

a. Visión

El Gobierno Autónomo Descentralizado de la provincia de Esmeraldas se ha propuesto alcanzar la siguiente visión:

> "Hacia el 2.014 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."

(GADPE, 2014); esta sirve como fuente de inspiración para la institución representando así la esencia que guía la iniciativa de cada uno de los trabajadores.

b. Misión

La misión en particular de tan emblemática institución pública de la ciudad de Esmeraldas 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."

(GADPE, 2014); dejando en claro el compromiso de la institución con la comunidad.

c. Objetivos

Los objetivos del Gobierno Autónomo descentralizado de la provincia de Esmeraldas están enfocados al crecimiento, fortalecimiento y mejoramiento de la provincia, y han sido descritos de la siguiente forma:

- Impulsar procesos periódicos de fortalecimiento institucional y de mejoramiento de las capacidades administrativas, financieras y operativas (GADPE, 2014).
- Construir una Agenda Territorial concertada entre Esmeraldas y las tres provincias hermanas de la zona 1 del Ecuador, y con otros actores.
- Liderar y fortalecer los procesos de participación ciudadana y de control social (GADPE, 2014).
- Apoyar un sistema educativo con la calidad necesaria para que sea en realidad un soporte a la preservación cultural, el desarrollo de valores y la creación técnico – científica necesaria en la Provincia (GADPE, 2014).
- Apoyar al Sistema Provincial de Salud que asegure la disminución continua de los indicadores de morbi – mortalidad y el incremento de la esperanza de vida (GADPE, 2014).

d. Plan Estratégico Informático

La Dirección de Tecnologías de la Información está posicionada dentro de la estructura organizacional de la entidad en un nivel que le permite efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participa en la toma de decisiones de la organización y genera cambios de mejora tecnológica. Además garantiza su independencia respecto de las áreas usuarias y asegura la cobertura de servicios a todas las unidades de la entidad u organismo ("Plan Estratégico Informático" GADPE, 2014).

a. Disposiciones Legales

Según la norma de control interno 410-03, establecida por Contraloría: "El Plan Informático Estratégico de Tecnología tendrá un nivel de detalle suficiente para permitir la definición de planes operativos de tecnología de Información y especifica cómo ésta contribuye a los objetivos estratégicos de la organización; incluye un análisis de la situación actual y las propuestas de mejora con la participación de todas las unidades de la organización, se considera la estructura interna, procesos, infraestructura, comunicaciones, aplicaciones y servicios a brindar, así como la definición de estrategias, riesgos, cronogramas, presupuesto de la inversión y operativo, fuentes de financiamiento y los requerimientos legales y regulatorios de ser necesario."

De acuerdo al plan estratégico informático de tecnologías 2012 – 2016, los planes operativos de tecnología de la información que la Dirección de TIC entregue anualmente deben estar alineados con el presente plan estratégico informático, que a su vez está alineado con los objetivos estratégicos de la institución. Según la misma norma citada anteriormente "…estos planes incluirán los portafolios de proyectos y de servicios, la arquitectura y dirección tecnológicas, las estrategias de migración, los aspectos de contingencia de los componentes de la infraestructura y consideraciones relacionadas con la incorporación de nuevas tecnologías de información vigentes a fin de evitar la obsolescencia".

b. Misión de la dirección de TIC

La Dirección de Tecnologías de la Información es una unidad posicionada dentro de la estructura organizacional al más alto nivel, que asesora y apoya a la máxima autoridad y demás direcciones; que participa en la toma de decisiones de la organización; que genera cambios de mejora tecnológica; que garantiza su independencia y asegura la cobertura de servicios a todas las unidades de la entidad. ("Plan Estratégico Informático" GADPE, 2014)

c. Visión de la dirección de TIC

La Dirección de Tecnologías de la Información en el 2014 se posicionará como referente nacional de calidad y mejora continua a través de la implementación del Gobierno Electrónico, creación de valor y conocimiento de la información para las autoridades y funcionarios que tienen que tomar decisiones y apoyar la gestión institucional. ("Plan Estratégico Informático" GADPE, 2014).

1.2 Tecnología de la Información y Comunicaciones (TIC)

1.2.1 Definición

Las TIC, según Gil (2002), constituyen un conjunto de aplicaciones, sistemas, herramientas, técnicas y metodologías asociadas a la digitalización de señales analógicas, sonidos, textos e imágenes, manejables en tiempo real. Por su parte, Ochoa y Cordero (2002), establecen que son un conjunto de procesos y productos derivados de las nuevas herramientas (hardware y software), soportes y canales de comunicación, relacionados con el almacenamiento, procesamiento y la transmisión digitalizada de la información.

Así mismo, Thompson y Strickland, (2004) definen las tecnologías de información y comunicación, como aquellos dispositivos, herramientas, equipos y componentes electrónicos, capaces de manipular información que soportan el desarrollo y crecimiento económico de cualquier organización. Cabe destacar que en ambientes tan complejos

como los que deben enfrentar hoy en día las organizaciones, sólo aquellos que utilicen todos los medios a su alcance, y aprendan a aprovechar las oportunidades del mercado visualizando siempre las amenazas, podrán lograr el objetivo de ser exitosas.

1.2.2 Las tecnologías

Con el paso del tiempo la tecnología ha ido ocupando un puesto privilegiado en el desarrollo de las actividades diarias de cada ser humano, convirtiéndose así para muchas personas en parte fundamental de su vida cotidiana, según Koontz y Weihrich (1998), es la suma total de conocimientos sobre la forma de hacer las cosas, incluyendo inventos, técnicas y el vasto acervo de conocimientos organizados; mientras Gaynor (1999), establece su denominación, en función de un conjunto de medios creados por personas para facilitar el esfuerzo humano. Valdes (2000), la define como un método o procedimiento para efectuar algo.

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

1.2.3 Papel de las TIC en las empresas

Varias son las empresas que han optado por las TIC para enrumbar su camino hacia el éxito e ir creciendo a paso agigantado y cumplir sus objetivos organizacionales. “La mayoría de nuestras instituciones económicas emergieron en un era de relativamente altos costos de comunicación y limitada capacidad computacional. La tecnología de la información tiene el inmenso poder de reducir los costos de coordinación, comunicación y procesamiento de información. Ante esto, no es sorprendente que la reducción masiva en los costos de computación y comunicación haya generado una reestructuración sustancial de la economía.” (Brynjolfsson and Hitt, 2000, pág. 152).

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

Sin embargo, pese a que la inserción de la informática a la empresa es cada vez mayor, su valor en el desarrollo de las actividades productivas ya no depende de las capacidades computacionales sino más bien de la habilidad de los gerentes en vincularla a la invención de nuevos procesos, procedimientos y estructuras de organización. Es decir, la empresa deberá invertir en activos complementarios, tales como capacitación al personal, innovaciones organizacionales, entre otros (Brynjolfsson and Hitt, 1996; 2002; Bresnahan et al, 2002; Giuri et al, 2006).

El motivo por el cual las Pymes enfrentan una brecha digital, no se debe tanto a la falta de acceso a las tecnologías de la información sino a la falta de un conocimiento adecuado, educación y capacitación de los empleados. Como afirman Chen and Wellman (2003) no existe una brecha digital, sino que existen varias brechas digitales. Por lo tanto, es más apropiado usar el concepto en plural-brechas digitales- porque la brecha digital es multifacética entre y dentro de las empresas.

1.3 Adquisición, desarrollo e implementación de sistemas de información.

Para Brys (2005) la implementación de un sistema de información dentro de una organización, cuando el gobierno de las Tic realiza un satisfactorio trabajo los nuevos sistemas es necesario atravesar tres fases:

1.3.1 Enfoque:

Es necesario analizar detenidamente los que se va a realizar en cualquiera que sea el proyecto, inicialmente las cuestiones son como y para que se lo va a utilizar. (Sanchez H. , 2015).

Por lo tanto el análisis de sistemas es el proceso en el cual se examinan los métodos con el propósito de mejorarlos de una manera objetiva, minuciosa y concisa. (Sanchez H. , 2015).

Dentro de la etapa de enfoque es indispensable establecer el propósito de factibilidad que es el que determina que tan factible es o no integrar nuevos procedimientos de procesamiento de datos, o equipos a áreas funcionales seleccionadas, generalmente el proyecto de renovación empieza con el planteamiento de un problema. (Sanchez H. , 2015).

Después de realizar este análisis, entender el propósito de factibilidad, y el impacto del problema, es posible llegar a la conclusión de si el sistema actual tiene solución o es necesaria realizar una inversión para la adquisición del sistema que cumpla con los requisitos planteados. Esta conclusión es analizada por la alta gerencia y comités formados por las distintas áreas, misma que estará pendiente de los procesos de estudio e implementación del sistema. (Sanchez H. , 2015).

1.3.2 Diseño del sistema.

Una vez determinados los objetivos, problemáticas, costes y cualquier situación relacionada con la implementación de un nuevo sistema, y los mismos previamente aprobados por los miembros del comité y la alta gerencia de la organización se debe proceder con la etapa de diseño o adquisición del sistema, hay que tener presente que un sistema no es más que la congregación de muchas partes. (Cabo, 2006).

El diseño implica tomar decisiones para cada una de sus partes y desencadena una serie de procesos entre los cuales tenemos:

1. Determinar las entradas, los archivos y las salidas de información.
2. Diseñar muchas posibilidades de diseño de sistemas a través de un criterio de bloques o modular.
3. Preparar los diagramas de flujo que muestren las relaciones modulares.
4. Seleccionar las alternativas más adecuadas.
5. Comparar los beneficios tangibles e intangibles.
6. Seleccionar el diseño que mejor satisfaga los requisitos.
7. Preparar los diagramas de flujo y las tablas de decisión.

8. Documentar el diseño final para el concurso de proveedores.

Pacheco (2008) sostiene que en las dos primeras etapas se diseña el nuevo sistema y en el resto de etapas, básicamente lo que se trata es de presentar varios métodos para realizar el sistema y es donde intervienen los diagramas de flujos que posteriormente todas las posibles soluciones son analizadas y se toman las más apropiadas, es aquí donde inicia la parte de ingeniería de software.

1.3.3 Implementación.

En esta etapa se involucra la selección de un equipo de trabajo, mismo que tendrá que analizar ciertos criterios para la selección del proveedor.

El criterio más óptimo consiste en presentar a cada uno de los proveedores fabricantes los diagramas de flujo ya analizados en donde constan las especificaciones del nuevo sistema, en esta información se incluye: Información de la organización, planes futuros de procesamiento, y la lista de las especificaciones del sistema. (Pacheco, 2008).

Otro criterio que puede ser tomado, pero no se recomienda ya que se torna algo ilógico puesto que son obviados los datos provistos en las dos primeras fases en las cuales se analizó y determinó los aspectos del sistema y su objetivo, en resumen, la compañía fabricante proveedor deberá llevar su personal a la compañía que requiere del sistemas puesto que tendrán que realizar las fases de análisis y diseño del sistema ya descritas anteriormente.

1.4 Operaciones, mantenimiento y soporte de sistemas de información.

Cuando se desarrollan planes para la estrategia de información, las organizaciones no pueden dejar de considerar que el mantenimiento de sistemas, talvez es considerada la fase más prolongada y costosa del ciclo de vida de los sistemas. Las implicaciones del volumen de trabajo para mantenimiento de los planes de estrategia de información en una organización es un tema que merece atención especial. La estructura de organización necesita flexibilidad para apoyar el mantenimiento de los sistemas existentes concurrentemente con la ejecución de nuevas tecnologías. (Villalobos, 2015).

Cuando se decide hacer mantenimiento lo correcto sería que todos los recursos son destinados para efectuarlo y no debe quedar ninguno para ser utilizado en otras actividades, según Villalobos (2015) esto se lo conoce como barrera de mantenimiento.

El mantenimiento de sistemas, como consecuencia de optimizar costes se lo puede clasificas en cuatro grupos, donde cada uno trasciende en el plan estratégico de información institucional de diferentes maneras. (Villalobos, 2015).

Correctivo: Ajustes necesarios para que las aplicaciones existentes funcionen adecuadamente. Atención de incidentes mediante mesa de servicio, administración de indicadores, seguimiento periódico con el cliente. (Tecnovaplus, 2015).

Adaptativo: Modificaciones que afectan a los entornos en los que el sistema opera, por ejemplo, cambios en la configuración del hardware, software de base, gestores de bases de datos, comunicaciones, etc. (Ugalde, 2010)

Perfectivo: La empresa AESIS (2010) en una publicacion web sostiene que este mantenimiento no estará únicamente enfocado a mejorar técnicamente una solución, sino que también incluye un proceso continuo de optimización a nivel funcional y de procesos. Este mantenimiento hace enfoque en:

- La optimización constante del rendimiento de las aplicaciones mediante análisis técnicos.
- La adaptación de las aplicaciones a las nuevas necesidades del cliente en función de los análisis funcionales.
- La detección de posibles puntos a mejorar en el diseño y uso de las bases de datos mediante el análisis de la base de datos.

Por lo tanto, el principal objetivo del mantenimiento perfectivo es llevar a cabo las tareas y procesos necesarios para identificar aquellos puntos susceptibles de mejora, aportando las soluciones óptimas y haciendo efectivos esos cambios en las aplicaciones. Entre otros, los procesos necesarios que se ponen en marcha para la consecución de estos objetivos son:

- ✓ Aseguramiento del rendimiento óptimo de los servicios del cliente.

- ✓ Análisis de posibles cambios de las necesidades del cliente, para aportar soluciones.
- ✓ Funcionales a sistemas existentes o a nuevos servicios.
- ✓ Análisis pro activo de puntos a mejorar o perfeccionar.

Evolutivo: Para (AESIS, 2010) significa la continuidad de las mejoras sobre cuestiones nuevas a desarrollar, por lo general deseables una vez que el sistema se pone a funcionar. Hay que tener claro que no son mejoras por errores de los proveedores si no oportunidades que se le presentan a los clientes ya que permitirá un sistema actualizado con la tecnología y procesos vigentes.

En pocos términos el mantenimiento se resume en cuatro grandes aspectos:

Gestión de peticiones: En un documento publicado por la versión 3 de ITIL (2014) se manifiesta que la gestión de peticiones, como su nombre indica, es la encargada de atender las peticiones de los usuarios proporcionándoles información y acceso rápido a los servicios estándar de la organización TI.

Es importante aclarar qué se entiende por petición de servicio, un concepto que engloba las solicitudes que los usuarios pueden plantear al departamento de TI:

- ❖ Solicitudes de información o consejo.
- ❖ Peticiones de cambios estándar (por ejemplo cuando el usuario olvida su contraseña y solicita una nueva)
- ❖ Peticiones de acceso a servicios IT.

Comprender el software y los cambios a realizar: Comprende aspectos muy importantes como la compresión del sistema en su totalidad, tener bien claro sus funciones internas como externas, objetivos, estructura y requisitos, así de esta manera se tendrá bien claro al momento de realizar una actualización o modificación el impacto que tendrá.

Modificar el sistema: Una vez previstas las necesidades en el paso anterior es importante enmarcar la modificación y cambio de algunos de los aspectos funcionales

del sistema entre estos podemos tener, equipos, procesos o talento humano involucrado con el sistema

Realizar pruebas: Cuando concluyen los cambios es necesario realizar pruebas con los procesos en los cuales se identificó falencias o en los cuales se ven involucrados la mayoría parte de las modificaciones realizadas al sistema TI.

1.5 Protección de activos de información.

Según Paredes (2013) es importante entender que es un activo de informacion y lo define como un recurso o bien economico propiedad de una empresa con el cual se almacena, procesa o se realiza cualquier actividad relacionada con la información, considerando que activo se relaciona con recurso.

La gestión del riesgo, desde la óptica de la protección de activos, propone un abordaje integral del tema a partir de una profunda compenetración sobre aquellos factores que se consideran más importantes y resaltan las posibilidades de que un riesgo se manifieste. En este contexto, los seguros y la acción de asegurarse constituyen solo una más de las opciones para administrar los riesgos. (Muzio, 2012).

Según Escobar (2011) para iniciar con el proceso de gestión de protección de los activos de información es recomendable cubrir, entre otros, los aspectos siguientes:

- ✓ Mantener actualizado el detalle de los Activos de Información que tiene la organización. Mejor aún si tiene una clasificación de los mismos.
- ✓ Obtener el compromiso y apoyo de la Alta Gerencia.
- ✓ Tener adecuadas políticas, procedimientos relacionados con la seguridad de los activos. Considerando que la información debe estar clasificada como Activo de Información.
- ✓ Concienciación de los usuarios sobre la importancia de la seguridad de la información.
- ✓ Procedimientos para validar el cumplimiento de las regulaciones aplicables, mantenimiento y monitoreo de todos los procesos implementados, incluso considerando un Plan de Seguridad de TI.

1.6 Seguridad de la información

1.6.1 Definición

La Seguridad de la Información (S-I) es algo más que un antivirus, cortafuego o cifrado de datos, la S-I es el resultado de operaciones realizadas por personas y que son soportadas por la tecnología (Álvarez, Pérez, 2004) también se encontró que la Seguridad Informática concierne a la protección de la información que se encuentra en una computadora o en una red de ellas y también a la protección del acceso a todos los recursos del sistema (CYBSEC S.A., 2011).

1.6.2 Planificación

El propósito u objetivo de la planificación de Seguridad es delinear las responsabilidades y comportamiento de todos los individuos que acceden y manipulan el sistema, además de proporcionar una visión general de los requerimientos de seguridad y descripción de los controles necesarios para mantenerla.

Dentro de la planificación de Sistemas se consideran las siguientes acciones:

- Creación del plan de Respuesta a incidentes

  Es de gran importancia la formulación de un plan de respuesta a incidentes, este proporcionará a la institución la minimización de los efectos de una posible intrusión y maximizar la seguridad de la información.

De acuerdo al manual de seguridad del "Red Hat Enterprise" El plan de respuesta a incidentes puede ser dividido en cuatro fases:

- Acción inmediata para detener o minimizar el incidente
- Investigación del incidente
- Restauración de los recursos afectados
- Reporte del incidente a los canales apropiados

Cualquier incidente debe ser detectado con rapidez, lo que es decisivo para evitar cualquiera que fuesen sus consecuencias, e inmediatamente deben ejecutarse las respuestas al incidente que previamente han sido previstas dentro del plan de respuestas.

Dentro de los requerimientos incluidos en el plan de respuestas se tienen, estrategia legal aprobada, soporte del ejecutivo de la institución, soporte financiero, recurso humano, recursos físicos entre otros; todos estos requisitos son el punto de partida para una correcta definición del plan de respuesta a incidentes, en caso de faltar alguno de estos requerimientos resultaría imposible la elaboración de plan, ya que cada uno de estos requerimientos es de gran importancia para la elaboración he implantación del plan.

1.6.3 Manejo de Riesgos

El manejo de riesgos es una clasificación de las alternativas para manejar los riesgos o posibles riesgos a los que está expuesta la información. Esto conlleva a una estructura bien definida, con un manejo y control adecuado, el manejo de riesgos cuenta con técnicas de manejo de riesgos como:

- Evitar
- Reducir
- Retener, Asumir o Aceptar el Riesgo
- Transferir

1.6.4 Proceso de Riesgo Tecnológico.

Por muy buena que sea la planificación de la seguridad resultará inútil si las medidas previstas no se ponen en práctica, así mismo asegurar reducir en un porcentaje considerable todos los riesgos y amenazas a los que se ve expuesta la información es un total desacierto y una imposibilidad, estos riesgos y amenazas pueden ser reducidos y controlados más no eliminados.

Es responsabilidad de la Gestión de Seguridad coordinar la implementación de los protocolos y medidas de seguridad establecidas en la Política y el Plan de Seguridad.

En primer lugar la Gestión de la Seguridad debe verificar que (itilv3.osiatis 2014):

- El personal conoce y acepta las medidas de seguridad establecidas así como sus responsabilidades al respecto.

- Los empleados firmen los acuerdos de confidencialidad correspondientes a su cargo y responsabilidad.
- Se imparte la formación pertinente.

1.6.5 Medios de transmisión de ataques

Los medios de transmisión de ataque son los métodos utilizados por actores que amenazan la seguridad para vulnerarla, encontrando espacios entre sus cerrojos, e ingresar de manera anónima.

Las principales amenazas emergentes para la transmisión de ataque son:

- Spam y Malware propagados por e-mail.
- La creciente propagación de Malware y botnets.
- Los ataques phishing.

La posibilidad de acceder a los recursos de manera remota, actualmente es grande, y una de las principales consecuencias de este hecho es el incremento en los delitos informáticos tales como fraudes informáticos, falsificaciones y venta de información personal.

1.6.6 Actores que amenazan la seguridad.

Como su nombre lo dice, son actores que buscan internarse anónimamente por cualquier medio de transmisión de ataque dentro del sistema para obtener información, y/o causar daños en el sistema, dentro de los actores de este tipo existen:

- Hackers: Son Actores altamente capacitados tecnológicamente, con conocimientos informáticos avanzados cuyas habilidades son la intrusión en sistemas con información cifrada y segura, sus capacidades les proporcionan un alto índice de éxito en sus actividades sin ser descubiertos a tiempo.
- Craker: Este tipo de actor es un gran conocedor de programación de hardware y software, y se dedica a la creación de softwares para vulnerar comunicaciones o el control de computadores de manera remota.

- Lamer: Este es un autor con conocimientos limitados que depende de aplicaciones creadas por hackers o crakers para realizar ataques informáticos.

1.6.7 Tecnologías referentes a la seguridad de la información.

Según la Guía de Políticas de Seguridad (2009) de la Universidad Tecnológica Nacional de Argentina las tecnologías de la información se refieren al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Universidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Entre las principales tecnologías referentes a la seguridad de la información se encuentran:

- Cortafuegos
- Administración de cuentas de Usuario
- Biometría
- Antivirus
- Detección de intrusos
- Prevención de intrusos
- Cifrado
- Firma Digital
- Monitoreo

1.7 Estándares de Seguridad

1.7.1 ISO/IEC 27000

Es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información

utilizable por cualquier tipo de organización, pública o privada, grande o pequeña (Portal ISO-27000).

Sabiendo así que en fase de desarrollo; su fecha de publicación fue Noviembre de 2008. Contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma está previsto que sea gratuita, a diferencia de las demás de la serie, que tendrán un coste (British Standards Institution 2008).

1.7.2 ISO/IEC 27001

ISO 27001 es un conjunto de requisitos para el desarrollo de un sistema de gestión de seguridad de la información. Esta es la norma que tendrá una organización para cumplir con el fin de recibir la certificación ISO 27001. Esta norma tiene varios componentes clave que se requieren con el fin de lograr el cumplimiento. De particular interés para esta discusión son requisito para la política de seguridad y la necesidad de un procedimiento documentado para la evaluación y tratamiento de riesgos.

El cumplimiento o la certificación en la norma ISO 27001 le darán fuertes controles relacionados con las TI, que también le ayudarán a satisfacer las necesidades de muchas de las normas reglamentarias a la institución. La profundidad a la que la norma ISO 27001 puede ayudar a lograr el cumplimiento de otras normas de regulación depende de que los controles correctos se seleccionen y cómo implementar esos controles.

1.7.3 ISO/IEC 27002

La Serie ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) que proporcionan un marco de gestión de la S-I utilizable para cualquier tipo de organización o institución. La serie ISO/IEC 27000 contiene las mejores prácticas recomendadas en S-I para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Esta investigación se basa en una de la norma ISO/IEC 27002, la cual pertenece a la serie ISO 27000 (Portal ISO/IEC 27000, 2008).

La ISO/IEC, llamada anteriormente ISO/IEC 17799, fue publicada en el año 2000 y traducida al español desde el año 2006 (Charles Cresson Wood, 2008), es una guía de buenas prácticas que describe los controles recomendables en cuanto a S-I, esta norma no es certificable y contiene 11 dominios, 39 objetivos de control y 133 controles. Es relevante indicar que para una Institución que no posee ninguna norma de S-I, no es imprescindible implementar todos los objetivos de control de la norma si no los más trascendentales para la misma.

1.7.4 Certificaciones

El número de certificaciones ha aumentado considerablemente en los últimos años como demostración de la relevancia que tiene la protección de la información para el desarrollo de las actividades de las organizaciones y para mantener y desarrollar el tejido industrial de los diferentes países y en todo el mundo.

La certificación de un SGSI es un proceso mediante el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado.

1.8 Análisis de Riesgo Según la Normativa ISO 27001.

El riesgo es la probabilidad de que una amenaza explote una vulnerabilidad y esta se convierta en un desastre. La vulnerabilidad o las amenazas, por separado, no representan un peligro. Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre, sin embargo los riesgos pueden reducirse o manejarse - si se está consciente de las debilidades y vulnerabilidades frente a las amenazas existentes, se pueden tomar medidas para asegurar que las amenazas no se conviertan en desastres.

El análisis de riesgo contempla los siguientes aspectos:

- Tasación de los activos identificados teniendo en consideración los parámetros de confidencialidad, integridad y disponibilidad.
- Identificación de amenazas y vulnerabilidades para cada activo identificado.

- Calculo de que la amenaza explote la vulnerabilidad.
- Ampliación de controles para mitigar los riesgos.

1.9 Inventario de Activos.

La institución posee un gran cantidad de activos los cuales están descritos en el tope o alcance del SGSI, dichos activos son de gran importancia para realizar el correcto análisis de los procesos que tienen ligados y de esta manera aplicar de forma correcta el SGSI, las observaciones, evaluación de riesgo y posteriores acciones que se realicen para mitigar el riesgo depende en gran cantidad de la correcta identificación de estos activos.

Se define a un activo como un bien que posee la institución y tiene una determinada utilidad para los procedimientos comerciales y la prolongación de los servicios prestados. Sabiendo esto es imprescindible que dichos activos que cumplen un rol esencial en toda empresa tengan una seguridad adecuada para que de esta manera se pueda garantizar el correcto funcionamiento de las diferentes operaciones.

De los activos se desprende una parte fundamental, los activos de información que constan de una estructura muy extensa y es transcendental tener bien claro que son los activos de información y que representan, de esta manera con los conceptos claros se puede realizar un estudio satisfactorio y una evaluación de riesgo que permitan la correcta aplicación de la norma ISO 27001.

Es fundamental que dentro del departamento de TIC el proceso de identificación y tasación de activos se haga en conjunto con los principales involucrados en el manejo de los procesos y subprocesos que están previamente establecidos en el alcance del SGSI para esto es vital que los propietarios de los activos estén identificados y notificados cada uno de cuál es su proceso y su activo a tener en cuenta.

Como responsable de proceso y activo se dice de la persona que tiene el compromiso y la capacidad del manejo, uso, seguridad y manteamiento de los activos y procesos a él asignados previamente debe ser aprobada por el director del área al que pertenece, por esta razón dentro del alcance deben dejarse bien en claro los activos de mayor

importancia y luego aplicar el proceso de tasación para saber la determinación que tienen dentro del departamento de TIC y en la situación determinados por los criterios de: disponibilidad, integridad y confidencialidad.

1.10. Amenazas y vulnerabilidades.

La mayor parte del tiempo los activos y activos de información se encuentra vulnerables antes amenazas de todo tipo, dicha amenaza puede ocasionar un suceso o incidente no previsto que afecte de manera significativa los objetivos de la Institución y sus activos de manera directa.

Por estos motivos es muy conveniente que el departamento de TIC inicie la correcta identificación de todas las amenazas que lograsen causar daño directo a los diferentes activos, para facilitar el trabajo es muy conveniente catalogar dichas amenazas por su naturaleza y así de esta manera lograr una fácil ubicación.

En esta clasificación pueden entrar las amenazas naturales que como su nombre lo indica son las ocasionadas por el poder de la naturaleza (inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales.), amenazas a la infraestructura de la institución estas son consideras por el impacto directo que tenga en las instalaciones (fuego, explosión, caída de energía, daño de agua, perdida de acceso, fallas mecánicas).

Amenazas tecnológicas se puede tomar en cuenta, en este apartado las fallas que tienen que ver directamente con los diferentes dispositivos utilizados en los procesos (virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas), amenazas humanas son todas aquellas fallas causadas directamente por el personal ya sea por falta de capacitación o conocimiento en general (huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave), amenazas operacionales son fallas netamente administrativas (crisis financieras, pérdida de proveedores, fallas en equipos, aspectos regulatorios, mala publicidad).

Las fuentes desconocidas o sucesos accidentales son las principales causas de que una amenaza se origine, para que esta amenaza llegue a representar un peligro significativo tiene que explotar una o varias vulnerabilidades de los servicios otorgados por los diferentes procesos en conjunto con los activos.

Las vulnerabilidades se definen como una falencia de seguridad que está asociada netamente con los activos de información del departamento de TIC y de toda la institución, estas vulnerabilidades por sí sola no representan ningún daño para el departe ni la institución pero frente a una amenaza pueden afectar directamente a los activos, de esta manera concluimos que las vulnerabilidades son debilidades de los sistemas de seguridad que pueden ser explotadas.

Al igual que las amenazas las vulnerabilidades se pueden catalogar o clasificar para su mayor comprensión:

Seguridad de los Recursos Humanos, falla en el proceso de contratación, no restringir el uso de recursos, falla en los controles de seguridad, falta de políticas que regulen el uso indebido de los activos y la entrega de estos cuando finaliza el periodo de un empleado estos puntos son vulnerabilidades relacionadas con el Recurso Humano de la empresa.

También es muy frecuente encontrar vulnerabilidades de gran escala en el Control de Acceso, donde se pueden apreciar falencia en el cifrado de las contraseñas, el uso indebido de los celulares para acceder a la red interna de la institución, no tener políticas de control de acceso seguro a la red.

La seguridad física y ambiental, también cumple un papel muy importante y por lo tanto suele tener vulnerabilidades tales como el libre acceso a zonas donde reposa información importante, mala ubicación de servidores en la Institución, descuido de los recursos utilizados por los empleados.

Gestión de operaciones y comunicación, presenta grandes vulnerabilidades puesto que trabajan con el flujo de datos y el tráfico de red que se maneja interna como externamente, las comunicaciones, envió y recepción de mensajes y no tener un control

adecuado que regule la conexión de diferentes dispositivos a la red podría significar la perdida de estos servicios.

1.11. Evaluación y Calculo del Riesgo.

La evaluación del riesgo se realiza basada en parámetros que permitan medir el nivel del riesgo con el que se cuenta (Impacto económico del riesgo, tiempo de recuperación de la Institución, posibilidad real de ocurrencia del riesgo, posibilidad de interrumpir las actividades de la empresa), con estos criterios identificados se debe realizar la evaluación y determinar el grado de impacto que representan las amenazas.

Los niveles deben ser identificados con la evaluación de riesgo estos niveles suelen ser de manera muy común aceptables, por lo tanto son riesgos que representan daños menores y pueden ser aceptados en el día a día de la institución y no se requiere una mayor acción a diferencia de los riesgos cuyo nivel es elevado y representa un gran peligro para la empresa estos deben ser tratados para reducir el impacto.

Para obtener el cálculo de los riesgos se aplican una serie de combinaciones que tienen en cuenta aspectos de los valores de los activos que expresan el impacto de pérdidas basados en confidencialidad, integridad y disponibilidad, teniendo en cuenta la posibilidad de que las amenazas exploten las vulnerabilidades y causen daños.

Los riesgos cuentan con dos características o factores fundamentales para tener mayor precisión al momento de ser calculados las cuales son la probabilidad de que la amenaza explote la vulnerabilidad y el impacto que causaría de materializarse la amenaza, la relación entre estos factores calificados del 1 al 5 arrojaran como resultado el nivel de riesgo el cual puede ser bajo representado con el color verde, medio representado con el color amarillo y alto representado con el color rojo.

1.12. Selección de Controles y objetivos de control.

Con el análisis y evaluación del riesgo terminado, el siguiente paso es preocuparse por las acciones que se van a realizar con los activos que representan un riesgo alto, para lo

cual es necesario que dichos riesgos puedan ser manejados aplicando los controles estipulados por la normativa de la ISO 270001.

La decisión que se tome con el riesgo suele estar sujeta a dos factores fundamentales: el posible impacto si el riesgo se materializa y que tan frecuente puede suceder, dichos factores nos permiten tener una idea clara del daño o perdida que se tiene que considerar si el riesgo ocurriera y no se realizara ninguna acción para mitigarlo.

El tratamiento de riesgo está sujeto a cuatro opciones que pueden ser utilizadas las cuales son, reducir el riesgo y esto se ejecuta con la aplicación de contramedidas o salvaguardas, especificadas en los controles del Anexo A de la norma ISO 27001:2013. Evitar el riesgo esto nos permite modificar las actividades de tal manera que la presencia del riesgo pueda ser evadida, transferir el riesgo esta medida se aplica cuando la Institución no tiene la capacidad ni cuenta con las herramientas necesarias para lidiar con el alto impacto del riesgo así que recurre a otras empresas para solucionar el problema.

Finalmente esta la opción de aceptar el riesgo, esto significa aceptar la presencia del riesgo y trabajar con el debido a que los controles no son efectivos o el costo de mitigar este riesgo es mayor al impacto que puede ocasionar si se llega a materializar la amenaza en este caso de existir la adecuada documentación donde se acepta la responsabilidad de trabajar con el riesgo.

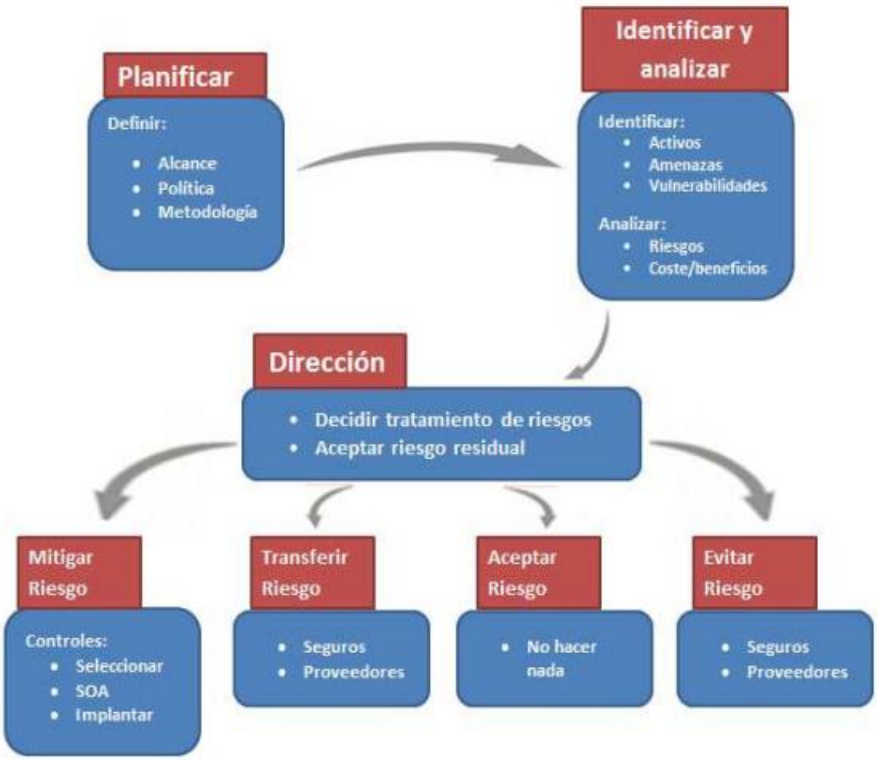

Ilustración 1: Selección de controles y objetivos de control

1.13. CICLO DE DEMING

El ciclo de DEMING se constituye como una de las principales herramientas para lograr la mejora continua en las organizaciones o empresas que desean aplicar a la excelencia en sistemas de calidad (Deming, 2008), el conocido Ciclo Deming o también se le denomina el ciclo PHVA que quiere decir según las iniciales (planear, hacer, verificar y actuar). Señalar que este ciclo fue desarrollado por Walter Shewhart, el cual fue pionero dando origen al concepto tan conocido hoy en día.

La utilidad del ciclo de Deming es ser utilizado para lograr la mejora continua de la calidad dentro de una empresa u organización públicas o privadas. Para describir el ciclo completo, este consiste en una secuencia lógica de cuatro pasos (Shewhart, 2009), los cuales son repetidos y que se deben de llevar a cabo secuencialmente. Estos pasos como ya se mencionó son: Planear, Hacer, Verificar y Actuar. Dónde:

1. Planificar (Plan): Se buscan las actividades susceptibles de mejora y se establecen los objetivos a alcanzar. Para buscar posibles mejoras se pueden realizar grupos de trabajo, escuchar las opiniones de los trabajadores, buscar nuevas tecnologías mejores a las que se están usando ahora, etc.

2. Hacer (Do): Se realizan los cambios para implantar la mejora propuesta. Generalmente conviene hacer una prueba piloto para probar el funcionamiento antes de realizar los cambios a gran escala.

3. Controlar o Verificar (Check): Una vez implantada la mejora, se deja un periodo de prueba para verificar su correcto funcionamiento. Si la mejora no cumple las expectativas iniciales habrá que modificarla para ajustarla a los objetivos esperados.

4. Actuar (Act): Por último, una vez finalizado el periodo de prueba se deben estudiar los resultados y compararlos con el funcionamiento de las actividades antes de haber sido implantada la mejora. Si los resultados son satisfactorios se implantará la mejora de forma definitiva, y si no lo son habrá que decidir si realizar cambios para ajustar los resultados o si desecharla. Una vez terminado el paso 4, se debe volver al primer paso periódicamente para estudiar nuevas mejoras a implantar.

   Vale recalcar que hay varias formas de aplicar los principios de "Planificar, Hacer, Controlar y Actuar" y esta será definida de acuerdo a las necesidades de la institución.

CAPITULO II: DIAGNÓSTICO

2.1 Antecedentes Diagnóstico

Al inicio de este proyecto la situación del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas es la siguiente:

En el departamento de TIC se observaron ciertas falencias en el control y acceso de personas ajenas al trabajo que se desarrolla diariamente.

El personal que labora en el Departamento de TIC tiene como responsabilidad la dirección y gestión de TIC, garantizar el correcto funcionamiento de la infraestructura tecnológica, la correcta gestión de redes y comunicaciones, el desarrollo e integración de sistemas y aplicaciones y finalmente la administración de proyectos y servicios web.

Se observó que la institución no cuenta con la normativa de seguridad ISO 27001 y sus diferentes etapas para la adecuada gestión de la seguridad de la información.

Cuentan con un manual de procesos donde se pudo observar que no están bien establecidos los recursos que se ocupan y el responsable en el área de seguridad de la información, todo se hace empíricamente porque el personal conoce sus obligaciones, esto es desfavorable puesto que una persona ajena al departamento que desee realizar una auditoria o realizar un trabajo con los procesos tendrá complicaciones debido a que no conoce el funcionamiento de los mismos.

La infraestructura tecnológica se encuentra en un estado 100% funcional para que así los trabajadores puedan cumplir con sus funciones diarias de manera rápida y eficaz.

El personal no encuentra inconvenientes en la inclusión de nuevas herramientas y recibir capacitaciones para mejorar el funcionamiento y evitar así sufrir perdida de información o ataques no deseados.

El control de acceso al área de los servidores sirve como soporte para monitorear quienes entran y salen del área, aunque en el departamento es notoria la falta de control riguroso con las personas que entran y salen lo que representa una desventaja porque pueden acceder a información privada sin ser descubiertos.

2.2 Objetivos Diagnóstico

Los objetivos permitieron conocer a fondo la situación actual basándose en información netamente necesaria para el desarrollo del presente proyecto.

1. Identificar la arquitectura organizativa de la seguridad de la Información.
2. Conocer la situación actual de la empresa con respecto a la seguridad de la información.
3. Establecer el nivel de conocimiento del personal en cuanto a seguridad de la información.

2.3 Variables Diagnóstico

- **Información General**: Esta variable recoge toda la información acerca del funcionamiento del departamento de TIC.
- **Conocimientos sobre normativas de seguridad**: Esta variable analiza el nivel actual de conocimiento del personal de TIC sobre normativas de seguridad.
- **Seguridad de la información:** Con esta variable se conocerá si el departamento cuenta con políticas de seguridad, controles de activos y un plan de continuidad de servicios.
- **Controles:** Mediante esta variable quedara claro si el departamento cuenta con los diferentes controles para el correcto trato de la información en todos sus niveles.
- **Normativas:** Con esta variable se pretende conocer si el departamento de TIC cuenta con alguna normativa para el correcto manejo de los activos de información.

2.4 Indicadores Diagnóstico

Información General

- Número de personas de la empresa
- Número de personas en el departamento de TI
- ISO 27001

Conocimiento sobre Normativas de seguridad

- Incidentes generales

Seguridad de la información

- Evaluación de riesgo

Controles

- Controles de procesos
- Controles de personas
- Controles tecnológicos

Normativas

- Políticas de Seguridad.
- Normas de seguridad.

2.5 MATRIZ RELACIÓN DIAGNÓSTICO

OBJETIVOS DIAGNÓSTICOS	VARIABLES	INDICADORES	TÉCNICAS	FUENTES DE INFORMACIÓN
Conocer la situación actual de la empresa con respecto a la seguridad de la información.	Información General. Conocimiento sobre normativas de seguridad.	• Normativa ISO 27001. • Número de personas en el departamento de TI. • Incidentes generales	• Entrevista • Encuesta	• Director del Departamento • Personal del departamento de TIC.
Establecer el nivel de conocimiento respecto a seguridad de la información.	Seguridad de la información Controles	• Evaluación de riesgos • Controles de procesos • Controles de personas • Controles tecnológicos.	• Entrevista	• Analista TIC
Identificar la arquitectura organizativa de la seguridad de la Información.	Normativas	• Políticas de Seguridad • Normas de Seguridad	• Entrevista	• Director del Departamento. • Analista TIC.

Tabla 1: Matriz Diagnóstico

2.6 Mecánica Operativa

La información recolectada, es necesaria para evaluar la situación actual de la institución corresponde al 2015. La población para este proyecto son un total de 9 personas, incluyendo al director del departamento de TIC.

La dirección de TIC está encargada de 4 áreas dentro de la institución, Redes y Comunicaciones, Desarrollo e Integración de Aplicaciones, Soporte e Infraestructura Tecnológica y Proyectos y Servicios Web; en cada una de estas áreas hay un responsable o jefe de área y un ayudante, constituyéndose así que cada área es responsabilidad de dos personas y todas son responsabilidad del director del departamento.

La población total del proyecto es de 9 personas, que corresponden a todo el personal del departamento y sus áreas, por ser la población tan pequeña la muestra es igual a la totalidad de esta, es decir la muestra es igual a 9 personas.

En este proyecto se utilizaron el método descriptivo y el método analítico sintético, que permitieron evaluar los resultados obtenidos y realizar hipótesis basados en los mismos.

Para recolectar información primaria se utilizaron encuestas que serán aplicadas a los trabajadores del departamento de TIC para saber la actividad que desempeñan el funcionamiento del departamento y su nivel de conocimientos en cuanto a normativas de seguridad y entrevistas que se aplicaron al director del departamento y personal en específico que cumpla una labor determinada para obtener información sobre la políticas de seguridad utilizadas en el caso de que cuenten con ellas.

2.7 Tabulación y Análisis de la Información

El departamento de TIC cuenta con personal que realiza cada uno, una tarea específica, de tal forma que las encuestas y entrevistas (revisar anexos 1, 2 y 3) fueron realizadas unas de manera individual y otras de manera colectiva dando un total de 9 personas encuestadas. Las encuestas y entrevistas fueron realizas en el periodo de noviembre del año 2015 hasta agosto del 2016.

La información se tabulo y los resultados son los siguientes:

Encuesta Dirigida al personal que trabaja en el Departamento de TIC.

1. **¿Considera usted que el departamento de TIC tiene el personal suficiente para cumplir eficientemente con su función?**

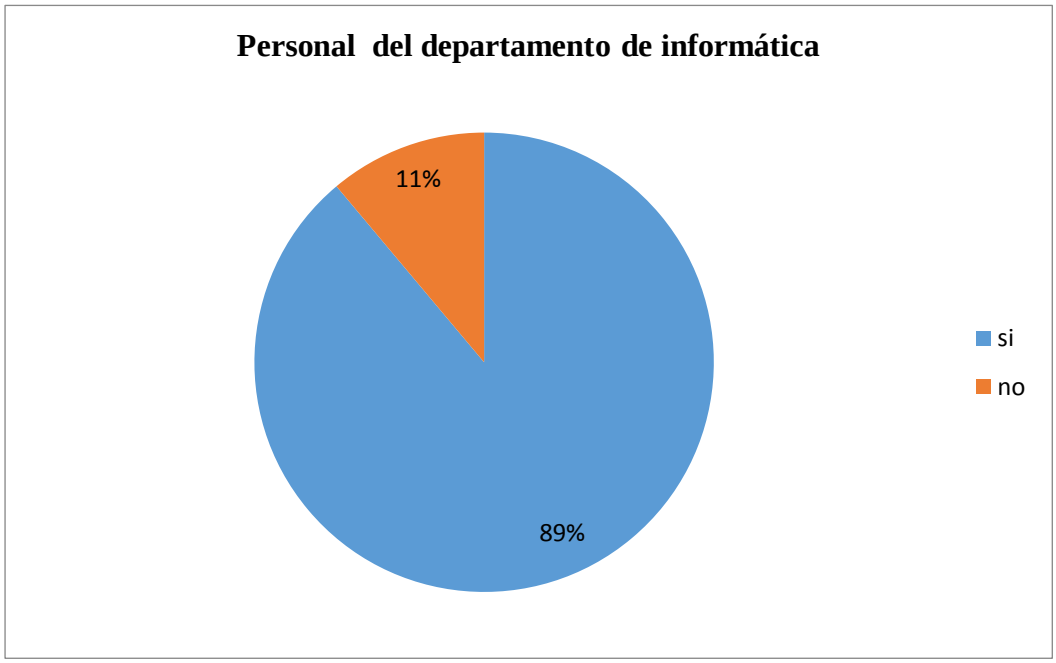

Gráfico 1: Personal del departamento de informática

Análisis:

En el departamento de TIC no cuentan con la cantidad exacta de personal para cubrir todas las necesidades que son requeridas por la institución de manera rápida y eficiente.

2. **¿El departamento de TIC cuenta con la normativa de seguridad ISO 27001?**

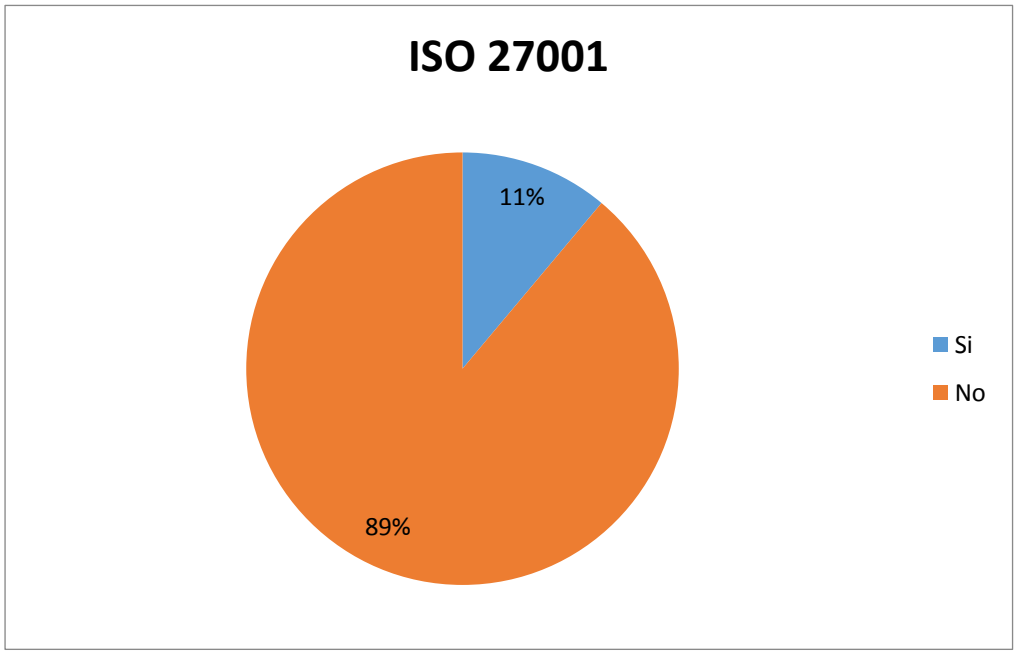

Gráfico 2: ISO 27001

Análisis:

Con estos resultados se corroboro el poco conocimiento que tiene cierto sector del personal acerca de las normativa de seguridad ISO 27001 debido a que la institución no cuenta con la normativa de seguridad.

3. **¿Tienen conocimiento en el departamento de TIC sobre las normativas de seguridad ISO 27001 o COBIT?**

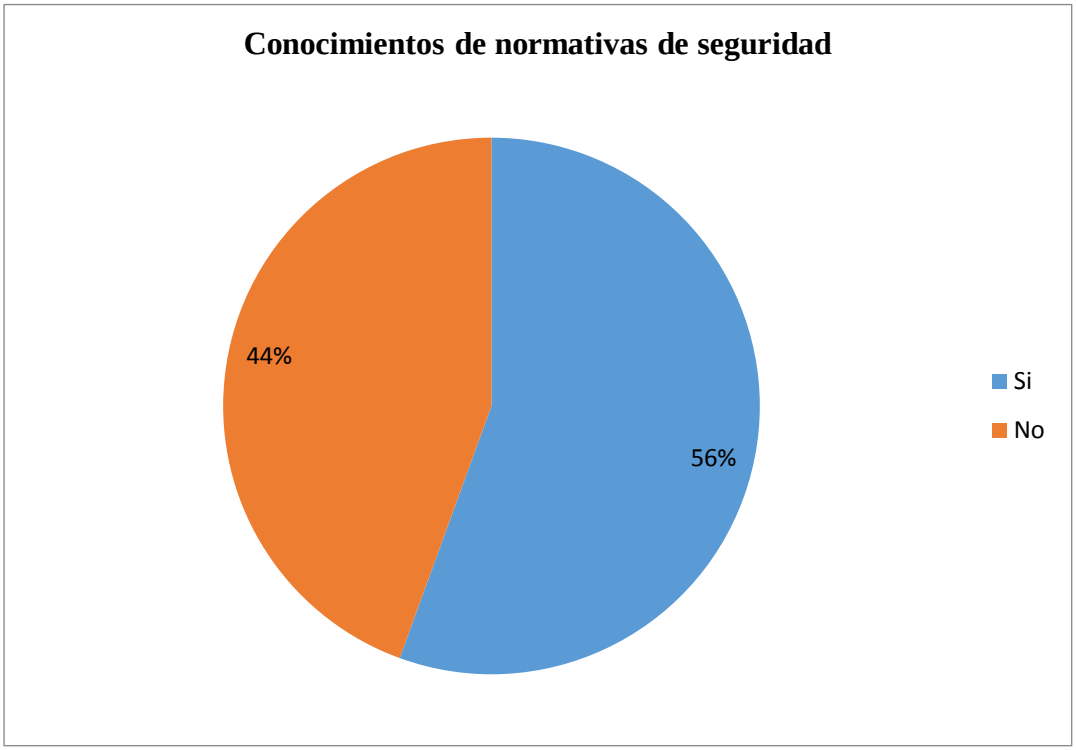

Gráfico 3: Conocimiento de normativas de seguridad

Análisis:

El personal necesita ser capacitado debido a su falta de conocimiento sobre estas normativas de seguridad y la función que desempeñan para el correcto funcionamiento del departamento.

4. **¿Ha sufrido alguna fuga o pérdida de información importante el departamento de TIC?**

Gráfico 4: Fuga o pérdida de información en el departamento de TIC

Análisis:

Según expresaron los encuestados no se ha sufrido fuga alguna de información ni perdida alguna por factores externos o internos. Esto puede deberse a las medidas de seguridad implementadas para el respaldo de información, a su vez el resultado refleja la importancia de credenciales para los usuarios y seguridad en el manejo de la información.

5. **¿Ha sufrido algún ataque de hackers en la institución?**

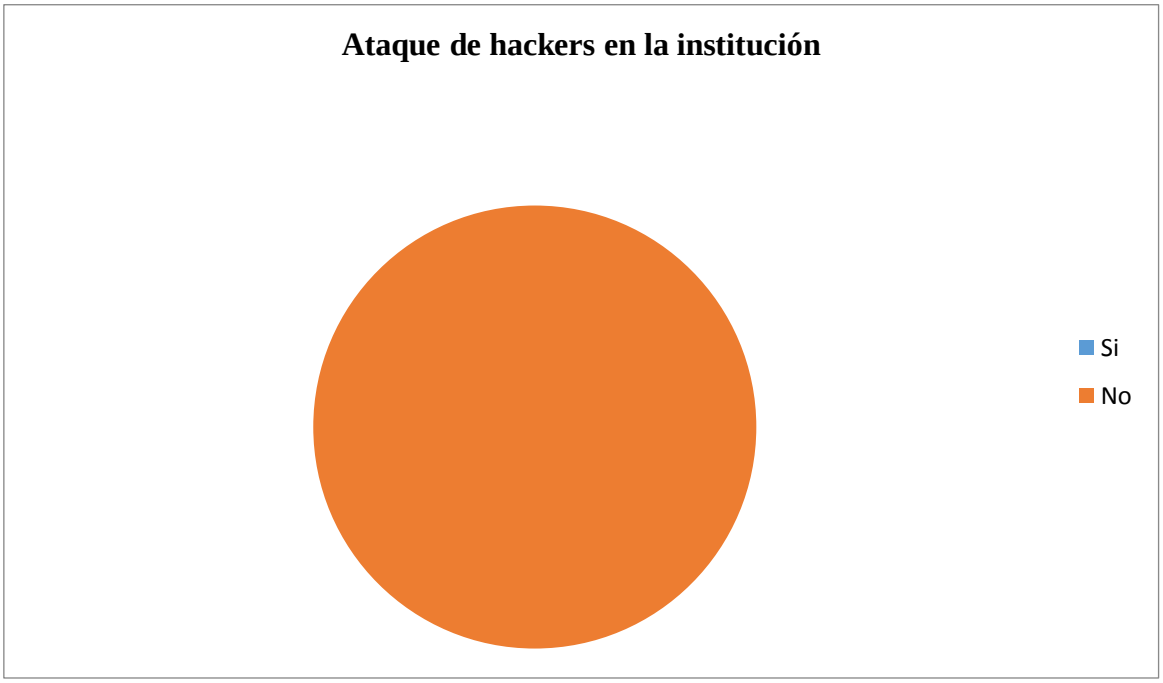

Gráfico 5: Ataque de hackers en la institución

Análisis:

La prácticas utilizadas en la institución parecen ser las indicadas puesto que según los encuestados no se ha sufrido ataques de hackers por lo que su sistemas no ha sido vulnerado, información que no es suficiente para saber si sus sistemas son totalmente seguro.

6. **¿Se han adoptado medidas de seguridad en del departamento de TIC?**

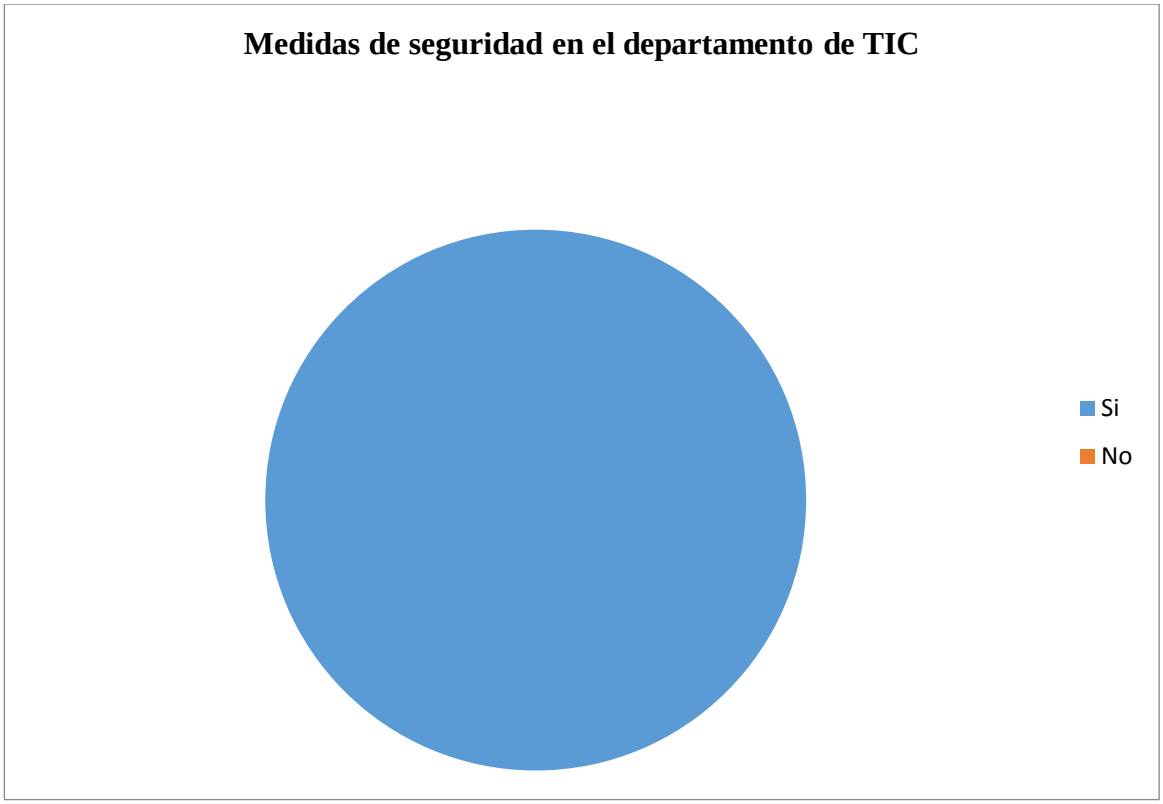

Gráfico 6: Medidas de seguridad en el departamento de TIC

Análisis:

Han sido implantadas medidas de seguridad para proteger los activos, recursos y de esta manera garantizar que las actividades que se realizan entreguen resultados positivos.

7. **¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?**

Gráfico 7: Responsabilidades en el departamento

Análisis:

Las responsabilidades están correctamente divididas entre todo el personal por lo que se facilita el control en la seguridad del departamento y se evitan riesgos innecesarios. Cada quién tiene a su cargo una función específica para que el trabajo que realice el personal sea óptimo.

Entrevista al director del Departamento de TIC.

Análisis:

Por medio de la entrevista queda claro que el departamento de TIC no cuenta con una normativa de seguridad aunque si basa sus procesos en los cuatro dominios del COBIT (Objetivos de Control para la Información y Tecnología Relacionada): **las aplicaciones, la información, la infraestructura y el personal**, esto gracias a que el director de TIC posee conocimientos acerca de estos dominios.

Hasta la actualidad no se han presentado incidentes referentes a fuga de información o ataques de terceras personas, los controles de acceso con los que cuenta el departamento no son del todo seguros debido a que entra personal que no trabaja ahí con frecuencia lo que representa un riesgo considerable.

El centro de datos es una zona restringida a la cual solo tiene acceso el personal que trabaja estrictamente en el departamento de TIC está equipado con tecnología de punta y con los respectivos controles de seguridad por lo que se puede decir que es una de las zonas más seguras de la institución.

Entrevista aplicada al Analista del Departamento de TIC.

Análisis:

El equipamiento tecnológico es de primera línea por lo que los empleados pueden realizar sus actividades de manera correcta sin ningún tipo de interrupción, el equipo recibe el mantenimiento adecuado para asegurar de esta manera la inversión realizada.

El departamento cuenta con una serie de políticas establecidas por el director del departamento y la máxima autoridad de la institución para evitar de cierta manera que se presenten inconvenientes en el desarrollo de las actividades que se realizan diariamente, también cuentan con los procesos definidos donde se da a conocer el funcionamiento interno pero no queda de manera explícita los recursos que se utilizan en el proceso.

Los controles aplicados al personal están ligados a las funciones que desempeñan los recursos que utilizan y el uso que le dan, dentro de estas políticas está contemplado un estudio de factibilidad previo a la adquisición de nueva tecnología, el proceso de contratación de nuevo personal está ligado al departamento de talento humano que aplica los filtros necesarios para no tener problemas en un futuro con los nuevos empleados. Los activos que se utilizan en los diferentes procesos cuentan con un responsable el cual no está debidamente identificado, lo que complica la presencia de informes que sirven para determinar si están siendo explotados al 100% y de una manera correcta.

2.1. F.O.D.A del departamento de TIC del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas.

Fortalezas:

F1: El departamento cuenta con personal profesional y capacitado para cumplir las actividades asignadas.

F2: Software adecuado para el cumplimiento del trabajo.

F3: Equipo informático adecuado

F4: Infraestructura adecuada

F5: Red local y Comunicaciones

Oportunidades

O1: Implementación de nuevos sistemas y tecnologías para aumentar la eficiencia

O2: Mejora de los procesos de Seguridad

O3: Apoyo de la máxima autoridad para generar cambios e innovaciones tecnológicas.

O4: Alto prestigio Institucional

Debilidades

D1: Falta de conocimiento sobre normativas de seguridad

D2: Falta de Sistemas de control de Información

D3: Falta de políticas para el correcto manejo de la información

D4: Costos elevados al aplicar los controles de seguridad apropiados

AMENAZAS:

A1: Ataques tecnológicos

A2: Situación política

A3: Oposición interna al aplicar los controles de seguridad.

2.2. FODA

FACTORES EXTERNOS / FACTORES INTERNOS	**FORTALEZAS:**	**DEBILIDADES:**
	F1: El departamento cuenta con personal profesional y capacitado para las actividades asignadas. **F2:** Software adecuado para el cumplimiento del trabajo. **F3:** Equipo informático adecuado **F4:** Reducción de Riesgos que afecten la disponibilidad, integridad y confiabilidad de la información. **F5:** Uso correcto de los recursos informáticos	**D1:** Falta de conocimiento sobre normativas de seguridad **D2:** Falta de Sistemas de control de Información **D3:** Falta de políticas para el manejo de la información **D4** Costos elevados al aplicar los controles de seguridad apropiados.
OPORTUNIDADES: **O1:** Implementación de nuevos sistemas y tecnologías para aumentar la eficiencia **O2:** Mejora de los procesos de seguridad **O3:** Apoyo de la máxima autoridad para generar cambios e innovaciones tecnológicas. **O4:** Alto prestigio Institucional	**FO1:** Aprovechar las capacidades del personal para mejorar los procesos de seguridad. O2, F1 **FO2:** Agilizar los procesos de manejo seguro de la información O1,F2	**DO1:** Capacitar al personal para mejorar el manejo de la información. O1,D3 **DO2**: Mejorar los procesos de seguridad mediante la aplicación de controles basados en la normativa ISO 27001. O2, D2

AMENAZAS: **A1:** Ataques tecnológicos **A2:** Situación política **A3:** Oposición interna al aplicar los controles de seguridad.	**FA1:** Reducir los riesgos actuales mediante la aplicación de controles de seguridad adecuados. A3,F4 **FA2:** Prevenir los ataques y la perdida de información, al realizar el análisis de riesgo de manera correcta aplicando los recursos informáticos. A1,F5	**DA1:** Aumentar los controles de seguridad de acceso a la información. A1, D2 **DA2:** Crear políticas de manejo de información de acuerdo a los controles sugeridos por la normativa y evitar el robo de la misma. A3, D4

Tabla 2: FODA

2.3.Determinación del problema DIAGNÓSTICO

El departamento de TIC del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas cuenta con un grupo trabajadores que desempeñan diferentes actividades en las cuales se destacan redes, desarrollo e integración de sistemas, proyectos web y soporte de infraestructura.

Cada una estas actividades cuenta con su respectivo control de seguridad, pero cada responsable lo aplica a su manera no está institucionalizado o no existe un proceso ni política de seguridad de la información que permita identificar los controles aplicados.

El problema encontrado es claramente la falta de una Normativa de Seguridad de la Información y la posterior implantación de un Sistema de Gestión de la Seguridad de la Información que evalué los riesgos existentes y brinde correcciones de manera adecuada para el correcto funcionamiento del departamento.

CAPÍTULO III: PROPUESTA

EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL DEPARTAMENTO DE TIC DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE ESMERALDA (GADPE) BASADO EN LA ISO 27001.

3.1 JUSTIFICACIÓN

En la actualidad la información se ha convertido en el activo más valioso de cualquier empresa u organización de tal manera que se invierten fuertes cantidades de dinero para evitar que esta información se sustraída y usada de manera perjudicial.

La Evaluación de la seguridad de la información del departamento de TIC del GADPE permitirá conocer el estado actual de los procesos de seguridad con los que cuenta el departamento para posteriormente aplicar las correcciones necesarias.

La corrección de los procesos que tengan falencias en el departamento de TIC del GADPE fortalecerá la seguridad de la información brindando así un ambiente seguro y procesos más robustos que permitan salvaguardar la integridad, confidencialidad y disponibilidad de la información manejada en el departamento antes mencionado y de esa manera brindar mejores servicios a la Institución.

La Seguridad de la Información aplicada de manera correcta, basada en un estándar de seguridad mundialmente reconocido como lo es la ISO-27001 garantiza el tratamiento correcto y seguro que va desde la información básica y publica, hasta la información más sensible y privada.

Con motivo de beneficiar al personal que labora en el departamento de TIC y a la institución en general se aplicará la Evaluación de la Seguridad de la Información para obtener como resultado la correcta aplicación de los procesos de seguridad.

3.2 OBJETIVOS

3.2.1 OBJETIVO GENERAL

- Evaluar la seguridad de la información del departamento de TIC del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas a través de la identificación de los riesgos tecnológicos para determinar los controles basados en la normativa ISO 27001.

3.2.2 OBJETIVOS ESPECÍFICOS

- Realizar el Análisis de brecha de la organización con respecto a ISO 27001.
- Definir el alcance del SGSI.
- Ejecutar una metodología de evaluación de riesgos.
- Seleccionar los controles de la ISO 27001.

3.3 DESARROLLO

3.3.1. ALCANCE DEL SGSI (SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN).

El Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas cuenta con una Dirección de Tecnologías de Información y Comunicación posicionada dentro de la estructura organizacional al más alto nivel, que asesora y apoya a la máxima autoridad y demás direcciones; que participa en la toma de decisiones de la organización; que genera cambios de mejora tecnológica; que garantiza su independencia y asegura la cobertura de servicios a todas las unidades de la entidad.

El propósito de este instrumento es servir como fuente de consulta en el desarrollo de los procedimientos que describen los pasos a efectuarse de manera secuencial para el logro de sus objetivos y transparentar el actuar institucional en el área de las Tecnologías de la Información y Comunicaciones (TIC).

La dinámica del desarrollo de las TIC hace necesaria la revisión y actualización periódica de los procedimientos que integraron el manual por lo que se realizarán revisiones que permitan mejorarlos y simplificarlos para obtener el óptimo desarrollo de las funciones asignadas al área.

Al aplicar la metodología, se establecen los límites o alcance del SGSI de donde se parte para realizar la investigación correspondiente que tendrá como resultado los procesos críticos de la empresa donde se trabajara con mayor énfasis.

3.3.2 METODOLOGÍA.

3.3.2.1 ANÁLISIS DE BRECHA.

Después de evaluar la tecnología del departamento de TIC con los parámetros estipulados por la normativa ISO-27001 se presenta la necesidad de implementar las correcciones en los

puntos que denotan falencia en el departamento y de esta manera logar fortalecer los procesos de Seguridad de la Información además de cumplir con los requisitos de la normativa.

Dominio	Objetivos	Estado (%)
Politicas de Seguridad	Políticas de Seguridad de Información	75%
Organización de la Seguridad de Información	Organización Interna	80%
	Partes Externas	80%
Manejo de Activos	Responsabilidad de Activos	90%
	Clasificación de Información	85%
Seguridad de Recursos Humanos	Previo al Empleo	100%
	Durante al Empleo	100%
	Terminación o Cambio de empleo	60%
Seguridad Física y Ambiental	Areas Seguras	70%
	Equipamiento de Seguridad	80%
Gestión de Comunicaciones y Operaciones	Procedimientos y Responsabilidades Operativas	80%
	Manejo de Entrega de Servicios Tercerizados	100%
	Planeamiento y Aceptación de Sistemas	80%
	Protección contra Código Malicioso y Móvil	100%
	Copias de Respaldo	75%
	Administración de la Seguridad en la Red	90%
	Manejo de Medios	70%
	Intercambio de Información	70%
	Servicios de Comercio Electrónico	100%
	Monitoreo	50%
Dominio	Objetivos	Estado (%)
Control de Acceso	Requerimientos del Negocio para Control de Acceso	90%
	Administración de Accesos de Usuarios	100%
	Responsabilidades de Usuarios	65%
	Control de Acceso a la Red	100%
	Control de Acceso a Sistemas Operativos	100%
	Control de Acceso a las Aplicaciones y a la Información	100%
	Computación Móvil y Teletrabajo	70%
Desarrollo, Adquisición y Mantenimiento de Sistemas de Inforación	Requerimientos de Seguridad de los Sistemas de Información	80%
	Procesamiento Correcto en las Aplicaciones	70%
	Controles Criptográficos	80%
	Seguridad de los Archivos de Sistemas	90%
	Seguridad en el Desarrollo y Servicios de Soporte	60%
	Gestión de Vulnerabilidades Técnicas	60%
Gestión de Incidentes de Seguridad de Información	Reportando Eventos de Seguridad y Vulnerabilidades	50%
	Gestión de Incidentes de Seguridad de la Información y Proceso de Mejoras	70%
Gestión de la Continuidad del Negocio	Aspectos de Seguridad en la Gestión de la Continuidad del Negocio	80%
Cumplimiento	Cumplimiento con Requerimientos Legales	100%
	Cumplimiento con las Políticas, Estándares y Regulaciones Técnicas	100%
	Consideraciones de Auditoría de Sistemas	60%

Ilustración 2: Análisis de brecha (fuente propia del autor, 2016)

3.3.2.2. IDENTIFICACIÓN DE LOS PROCESOS CLAVES DEL DEPARTAMENTO

La ISO 27001 ofrece la adopción de un enfoque basado en procesos para todas las fases del Sistema de Gestión de Seguridad de la Información permitiendo así la identificación de actividades sistemáticas que tienen interacción de manera directa con los procesos de tal manera que se permita identificar los procesos vitales de un departamento o empresa.

Para mantener la misma línea del Estándar, el departamento de TIC de no poseer todavía sus actividades organizadas en procesos deben hacerlo, un proceso es una actividad o conjunto de actividades que utiliza los recursos disponibles para transformar elementos de entradas en resultados, generalmente toda salida o resultado de un proceso se transforma automáticamente en la entrada a otro proceso.

Los procesos para ejecutarse y cumplir con su objetivo utilizan los recursos disponibles dichos recursos pueden ser: personas, dispositivos tecnológicos, dinero, parte de las instalaciones, etc. Cada procedimiento muestra el método y recursos que utiliza para cumplir con su actividad asignada.

Los procesos pueden ser presentados en tres grupos: de soporte, operativos y estratégicos. Lo procesos de soporte facilitan la ejecución de las actividades que integran los procesos operativos, y generan valor añadido tanto al cliente interno como externo, los procesos operativos se orienta a la prestación de servicios y aportan valor añadido al cliente externo, es decir, a los ciudadanos, organizaciones o sociedad en general son considerados como la columna vertebral de un departamento o de la propia institución finalmente los procesos estratégicos no se relacionan directamente con el cliente pero ayudan a mantener la organización y especificar puntos esenciales.

Luego de aplicar la metodología correspondiente se lograron identificar los procesos críticos del departamento de TIC teniendo como parámetros una serie de preguntas que son evaluadas por puntajes del 1 al 5 luego de tabular los datos el proceso puede ser catalogado como (Critico, Importante, Criticidad-Maja, Criticidad-Baja, Proceso Criticidad-muy-Baja), los cuales son descritos a continuación:

a) **COMPETENCIA TECNOLÓGICA**

- **Objetivo.**

Asesorar, administrar, gestionar recursos y proveer soluciones en el área tecnológica, así como, preparar los reportes sobre la situación y el avance programático con el fin de que se conozca el estado que guardan los diferentes proyectos.

- **Esquema del proceso**

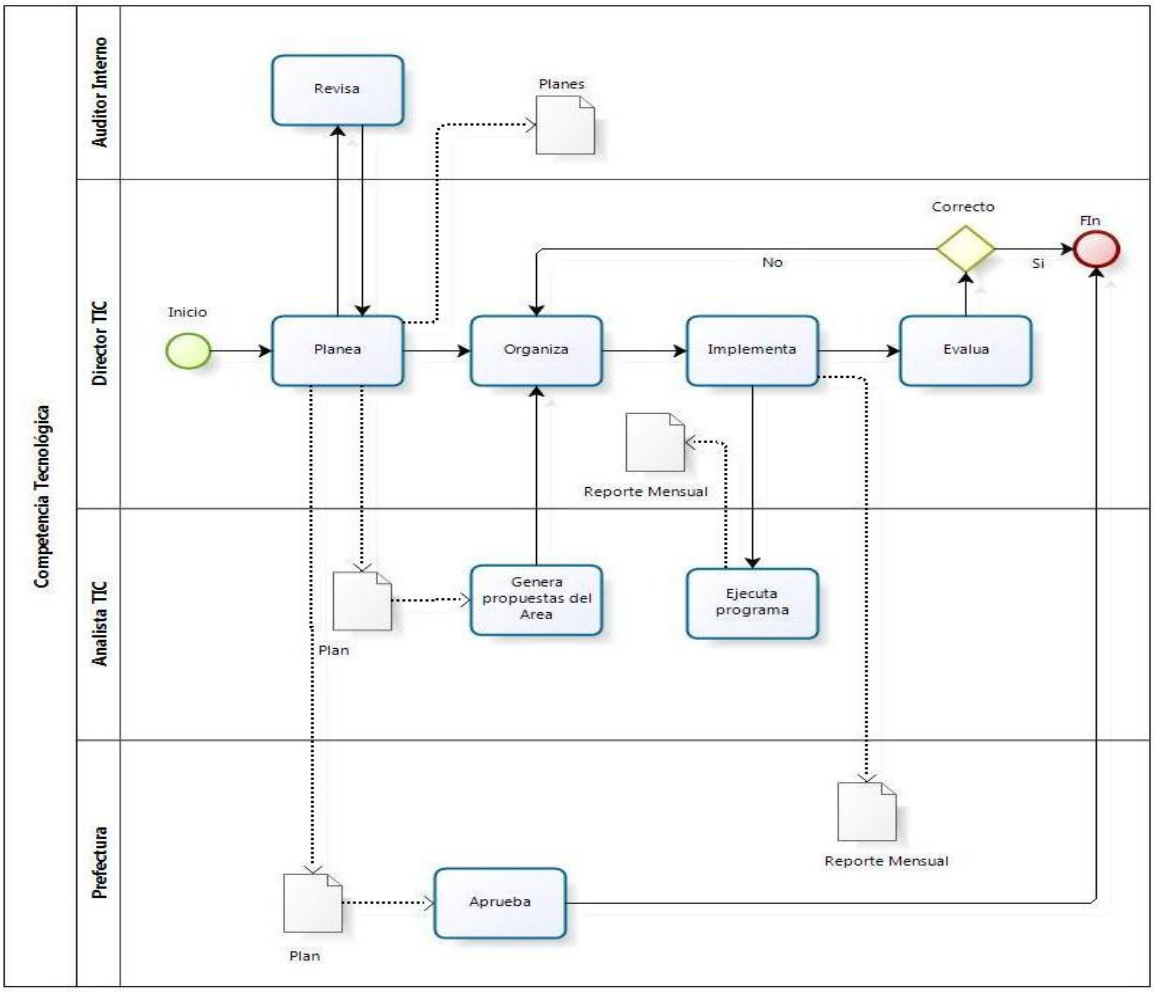

Ilustración 3: Esquema del proceso de Competencia Tecnológica (GADPE, 2014)

b) MODELO DE INFORMACIÓN ORGANIZACIONAL

- **Objetivo.**

Establecer un modelo de datos institucional que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos.

- **Esquema del proceso.**

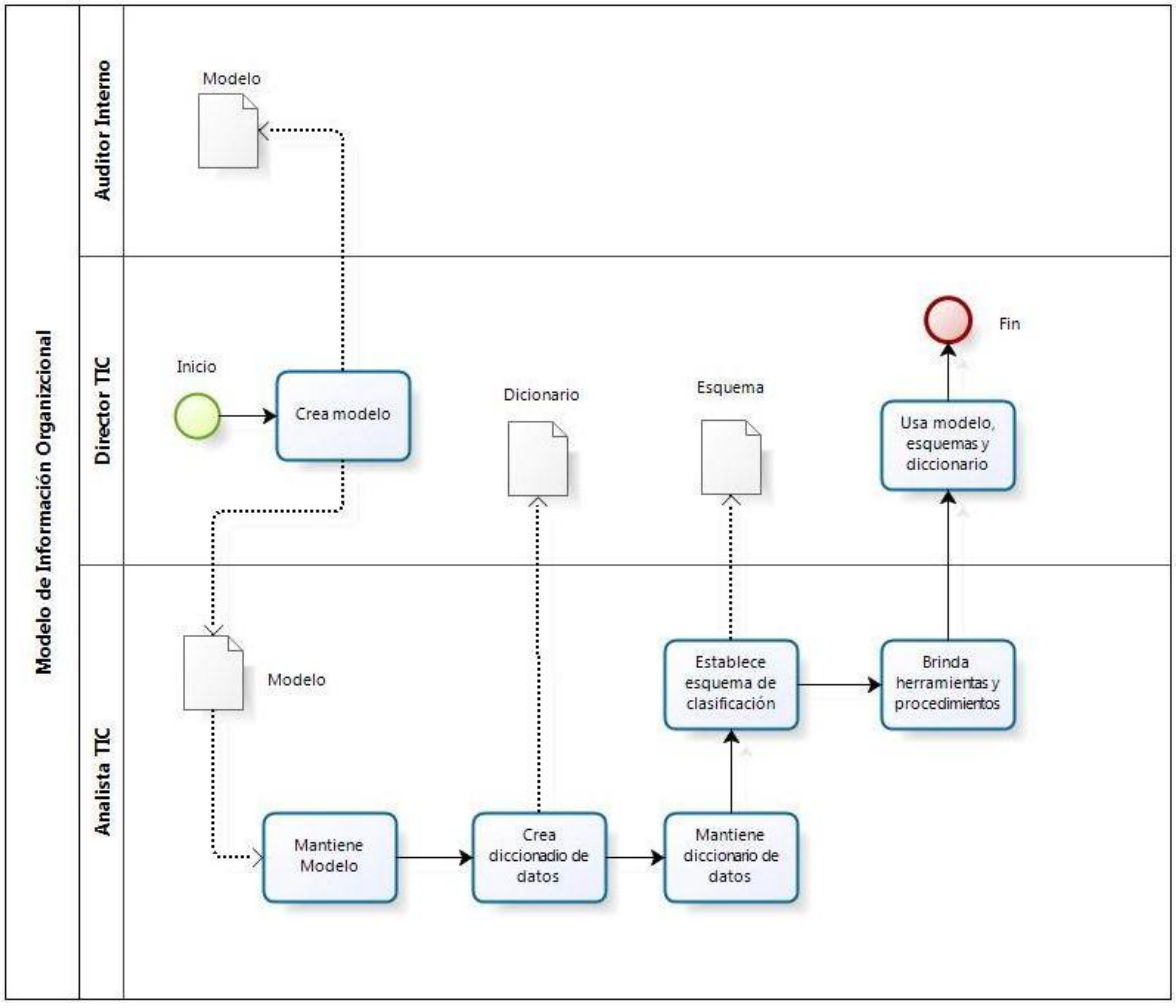

Ilustración 4: Esquema del proceso de información organizacional (GADPE, 2014)

c) GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS DE INTRANET.

- **Objetivo.**

Mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de las vulnerabilidades e incidentes de seguridad, el procedimiento es aplicable para todas las direcciones de la institución.

- **Esquema del proceso.**

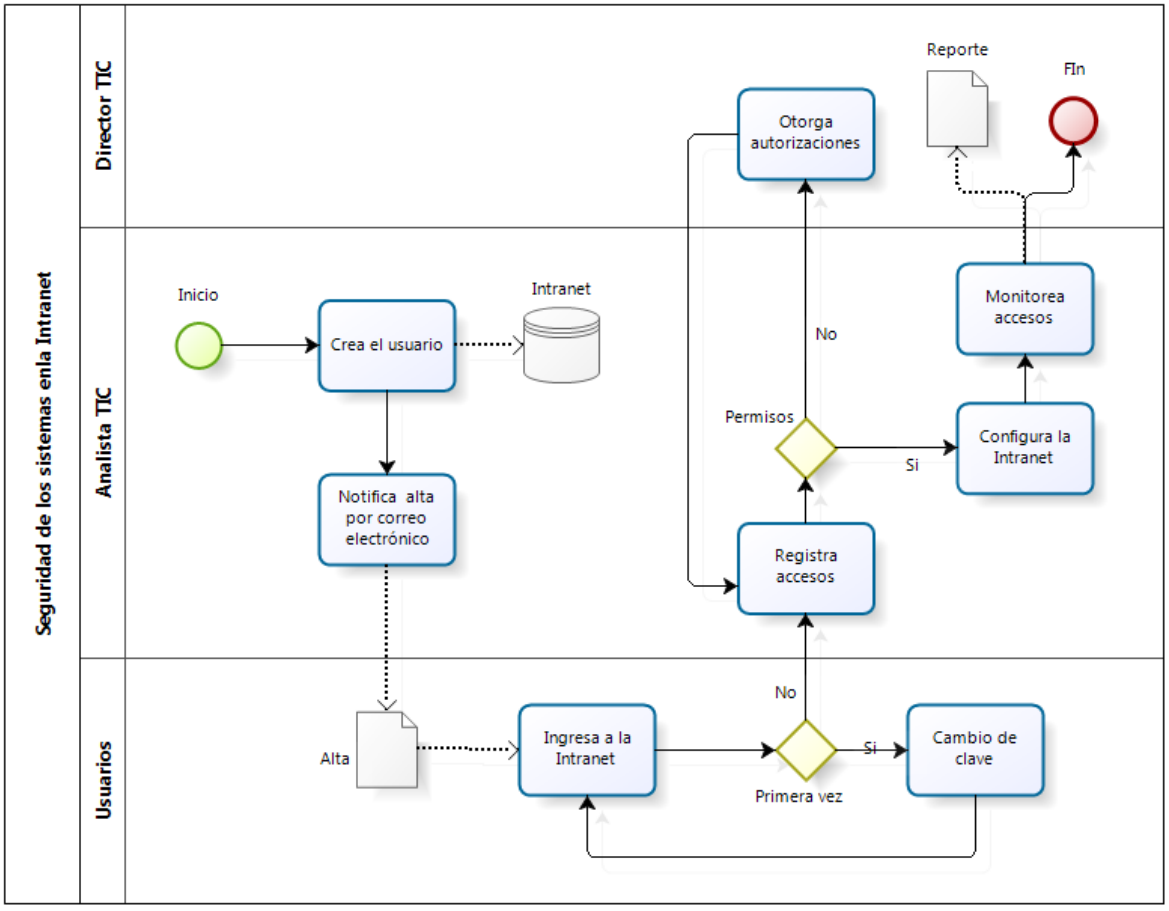

Ilustración 5: Esquema del proceso de garantizar la seguridad de los sistemas de intranet (GADPE, 2014)

d) POLÍTICAS DE SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN.

Objetivo.

Proteger los activos de Tecnologías de la Información de la Institución, a fin de preservar la confidencialidad, integridad y disponibilidad de la información mediante la implementación de políticas. El procedimiento es aplicable a nivel Institucional.

Esquema del proceso.

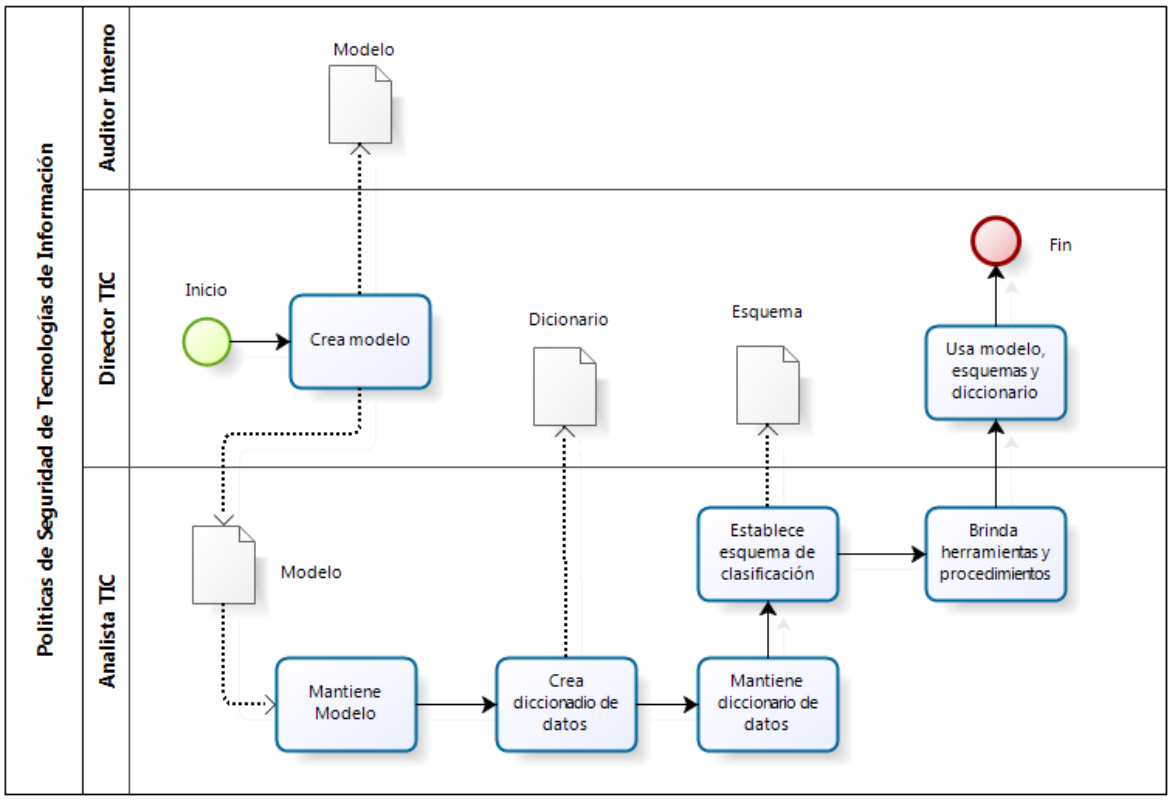

Ilustración 6: Esquema del proceso de políticas de seguridad de tecnología de información (GADPE, 2014)

e) GESTIÓN DEL RIESGO INFORMÁTICO.

- **Objetivo.**

Proteger los activos de Tecnologías de la Información de la Institución con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información, el procedimiento es aplicable a nivel Institucional.

- **Esquema del proceso.**

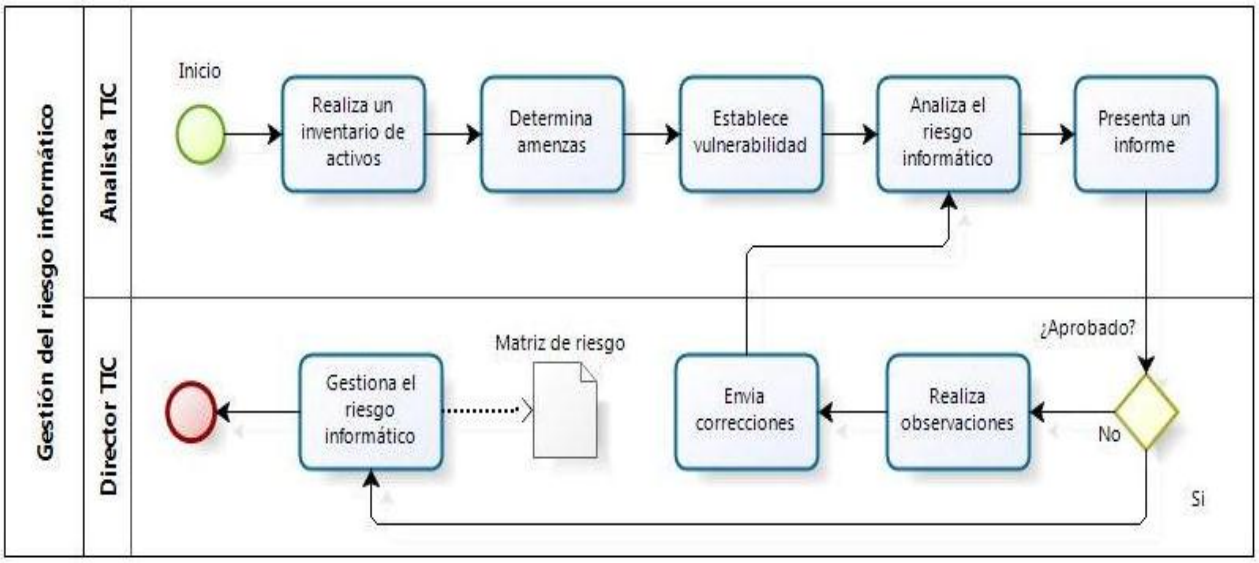

Ilustración 7: Esquema del proceso de gestión del riesgo informático (GADPE, 2014)

f) CONTINUIDAD DE LOS SERVICIOS.

- **Objetivo.**

Proporcionar los servicios de cómputo en servidores, almacenamiento, resguardo y restauración de información institucional, este procedimiento es aplicable a nivel de la Dirección de Tecnologías de Información y Comunicación y debe cumplir todas las políticas operacionales.

- **Esquema del proceso.**

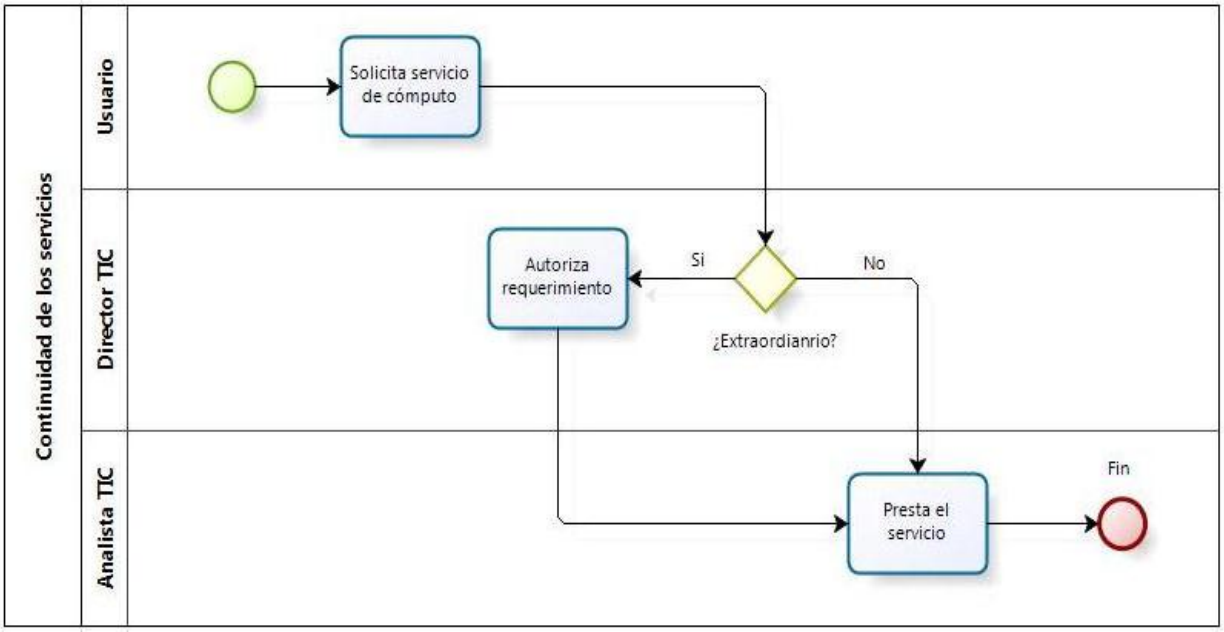

Ilustración 8: Esquema del proceso de continuidad de los servicios (GADPE, 2014)

g) MONITOREO DE REDES Y COMUNICACIONES.

- **Objetivo.**

Verificar las condiciones de operación básica de la red de voz y datos instalada en el Edificio, a fin de garantizar el funcionamiento de la red telefónica y de computadores, este procedimiento es aplicable a nivel de la Dirección de Tecnologías de Información y Comunicación.

- **Esquema del proceso.**

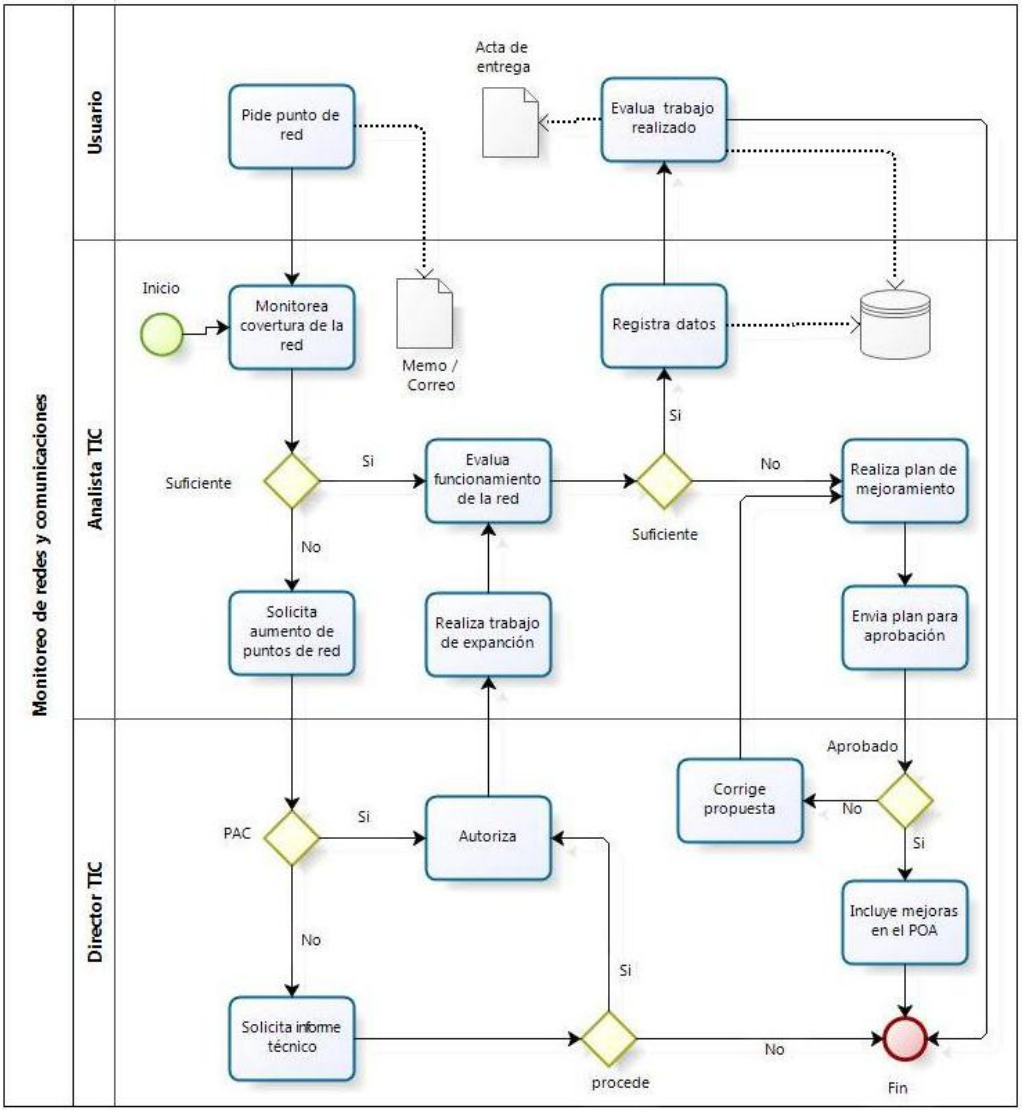

Ilustración 9: Esquema del proceso de monitoreo de redes y comunicaciones (GADPE, 2014)

h) RESGUARDO DE LA INFORMACIÓN.

Objetivo.

Minimizar el riesgo de pérdida de información a nivel de base de datos a través de la planeación, organización y control de respaldos, con la finalidad de brindar un servicio oportuno a los proyectos institucionales que utilizan información, el procedimiento es aplicable a nivel de la Dirección de Tecnologías de Información y Comunicación.

Esquema del proceso.

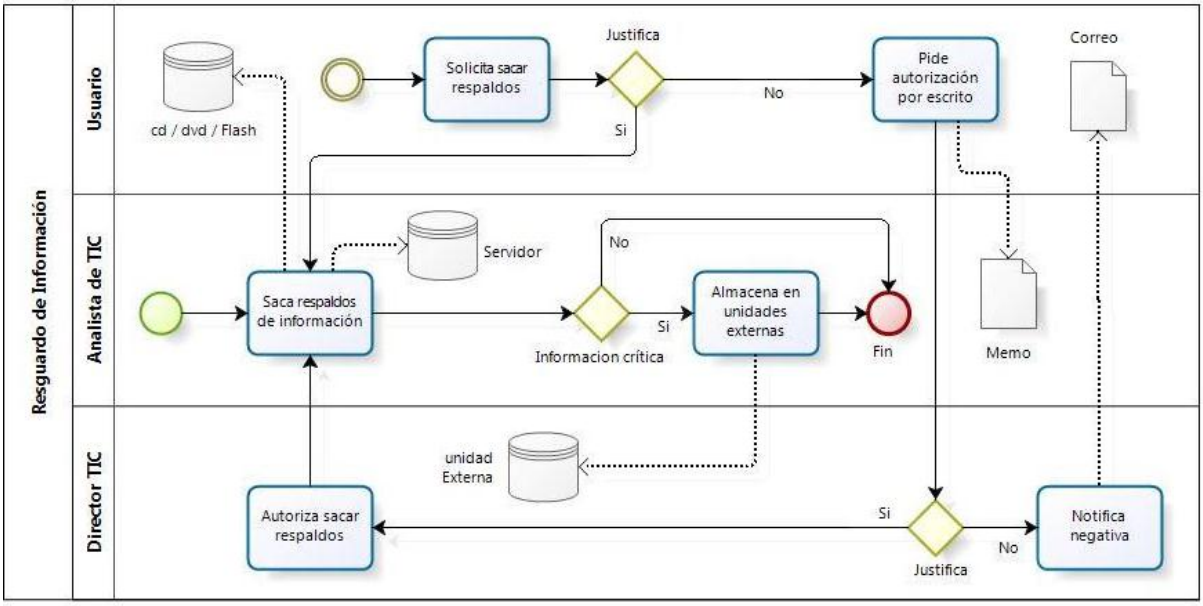

Ilustración 10: Esquema del proceso de resguardo de la información (GADPE, 2014)

i) INSTALACIÓN Y ACTUALIZACIÓN DE SOFTWARE EN LAS COMPUTADORAS.

- **Objetivo.**

Mantener actualizado el inventario de software de cada área y dirección, así como consolidar el Inventario Institucional de Software, permitiendo identificar la ubicación de cada uno de los programas de software de la institución.

- **Esquema del proceso**

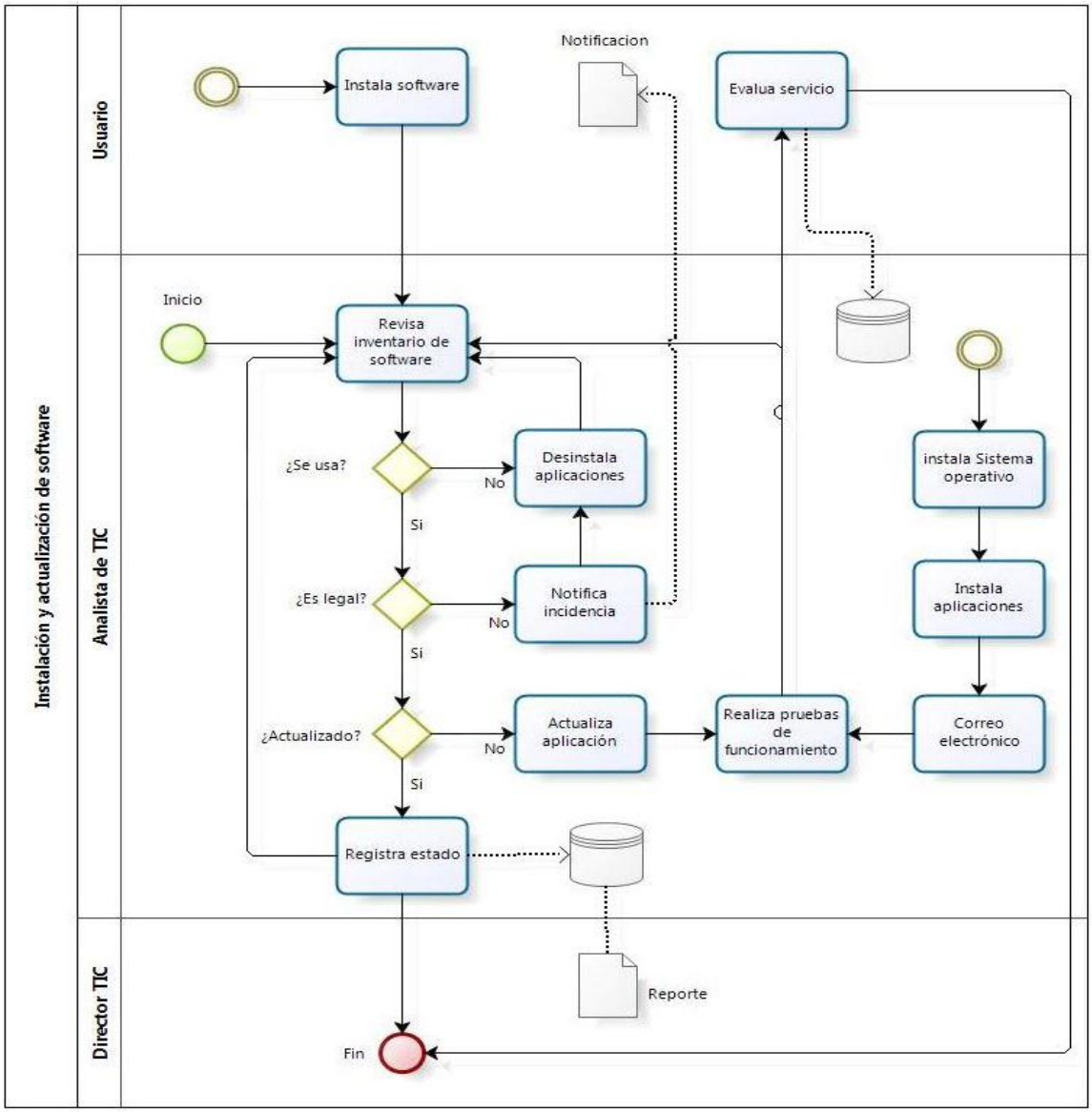

Ilustración 11: Esquema del proceso de instalación y actualización de software en las computadoras (GADPE, 2014)

j) ADMINISTRACIÓN DE LA INTRANET, INTERNET Y CORREO ELECTRÓNICO.

- **Objetivo.**

Proporcionar los servicios de activación de acceso a internet, servicio de red privada virtual, intranet y correo electrónico mediante la red local cableada e inalámbrica y es aplicable a nivel de la Dirección de Tecnologías de Información y Comunicación.

- **Esquema del proceso.**

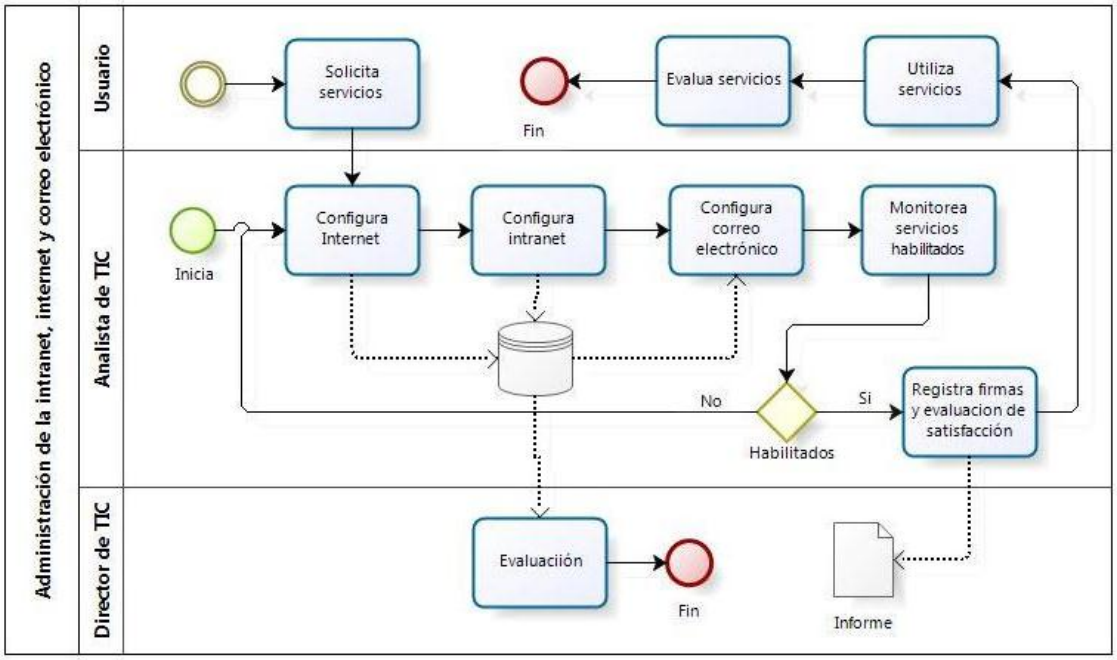

Ilustración 12: Esquema del proceso de administración de la intranet, internet y correo electrónico (GADPE, 2014)

k) DESARROLLO E INTEGRACIÓN DE SISTEMAS.

Objetivo.

Desarrollar los sistemas de información necesarios para la captación, digitalización, tratamiento, explotación y difusión de la información estadística correspondiente a los proyectos encomendados que permitan la generación oportuna de resultados; así como de los sistemas administrativos que lleven a la automatización de los procesos con la finalidad de contar con información oportuna para la toma de decisiones, el proceso es aplicable a nivel institucional y podrá ser aplicado solo si cumple todas las políticas operativas.

Esquema del proceso.

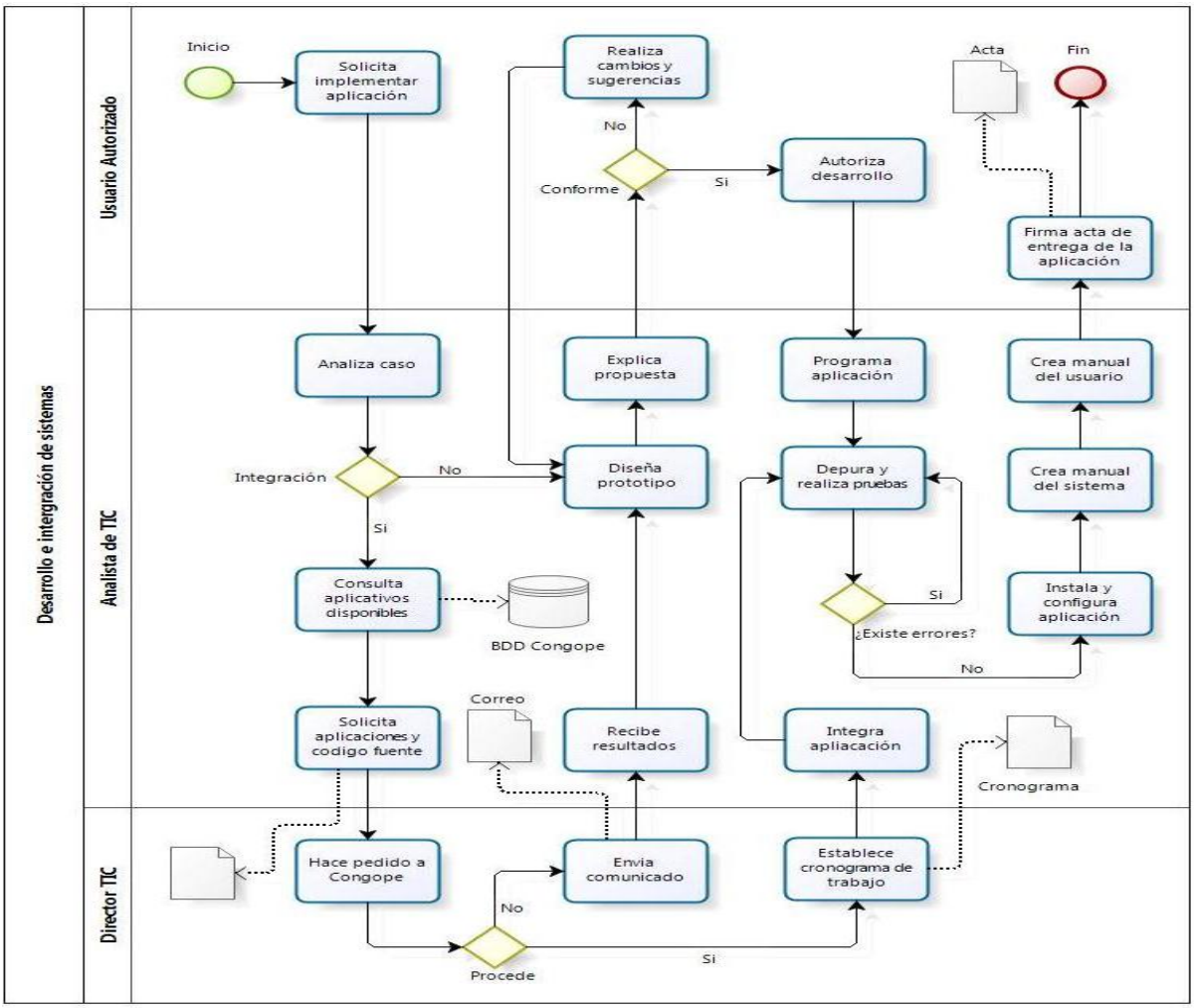

Ilustración 13: Esquema del proceso de desarrollo e integración de sistemas (GADPE, 2014)

3.3.2.3 IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN.

La identificación de activos de información es una parte vital, porque permite saber cuáles son los activos que se encuentran asociados a los procesos de la organización, así como el dueño del proceso, cada proceso involucra activos de información específicos, en sus diversos tipos y formatos a continuación se detalla:

1. **GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS EN LA INTRANET.**

   Responsable: (Analista TIC)

   Activos (computador portátil, servidores. Red interna).

   a) Creación de usuario.
   b) Notificación de alta al usuario
   c) Reporte mensual.
   d) Base de datos.

2. **MODELO DE INFORMACIÓN ORGANIZACIONAL.**

   Responsable: (Analista TIC)

   Activos: (computador portátil, servidores. Red interna,)

   a) Modelo Organizacional
   b) Diccionario de datos
   c) Esquema.
   d) Base de datos

3. **GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS EN LA INTRANET.**

   Responsable: (Analista tic)

   Activos: (computador portátil, servidores. Red interna,)

   a) Creación de usuario.
   b) Notificación de alta al usuario
   c) Reporte mensual.
   d) Base de datos.

4. POLÍTICAS DE SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN

Responsable: (Analista TIC)

Activos: (computador portátil)

a) Modelo
b) Diccionario
c) Esquema

5. GESTIÓN DEL RIESGO INFORMÁTICO

Responsable: (Analista TIC)

Activos: (computador portátil)

a) Matriz de riesgo
b) Activos GADPE

6. CONTINUIDAD DE LOS SERVICIOS

Responsable: (Analista)

Activos: (Todos)

a) Solicitud de servicio.
b) Autorización de servicio

7. MONITOREO DE REDES Y COMUNICACIONES.

Responsable: (Analista de Redes)

Activos: (servidores, redes en general)

a) Memo de petición de aumento de punto
b) Acta de entrega de punto.
c) Reporte de tráfico de la red.
d) Base de datos.

8. RESGUARDO DE LA INFORMACIÓN

Responsable: (Analista de sistemas)

Activos: (servidores, computadores, aplicaciones, licencias, biométricos)

a) Memo Solicitud de respaldo.
b) Información respaldada
c) Notificación de negación de respaldo
d) Base de datos

9. INSTALACIÓN Y ACTUALIZACIÓN DE SOFTWARE

Responsable: (Analista de sistemas)

Activos: (aplicaciones, computadores)

a) Inventario de software.
b) Notificación de incidencia.
c) Reporte de estado.

10. ADMINISTRACIÓN DE INTRANET, INTERNET Y CORREO ELECTRÓNICO.

Responsable: (Analista de sistemas**)**

Activos: (servidores, aplicaciones, redes)

a) Solicitud de servicio.
b) Informe de satisfacción de servicio.

11. DESARROLLO E INTEGRACIÓN DE SISTEMAS

Responsable: (Analista de sistemas)

Activos: (computador, servidores, aplicaciones)

a) Solicitud de implementación.
b) Código fuente.
c) Correo de petición.
d) Cronograma de trabajos.
e) Manual de sistema y de usuario.
f) Acta de entrega del sistema.

3.3.2.4 TASACIÓN DE ACTIVOS

La tasación de activos cumple la función de dar a entender el valor que tienen los activos para el departamento de TIC y la institución en general y de esta manera tener en cuenta cuales representan mayor relevancia. La información levantada en la tasación de activos será de vital importancia en el posterior proceso de Gestión de Riesgo debido a que se tendrá conocimiento de los activos cuyo valor es de mayor importancia y por ende deberá tener un mayor grado de salvaguarda.

La manera correcta de determinar el valor exacto de una activo para la institución es aplicando los parámetros de disponibilidad, integridad y confidencialidad y saber que impacto ocasionaría la burla de estos controles y daño del activo, si dicho impacto o daño en referencia a las actividades que cumple el activo dentro del departamento de TIC y la institución es de un rango alto ante una posible falla de la seguridad de la información tendremos claro el nivel de sensibilidad de la información que está siendo procesada y distribuida por el departamento de TIC y la instrucción en general.

El procedimiento a seguir para la tasación de activos se inicia con la identificación del proceso al cual se le aplicara la tasación de activos, luego de tener identificados el proceso y los activos que trabajan en el proceso se procede a aplicar los parámetros de confidencialidad, integridad y disponibilidad otorgando una calificación para cada aspecto que va desde 1 hasta 3, siendo 1 igual a Bajo, 2 igual Medio y 3 igual Alto, dichas calificaciones se promedian y de acuerdo al resultado se establece la importancia del activo implicado en el proceso.

Descripción.	Valor.
Alto	3
Medio	2
Bajo	1

Tabla 3: Tasación de activos

Luego de aplicar la tasación de activos a todos los procesos y activos previamente establecidos en el alcance del proyecto la lista se redujo a un número considerable de activos que tienen una gran importancia y por lo tanto se tienen que aplicar los controles con mayor rigurosidad en ellos, los activos son los siguientes:

Tasación de activos				
Proceso: Competencias tecnológicas				
Activos	**Tasación**			
	Confidencialidad	**Integridad**	**Disponibilidad**	**Total**
Computador personal Lenovo	2	3	3	3
Programa Anual	1	3	3	3
Reporte Mensual	1	2	2	2

Tabla 4: Tasación de activos de competencias tecnológicas

Tasación de activos				
Proceso: Modelo de Información				
Activos	**Tasación**			
	Confidencialidad	**Integridad**	**Disponibilidad**	**Total**
Computador personal HP	2	3	3	3
Servidor Panasonic	3	3	3	3
Data center liberti	3	3	3	2
modelo organizacional	2	2	3	2
diccionario de datos	2	2	3	3
Esquema	2	2	3	3
Base de datos	3	3	3	3

Tabla 5: Tasación de activos de modelo de información

Tasación de activos				
Proceso: Garantizar la seguridad de los sistemas de intranet				
Activos	**Tasación**			
	Confidencialidad	Integridad	Disponibilidad	Total
Computador personal HP	2	3	3	3
Servidor Panasonic	3	3	3	3
Data center liberti	3	3	3	2
Datos del Usuario	3	3	3	3
Notificación de Alta	3	2	2	2
Reporte Mensual	2	2	2	2
Base de datos	3	3	3	3

Tabla 6: Tasación de activos de garantizar la seguridad de los sistemas de intranet

Tasación de activos				
Proceso: Gestión de riesgo informático				
Activos	**Tasación**			
	Confidencialidad	Integridad	Disponibilidad	Total
Computador personal HP	2	3	3	3
Matriz de Riesgo	3	3	3	3
Activos GADPE	3	3	3	3

Tabla 7: Tasación de activos de gestión de riesgo informático

Tasación de activos				
Proceso: Continuidad de los servicios				
Activos	**Tasación**			
	Confidencialidad	Integridad	Disponibilidad	Total
Activos GADPE	3	3	3	3

Tabla 8: Tasación de activos de continuidad de los servicios

Tasación de activos				
Proceso: Monitoreo de redes				
Activos	**Tasación**			
	Confidencialidad	Integridad	Disponibilidad	Total
Servidor Panasonic	2	3	3	3
Base de datos	3	3	3	3
Data Center Libert	3	3	3	3
Servidor tipo IBM	3	3	3	3
Redes de datos	3	3	3	3
Contrato de Redes y telecomunicaciones	3	3	2	3
Reporte de trafico de red	2	3	2	2

Tabla 9: Tasación de activos de monitoreo de redes

Tasación de activos				
Proceso: Políticas de Seguridad de tecnologías de Información				
Activos	**Tasación**			
	Confidencialidad	Integridad	Disponibilidad	Total
Computador personal HP	2	3	3	3
Modelo de datos	2	3	3	3
Diccionario de Datos	2	3	2	2
Esquema de datos	3	3	3	3

Tabla 10: Tasación de activos de políticas de seguridad de tecnologías de información

Tasación de activos				
Proceso: Resguardo de la Información				
Activos	**Tasación**			
	Confidencialidad	Integridad	Disponibilidad	Total
SERVIDOR PANASONIC	2	3	3	3
BASE DE DATOS	3	3	3	3
DATA CENTER LIBERT	3	3	3	3
SERVIDOR TIPO IBM	3	3	3	3
REDES DE DATOS	3	3	3	3
CONTRATO DE REDES Y TELECOMUNICACIONES	3	3	2	3
REPORTE DE TRAFICO DE RED	2	3	2	2
COMPUTADOR PERSONAL HP	2	3	3	3
COMPUTADOR PERSONAL LENOVO	2	3	3	3
COMPUTADOR HP	2	3	3	3
COMPUTADOR COMPAQ	2	3	3	3
COMPUTADOR APPLE	2	3	3	3
COMPUTADOR PORTÁTIL TOSHIBA	2	3	3	3
COMPUTADOR ADITK	2	3	3	3
COMPUTADOR ALTEK	2	3	3	3
SISTEMA PROGRAMA DE CONTABILIDAD-Olimpo	3	3	3	3

LICENCIA WINDOWS-Server 2003	3	3	3	3
SISTEMA INF. DE CONT. Y FISCAL. DE OBRAS	3	3	3	3
SIST. CAPTURA DATOS CONTROL ACTIVOS-Symbol	3	3	3	3
SISTEMA DE AUTOMATIZACIÓN DE TEMPERATURA	3	3	3	3
PAQUETE TÉCNICO DE CALCULO	3	3	3	3
PROGRAMA DE ROLES DE PAGO SYSPAGO V30	3	3	3	3
PROGRAMA DE CONTABILIDAD SIA XP	3	3	3	3
PROGRAMA DE CONTABILIDAD ALFA G	3	3	3	3
SOLICITUD DE RESPALDO	3	3	3	3
INFORMACIÓN RESPALDADA	3	3	3	3
SOFTWARE DE INFORM. GEOGRÁFICA	3	3	3	3

Tabla 11: Tasación de activos de resguardo de la información

Tasación de activos				
Proceso: Instalación y Actualización de Software				
Activos	**Tasación**			
	Confidencialidad	Integridad	Disponibilidad	Total
COMPUTADOR PERSONAL HP	2	3	3	3
COMPUTADOR PERSONAL LENOVO	2	3	3	3
COMPUTADOR HP	2	3	3	3
COMPUTADOR COMPQ	2	3	3	3
COMPUTADOR APPLE	2	3	3	3
COMPUTADOR PORTÁTIL TOSHIBA	2	3	3	3
COMPUTADOR ADITK	2	3	3	3
COMPUTADOR ALTEK	2	3	3	3
SISTEMA PROGRAMA DE CONTABILIDAD-Olimpo	3	3	3	3
LICENCIA WINDOWS-Server 2003	3	3	3	3
SISTEMA INF. DE CONT. Y FISCAL. DE OBRAS	3	3	3	3
SIST. CAPTURA DATOS CONTROL ACTIVOS-Symbol	3	3	3	3
SISTEMA DE AUTOMATIZACIÓN DE TEMPERATURA	3	3	3	3
PAQUETE TÉCNICO DE CALCULO	3	3	3	3

PROGRAMA DE ROLES DE PAGO SYSPAGO V30	3	3	3	3
PROGRAMA DE CONTABILIDAD SIA XP	3	3	3	3
PROGRAMA DE CONTABILIDAD ALFA G	3	3	3	3
SOLICITUD DE RESPALDO	3	3	3	3
BACKUP	3	3	3	3
SOFTWARE DE INFORM. GEOGRÁFICA	3	3	3	3

Tabla 12: Tasación de activos de instalación y actualización de software

Tasación de activos				
Proceso: Administración de redes y correo electrónico				
Activos	**Tasación**			
	Confidencialidad	Integridad	Disponibilidad	Total
Servidor Panasonic	2	3	3	3
Base de datos	3	3	3	3
Data Center Libert	3	3	3	3
Servidor tipo IBM	3	3	3	3
Redes de datos	3	3	3	3
Contrato de Redes y telecomunicaciones	3	3	2	3

Tabla 13: Tasación de activos de administración de redes y correo electrónico

Tasación de activos				
Proceso: Desarrollo e integración de sistemas				
Activos	**Tasación**			
	Confidencialidad	Integridad	Disponibilidad	Total
Servidor Panasonic	2	3	3	3
Base de datos	3	3	3	3
Data Center Libert	3	3	3	3
Servidor tipo IBM	3	3	3	3
Redes de datos	3	3	3	3
Aplicaciones Desarrolladas	3	3	2	3
Código Fuente	3	3	3	3

Manual de usuario	2	3	2	2
Manual de Instalación de Sistema	2	3	3	3
Cronograma de Trabajo	2	2	2	2
Acta de entrega del Sistema	2	3	2	2

Tabla 14: Tasación de activos de desarrollo e integración de sistemas

3.3.2.5 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

Luego del proceso de identificación de las vulnerabilidades se tiene que tener en cuenta la posibilidad que existe que una amenaza pueda explotar dicha vulnerabilidad, teniendo bien claro que ambas deben presentarse al mismo tiempo para tener un impacto negativo dentro del Departamento de TIC y la Institución, por este motivo debe ser preciso el dato de **que amenaza puede explotar cual vulnerabilidad.**

Ilustración 14: Activo de información

A continuación se puede observar las amenazas identificadas con las vulnerabilidades correspondientes:

TIPIFICACIÓN RIESGO	PROCESO	ACTIVO DE INFOMACIÓN	PROPIETARIO DEL ACTIVO	AMENAZA	VULNERABILIDAD
R1	**Competencias tecnológicas**	Computador Personal- Lenovo	**Director de Tic**	Contagio de virus	Falta de antivirus con licencia
				Sustracción de información	Puertos USB habilitados
				Instalación no autorizada de software	Falta de inventario de licencias instaladas
				Acceso no autorizado a la red	Sesiones activas después del horario laboral
R2		Programa Anual		Espionaje industrial	Inadecuada supervisión del trabajo de los empleados
R3		Reporte Mensual		Interceptación de información	Información disponible para personas no autorizadas
R4	**Modelo de Información Organizacional**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia
R5		Servidor- Panasonic		Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral
R6		Data Center – Libert		Acceso no autorizado al sistema de información	Contraseñas inseguras
R7		modelo organizacional		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado
R8		diccionario de datos		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas
R9		esquema		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos
R10		Base de Datos		Destrucción de registros	Sesiones activas después del horario laboral

				Espionaje industrial	Mantenimiento inadecuado
				Falsificación de registros	Inadecuados derechos de usuario
R11	**Garantizar la seguridad de los sistemas de intranet**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia
R12		Servidor-Panasonic		Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral
R13		Base de Datos		Acceso no autorizado al sistema de información	Contraseñas inseguras
R14		Data Center – Libert		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado
R15		Datos del Usuario		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas
				Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos
R16		Notificación de alta		Modificación no autorizada de registros	Bases de datos con protección desactualizada contra códigos maliciosos
R17		Reporte Mensual		Sustracción de información	Nivel de confidencialidad no definido con claridad
R18	**Políticas de Seguridad de Tecnologías de Información**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia
				Sustracción de información	Puertos USB habilitados
				Instalación no autorizada de software	Falta de inventario de licencias instaladas
				Acceso no autorizado a la red	Sesiones activas después del horario laboral

R19		Modelo de datos		Fuga o revelación de información	Falta de control en datos de entrada y salida
R20		diccionario de datos		Fuga o revelación de información	Falta de control en datos de entrada y salida
R21		Esquema de datos		Fuga o revelación de información	Falta de control en datos de entrada y salida
R22	**Gestión de Riesgo Informático**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia
				Sustracción de información	Puertos USB habilitados
R23		Matriz de riesgo		Instalación no autorizada de software	Falta de inventario de licencias instaladas
R24		Activos GADPE		Acceso no autorizado a la red	Sesiones activas después del horario laboral
R25	**Continuidad de los Servicios**	Solicitud de nuevo servicio	**Analista Tic**	Incumplimiento de leyes	Inadecuada capacidad de gestión
R26	**Monitoreo de Redes y Comunicaciones**	Servidor-Panasonic	**Analista de Redes**	Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral
R27		Base de Datos		Acceso no autorizado al sistema de información	Contraseñas inseguras
R28		Data Center - Libert		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado
R29		Servidor tipo Blade-IBM		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas
R30		Redes de datos		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos
R31		Contrato de Redes y Telecomunicaciones		Incumplimiento de relaciones contractuales	Inadecuada capacidad de gestión

R32		Reporte de Trafico de Red		Incumplimiento de leyes	Inadecuado nivel de conocimiento y/o concienciación de empleados
				Interceptación de información	Inadecuada gestión de redes
R33	**Resguardo de la información**	Servidor-Panasonic	**Alasita de Sistemas Activos**	Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral
R34		Data Center - Libert		Acceso no autorizado al sistema de información	Contraseñas inseguras
R35		Base de Datos		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado
R36		Servidor tipo Blade-IBM		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas
R37		Redes de datos		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos
R38		Computador personal HP		Contagio de virus	Falta de antivirus con licencia
R39		computador personal LENOVO		Sustracción de información	Puertos USB habilitados
R40		Computador HP		Instalación no autorizada de software	Falta de inventario de licencias instaladas
R41		Computador COMPQ		Acceso no autorizado a la red	Sesiones activas después del horario laboral
R42		Computador Apple		Uso no autorizado de software	Sesiones activas después del horario laboral
R43		Computador Portátil Toshiba		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral

R44		Computador Aditk		Error de usuario	Eliminación de soportes de almacenamiento sin borrado de datos
R45		Computador Altek		Modificación no autorizada de registros	Claves criptográficas accesibles a personas no autorizadas
R46		SISTEMA PROGRAMA DE CONTABILIDAD-Olimpo		Daños provocados por actividades de terceros	Redes accesibles a personas no autorizadas
R47		LICENCIA WINDOWS-Server 2003		Daños ocasionados durante pruebas de intrusión	Bases de datos con protección desactualizada contra códigos maliciosos
R48		SISTEMA INF. DE CONT. Y FISCAL. DE OBRAS		Destrucción de registros	Sistemas desprotegidos ante acceso no autorizado
R49		SIST. CAPTURA DATOS CONTROL ACTIVOS-Symbol		Uso erróneo de herramientas de auditoría	Inadecuado nivel de conocimiento y/o concienciación de empleados
R50		SISTEMA DE AUTOMATIZACION DE TEMPERATURA		Modificación no autorizada de registros	Falta de desactivación de cuentas de usuario luego de finalizado el empleo
R51		PAQUETE TECNICO DE CALCULO		Sustracción de información	Copiado sin control
R52		PROGRAMA DE ROLES DE PAGO SYSPAGO V30		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral

R53		PROGRAMA DE CONTABILIDAD SIA XP		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral
R54		PROGRAMA DE CONTABILIDAD ALFA G		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral
R55		Solicitud de Respaldo		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral
R56		Información Respaldada		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral
R57		SOFTWARE DE INFORM. GEOGRAFICA		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral
R58	**Instalación y Actualización de Software**	computador personal HP	**analista de sistemas**	Contagio de virus	Falta de antivirus con licencia
R59		computador personal LENOVO		Sustracción de información	Puertos USB habilitados
R60		Computador HP		Instalación no autorizada de software	Falta de inventario de licencias instaladas
R61		Computador COMPQ		Acceso no autorizado a la red	Sesiones activas después del horario laboral
R62		Computador Apple		Uso no autorizado de software	Sesiones activas después del horario laboral
R63		Computador Portátil Toshiba		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral
R64		Computador Aditk		Daños provocados por actividades de terceros	Eliminación de Registros y datos de funcionamiento de la información
R65		Computador Altek		Errores de mantenimiento	Inadecuado control de cambios

R66		SISTEMA PROGRAMA DE CONTABILIDAD-Olimpo		Robo	Inadecuada gestión del empleador
R67		LICENCIA WINDOWS-Server 2003		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral
R68		SISTEMA INF. DE CONT. Y FISCAL. DE OBRAS		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral
R69		SIST. CAPTURA DATOS CONTROL ACTIVOS-Symbol		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral
R70		SISTEMA DE AUTOMATIZACION DE TEMPERATURA		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral
R71		PAQUETE TECNICO DE CALCULO		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral
R72		SOFTWARE DE INFORM. GEOGRAFICA		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral
R73	**Administración de intranet, internet y correo electrónico**	Servidor-Panasonic	**analista de sistemas activos**	Contagio de virus	Falta de antivirus con licencia
R74		Data Center - Libert		Sustracción de información	Puertos USB habilitados
R75				Instalación no autorizada de software	Falta de inventario de licencias instaladas
R76				Acceso no autorizado a la red	Sesiones activas después del horario laboral
R77				Uso no autorizado de software	Sesiones activas después del horario laboral

R78				Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral
R79				Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral
R80		Base de Datos		Acceso no autorizado al sistema de información	Contraseñas inseguras
R81		Servidor tipo Blade-IBM		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado
R82		Redes de datos		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas
R83		Contrato de Redes y Telecomunicaciones		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos
R84	**Desarrollo e Integración de Sistema**	Aplicaciones Desarrolladas	**analista de sistemas activos**	Contagio de virus	Falta de antivirus con licencia
R85		Servidor-Panasonic		Sustracción de información	Puertos USB habilitados
R86		base de Datos		Instalación no autorizada de software	Falta de inventario de licencias instaladas
R87		Servidor tipo Blade-IBM		Acceso no autorizado a la red	Sesiones activas después del horario laboral
R88		Redes de datos		Uso no autorizado de software	Sesiones activas después del horario laboral
R89		Data Center - Libert		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral
R90				Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral

R91		Manual de usuario		Mala utilización de la aplicación	Mala redacción del manual
R92		Manual de Instalación de Sistema		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado
R93		Cronograma de Trabajo		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas
R94		Acta de entrega del Sistema		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos
R95		Código Fuente		Plagio	Falta de control de desarrollo
				Mala utilización de la aplicación	Mala redacción del manual

Tabla 15 :Matriz de riesgo, identificación de amenazas y vulnerabilidades

Después de tener bien claras las amenazas y vulnerabilidades, se requiere evaluar la posibilidad que ambas puedan coincidir y provocar daños a los activos, esto envuelve el cálculo de probabilidad de la ocurrencia de la amenaza y la facilidad con que esta puede llegar a ser explotada por la vulnerabilidad así la conclusión llega a ser que el objetivo del análisis del riesgo es identificar y calcular los riesgos basados en la identificación de los activos y en el cálculo de las amenazas y vulnerabilidades.

3.3.2.6 EVALUACIÓN Y CÁLCULO DEL RIESGO.

Los riesgos cuentan con dos características o factores fundamentales para tener mayor precisión al momento de ser calculados las cuales son la probabilidad de que la amenaza explote la vulnerabilidad y el impacto que causaría de materializarse la amenaza, la relación entre estos factores calificados del 1 al 5 arrojaran como resultado el nivel de riesgo el cual puede ser bajo representado con el color verde, medio representado con el color amarillo y alto representado con el color rojo.

Nivel	Impacto
Entre 1 y 3	Bajo
Entre 2 y 4	Medio
Entre 3 y 5	Alto

Tabla 16: Medición de impactos

A continuación se apreciara el cálculo realizado a los activos con las amenazas y vulnerabilidades previamente edificadas:

TIPIFICACIÓN RIESGO	PROCESO	ACTIVO DE INFORMACIÓN	PROPIETARIO DEL ACTIVO	AMENAZA	VULNERABILIDAD	PROPIETARIO DEL RIESGO	RIESGO DEL ACTIVO
R1	**Competencias tecnológicas**	Computador Personal-Lenovo	**Director de Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	Alto
				Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	Medio
				Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	Alto
				Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R2		Programa Anual		Espionaje industrial	Inadecuada supervisión del trabajo de los empleados	**Analista de Sistemas**	Bajo
R3		Reporte Mensual		Interceptación de información	Información disponible para personas no autorizadas	**Analista de Sistemas**	Bajo
R4	**Modelo de Información Organizacional**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	Alto
R5		Servidor-Panasonic		Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R6		Data Center – Libert		Acceso no autorizado al sistema de	Contraseñas inseguras	**Analista de Redes**	Alto

				información			
R7		modelo organizacional		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	Alto
R8		diccionario de datos		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	Medio
R9		esquema		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	Medio
R10		Base de Datos		Destrucción de registros	Sesiones activas después del horario laboral	**Analista de Redes**	Medio
				Espionaje industrial	Mantenimiento inadecuado	**Analista de Redes**	Bajo
				Falsificación de registros	Inadecuados derechos de usuario	**Analista de Redes**	Medio
R11	**Garantizar la seguridad de los sistemas de intranet**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	Alto
R12		Servidor-Panasonic		Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R13		Base de Datos		Acceso no autorizado al sistema de información	Contraseñas inseguras	**Analista de Redes**	Alto
R14		Data Center – Libert		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	Alto

R15		Datos del Usuario		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	Medio
				Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	Medio
R16		Notificación de alta		Modificación no autorizada de registros	Bases de datos con protección desactualizada contra códigos maliciosos	**Analista de Redes**	Alto
R17		Reporte Mensual		Sustracción de información	Nivel de confidencialidad no definido con claridad	**Analista de Redes**	Alto
R18	**Políticas de Seguridad de Tecnologías de Información**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	Alto
				Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	Medio
				Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	Alto
				Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R19		Modelo de datos		Fuga o revelación de información	Falta de control en datos de entrada y salida	**Analista de Sistemas**	Bajo
R20		diccionario de datos		Fuga o revelación de información	Falta de control en datos de entrada y salida	**Analista de Sistemas**	Bajo

R21		Esquema de datos		Fuga o revelación de información	Falta de control en datos de entrada y salida	**Analista de Sistemas**	Bajo
R22	**Gestión de Riesgo Informático**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	Alto
				Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	Medio
R23		Matriz de riesgo		Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	Alto
R24		Activos GADPE		Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R25	**Continuidad de los Servicios**	Solicitud de nuevo servicio	**Analista Tic**	Incumplimiento de leyes	Inadecuada capacidad de gestión	**Analista Tic**	Alto
R26	**Monitoreo de Redes y Comunicaciones**	Servidor-Panasonic	**Analista de Redes**	Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R27		Base de Datos		Acceso no autorizado al sistema de información	Contraseñas inseguras	**Analista de Redes**	Alto
R28		Data Center - Libert		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	Alto
R29		Servidor tipo Blade-IBM		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	Medio

R30		Redes de datos		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	Alto
R31		Contrato de Redes y Telecomunicaciones		Incumplimiento de relaciones contractuales	Inadecuada capacidad de gestión	**Analista de Redes**	Bajo
R32		Reporte de Trafico de Red		Incumplimiento de leyes	Inadecuado nivel de conocimiento y/o concienciación de empleados	**Analista de Redes**	Medio
				Interceptación de información	Inadecuada gestión de redes	**Analista de Redes**	Medio
R33	**Resguardo de la información**	Servidor-Panasonic	**Alasita de Sistemas Activos**	Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R34		Data Center - Libert		Acceso no autorizado al sistema de información	Contraseñas inseguras	**Analista de Redes**	Alto
R35		Base de Datos		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	Alto
R36		Servidor tipo Blade-IBM		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	Medio
R37		Redes de datos		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	Alto

R38		Computador personal HP		Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	Alto
R39		computador personal LENOVO		Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	Medio
R40		Computador HP		Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	Alto
R41		Computador COMPAQ		Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R42		Computador Apple		Uso no autorizado de software	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R43		Computador Portátil Toshiba		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Alto
R44		Computador Aditk		Error de usuario	Eliminación de soportes de almacenamiento sin borrado de datos	**Analista de Sistemas**	Bajo
R45		Computador Altek		Modificación no autorizada de registros	Claves criptográficas accesibles a personas no autorizadas	**Analista de Sistemas**	Medio
R46		SISTEMA PROGRAMA DE CONTABILIDAD-Olimpo		Daños provocados por actividades de terceros	Redes accesibles a personas no autorizadas	**Analista de Sistemas**	Alto

R47		LICENCIA WINDOWS-Server 2003		Daños ocasionados durante pruebas de intrusión	Bases de datos con protección desactualizada contra códigos maliciosos	**Analista de Sistemas**	Medio
R48		SISTEMA INF. DE CONT. Y FISCAL. DE OBRAS		Destrucción de registros	Sistemas desprotegidos ante acceso no autorizado	**Analista de Sistemas**	Alto
R49		SIST. CAPTURA DATOS CONTROL ACTIVOS-Symbol		Uso erróneo de herramientas de auditoría	Inadecuado nivel de conocimiento y/o concienciación de empleados	**Analista de Sistemas**	Bajo
R50		SISTEMA DE AUTOMATIZACIÓN DE TEMPERATURA		Modificación no autorizada de registros	Falta de desactivación de cuentas de usuario luego de finalizado el empleo	**Analista de Sistemas**	Medio
R51		PAQUETE TÉCNICO DE CALCULO		Sustracción de información	Copiado sin control	**Analista de Sistemas**	Alto
R52		PROGRAMA DE ROLES DE PAGO SYSPAGO V30		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R53		PROGRAMA DE CONTABILIDAD SIA XP		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Bajo

R54		PROGRAMA DE CONTABILIDAD ALFA G		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Bajo
R55		Solicitud de Respaldo		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Bajo
R56		Información Respaldada		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Bajo
R57		SOFTWARE DE INFORM. GEOGRÁFICA		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Bajo
R58	**Instalación y Actualización de Software**	computador personal HP	**analista de sistemas**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	Alto
R59		computador personal LENOVO		Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	Medio
R60		Computador HP		Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	Alto
R61		Computador COMPAQ		Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R62		Computador Apple		Uso no autorizado de software	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio

R63		Computador Portátil Toshiba		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Alto
R64		Computador Aditk		Daños provocados por actividades de terceros	Eliminación de Registros y datos de funcionamiento de la información	**Analista de Sistemas**	Medio
R65		Computador Altek		Errores de mantenimiento	Inadecuado control de cambios	**Analista de Sistemas**	Medio
R66		SISTEMA PROGRAMA DE CONTABILIDAD-Olimpo		Robo	Inadecuada gestión del empleador	**Analista de Sistemas**	Medio
R67		LICENCIA WINDOWS-Server 2003		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Bajo
R68		SISTEMA INF. DE CONT. Y FISCAL. DE OBRAS		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Bajo
R69		SIST. CAPTURA DATOS CONTROL ACTIVOS-Symbol		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Bajo

R70		SISTEMA DE AUTOMATIZACIÓN DE TEMPERATURA		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Bajo
R71		PAQUETE TÉCNICO DE CALCULO		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Bajo
R72		SOFTWARE DE INFORM. GEOGRÁFICA		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Bajo
R73	**Administración de intranet, internet y correo electrónico**	Servidor-Panasonic	**analista de sistemas activos**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	Alto
R74		Data Center - Libert		Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	Medio
R75				Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	Alto
R76				Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R77				Uso no autorizado de software	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R78				Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Alto

R79				Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R80		Base de Datos		Acceso no autorizado al sistema de información	Contraseñas inseguras	**Analista de Redes**	Alto
R81		Servidor tipo Blade-IBM		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	Alto
R82		Redes de datos		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	Medio
R83		Contrato de Redes y Telecomunicaciones		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	Alto
R84	**Desarrollo e Integración de Sistema**	Aplicaciones Desarrolladas	**analista de sistemas activos**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	Alto
R85		Servidor-Panasonic		Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	Medio
R86		base de Datos		Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	Alto
R87		Servidor tipo Blade-IBM		Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio

R88		Redes de datos		Uso no autorizado de software	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R89		Data Center - Libert		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	Alto
R90				Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	Medio
R91		Manual de usuario		Mala utilización de la aplicación	Mala redacción del manual	**Analista de Redes**	Alto
R92		Manual de Instalación de Sistema		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	Alto
R93		Cronograma de Trabajo		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	Medio
R94		Acta de entrega del Sistema		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	Alto
R95		Código Fuente		Plagio	Falta de control de desarrollo		Medio
				Mala utilización de la aplicación	Mala redacción del manual		

Tabla 17: Evaluación y cálculo de riesgo

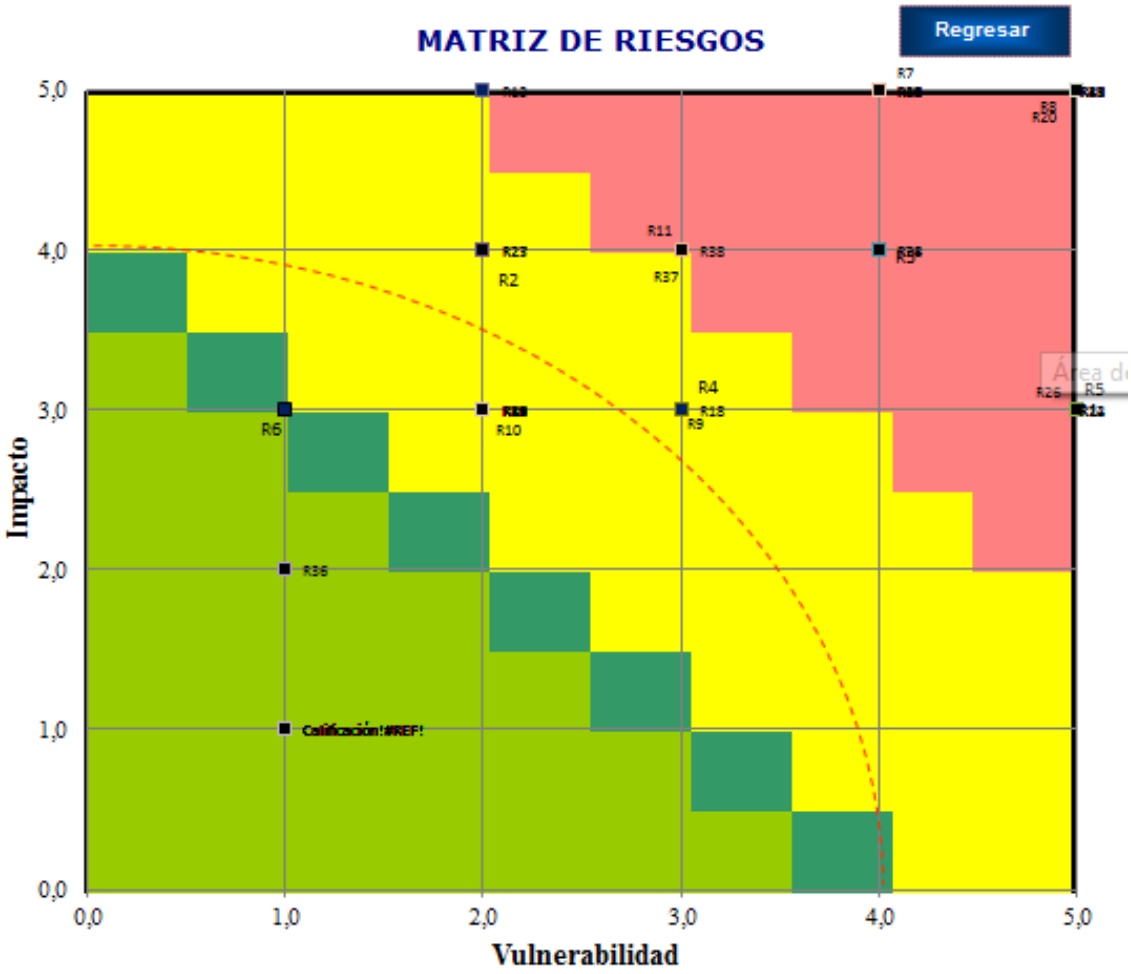

Ilustración 15: Mapa de riesgos

3.3.2.7 SELECCIÓN DE CONTROLES Y OBJETIVOS DE CONTROL.

Con el análisis y evaluación del riesgo terminado, el siguiente paso es preocuparse por las acciones que se van a realizar con los activos que representan un riesgo alto, para lo cual es necesario que dichos riesgos puedan ser manejados aplicando los controles estipulados por la normativa de la ISO 270001.

Todos estos controles y objetivos de control deben ser tomados del Anexo A (ver anexos) de la normativa, en donde se elegirá la acción que más beneficie al tratamiento del riesgo basado en un análisis de riesgo y los criterios de valoración.

TIPIFICACIÓN RIESGO	PROCESO	ACTIVO DE INFORMACIÓN	PROPIETARIO DEL ACTIVO	AMENAZA	VULNERABILIDAD	PROPIETARIO DEL RIESGO	OBJETIVO DE CONTROL	CONTROL
R1	**Competencias tecnológicas**	Computador Personal-Lenovo	**Director de Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
				Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	16.1	16.1.3 16.1.5
				Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	8.1 12.6	8.1.1 12.6.2
				Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	9.2	9.2.1 9.2.3 9.2.6
R2		Programa Anual		Espionaje industrial	Inadecuada supervisión del trabajo de los empleados	**Analista de Sistemas**	7.1	7.1.1 7.1.2
R3		Reporte Mensual		Interceptación de información	Información disponible para personas no autorizadas	**Analista de Sistemas**	16.1	16.1.1
R4	**Modelo de Información Organizacional**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
R5		Servidor-Panasonic		Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	12.1	12.1.1

R6		Data Center – Libert		Acceso no autorizado al sistema de información	Contraseñas inseguras	**Analista de Redes**	9.1 9.4 10.1	9.1.1 9.1.2 9.4.2 10.1.2
R7		modelo organizacional		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	11.1	11.1.2
R8		diccionario de datos		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	13.1	13.1.1
R9		esquema		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	7.2	7.2.1 7.2.2
R10		Base de Datos		Destrucción de registros	Sesiones activas después del horario laboral	**Analista de Redes**	9.2	9.2.1 9.2.5 9.2.6
				Espionaje industrial	Mantenimiento inadecuado	**Analista de Redes**	7.1	7.1.1 7.1.2
				Falsificación de registros	Inadecuados derechos de usuario	**Analista de Redes**	9.1 9.4	9.1.1 9.4.1 9.4.2 9.4.3
R11	**Garantizar la seguridad de los sistemas de intranet**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
R12		Servidor-Panasonic		Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	12.5 12.7	12.5.1 12.7.1

R13		Base de Datos		Acceso no autorizado al sistema de información	Contraseñas inseguras	**Analista de Redes**	9.1 9.4	9.1.1 9.4.1
R14		Data Center – Libert		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	11.1	11.1.2
R15		Datos del Usuario		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	13.1	13.1.1
				Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	7.2	7.2.1 7.2.2
R16		Notificación de alta		Modificación no autorizada de registros	Bases de datos con protección desactualizada contra códigos maliciosos	**Analista de Redes**	12.2	12.2.1
R17		Reporte Mensual		Sustracción de información	Nivel de confidencialidad no definido con claridad	**Analista de Redes**	9.2	9.2.2 9.2.3 9.2.4 9.2.5 9.2.6
R18	**Políticas de Seguridad de Tecnologías de Información**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
				Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	16.1	16.1.3 16.1.5

				Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	8.1 12.6	8.1.1 12.6.2
				Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	9.2	9.2.1 9.2.3 9.2.6
R19		Modelo de datos		Fuga o revelación de información	Falta de control en datos de entrada y salida	**Analista de Sistemas**	12.4	12.4.1 12.4.2 12.4.3
R20		diccionario de datos		Fuga o revelación de información	Falta de control en datos de entrada y salida	**Analista de Sistemas**	12.4	12.4.1 12.4.2 12.4.3
R21		Esquema de datos		Fuga o revelación de información	Falta de control en datos de entrada y salida	**Analista de Sistemas**	12.4	12.4.1 12.4.2 12.4.3
R22	**Gestión de Riesgo Informático**	Computador Personal - HP	**Analista Tic**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
				Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	16.1	16.1.3 16.1.5
R23		Matriz de riesgo		Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	8.1 12,6	8.1.1 12,6,2
R24		Activos GADPE		Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	9.2	9.2.1 9.2.3 9.2.6
R25	**Continuidad de los Servicios**	Solicitud de nuevo servicio	**Analista Tic**	Incumplimiento de leyes	Inadecuada capacidad de gestión	**Analista Tic**	17.1 17.2 18.1	17.1 .2 17.1.2 17.1.3 17.2.1 18.1.1

R26		Servidor-Panasonic		Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	12.1	12.1.1
R27		Base de Datos		Acceso no autorizado al sistema de información	Contraseñas inseguras	**Analista de Redes**	9.1 9.4 10.1	9.1.1 9.1.2 9.4.2 10.1.2
R28		Data Center - Libert		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	11.1	11.1.2
R29	**Monitoreo de Redes y Comunicaciones**	Servidor tipo Blade-IBM	**Analista de Redes**	Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	13.1	13.1.1
R30		Redes de datos		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	7.2	7.2.1 7.2.2
R31		Contrato de Redes y Telecomunicaciones		Incumplimiento de relaciones contractuales	Inadecuada capacidad de gestión	**Analista de Redes**	7.1	7.1.1
R32		Reporte de Trafico de Red		Incumplimiento de leyes	Inadecuado nivel de conocimiento y/o concienciación de empleados	**Analista de Redes**	7.2 18.2	7.2.1 7.2.2 18.2.2
				Interceptación de información	Inadecuada gestión de redes	**Analista de Redes**	13.1 13.2	13.1.1 13.2.1 13.2.2
R33	**Resguardo de la información**	Servidor-Panasonic	**Alasita de Sistemas**	Daños ocasionados	Sesiones activas después del	**Analista de**	12.1	12.1.1

			Activos	durante pruebas de intrusión	horario laboral	**Sistemas**		
R34		Data Center - Libert		Acceso no autorizado al sistema de información	Contraseñas inseguras	**Analista de Redes**	9.1 9.4 10.1	9.1.1 9.1.2 9.4.2 10.1.2
R35		Base de Datos		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	11.1	11.1.2
R36		Servidor tipo Blade-IBM		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	13.1	13.1.1
R37		Redes de datos		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	7.2	7.2.1 7.2.2
R38		Computador personal HP		Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
R39		computador personal LENOVO		Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	16.1	16.1.3 16.1.5
R40		Computador HP		Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	8.1 12,6	8.1.1 12,6,2
R41		Computador COMPAQ		Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	9.2	9.2.1 9.2.3 9.2.6
R42		Computador Apple		Uso no autorizado de software	Sesiones activas después del horario laboral	**Analista de Sistemas**	10.1 11.1	10.1.2 11.1.2

							11.2	11.2.4
R43		Computador Portátil Toshiba		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R44		Computador Aditk		Error de usuario	Eliminación de soportes de almacenamiento sin borrado de datos	**Analista de Sistemas**		
R45		Computador Altek		Modificación no autorizada de registros	Claves criptográficas accesibles a personas no autorizadas	**Analista de Sistemas**	10.1	10.1.1 10.1.2
R46		SISTEMA PROGRAMA DE CONTABILIDAD-Olimpo		Daños provocados por actividades de terceros	Redes accesibles a personas no autorizadas	**Analista de Sistemas**	15.1	15.1.1 15,1,2 15,1,3
R47		LICENCIA WINDOWS-Server 2003		Daños ocasionados durante pruebas de intrusión	Bases de datos con protección desactualizada contra códigos maliciosos	**Analista de Sistemas**	12.2	12.2.1
R48		SISTEMA INF. DE CONT. Y FISCAL. DE OBRAS		Destrucción de registros	Sistemas desprotegidos ante acceso no autorizado	**Analista de Sistemas**	9.4 11.1	9.4.1 9.4.2 9.4.3 11.2 11.3

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

R55		Solicitud de Respaldo		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R56		Información Respaldada		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R57		SOFTWARE DE INFORM. GEOGRÁFICA		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R58	**Instalación y Actualización de Software**	computador personal HP	**analista de sistemas**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
R59		computador personal LENOVO		Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	16.1	16.1.3 16.1.5
R60		Computador HP		Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	8.1 12,6	8.1.1 12,6,2
R61		Computador COMPAQ		Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	9.2	9.2.1 9.2.3 9.2.6
R62		Computador Apple		Uso no autorizado de software	Sesiones activas después del horario laboral	**Analista de Sistemas**	10.1 11.1 11.2	10.1.2 11.1.2 11.2.4

R63		Computador Portátil Toshiba		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R64		Computador Aditk		Daños provocados por actividades de terceros	Eliminación de Registros y datos de funcionamiento de la información	**Analista de Sistemas**		
R65		Computador Altek		Errores de mantenimiento	Inadecuado control de cambios	**Analista de Sistemas**		
R66		SISTEMA PROGRAMA DE CONTABILIDAD-Olimpo		Robo	Inadecuada gestión del empleador	**Analista de Sistemas**	7.1	7.1.1 7.1.2
R67		LICENCIA WINDOWS-Server 2003		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R68		SISTEMA INF. DE CONT. Y FISCAL. DE OBRAS		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R69		SIST. CAPTURA DATOS CONTROL ACTIVOS-		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3

		Symbol						
R70		SISTEMA DE AUTOMATIZACIÓN DE TEMPERATURA		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R71		PAQUETE TÉCNICO DE CALCULO		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R72		SOFTWARE DE INFORM. GEOGRÁFICA		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R73	**Administración de intranet, internet y correo electrónico**	Servidor-Panasonic	**analista de sistemas activos**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
R74		Data Center - Libert		Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	16.1	16.1.3 16.1.5
R75				Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	8.1 12.6	8.1.1 12.6.2
R76				Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	9.2	9.2.1 9.2.3 9.2.6
R77				Uso no autorizado de software	Sesiones activas después del horario laboral	**Analista de Sistemas**	10.1 11.1 11.2	10.1.2 11.1.2 11.2.4

R78				Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R79				Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**	12.1	12.1.1
R80		Base de Datos		Acceso no autorizado al sistema de información	Contraseñas inseguras	**Analista de Redes**	9.1 9.4 10.1	9.1.1 9.1.2 9.4.2 10.1.2
R81		Servidor tipo Blade-IBM		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	11.1	11.1.2
R82		Redes de datos		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	13.1	13.1.1
R83		Contrato de Redes y Telecomunicaciones		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	16.1	16.1.1
R84	**Desarrollo e Integración de Sistema**	Aplicaciones Desarrolladas	**analista de sistemas activos**	Contagio de virus	Falta de antivirus con licencia	**Analista de Sistemas**	12.2	12.2.1
R85		Servidor-Panasonic		Sustracción de información	Puertos USB habilitados	**Analista de Sistemas**	16.1	16.1.3 16.1.5

R86		base de Datos		Instalación no autorizada de software	Falta de inventario de licencias instaladas	**Analista de Sistemas**	8.1 12.6	8.1.1 12.6.2
R87		Servidor tipo Blade-IBM		Acceso no autorizado a la red	Sesiones activas después del horario laboral	**Analista de Sistemas**	9.2	9.2.1 9.2.3 9.2.6
R88		Redes de datos		Uso no autorizado de software	Sesiones activas después del horario laboral	**Analista de Sistemas**	10.1 11.1 11.2	10.1.2 11.1.2 11.2.4
R89		Data Center - Libert		Modificación accidental de datos del sistema de información	Sesiones activas después del horario laboral	**Analista de Sistemas**	7.2 9.4	7.2.1 9.4.3
R90				Daños ocasionados durante pruebas de intrusión	Sesiones activas después del horario laboral	**Analista de Sistemas**		
R91		Manual de usuario		Mala utilización de la aplicación	Mala redacción del manual	**Analista de Redes**	9.1 9.4 10.1	9.1.1 9.1.2 9.4.2 10.1.2
R92		Manual de Instalación de Sistema		Acceso físico no autorizado	Sistemas desprotegidos ante acceso no autorizado	**Analista de Redes**	11.1	11.1.2
R93		Cronograma de Trabajo		Acceso no autorizado a la red	Redes accesibles a personas no autorizadas	**Analista de Redes**	13.1	13.1.1

R94		Acta de entrega del Sistema		Otros desastres (causados por el hombre)	Falta de separación de entornos de prueba y operativos	**Analista de Redes**	14.1 14.2	14.1.1 14.1.2 14.1.3 14.2.1 14.2.3 14.2.6
R95		Código Fuente		Plagio	Falta de control de desarrollo			
				Mala utilización de la aplicación	Mala redacción del manual		14.2	14.2.1

Tabla 18: Selección de controles y objetivos de control

CAPITULO IV: ANÁLISIS DE IMPACTOS.

4.1 ANTECEDENTES

Luego de culminar con la evaluación de la seguridad de la información en el departamento de TIC del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas, se han considerado los siguientes impactos: Tecnológico, Económico y Administrativo.

Para la correcta interpretación de estos impactos se utilizara la matriz de impacto que dicta lo siguiente:

VALOR IMPACTO	DESCRIPCIÓN
-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.

Tabla 19: Tabla de impactos

4.2 Impacto Tecnológico.

IMPACTO TECNOLÓGICO							
NIVELES DE IMPACTO **INDICADORES**	**-3**	**-2**	**-1**	**0**	**1**	**2**	**3**
• Controles tecnológicos. • Optimización de la seguridad. • Avance de los servicios tecnológicos.							X X X
TOTAL							**9**

$$\sum = 9$$

$$NI = \frac{9}{3} = 3$$

Nivel de impacto tecnológico = Alto Positivo.

Tabla 20: Impacto tecnológico

Análisis:

- Los controles tecnológicos tendrán un impacto alto positivo con la aplicación de la normativa de seguridad porque esta permite llevar un registro de errores y ofrece soluciones para los mismos.

- La optimización de la seguridad tendrá un impacto alto positivo debido a que con las diferentes etapas impuestas por la normativa de seguridad se corregirán errores en los procesos de control.

- El avance tecnológico tendrá un impacto alto positivo puesto que se aprovechara al máximo la infraestructura tecnológica para lograr que los servicios estén funcionales.

4.3 Impacto Económico.

IMPACTO ECONÓMICO							
NIVELES DE IMPACTO **INDICADORES**	**-3**	**-2**	**-1**	**0**	**1**	**2**	**3**
• Inversión en equipo tecnológico. • Gastos por capitación del personal. • Ahorro de dinero en consultorías.	X	X					X
TOTAL	**-3**	**-2**					**3**

$\sum = -2$

$$NI = \frac{-2}{3} = -0,67 \approx 1$$

Nivel de impacto económico = Bajo Negativo.

Tabla 21: Impacto económico

Análisis:

- La inversión en equipo tecnológico tendrá un impacto alto negativo por las adquisiciones que se deben hacer para logra un óptimo desempeño en la seguridad de la información.

- Los gastos por capacitación del personal tendrá un impacto medio negativo debido a que será una inversión para que el personal esté capacitado y pueda comprender la seguridad de la información.

- El ahorro de dinero en consultorías tendrá un impacto alto positivo debido a que la capacitación correcta del personal servirá para dar soluciones a problemas puntuales que puedan presentare con la normativa de seguridad.

4.4 Impacto Administrativo.

IMPACTO ADMINISTRATIVO							
NIVELES DE IMPACTO **INDICADORES**	**-3**	**-2**	**-1**	**0**	**1**	**2**	**3**
• Aplicación de estándares. • Seguridad de la información. • Metodología de gestión de riesgo tecnológico. • Evaluación de procesos y activos utilizados.							X X X X
TOTAL							**12**

$\sum = 12$

$$NI = \frac{12}{4} = 3$$

Nivel de impacto económico = Alto Positivo.

Tabla 22: Impacto administrativo

Análisis:

- La aplicación de estándares tendrá un impacto alto positivo porque siguiendo las diferentes etapas de la normativas se logra un funcionamiento adecuado de los diferentes servicios ofrecidos por el departamento de TIC.

- La seguridad de la información tendrá un impacto alto positivo puesto que la normativa tiene como uno de sus objetivos principales corregir las falencias que se encuentre en cuanto a la seguridad.

- La metodología de gestión de riesgo tiene un impacto alto positivo debido a que se cumplió con todos los parámetros establecidos por la normativa para realizar la correcta gestión de riesgo.

- La evaluación de procesos y activos asignados tendrá un impacto alto positivo debido a que serán identificados los procesos vitales del departamento y los recursos que utilizan para llevar acabo sus actividades.

4.5 Impacto General.

IMPACTO GENERAL							
NIVELES DE IMPACTO **INDICADORES**	**-3**	**-2**	**-1**	**0**	**1**	**2**	**3**
• Impacto Tecnológico. • Impacto Económico. • Impacto Administrativo.			X				X X
TOTAL			-1				**6**

$$\sum = 5$$

$$NI = \frac{5}{3} = 1{,}66 \approx 2$$

Nivel de impacto General = Medio Positivo

Tabla 23: Impacto general

Análisis:

- El presente proyecto genera en si un impacto en general **Medio Positivo** teniendo en cuenta los tres impactos evaluados (Tecnológico, Económico y Administrativo), la inversión realizada en equipos tecnológico se justifica con la correcta gestión y tratamiento de riesgo debido a que esto permitirá que la información se encuentre protegida con controles adecuados el personal este correctamente capacitado y los activos de la institución sean utilizados de manera correcta.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Al establecer un alcance en el Sistema de Gestión de Seguridad de la Información se establece una delimitación del campo de acción y uso de los recursos.

- Personal interno con experiencia en la Normativa ISO 27001 reducirá gastos debido a que no será necesario contar con servicios de consultorías externas en el momento que se presente algún inconveniente.

- La normativa ISO27000 ofrece un conjunto de controles para tratar de manera adecuada la información vital de una institución, ofreciendo un rol protagónico a la alta gerencia y llenar así sus expectativas.

- El objetivo principal de la gestión de seguridad de la información es identificar de manera exacta los riesgos a los cuales están expuestos los activos y de esta manera evitar pérdidas significativas para la institución.

- La selección de controles permite que los riesgos sean tratados para proteger la integridad de los activos y de manera el impacto causado en la institución sea bajo, teniendo en cuenta que la aplicación del control no debe exceder en costo al impacto que podría generar la materialización de la amenaza.

4.2 RECOMENDACIONES

- El rol protagónico que cumple la alta gerencia en esta normativa es fundamental por lo cual deben estar predispuestos a colaborar y participar en cada uno de las etapas que se realizan dentro de la implantación de la normativa.

- Capacitar constantemente al personal y estimular a cumplir con todos los procesos asignados servirá de ayuda para el correcto funcionamiento de los controles establecidos.

- Realizar la evaluación de riesgos en un determinado lapso de tiempo para identificar y analizar las amenazas o riesgos que permanentemente están presentes en los sistemas de información y los activos, con el propósito de seleccionar los controles necesarios para que sean reducidos.

- La institución debe facilitar las tareas operativas y adaptación del SGSI mediante el uso de herramientas tecnológicas para la automatización de las etapas del proceso del Sistema de Seguridad de la Información.

BIBLIOGRAFÍA

- AESIS. (04 de Octubre de 2010). Software para soluciones empresariales. Obtenido de AESIS: http://www.aesist.com/soporte/mantenimiento-perfectivo
- Anaya, L., Herrera, E., Tarazona, J., & Tarazona, J. (s.f.). Auditoria de sistemas.
- Areiza Correa, J. D., Carvajar Raigosa, J. M., & Gomez Ocampo, S. (2009). Definicion de un cuadro de mando para la gestiónde servicios de TI, que apoye la toma de decisiones en una empresa de servicios, aplicando los modelos de gobierno. Medellin.
- Arens, A. A. (1995). Auditoría Un enfoque general. New Jersy.
- Bligoo. (19 de 06 de 2014). Aspectos de Seguridad de un Sistema de Información. Obtenido de Aspectos de Seguridad de un Sistema de Información: http://seguridadsistemadeinformacion.bligoo.es/medios-de-transmision-de-ataques-a-los-sistemas-de-seguridad#.U6z5v_l5O5U
- Bligoo. (19 de 06 de 2014). Aspectos de Seguridad de un Sistema de Información. Obtenido de Aspectos de Seguridad de un Sistema de Información: http://seguridadsistemadeinformacion.bligoo.es/
- Brenner, J. (19 de 06 de 2014). Questia. Obtenido de Questia: http://www.questia.com/read/1P3-1195022701/iso-27001-risk-management-and-compliance
- Brys, C. (2005). Plan estrategico del gobierno electronico. San Luis: Universitaria de misiones.
- Cabo, A. M. (23 de Junio de 2006). Evaluación del uso de los sistemas. Obtenido de Congreso Iberoamericano de Ciencia, Tecnologia, Sociedad e innovacion: http://www.oei.es/memoriasctsi/mesa8/m08p15.pdf
- Calder, A. (2009). Information Security based on ISO27001/ISO27002. Amersfoort-NL: Van Haren Publishing.
- Calder, A. (2013). Nine Steps to Success. Reino Unido: It Governance.
- Carrasco, L. (2015). Gobierno y gestion TI. Mataro.
- Comunidad Internacional de Implantadores de ISO27000. (20 de 06 de 2014). ISO27001 Security. Obtenido de ISO27001 Security:

http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf

- (Madrid). Enciclopedia de la auditoria. Océano.
- Escobar, E. (13 de ABRIL de 2011). SlideShare. Obtenido de PROCESO DE AUDITORIA DE SISTEMAS: http://es.slideshare.net/EdgarEscobar2/proceso-de-auditora-de-sistemas
- Espinosa, L. (2012). Programa de Maestría en Evaluación. Quito.
- Fernandez, E. (2009). El gobierno y la gestión de las TIC. Caracas: Dikinson.
- Franco G, J. (05 de Enero de 2014). Monografias. Obtenido de Auditoria Fiscal: www.monografias.com/trabajos13/audfisc/audfisc.shtml
- GADPE. (2014). POLITICAS, PROCESOS Y PROCEDIMIENTOS DE TIC.
- GesConsultor. (20 de 06 de 2014). GesConsultor. Obtenido de GesConsultor: http://www.gesconsultor.com/iso-27001.html
- Harrison, P. (2011). Gobierno de TI. Australia: Agosto.
- INDECOPI. (20 de 06 de 2014). INDECOPI. Obtenido de INDECOPI: http://bvirtual.indecopi.gob.pe/normas/isoiec27001.pdf
- ISO 27000.es. (20 de 06 de 2014). El portal de la ISO27000. Obtenido de El portal de la ISO27000: http://www.iso27000.es/sgsi.html
- ITIL. (04 de Diciembre de 2014). ITILI V3. Obtenido de Gestion de servicios TI: http://itilv3.osiatis.es/operacion_servicios_TI/peticion_servicios_ti.php
- Lainhart, J. W. (2011). COBIT. Belgica.
- Lázzaro, V. (2009). Sistemas y Procedimientos. Almeria.
- mmujica. (20 de 06 de 2014). Tecnología de Información BETA. Obtenido de Tecnología de Información BETA: https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf
- Muzio, F. J. (22 de Mayo de 2012). Proteccion de activos, vision del riesgo. Obtenido de Mecalux: http://www.logisticasud.enfasis.com/articulos/64054-proteccion-activos-vision-del-riesgo
- Naranjo, A. (2012). Conceptos de la auditoria de sistemas. Madrid.

- Nissen, C. (2011). CGEIT. Dinamarca.
- Oviedo Sotelo, P. B. (22 de Julio de 2010). Monografias. Obtenido de Auditoria finaciera: www.monografias.com/trabajos607
- Oviedo, S. P. (22 de Julio de 2010). Monografias. Obtenido de Auditoria Financiera: www.monografias.com/trabajos60/auditoria-financiera/auditoria-financiera-shtml
- Pacheco, O. R. (2008). Gestion de las TIC en una organizcion. Madrid.
- Paredes, V. V. (22 de Noviembre de 2013). Auditoria de Sistemas - Proteccion de los activos de Informacion. Obtenido de SlideShare: http://www.scribd.com/doc/56068563/Auditoria-de-Sistemas-Proteccion-de-los-activos-de-Informacion#scribd
- Parra Galvis, A. F., & Cardona, E. (2011). PRINCIPIOS DE AUDITORIA. Bogotá.
- Pascual, L. V. (17 de Julio de 2011). Planeacion y programacion de una auditoria informática. Obtenido de Universidad Autonoma del Estado de Hidalgo: http://www.uaeh.edu.mx/docencia/P_Presentaciones/huejutla/sistemas/auditoria_informatica/auditoria.pdf
- Prefectura de Esmeraldas. (19 de 06 de 2014). Prefectura de Esmeraldas. Obtenido de Prefectura de Esmeraldas: http://www.prefecturadeesmeraldas.gob.ec/index.php/en/
- Prefectura de Esmeraldas. (19 de 06 de 2014). Prefectura de Esmeraldas. Obtenido de Prefectura de Esmeraldas: http://www.prefecturadeesmeraldas.gob.ec/images/pdf/POA%20GADPE%202013.pdf
- Red Hat, Inc. (18 de 06 de 2014). Red Hat Enterprise Linux 4. Obtenido de Red Hat Enterprise Linux 4: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-response-plan.html
- Rondon, F. G. (2006). Auditoria Administrativa. Buenos Aires.
- Sanchez, H. (10 de Febrero de 2015). Diseño e implantacion de sistemas de informacion y procesamiento de datos para empresas. Obtenido de Monografias.com: http://www.monografias.com/trabajos14/implantacion-datos/implantacion-datos.shtml
- Sanchez, J. A. (2010). Auditoría de los Sistemas de Información. Madrid.
- Solarte, F. N. (04 de Noviembre de 2012). Blogspot. Obtenido de Metodología para realizar auditoria: http://auditordesistemas.blogspot.com/2011/11/metodologia-para-realizar-auditoria.html

- Tecnovaplus. (7 de Febrero de 2015). Soporte y mantenimiento de sistemas de información. Obtenido de Tecnovaplus: http://www.tecnovaplus.com/nuestros-servicios-menuizquierda/soporte-y-mantenimiento.html

- Ugalde, F. (25 de Septiembre de 2010). Mantenimiento Adaptativo. Obtenido de Jummp: https://jummp.wordpress.com/2010/09/25/mantenimiento-adaptativo/

- Vander, K. L. (10 de Mayo de 2012). Un marco de negocio para el gobierno y la gestion de las TI de la empresa. Obtenido de ISACA COBIT: www.isaca.org/COBIT/Documents/COBIT5-Framework-Spanish.pdf

- Villalobos, J. (10 de Enero de 2015). Sistemas de informacion Mantenimiento. Obtenido de Monografias.com: http://www.monografias.com/trabajos94/sistemas-de-informacion-mantenimiento/sistemas-de-informacion-mantenimiento.shtml

- Wikipedia. (18 de 06 de 2014). Wikipedia. Obtenido de Wikipedia: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

- Wikipedia. (19 de 06 de 2014). Wikipedia. Obtenido de Wikipedia: http://es.wikipedia.org/wiki/ISO/IEC_27001

ANEXOS

Anexo 1

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE ESMERALDAS

ENCUESTA DIRIGIDA AL PERSONAL DEL DEPARTAMENTO DE TIC DEL GADPE

OBJETIVO: Conocer la infraestructura tecnológica y el conocimiento sobre normativas de seguridad.

1. **¿Considera usted que el departamento de informática tiene el personal suficiente para cumplir eficientemente con su función?**

2. **¿El departamento de TIC cuenta con la normativa de seguridad ISO 27001?**

3. **¿Tienen conocimiento en el departamento de TIC sobre las normativas de seguridad ISO 27001 o COBIT?**

4. **¿Ha sufrido alguna fuga o pérdida de información importante el departamento de TIC?**

5. **¿Ha sufrido algún ataque de hackers en la institución?**

6. **Se han adoptado medidas de seguridad en del departamento de TIC?**

7. **¿Se ha dividido la responsabilidad para temer un mejor control de la seguridad?**

Anexo 2

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE ESMERALDAS

ENTREVISTA DIRIGIDA AL DIRECTOR DEL DEPARTAMENTO DE TIC

OBJETIVO: Conocer el tipo de información manejada en el departamento de TIC del GADPE.

1. **¿Qué tipo de información maneja el departamento?**

2. **¿Cuáles son las Áreas que maneja el departamento dentro de la institución?**

3. **¿Cómo es manejada la información no confidencial en el departamento?**

4. **¿Cómo es tratada la información de tipo confidencial en el departamento?**

5. **¿Quién o quienes se encargan específicamente de la información confidencial manejada por el departamento?**

6. **¿Cuáles son las reglas que debe seguir el personal en el manejo de la información confidencial manejada por el departamento?**

Anexo 3

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE ESMERALDAS

ENTREVISTA DIRIGIDA AL ANALISTA DEL DEPARTAMENTO DE SISTEMAS DEL GADPE

OBJETIVO: Conocer el funcionamiento y los diferentes controles que se aplican dentro del departamento de Informatica del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas.

.

1. **¿Cuáles son las especificaciones técnicas del equipo informático con el que cuenta el departamento?**

2. **¿Con que frecuencia se les da mantenimiento a los equipos de departamento?**

3. **¿Cuáles son las adecuaciones y condiciones de departamento implantadas para mejorar y facilitar el trabajo de los empleados y la operación equipos informáticos?**

4. **¿Cuáles son las funciones específicas del departamento dentro de la Institución?**

5. **¿Cuáles son los procesos que lleva a cabo el departamento para el cumplimiento de sus funciones?**

6. ¿**El departamento cuenta con políticas que regulen el funcionamiento**?

7. ¿**Las actividades esta dividas en procesos**?

8. ¿**Los activos están asociados a los procesos, de ser así están correctamente identificados**?

Anexo A ISO 27000

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ISO27002.es PATROCINADO POR:

Octubre-2013