PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE ESMERALDAS

ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TESIS DE GRADO

TEMA: PLAN DE GESTIÓN DE RIESGO INFORMÀTICO PARA EL GOBIERNO AUTONOMO DESCENTRALIZADO DE LA PROVINCIA DE ESMERALDAS.

LÍNEA DE INVESTIGACIÓN:

GOBIERNO Y ADMINISTRACIÓN DE TECNOLOGÍA DE INFORMACIÓN

AUTOR: CEDEÑO CANESSA GABRIELA SUGEY

ASESOR: MGT. DAVID RODRIGUEZ PORTES

MES / AÑO: ENERO 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.

Ing. Kleber Vera T

PRESIDENTE DEL TRIBUNAL DE GRADUACIÓN.

Ing. Kleber Vera T.

LECTOR 1

Mgt. Xavier Quiñonez Ku

LECTOR 2

Mgt- David Rodríguez P.

DIRECTOR DE TESIS.

Mgt. Xavier Quiñonez Ku

DIRECTOR DE ESCUELA

FECHA: _____

AUTORÍA

Yo, Gabriela Sugey Cedeño Canessa, portadora de la cédula de ciudadanía Nº0802487736, declaro bajo juramento que la presente investigación es de total responsabilidad de la autora, y que se ha respetado las fuentes de información consultadas, realizando las citas correspondientes.

_____

Gabriela Sugey Cedeño Canessa

AUTORA

DEDICATORIA

A Dios, por darme sabiduría y optimismos y sobretodo la debida perseverancia para poder lograr un éxito más en mi vida y permitir vivir cosas buenas y malas, gracias a eso soy una persona de bien.

A mi padre querido Yomar Cedeño por día a día inculcar a mis hermanos y a mí el significado de la superación y mi madre Gina Canessa por guiarme por el camino del bien amados, por ser ellos los pilares esenciales en mi vida, sin ellos jamás hubiese podido lograr lo que hasta ahora, y hacer que mis hermanos Abraham Cedeño y Nayeli Cedeño sigan este camino del bien.

A mi esposo Fausto Cabezas, mi amado compañero que Dios y la vida puso en mi camino, por motivarme a dar ese último paso para alcanzar este hermoso y tan anhelado logro.

Gabriela Sugey Cedeño Canessa

AGRADECIMIENTO

En mi primer lugar a Dios, por darme las ganas de seguir adelante y hacer que cumpla mis logros diariamente, a mis padres, hermanos que me han dado su apoyo en todo momento.

A los docentes de la PUCESE, por los conocimientos y valores infundidos en el transcurso de mi carrea universitaria.

Al Ing. David Rodríguez, asesor de tesis, por su apoyo incondicional y por la paciencia en esclarecer dudas, y como no decir por su valiosa ayuda para la elaboración del proyecto, a mis lectores Ing. Kleber Vera T. por todo la dedicación, y porque no agradecerle al Ing. Xavier Quiñonez, por enseñarme que la perseverancia se logran muchos objetivos.

RESUMEN

La presente investigación de tipo descriptiva es 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 mejorar la administración y gobierno de las Tecnologías de Información y Comunicación mediante una adecuada gestión de riesgo informático.

Durante el desarrollo del proyecto el principal problema fue acceder a información de cada proceso considerada como crítica, para según eso priorizar y clasificar los activos asignados como recursos necesarios para la operatividad de cada función dentro de la institución. Para lo cual, el uso de técnicas como: encuesta, entrevista y observación han sido de vital importancia en la sistematización de la información a través de los procesos estadísticos y la generación de gráficos que permitan un correcto análisis de cada aspecto determinado en la respectiva matriz de operacionalización diagnóstica.

Con la elaboración del Plan de Gestión de Riesgo Informático no solo se mejora el nivel de seguridad de los procesos que utilizan TIC sino que se optimizan los recursos existentes y se corrigen aspectos descuidados. Los resultados medidos en los impactos establecen que la institución obtuvo como beneficios la identificación y clasificación de los riesgos de sus activos informáticos de manera que pueda gestionar oportuna y eficientemente su tratamiento minimizando su impacto y optimizado los recursos existentes garantizando la disponibilidad, integridad y confidencialidad de la información ante cualquier contingencia.

Palabras claves:*Planificación, gestión, riesgo, activo informático, Contingencia*

ABSTRACT

The present research of descriptive type is of great importance for the Autonomous Government Decentralized of the Province of Esmeraldas and the department of TIC because the main objective is to improve the administration and government of the Information and Communication Technologies through an adequate risk management Computer science.

During the development of the project the main problem was to access information from each process considered as critical, so as to prioritize and classify the assigned assets as resources necessary for the operation of each function within the institution. For this, the use of techniques such as: survey, interview and observation have been of vital importance in the systematization of information through the statistical processes and the generation of graphs that allow a correct analysis of each determined aspect in the respective matrix of diagnostic operation.

With the IT Risk Management Plan, not only does it improve the level of security of the processes that use ICT, but also optimize existing resources and correct neglected aspects. Impact-based results establish that the institution obtained as benefits the identification and classification of the risks of its IT assets so that it can manage its home treatment in a timely and efficient manner, minimizing its impact and optimizing the existing resources, guaranteeing the availability, Integrity and confidentiality of the information before any contingency.

Key words: *Planning, management, risk, computer asset, Contingency*

CONTENIDO

ANEXOS 121

CONTENIDO DE TABLAS

CONTENIDO DE FIGURAS

INTRODUCCIÓN

Se viven tiempos en donde los factores exógenos muchas veces alteran el orden establecido, desde aspectos como los fenómenos naturales a otros tan complejos como los políticos, religiosos o culturales; todos impredecibles muchas veces, y paralelo a ello el vertiginoso avance de las tecnologías de información y comunicación presentes en casi toda actividad humana que amerite el procesamiento de datos y la generación de conocimiento a nivel individual o institucional, o personal comunitario, básico o complejo, no importa la taxonomía que se cite, se viven tiempos en los cuales la información tiene valor para quienes la gestionan y son el activo principal para aquellos que toman decisiones que impactan sobre la población. De allí que garantizar que esa información esté disponible, sea útil, relevante, completa, económica y ágil no solo depende de tener tecnologías o recursos tecnológicos sino también de contar mecanismos que aseguren y garanticen la continuidad de las operaciones y el funcionamiento de una institución ante cualquier contingencia.

En el primer capítulo se desarrolló una fundamentación teórica con los temas más relevantes relacionados al tema central de la gestión de riesgo informático con un enfoque orientado al sector público, y específicamente aplicado a la gestión de las Tecnologías de Información y Comunicación en el Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas a través del cumplimiento de las leyes y normas de control interno establecidas por la Contraloría General del Estado.

En el segundo capítulo se realizó un diagnóstico mediante la aplicación de instrumentos metodológicos utilizando las técnicas de investigación como son la entrevista, encuesta y observación de cada uno de los aspectos que describen a las variables en una matriz de relación diagnóstica que sirvió como guía para la sistematización de los resultados mediante cuadros estadísticos, la respectiva interpretación y análisis de los resultados obtenidos que posibilitaron el establecimiento del problema.

En el tercer capítulo se presenta en calidad de propuesta un Plan de Gestión del Riesgo en base a metodologías y estándares considerados como las mejores prácticas en el gobierno

de las TI en lo que a riesgo se refiere, esto incluye el diseño de una matriz de riesgo así como la incorporación de los recursos actualizados, responsables, calendario y procedimientos en caso de contingencias propias de la naturaleza de la institución.

En el capítulo cuarto, se establecen los impactos más selectos que la investigación generó, genera y generará en los ámbitos: tecnológico, administrativo, organizacional, legal, ético e incluso ambiental, a través de la definición de indicadores para cada tipo de impacto que han sido cuantificados y valorados mediante una matriz resumen que permite representar el nivel de cada impacto.

Por último, se establecieron las conclusiones generales obtenidas y relacionadas con el tema de investigación en cada fase del proceso, así como también las recomendaciones sugeridas a la institución objeto de estudio, el departamento de TIC, la universidad, y los estudiantes de la carrera de ingeniería de sistemas que puedan utilizar los resultados y anexos.

CAPITULO I: MARCO TEÓRICO

1.1 Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas

1.1.1 Fundamentación legal

Los Consejos Provinciales en el año 1928 – 1929, aparecen cuando en la Constitución Política del Estado se crean oficialmente dichos organismos seccionales en el Art. 139 de la Carta Magna. Es en cumplimiento de este mandato constitucional que se organizan en el Ecuador los Consejos Provinciales en representación y administración del Estado a nivel del Gobierno intermedio.

Hasta la actualidad en que la Constitución del año 2008 define las competencias exclusivas de los ahora llamados Gobiernos Autónomos Descentralizados, dentro de los cuales los Gobiernos Provinciales redefinen su denominación a Gobiernos Autónomos Descentralizados Provinciales. Las funciones, atribuciones y competencias se detallan en el Código Orgánico de Organización Territorial, Autonomías y Descentralización. (COOTAD, 2011)

1.1.2. Historia del GADPE

El Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas (GADPE) es una institución honorable, responsable y vinculada al desarrollo de la sociedad dentro del marco de los siguientes ejes: Salud, Vialidad, Educación, Turismo, Cultura, Medio Ambiente y mediante el programa PRODERENA que es un "Programa de Apoyo a la Gestión Descentralizada de los Recursos Naturales en las Tres Provincias del Norte del Ecuador" el cual tiene como fin mejorar las condiciones de vida de la población de las Provincias de Imbabura, Carchi y Esmeraldas, fortaleciendo el proceso de descentralización de la gestión de los recursos naturales.

En la Constitución Política No. 18 de la República, Registro Oficial No 1 del 11 de Agosto del año 1998 se constituye el Gobierno Provincial como la entidad estatal que a nombre del Estado, en la Provincia, ejerce su gobierno, la representación y administración política, articula y ejerce la intermediación de las acciones de los gobiernos nacionales y municipalidades.

En el período 2000 – 2004 ocupa la Prefectura don Homero Horacio López Saúd, y desde el 2005 hasta la fecha, cumpliendo ahora su segunda administración, fue re-electa como Prefecta la Ing. Lucía de Lourdes Sosa Robinzón de Pimentel. (López Estupiñan, Luis, 2007)

1.1.3 Misión y Visión

Según GADPE (2014) la Prefectura de Esmeraldas tiene definido:

> **Misión:** 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.
>
> **Visión:** El Gobierno Autónomo Descentralizado Provincial de Esmeraldas, al 2019 seguirá posicionada como Institución gestora del desarrollo, progreso y cambio en el territorio provincial, reconocida por la capacidad de gestión ante organismos gubernamentales y no gubernamentales, aplicando el modelo de gestión por procesos, altamente sistematizada, orientado a resultados y a servicios ágiles, eficiente de calidad y calidez a la ciudadanía en general.

1.1.4 Organigrama y modelo de gestión

En base al MANUAL INTEGRADO DE PROCESOS, PROCEDIMIENTOS Y PUESTOS DE TRABAJO (MPPP), aprobado como estrategia del GADPE para llegar a una Gestión por Procesos y Competencias, La estructura orgánica (Ver anexo N°1) funcional de la institución está basada en el nuevo modelo de gestión por procesos.

Según GADPE (2014) la Dirección de Tecnologías de la Información y Comunicación depende la implementación de una administración por procesos y sobretodo, de una gestión cero papeles, por lo que deberá:

- Definir un estándar de: servidor de correo electrónico, gestión documental y firma electrónica; de acuerdo a los documentos identificados en cada procedimiento, cada responsable de Proceso establecerá los Formatos de los documentos pertinentes que serán remitidos a Informática para ser codificados y subidos al Gestor Documental.

- En la Intranet, cada Dirección podrá contar con su página web que le permita colocar información y los formatos de los documentos pertinentes a ella.

- La Dirección de Gestión de TIC deberá dedicar recurso humano, recursos de hardware, de software y de conectividad que garantice el flujo de documentos, correos y la Gestión de un Archivo Electrónico que cumpla las regulaciones que tiene la Contraloría General del Estado sobre custodia y mantenimiento en forma conjunta con Secretaría General.

- Toda la documentación electrónica interna, de ida y vuelta entre Direcciones, será conservada en un Archivo Digital por el tiempo que estipula la Ley.

1.2. Dirección de Tecnologías de Información y Comunicación (TIC)

1.2.1. Funciones

El Departamento Tecnología de Información y Comunicación (TIC) del GADPE se encarga de planificar, desarrollar, dirigir, controlar, dar mantenimiento, operar y optimizar un sistema de tecnología de información y comunicación (TIC) para la institución, coordinando con todas los departamentos del GADPE a corto, mediano y largo plazo. (GADPE 2014).

De igual manera el GADPE provee a los empleados de todo lo necesario en cuanto a medios tecnológicos, normas, procedimientos y leyes para usar eficazmente los equipos y sistemas que posee la institución para así dar análisis, diseño, implantación y mantenimiento de los sistemas de acuerdo a las resoluciones aprobadas por el GADPE.

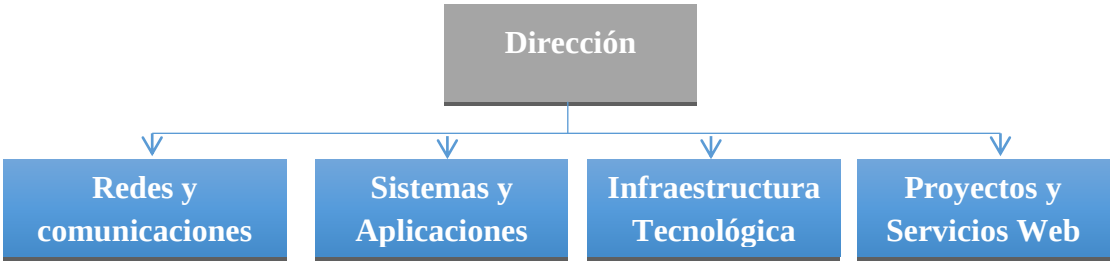
1.2.2. Misióny Visión

La misión de la Dirección de Tecnologías de la Información es un mecanismo posicionado 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.

LaDirección de Tecnologías de la Información en el 2019 se posicionará como referente de calidad y mejora continua en los GAD de la provincia 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.

1.2.3. Estructura Organizacional

Figura N°1: Organigrama del departamento de TIC



- **Dirección de gestión de TIC.-** Planificar, organizar, ejecutar y evaluar los sistemas, servicios e infraestructura de tecnología de información y comunicación de que requieren las diferentes instancias del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas.
- **Infraestructura Tecnológica.-** Garantizar la operación, funcionamiento continuo, y uso eficiente de la Infraestructura Tecnológica utilizada, para alcanzar los objetivos del plan informático de la Institución.
- **Redes y Comunicaciones.-** Planificar, organizar y controlar la red, los equipos de hardware y el software utilizado en el Gobierno Provincial para optimizar su uso en los procesos y actividades laborales.
- **Sistemas y Aplicaciones.-** Desarrollar e integrar sistemas, programas y aplicaciones informáticas definidas para las diferentes unidades administrativas, documentar los procesos de desarrollo y/o integración, adiestrar en el manejo a los usuarios del sistema.
- **Proyectos y Servicios Web.-** Administrar proyectos de tecnología y proveer servicios de internet, intranet, correo electrónico y sitio web de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos.

1.2.4. Procesos

Los macro-procesos definidos por la dirección se basan en los cuatro dominios de COBIT - Control Objectives for Information and related Technology (Objetivos de Control para la Información y Tecnología Relacionada), considerando como recursos de TIC lo siguiente:

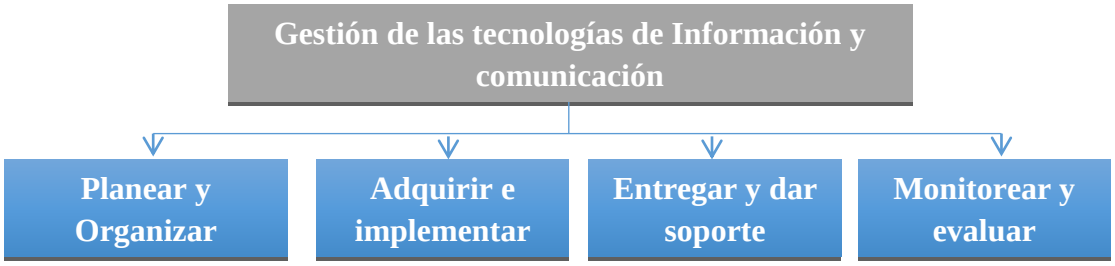
- **Las aplicaciones.-** incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

- **La información.-** son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.
- **La infraestructura.-** es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc.) que permiten el procesamiento de las aplicaciones.
- **Las personas.-** son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información.

1.2.5 Gestión

Según ISACA (2010) los dominios establecidos para un buen gobierno de TI son:

Figura N°2: Dominios del gobierno de TIC



- **Planear y Organizar (PO).-** Estrategias y tácticas. Identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio.

Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).

- **Adquirir e Implementar (AI)**: Identificación de soluciones, desarrollo o adquisición, cambios y/o mantenimiento de sistemas existentes. Proporciona las soluciones y las pasa para convertirlas en servicios.

- **Entregar y Dar Soporte (DS):** Cubre la entrega de los servicios requeridos. Incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios.

- **Monitorear y Evaluar (ME):** Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control.

1.3. Gestión del riesgo Informático

1.3.1. Definición de riesgo

Para Ambrustery (2014) el riesgo se define como: "cualquier condición que produzca una condición adversa en detrimento del producto, el paciente o el profesional de la salud".

Duarte (2013) señala que el riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos. Por último en estas referencias, Cancelado (2009) manifiesta que el riesgo es una condición del mundo real en el cual hay una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidad de pérdidas.

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).

1.3.2. Clasificación de Riesgos

Según Quirós(2013) los riesgos se pueden clasificar en:

- **Riesgo laboral:** Conjunto de entidades públicas y privadas, normas y procedimientos, destinados a prevenir, proteger y atender a los trabajadores de los efectos, de las enfermedades y los accidentes que puedan ocurrirles con ocasión o como consecuencia del trabajo que desarrollan.
- **Riesgo de Negocios:** Es el riego de los negocios estratégicos de la empresa y de sus procesos claves. En otras palabras, es un riesgo crítico de la empresa.
- **Riesgo Inherente:** Es la posibilidad de errores o irregularidades en la información financiera, administrativa u operativa, antes de considerar la efectividad de los controles internos diseñados y aplicados por el ente.
- **Riesgo de Auditoría:** Existe al aplicar los programas de auditoría, cuyos procedimientos no son suficientes para descubrir errores o irregularidades significativas.
- **Riesgo de Control:** Está asociado con la posibilidad de que los procedimientos de control interno, incluyendo a la unidad de auditoría interna, no puedan prevenir o detectar los errores e irregularidades significativas de manera oportuna.
- **Riesgo Estratégico:** Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con el cumplimiento de la misión de la Entidad, la cual busca la vigilancia de la conducta de los servidores públicos, defender el orden jurídico y los derechos fundamentales.
- **Riesgo Operativo:** Comprende tanto el riesgo en sistemas como operativo provenientes de deficiencias en los sistemas de información, procesos, estructura,

que conducen a ineficiencias, oportunidad de corrupción o incumplimiento de los derechos fundamentales.

- **Riesgo Financiero:** Se relaciona con las exposiciones financieras de la empresa. El manejo del riesgo financiero toca actividades de tesorería, presupuesto, contabilidad y reportes financieros, entre otros.
- **Riesgo de Cumplimiento:** Se asocia con la capacidad de la empresa para cumplir con los requisitos regulativos, legales, contractuales, de ética pública, democracia y participación, servicio a la comunidad, interacción con el ciudadano, respeto a los derechos, a la individualidad, la equidad y la igualdad.
- **Riesgo tecnológico:** Se asocia con la capacidad de la empresa en que la tecnología disponible satisfaga las necesidades actuales y futuras de la empresa y soporten el cumplimiento de la misión.

1.3.3. Causas de Riesgos de TI

Las causas de riesgo más comunes, para efectos del tema, se dividen en: Internas y Externas. Las causas de riesgo externas pueden ser de dos clases: Naturales (inundaciones, temblores, tornados, tormentas, huracanes, erupciones Volcánicas, etc.) y Motivadas por el Hombre (incendios, explosiones, accidentes laborales, destrucción intencional, sabotaje, robo, fraude, contaminación Ambiental, etc.); mientras que las causas internas de riesgo, se generan a partir de las mismas organización. (Coopers y Lybrand, 2007)

Son más frecuentes las causas internas de riesgo que las causas externas, entre las causas internas de riesgo se tiene básicamente: Robo (de materiales, de dinero y de información), sabotaje, insuficiencia de dinero, destrucción (de datos y de recursos), personal no capacitado, paros o huelgas, fraudes, ausencia de seguridades físicas (tanto de la institución como dela información).(Carrasco, 2015)

1.3.4. Riesgos de Tecnología de Información

El concepto de riesgo de TI puede definirse como el efecto de una causa multiplicado por la frecuencia probable de ocurrencia dentro del entorno de TI. Es el control el que actúa sobre la causa del riesgo para minimizar sus efectos. Cuando se dice que los controles minimizan los riesgos, lo que en verdad hacen es actuar sobre las causas de los riesgos, para minimizar sus efectos. (ITIL, 2014)

1.3.4.1 Valoración del Riesgo

La valoración del riesgo consta de tres etapas: La identificación, el análisis y la determinación del nivel del riesgo. Para cada una de ellas es necesario tener en cuenta la mayor cantidad de datos disponibles y contar con la participación de las personas que ejecutan los procesos y procedimientos para lograr que las acciones determinadas alcancen los niveles de efectividad esperados.

1.3.4.2. Identificación del Riesgo

El proceso de la identificación del riesgo debe ser permanente, integrado al proceso de planeación y responder a las preguntas qué, cómo y por qué se pueden originar hechos que influyen en la obtención de resultados.

Una manera de realizar la identificación del riesgo es a través de la elaboración de un mapa de riesgos, el cual como herramienta metodológica permite hacer un inventario de los mismos, ordenada y sistemáticamente, definiendo en primera instancia los riesgos, posteriormente presentando una descripción de cada uno de ellos y las posibles consecuencias.

1.3.4.3 Análisis del Riesgo

Luhmann (2000) sostiene que el Analisis del Riesgo establece una valoración y priorización de los riesgos con base en la información ofrecida por los mapas elaborados en la etapa de identificación, con el fin de clasificar los riesgos y proveer información para establecer el nivel de riesgo y las acciones que se van a implementar. Se han establecido dos aspectos para realizar el análisis de los riesgos identificados:

- **Probabilidad:** La posibilidad de ocurrencia del riesgo, la cual puede ser medida con criterios de frecuencia o teniendo en cuenta la presencia de factores internos y externos que puedan propiciar el riesgo, aunque éste no se haya presentado nunca.

  Para el análisis cualitativo se establece una escala de medida, en donde se crean categorías que van hacer utilizadas y la descripción de cada una de ellas, con el fin que cada persona aplique por ejemplo:
  ALTA: Es muy factible que el hecho se presente.
  MEDIA: Es factible que el hecho se presente.
  BAJA: Es poco factible que el hecho se presente.

- **Impacto:** Consecuencias que puede ocasionar a la organización la materialización del riesgo. Ese mismo diseño puede aplicarse para la escala de medida cualitativa de IMPACTO, estableciendo las categorías y la descripción, por ejemplo:
  ALTO: Si el hecho llegara a presentarse, tendría alto impacto o efecto sobre la Entidad;
  MEDIO: Si el hecho llegara a presentarse tendría medio impacto o efecto en la entidad;
  BAJO: Si el hecho llegara a presentarse tendría bajo impacto o efecto en la entidad.

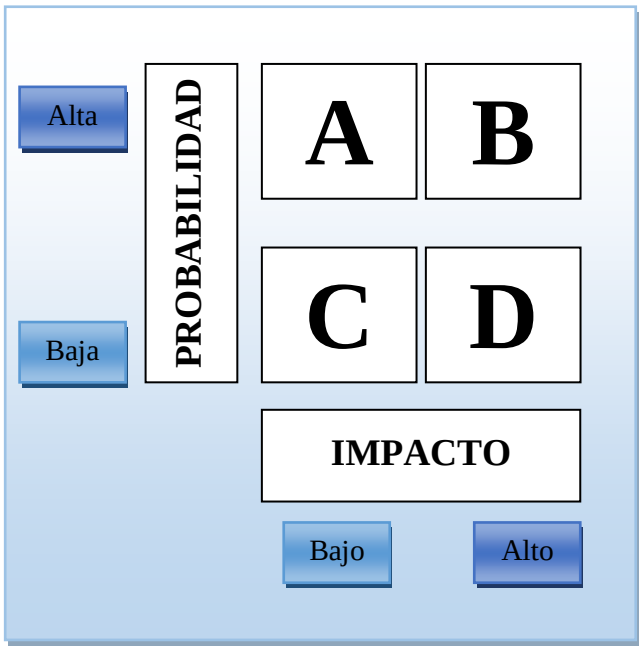
Los objetivos específicos del Análisis de Riesgo son: Analizar el tiempo, esfuerzo y recursos disponibles y necesarios para atacar los problemas; Definir cuáles son los recursos existentes; Llevar a cabo un minucioso análisis de los riesgos y debilidades; Identificar,

definir y revisar todos los controles de seguridad ya existentes; y por último, Determinar si es necesario incrementar las medidas de seguridad, los costos del riesgo y los beneficios esperados.

1.3.4.4. Matriz de Priorización de los Riesgos

Una vez realizado el análisis de los riesgos con base en los aspectos de probabilidad e impacto, se recomienda utilizar la matriz de priorización que permite determinar cuáles riesgos requieren de un tratamiento inmediato.

Figura N°3: Matriz de priorización de riesgos



Cuando se ubican los riesgos en la matriz se define cuáles de ellos requieren acciones inmediatas, que en este caso son los del cuadrante B, es decir los de alto impacto y alta probabilidad, respecto a los riesgos que queden ubicados en el cuadrante A y D, se debe seleccionar de acuerdo a la naturaleza del riesgo, ya que estos pueden ser peligrosos para el alcance de los objetivos institucionales por las consecuencias que presentan los ubicados en el cuadrante D o por la constante de su presencia en el caso del cuadrante A.

1.3.4.5. Determinación del Nivel del Riesgo

Según Ambrustery (2011) la determinación del nivel de riesgo es el resultado de confrontar el impacto y la probabilidad con los controles existentes al interior de los diferentes procesos y procedimientos que se realizan. Para adelantar esta etapa se deben tener muy claros los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones, estos niveles de riesgo pueden ser:

- **ALTO:**El riesgo hace altamente vulnerable a la entidad o dependencia. (Impacto y probabilidad alta versus controles existentes)
- **MEDIO:**El riesgo presenta una vulnerabilidad media. (Impacto alto - probabilidad baja o Impacto bajo - probabilidad alta versus controles existentes).
- **BAJO:**El riesgo presenta vulnerabilidad baja. (Impacto y probabilidad baja versus controles existentes).

1.3.4.6. Manejo del Riesgo

Cualquier esfuerzo que emprendan las entidades en torno a la valoración del riesgo llega a ser en vano, si no culmina en un adecuado manejo y control de los mismos definiendo acciones factibles y efectivas, tales como la implantación de políticas, estándares, procedimientos y cambios físicos entre otros, que hagan parte de un plan de manejo, las cuales pueden considerarse cada una de ellas independientemente, interrelacionadas o en conjunto:

- **Evitar el riesgo:** Es siempre la primera alternativa a considerar. Se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.
- **Reducir el riesgo:** Si el riesgo no puede ser evitado porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al más bajo nivel posible.

La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.

- **Dispersar y atomizar el riesgo:** Se logra mediante la distribución o localización del riesgo en diversos lugares. Es así como por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.
- **Transferir el riesgo:** Hace referencia a buscar respaldo y compartir con otro parte del riesgo como por ejemplo tomar pólizas de seguros; se traslada el riesgo a otra parte o físicamente se traslada a otro lugar. Esta técnica es usada para eliminar el riesgo de un lugar y pasarlo a otro o de un grupo a otro. Así mismo, el riesgo puede ser minimizado compartiéndolo con otro grupo o dependencia.
- **Asumir el riesgo:** Luego que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene. En este caso, el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Una vez establecidos cuáles de los anteriores manejos del riesgo se van a concretar, éstos deben evaluarse con relación al beneficio-costo para definir cuáles son susceptibles de ser aplicados y proceder a elaborar el plan de manejo de riesgo, teniendo en cuenta, el análisis elaborado para cada uno de los riesgos de acuerdo con su impacto, probabilidad y nivel de riesgo.

Posteriormente se definen los responsables de llevar a cabo las acciones especificando el grado de participación de las dependencias en el desarrollo de cada una de ellas. Así mismo, es importante construir indicadores, entendidos como los elementos que permiten determinar de forma práctica el comportamiento de las variables de riesgo que van a permitir medir el impacto de las acciones.

1.3.5. Plan de manejo de Riesgos

La planificación en términos generales, es la acción o resultado de planificar algún tipo de trabajo que es administrado por un individuo. En la planificación también se debe considerar técnicas como la observación la cual permitirá revisar de manera minuciosa cada una de las etapas para llegar a un producto terminado. (Pedraza, 2009)

Para elaborar el plan de manejo de riesgos es necesario tener en cuenta si las acciones propuestas reducen la materialización del riesgo y hacer una evaluación jurídica, técnica, institucional, financiera y económica, es decir considerar la viabilidad de su adopción. La selección de las acciones más convenientes para la entidad se puede realizar con base en los siguientes factores: Nivel del riesgo y Balance entre el costo de la implementación de cada acción contra el beneficio de la misma.

Luego de ser realizada la selección de las acciones más convenientes se debe proceder a la preparación e implantar del plan, identificando responsabilidades, programas, resultados esperados, medidas para verificar el cumplimiento y las características del monitoreo. El éxito de la adopción y/o ejecución del plan requiere de un sistema gerencial efectivo el cual tenga claro el método que se va a aplicar.

1.3.6. Matriz de Riesgos

Este método utiliza una matriz para mostrar gráficamente tanto las amenazas a que están expuestos los sistemas computarizados como los objetos que comprenden el sistema. Dentro de cada celda se muestran los controles que atacan a las amenazas.

1.3.7 Administración de Riesgos

Es un proceso interactivo e iterativo basado en el conocimiento, evaluación y manejo de los riesgos y sus impactos, con el propósito de mejorar la toma de decisiones organizacionales.

Es aplicable a cualquier situación donde un resultado no deseado o inesperado pueda ser significativo o donde se identifiquen oportunidades de mejora.

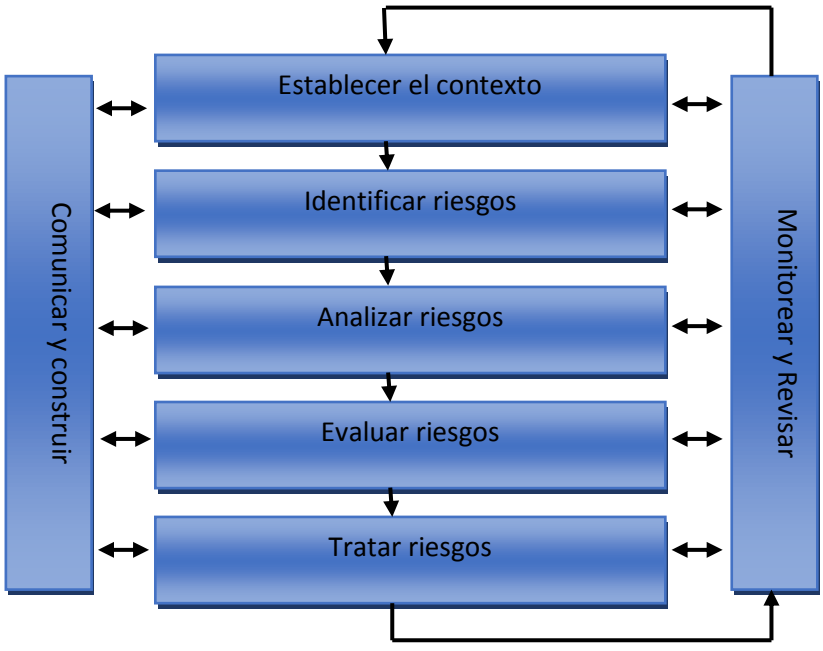
Los principales factores que se deben considerar en la Administración de Riesgos de TI son: Seguridades, Controles (Preventivos, Detectivos y Correctivos), Objetivos, Manuales de usuarios y Políticas. Si no existe una adecuada consideración de los factores antes descritos y si los controles y seguridades fueran errados, los planes organizacionales, financieros, administrativos y de sistemas se verían seriamente afectados ya que no sólo el área de sistemas será el afectado.

1.3.8. Administración de Riesgos de TI

La Administración de Riesgos de TI es el proceso continuo basado en el conocimiento, evaluación, manejo de los riesgos y sus impactos que mejora la toma de decisiones organizacionales, frente a los riesgos de TI.

1.3.8.1. Proceso de Administración de Riesgos de TI: Según INTECO(2012) a continuación se describen las principales etapas definidas para el Proceso de Administración de Riesgos de TI.

Figura N°4: Proceso de administración de riesgo de TI



- **Establecer el contexto**: Establecer el contexto estratégico, organizacional y de administración de riesgos en el cual tendrá lugar el resto del proceso. Deberían establecerse criterios contra los cuales se evaluarán los riesgos y definirse la estructura del análisis.
- **Identificar riesgos**: Identificar qué, por qué y cómo pueden surgir las cosas como base para análisis posterior.
- **Analizar riesgos**: Determinar los controles existentes y analizar riesgos en términos de consecuencias y probabilidades en el contexto de esos controles. El análisis debería considerar el rango de consecuencias potenciales y cuán probable es que ocurran esas consecuencias. Consecuencias y probabilidades pueden ser combinadas para producir un nivel estimado de riesgo.
- **Evaluar riesgos**: Comparar niveles estimados de riesgos contra los criterios preestablecidos. Esto posibilita que los riesgos sean ordenados como para identificar las prioridades de administración. Si los niveles de riesgo establecidos son bajos, los riesgos podrían caer en una categoría aceptable y no se requeriría un tratamiento.
- **Tratar riesgos**: Aceptar y monitorear los riesgos de baja prioridad. Para otros riesgos, desarrollar e implementar un plan de administración específico que incluya consideraciones de fondeo.
- **Monitorear y revisar**: Monitorear y revisar el desempeño del sistema de administración de riesgos y los cambios que podrían afectarlo.
- **Comunicar y consultar**: Comunicar y consultar con interesados internos y externos según corresponda en cada etapa del proceso de administración de riesgos y concerniendo al proceso como un todo.

1.4. Metodologías de Gestión de Riesgos de TI y Seguridad

1.4.1. Introducción a las Metodologías

Las metodologías usadas por un profesional dicen mucho de su forma de entender su trabajo, y están directamente relacionadas con su experiencia profesional acumulada como parte del comportamiento humano de acierto o error. Asimismo, una metodología es

necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera uno solo, por lo que resulta habitual el uso de metodologías en las empresas auditoras / consultoras profesionales, desarrolladas por los más expertos, para conseguir resultados homogéneos en equipos de trabajo heterogéneos.

1.4.2 Procedimientos de control

Son los procedimientos operativos de las distintas áreas de la empresa, obtenidos con una metodología apropiada, para la consecución de uno o varios objetivos de control y, por tanto, deben de estar documentados y aprobados por la dirección. La tendencia habitual de los informáticos es la de dar más peso a la herramienta que al control o contramedida, pero no se debe olvidar que: una herramienta nunca es una solución sino una ayuda para conseguir un control mejor. Sin la existencia de estos procedimientos, las herramientas de control son sólo una anécdota.Quiroz (2012).

1.4.3. Las herramientas de control

Son los elementos software que permiten definir uno o varios procedimientos de control para cumplir una normativa y un objetivo de control. Todos estos factores están relacionados entre sí, así como la calidad de cada uno con la de los demás. Al finalizar el plan se habrá conseguido una situación nueva en la que el nivel de control sea superior al anterior.

1.4.4. Tipos de Metodologías

Todas las metodologías existentes desarrolladas y utilizadas en la auditoría y el control informático, se pueden agrupar en dos grandes familias.

1.4.4.1 Metodologías Cuantitativas

Este tipo de metodologías han sido diseñadas para producir una lista de riesgos que pueden comparables entre sí, con facilidad de poder asignarles valores numéricos. Estos valores en el caso de metodologías de análisis de riesgos, son datos de probabilidad de ocurrencia de una situación o evento que se debe extraer de un registro de incidencias donde el número de incidencias sea suficientemente grande o tienda al infinito. Esto no se aplica con precisión en la práctica, pero se aproxima ese valor de forma subjetiva restando así rigor científico al cálculo. Pero dado que el cálculo se hace para ayudar a elegir el método entre varias contramedidas podría ser aceptado.

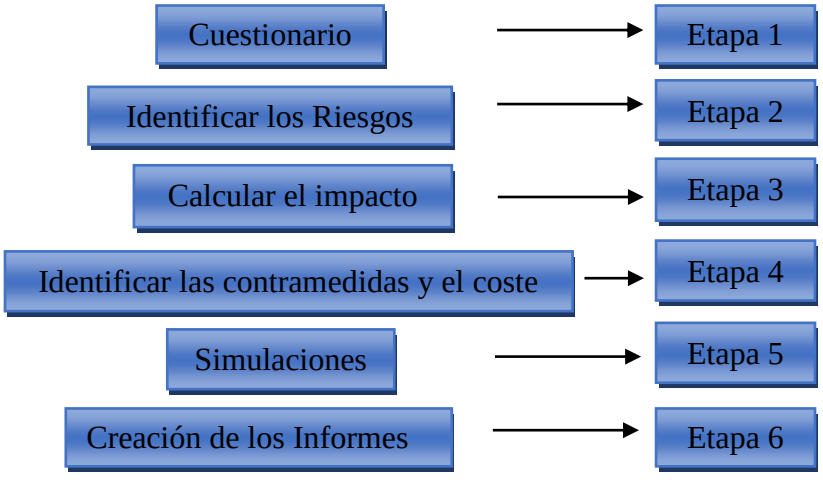
1.4.4.2 Metodologías Cualitativas

Precisan de la involucración de un profesional experimentado. Basadas en métodos estadísticos y lógica borrosa (humana, no matemática). Pero requieren menos recursos humanos / tiempo que las metodologías cuantitativas. (Peña, 2014).

1.4.5. Metodologías de Análisis de Riesgo

Están desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas. Existen dos tipos: Las cuantitativas y las cualitativas, de las que existen gran cantidad de ambas clases y sólo se citó algunas de ellas. El esquema básico de una metodología de análisis de riesgos es, en esencia, el representado a continuación:

Figura N°5: Funcionamiento esquemático básico de cualquier metodología



En base a estos cuestionarios se identifican vulnerabilidades y riesgos y se evalúa el impacto para más tarde identificar las contramedidas y el coste. La siguiente etapa es la más importante, pues mediante un juego de simulación (que se llamará "¿Qué pasa si..?") que analizará el efecto de las distintas contramedidas en la disminución de los riesgos analizados, eligiendo de esta manera un plan de contramedidas (plan de seguridad) que compondrá el informe final de la evaluación. (Peña, 2014)

Se han identificado más de cincuenta metodologías. Entre ellas están: ANALIZY, BDSS, BIS RISK ASESOR, BUDDY SYSTEM, COBRA, CRAMM, DDIS MARION AP+, MELISA, RISAN, RISKPAC, RISKWATCH. Después de estas metodologías han nacido muchas otras como la MAGERIT, desarrollada por la administración española; MARION, PRIMA (Prevención de Riesgos Informáticos con Metodología Abierta) y DELPHI.

1.5. Tratamiento del riesgo en la Gestión Pública

1.5.1. Administración pública

Es la actividad racional, técnica, jurídica y permanente, ejecutada por el Estado, que tiene por objeto planificar, organizar, dirigir, coordinar, controlar y evaluar el funcionamiento de los servicios públicos. Constituye una disciplina de la Administración, encargada del manejo de los recursos humanos, financieros y materiales, que brinden satisfacción al interés público.

La Constitución de la República del Ecuador, en su Artículo 227, define que "la administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación".

1.5.2. Sector público

La Constitución de la República del Ecuador, en su Artículo 225, establece que: "El sector público comprende: 1. Los organismos y dependencias de las funciones Ejecutiva, Legislativa, Judicial, Electoral y de Transparencia y Control Social. 2. Las entidades que integran el régimen autónomo descentralizado. 3. Los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado. 4. Las personas jurídicas creadas por acto normativo de los gobiernos autónomos descentralizados para la prestación de servicios públicos".

1.5.3. Proceso Administrativo

Son el conjunto de acciones sistemáticas enmarcadas desde la planeación hasta la comprobación en el seguimiento de objetivos. Considerando la existencia de la Planificación estratégica (Objetivos a largo plazo) y Operativa (Objetivos específicos y metas a corto plazo) en una Organización (Estructural o vertical, Horizontal o de procesos) que bajo una Dirección (Ejecución de lo planificado) controla y evaluación del desempeño individual y colectivo de la Organización y aplicación de medidas correctivas.

1.5.4. Proceso Sistema de control

El término control de modo general se lo concibe como la supervisión del cumplimiento de los objetivos previstos en el plan, para establecer, en su caso, las acciones correctoras,

> Según CGE(2010) el Art. 1. La Ley Orgánica de la Contraloría General del Estado, tiene por objeto: "…establecer y mantener, bajo la dirección de la Contraloría General del Estado, el sistema de control, fiscalización y auditoría del Estado, y regular su funcionamiento, con la finalidad de examinar, verificar y evaluar el cumplimiento de la visión, misión y objetivos de las instituciones del Estado y de la utilización de recursos, administración y custodia de los bienes públicos."

1.5.5. Sistema de control Interno

El control interno es el proceso aplicado por la máxima autoridad, dirección, y el personal de cada institución, que proporciona seguridad razonable de que se protegen los recursos públicos y se alcancen los objetivos institucionales. (ISACA, 2014).

Según la CGE (2015) constituyen componentes del control interno el ambiente de control, la evaluación de riesgos, las actividades de control, los sistemas de información y comunicación y el seguimiento.

Los objetivos del control interno en las entidades, organismo del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos para alcanzar la misión institucional, son los siguientes:

- Promover la eficiencia, eficacia y economía de las operaciones bajo principios éticos y de transparencia.
- Garantizar la confiabilidad, integridad y oportunidad de la información.
- Cumplir con las disposiciones legales y la normativa de la entidad para otorgar bienes y servicios públicos de calidad.
- Proteger y conservar el patrimonio público contra pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.

1.5.6. Aspectos legales de la evaluación del riesgo en el sector público

Según la CGE(2014) se establece en la norma de control interno 300, que la máxima autoridad establecerá los mecanismos necesarios para identificar, analizar y tratar los riesgos a los que está expuesta la organización para el logro de sus objetivos.

En la subnorma 300-01, se establece que los directivos de la entidad identificarán los riesgos que puedan afectar el logro de los objetivos institucionales debido a factores internos o externos, así como emprenderán las medidas pertinentes para afrontar exitosamente tales riesgos. Los factores externos pueden ser económicos, políticos,

tecnológicos, sociales y ambientales. Los internos incluyen la infraestructura, el personal, la tecnología y los procesos. Es imprescindible identificar los riesgos relevantes que enfrenta una entidad en la búsqueda de sus objetivos. La identificación de los riesgos es un proceso interactivo y generalmente integrado a la estrategia y planificación. CGE(2009).

Algo fundamental para la evaluación de riesgos es la existencia de un proceso permanente para identificar el cambio de condiciones gubernamentales, económicas, industriales, regulatorias y operativas, para tomar las acciones que sean necesarias. Los perfiles de riesgo y controles relacionados serán continuamente revisados para asegurar que el mapa del riesgo siga siendo válido, que las respuestas al riesgo son apropiadamente escogidas y proporcionadas, y que los controles para mitigarlos sigan siendo efectivos en la medida en que los riesgos cambien con el tiempo.

La CGE(2009) en la subnorma 300-02, establece que los directivos de las entidades del sector público y las personas jurídicas de derecho privado que dispongan de recursos públicos, realizarán el plan de mitigación de riesgos desarrollando y documentando una estrategia clara, organizada e interactiva para identificar y valorar los riesgos que puedan impactar en la entidad impidiendo el logro de sus objetivos.

En el plan de mitigación de riesgos se debe desarrollar una estrategia de gestión, que incluya su proceso e implementación. Se definirán objetivos y metas, asignando responsabilidades para áreas específicas, identificando conocimientos técnicos, describiendo el proceso de evaluación de riesgos y las áreas a considerar, detallando indicadores de riesgos, delineando procedimientos para las estrategias del manejo, estableciendo lineamientos para el monitoreo y definiendo los reportes, documentos y las comunicaciones necesarias.CGE(2009).

Los directivos de las entidades del sector público y las personas jurídicas de derecho privado que dispongan de recursos públicos, desarrollarán planes, métodos de respuesta y monitoreo de cambios, así como un programa que prevea los recursos necesarios para definir acciones en respuesta a los riesgos. Una adecuada planeación de la administración

de los riesgos, reduce la eventualidad de la ocurrencia y del efecto negativo de éstos (impacto) y alerta a la entidad respecto de su adaptación frente a los cambios.

En la subnorma 300-03, se señala que la valoración del riesgo estará ligada a obtener la suficiente información acerca de las situaciones de riesgo para estimar su probabilidad de ocurrencia, este análisis le permitirá a las servidoras y servidores reflexionar sobre cómo los riesgos pueden afectar el logro de sus objetivos, realizando un estudio detallado de los temas puntuales sobre riesgos que se hayan decidido evaluar.

La administración debe valorar los riesgos a partir de dos perspectivas, probabilidad e impacto, siendo la probabilidad la posibilidad de ocurrencia, mientras que el impacto representa el efecto frente a su ocurrencia. Estos supuestos se determinan considerando técnicas de valoración y datos de eventos pasados observados, los cuales pueden proveer una base objetiva en comparación con los estimados.

La metodología para analizar riesgos puede variar, porque algunos son difíciles de cuantificar, mientras que otros se prestan para un diagnóstico numérico. Se consideran factores de alto riesgo potencial los programas o actividades complejas, el manejo de dinero en efectivo, la alta rotación y crecimiento del personal, el establecimiento de nuevos servicios, sistemas de información rediseñados, crecimientos rápidos, nueva tecnología, entre otros. La valoración del riesgo se realiza usando el juicio profesional y la experiencia.

Según CGE(2009) en la subnorma300-04, se establece que los directivos de la entidad identificarán las opciones de respuestas al riesgo, considerando la probabilidad y el impacto en relación con la tolerancia al riesgo y su relación costo/beneficio. La consideración del manejo del riesgo y la selección e implementación de una respuesta son parte integral de la administración de los riesgos. Los modelos de respuestas al riesgo pueden ser: evitar, reducir, compartir y aceptar. Evitar el riesgo implica, prevenir las actividades que los originan. La reducción incluye los métodos y técnicas específicas para tratar con ellos, identificándolos y proveyendo acciones para la reducción de su probabilidad e impacto. El compartirlo reduce la probabilidad y el impacto mediante la transferencia u otra manera de

compartir una parte del riesgo. La aceptación no realiza acción alguna para afectar la probabilidad o el impacto.

Como parte de la administración de riesgos, los directivos considerarán para cada riesgo significativo las respuestas potenciales a base de un rango de respuestas. A partir de la selección de una respuesta, se volverá a medir el riesgo sobre su base residual, reconociendo que siempre existirá algún nivel de riesgo residual por causa de la incertidumbre inherente y las limitaciones propias de cada actividad.Adicional a estas normas existe la norma 410-11, se exige a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

1.6. Gestión de la seguridad de los activos de TIC

1.6.1. Las TIC

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.

1.6.2. Gestión de peticiones

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

1.6.3. 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 económico 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.

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. Se considera 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.

1.6.4. Seguridad de la información

La Seguridad de la Información 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 Marañon, Pérez García, 2004) también se encuentra 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).

ITIL(2014) establece en primer lugar que la Gestión de la Seguridad debe verificar que: 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; y por último se imparte la formación pertinente.

1.6.5. Activo informático

Según el GADPE (2014) la institución posee un gran cantidad de activos, 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 cualquier metodología de gestión de riesgo informático, 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. (Martínez, 2010)

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 informáticos y que representan, de esta manera con los conceptos claros se puede realizar un estudio satisfactorio y una evaluación de riesgo.

1.6.6. Amenazas y vulnerabilidades.

Según ISACA (2009) 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, mismas que son consideradas por el impacto directo que tenga en las instalaciones (fuego, explosión, caída de energía, daño de agua, perdida de acceso, fallas mecánicas).

ICONTEC (2011) establece que las 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 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 departamento ni la institución pero frente a una amenaza pueden afectar directamente a los activos, de esta manera se concluye que las vulnerabilidades son debilidades de los sistemas de seguridad que pueden ser explotadas. (ICONTEC, 2011).

CAPÍTULO II: DIAGNÓSTICO

2.1. Antecedentes Diagnósticos

La Dirección de Gestión de TIC del GADPE creada en el 2012, ha integrado tecnología a nivel de Infraestructura, redes y comunicaciones. A nivel de Software y Aplicaciones automatizando procesos y fortaleciendo el uso y capacidades tecnológicas de los funcionarios cumpliendo las normas de control interno que establece la Contraloría General del Estado a nivel de las instituciones del sector público.

Lo antes citado implica una relación directamente proporcional entre el crecimiento tecnológico y los riesgos que esto conlleva. Actualmente, el Departamento de TIC realiza la integración de nuevos sistemas: Gestión de flota vehicular, Gestión de Archivos, Gestión de Riesgo laboral y Salud ocupacional, entre otros; lo que genera mayor dependencia en los funcionarios, de los activos de TI para realizar sus procesos internos y por consiguiente su normal desempeño, dejando latente los nuevos riesgos fruto del normal avance tecnológico institucional.

Por tal motivo, se ha visto la necesidad de gestionar el riesgo informático a través de la elaboración de un plan, que bajo las normas legales ecuatorianas y basadas en las mejores prácticas a nivel internacional garantice la continuidad de las operaciones de esta institución que brinda servicios a toda la provincia en el marco de las competencias otorgadas por la ley.

Para el diagnostico, se consideró importante obtener información tanto del personal del GADPE como de los procesos de TI y metodologías para la gestión de riesgos existentes a nivel internacional. Iniciando con el levantamiento y valoraciónde los activos informáticos, la revisión y análisis de los procesos de TI, la valoración de los controles internos establecidos por la Dirección de TIC; y se recopiló información referente a las vulnerabilidades que permitan establecer el nivel de riesgo que la institución presenta en la actualidad.

2.2. Objetivos Diagnósticos

- Determinar los activos y recursos informáticos a proteger.
- Identificar los puntos vulnerables de cada proceso y las amenazas asociadas a los mismos.
- Conocer la viabilidad y efectividad de los controles de TI existentes utilizados para reducir los riesgos de exposición a las amenazas.
- Establecer el nivel de riesgo tolerado por la institución considerando el costo y el impacto de la materialización de cada amenaza y los recursos para gestionarlas.

2.3. Variables Diagnósticas

2.3.1. Activo Informático.- abarca los tipos de equipos de hardware se están utilizando en la institución, los modelos, y tipos de cada equipo, estándares, configuraciones; así como todo el software que existe dentro de sus equipos de cómputo, debidamente identificado.

2.3.2. Procesos de TI.-Son la configuración y combinación de elementos o recursos, utilizando políticas, normas, planes, sistemas de gestión, métodos, procedimientos, e información de manera que los objetivos se alcancen con funcionalidad, seguridad, eficiencia, economía y efectividad.

2.3.3. Controles de TI.- Son todos los controles considerados y clasificados, con los cuales se puede verificar si lo que fue considerado es efectivo y rentable, así como si pueden reducir la exposición de riesgo de más de una amenaza, aumentando así su costo-beneficio.

2.3.4. Nivel de riesgo.- Es el grado aceptable con el cual puede vivir una organización, y la capacidad del sistema de gestión de seguridad para detectar las amenazas y proponer las alternativas para poder manejarlos.

2.4. Indicadores por Variable

2.4.1. Activo Informático

- Valor intrínseco del activo a proteger (hardware: Las computadoras y de sus periféricos; Software. Programas y aplicaciones; Información almacenada.
- Marca, modelo, antigüedad, código interno.
- Empleado a cargo del activo
- Ubicación y estado del activo
- Costo del esfuerzo y material invertido para obtener los datos.
- Valor de la información alojada en la red.
- Software instalado dentro de los equipos de cómputo
- Licencias debidamente identificadas
- Equipos (estaciones, servidores y de comunicación) que se utilizan
- Información esencial en cada servidor o equipo que debe ser respaldada para garantizar la continuidad las operaciones.
- Estándar de equipos, con semejantes configuraciones,
- Tipo de reparación
- Tipo de piezas de repuestos
- Stock para una sustitución

2.4.2. Procesos de TI

- Nombre y descripción del procesos
- Responsable o líder del proceso
- Diagrama, procedimiento y documentación de cada proceso
- Funciones internas de los miembros de la dirección de TIC
- Importancia o nivel de criticidad de cada proceso en el sistema.
- Secuencia de tareas que componen cada proceso.
- Clasificación y valor de la información que se procesa, se utiliza o genera en cada proceso para la entidad y/o terceros.

- Software o aplicaciones que se utilizan para gestionar cada proceso en las estaciones y los servidores.
- Prestaciones y configuración de las estaciones y servidores que ejecutan las tareas
- Asignación de prioridades y los tiempos de recuperación para cada proceso
- Valor del proceso o partes del mismo a proteger y los costos derivados de su pérdida.
- Sistema de gestión
- Políticas y planes de seguridad
- Base reglamentaria: normas de control interno

2.4.3. Controles de TI

- Seguridad Física y ambiental
- Uso y asignación de recursos de TI de la institución.
- Respaldo y almacenaje de Información.
- Copias de seguridad y su almacenaje.
- Normas para el acceso y uso de servicios: Correo electrónico, internet, sistemas, intranet, accesos remoto y sitio web.
- Mantenimiento Preventivo, adquisición, modernización y baja técnica de equipos.
- Costos derivados de su pérdida (Valor de sustituir el activo).
- Configuración de la red.
- Inventario de las direcciones IP públicas (uso y/o propósito de cada una)
- Políticas de navegación aplicadas a nivel de Firewall de Software
- Ancho de banda contratado del enlace
- Tiempo y niveles de uso de internet de los empleados.
- Herramientas de monitoreo de red y detección de vulnerabilidades.
- Bitácoras de acceso al área de servidores.
- Bitácoras de Video.

2.4.4. Nivel de riesgo

- Sistema de actualización de los parches de seguridad
- Vulnerabilidades de los servidores y de las estaciones de trabajo.
- Productos antivirus
- Inspección total de paquetes en tránsito.
- Nivel de Seguridad de los servidores
- Control por parte del administrador de los accesos al mismo.
- Nivel de autorización, registro e identificación de usuarios
- Nivel de complejidad de los password o contraseñas de los usuarios,
- Métodos de acceso al local de servidores.
- Sistema de monitoreo por medio de video.
- Temperatura ambiente del área de servidores.
- Circuito eléctrico independiente del cuarto de servidores.
- Sistema de protección de descargas electro atmosféricas para el local de servidores
- Ubicación, distribución de los Rack y propósito del rack.
- Sistemas detección de incendios
- Sistemas de protección contra intrusos.
- Climatización del local de servidores.
- Canales aéreos de trasporte del cableado estructurado que ingresa al datacenter.
- Mapas disponibles de los diferentes puntos de red y su uso.
- Métodos y frecuencia de limpieza del área de servidores
- Entrenamiento del personal que la realiza limpieza

2.5. Matriz de Relación

Tabla N°1: Matriz de relación

OBJETIVO	VARIABLES	INDICADORES	TÉCNICA	FUENTE
Determinar los activos y recursos informáticos a proteger.	Activo Informático	• Valor intrínseco del activo a proteger • Marca, modelo, antigüedad, código interno. • Empleado a cargo , ubicación y estado del activo • Costo y material invertido para obtener los datos. • Valor de la información alojada en la red. • Software y Licencias instaladas • Estaciones, servidores y equipo de comunicación • Información esencial • Tipos de reparaciones • Stock y tipo de piezas de repuesto	Observación Entrevista Investigación Documental Entrevista	Gadpe Director de TIC Dirección de TIC Encargado de Infraestructura tecnológica
Identificar los puntos vulnerables de cada proceso y las amenazas asociadas a los mismos.	Procesos de TI	• Nombre, descripción, Responsable • Diagrama, procedimiento y documentación • Funciones internas • Nivel de criticidad de cada proceso • Secuencia de tareas que componen cada proceso. • Clasificación y valor de la información • Software o aplicaciones • Prestaciones y configuración de los equipos • Asignación de prioridades y los tiempos	Entrevista Encuesta Entrevista	Director de TIC Funcionarios del departamento de TIC Encargada de la Gestión de Calidad

		• Valor del proceso • Políticas, planes de seguridad y normas	Entrevista Investigación Documental	Auditora Interna Dirección de TIC
Conocer la viabilidad y efectividad de los controles de TI existentes utilizados para reducir los riesgos de exposición a las amenazas.	Controles de TI	• Seguridad Física y ambiental • Respaldo y almacenaje de Información. • Normas para el acceso y uso de recursos • Mantenimiento, adquisición, modernización • Costos derivados de su pérdida • Configuración, monitoreo y estructura de la red. • Inventario de las direcciones IP públicas • Políticas de navegación a nivel de Firewall • Ancho de banda contratado del enlace • Tiempo y niveles de uso de internet e intranet • Detección de vulnerabilidades, Bitácoras de acceso	Observación Entrevista Encuesta Entrevista Entrevista	Data center Administrador de la red Usuarios de la red, sistemas y equipos Director de TIC Desarrollador de aplicaciones

Establecer el nivel de riesgo tolerado por la institución considerando el costo y el impacto de la materialización de cada amenaza y los recursos para gestionarlas.	Nivel de riesgo	• Sistema de actualización de los parches de seguridad • Vulnerabilidades de los servidores y de las estaciones • Antivirus, Inspección total de paquetes en tránsito. • Nivel de Seguridad y Control de accesos. • Nivel de autorización, registro e identificación • Nivel de complejidad de los password • Métodos de acceso al local de servidores. • Sistema de monitoreo por medio de video. • Temperatura ambiente del área de servidores. • Sistema de protección de descargas • Ubicación, distribución de los Rack y propósito Sistemas detección de incendios y contra intrusos. • Mapas disponibles de los diferentes puntos de red	Entrevista Encuesta Observación Encuesta Observación Investigación Documental	Director de TIC Usuarios Data center Funcionarios del departamento de TIC Instalaciones GADPE Dirección de TIC

2.6. Mecánica Operativa

2.6.1. Población o Universo

La población objeto de estudio está compuesta por los 282 funcionarios que utilizan infraestructura tecnológica ya sea a nivel de PC, correo electrónico, intranet, página web, sistemas, aula virtual, etc.

2.6.2. Muestra

Se aplicará muestreo aleatorio simple sin reposición, la información será analizada de acuerdo al uso de las Técnicas estadísticas para visualizar cada fase e interpretar los resultados, que determinarán el nivel de riesgo informático que existe en el GADPE, luego de procesar la información primaria, con las muestras obtenidas a través de la siguiente fórmula estadística:

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

Dónde:

n = Tamaño de la muestra

Z = Nivel de confiabilidad: 90% 0.90/2 = 0.45 Z = 1.96

P = Probabilidad de ocurrencia: 0.50

Q = Probabilidad de no ocurrencia: 1 – 0.5 = 0.50

N = Población: 282

e = Error de muestreo: 0.05 (5%)

$$n = \frac{(1.96)^2 \times 0.50 \times 0.50 \times 282}{\left((1.96)^2 \times 0.50 \times 0.50\right) \pm \left(282 \times (0.05)^2\right)}$$

$$n = 99.35$$

Por lo tanto la muestra es de 99 funcionarios en el GADPE a los cuales se les realizarán las encuestas respectivas según la matriz antes descrita.

La otra población objeto de estudio está conformada por los miembros de la direccion de TIC que suman 9 personas, debido a que es una cifra pequeña, no es necesario realizar muestreo, sino trabajar con la totalidad de la poblacion en las entrevistas y encuestas que se han planificado.

2.6.3. Información Primaria

Para la recolección de la información primaria se utilizó las técnicas de la encuesta a la muestra seleccionadas anteriormente a traves del modelo CHECKLIST (Ver Anexo N° 2) desarrollado por Perez Alfaro (2009). Estos instrumentos se aplicaron a comienzos de febrero del 2016 de manera aleatoria entre varios funcionarios de las direcciones de la institución considerados usuarios de TIC.

También se utilizó la tecnica de la entrevista para recabar información del Director del Departamento de Tecnologias de Informacion y Comunicación del GADPE (Ver Anexo N°3), en algunas instancia comprendidas en el primer semestre del 2016.

Aparte se realizaron otras entrevistas en conjunto con todos los miembros del departamento de TIC (Ver Anexos N° 4, 5, 6, 7) entre los meses de febrero y marzo del 2016.

La técnica de la observación (Ver Anexo N°8) se empleó en esta investigación, la que permitió observar la infraestructura tecnologica existente, a nivel del centro de datos, parque informático, aulavirtual, servidores, redes y equipos de comunicación, para lo cual se realizaron multiples visitas a las instalacioens durante el primer semestre del 2016.

Debido al terremoto suscitado el 16 de abril fue necesario entrevistar nuevamente al Director de TIC con la finalidad de retroalimentar la información proporcionada considerando las contingencias existentes ante este desastre natural.

2.6.4. Información Secundaria

Para efecto de este proyecto se procedió a investigar como gestionan el riesgo informático en los departamentos de sistemas o TIC de otras instituciones, mediante la información que

estas suben a sus páginas web como parte del cumplimiento de la Ley de Transparencia durante el segundo semestre del año 2016.

2.7. Tabulación y Análisis de Encuestas

2.7.1. Encuesta tipo Lista de chequeo aplicada a los funcionarios

Debido a que las matrices de contienen demasiada información es necesaria la presentación de los resultados utilizando cuadros y no gráficos ya que se hace énfasis en los resultados procesados y ponderados según la metodología antes descrita,

Grupo de preguntas N°1: Con relación a las Políticas de seguridad de la información.

Tabla N° 2: Políticas de Seguridad

Item	Pregunta	Si	Parcial	No	Puntos	Índice
a	¿Se han elaborado políticas de seguridad de la información?	8	19	72	35	17.68%
b	¿Se están aplicando las políticas de seguridad de la información?	2	11	86	15	7.57%
c	¿Se hacen de conocimiento al personal de la institución las políticas de seguridad de la información?	15	48	36	78	39.39%
d	¿Realizan evaluaciones y actualizaciones constantes de las políticas de seguridad de la información?	4	12	83	20	10.10%
e	¿Las políticas de seguridad de la información están basadas en algún estándar nacional o internacional?	1	6	92	8	4.04%
	Totales	30	96	369	156	15.75%

Análisis

Como se puede notar, la mayoría de los usuarios no tiene conocimientos sobre las políticas de seguridad que se tienen en la institución. Según la metodología utilizada este factor apenas está cubierto en un 15.75% lo que supone la falta de socialización o difusión de las mismas. Apenas los que respondieron positivamente a estas preguntas fueron los usuarios del área de TIC.

Grupo de preguntas N°2: Con relación a la organización para la seguridad de la información

Tabla N° 3: Políticas de Seguridad

tem	Pregunta	Si	Parcial	No	Puntos	Índice
a	¿Tiene la institución un área o una persona asignada para labores exclusivas de seguridad de la información?	12	30	57	54	27,27%
b	¿El área de seguridad de la información está formalizada dentro del organigrama de la institución?	0	8	91	8	4,04%
c	¿Tienen un comité de seguridad de la información a nivel de alta dirección?	6	11	82	23	11,62%
d	¿Realizan evaluaciones de seguridad de la información a través de otras entidades públicas o privadas?	2	9	88	13	6,57%
e	¿Al realizar contratos con empresas externas exige requerimientos de seguridad de la información?	3	9	87	15	7,58%
	Totales	23	67	405	113	11,41%

Análisis

No existe planificación ni organización en lo referente a seguridades, el nivel de desempeño que arroja el test es muy bajo, pues solo se cumple en un 11% la cobertura que este factor debe tener, no hay formalidad, pues la inexistencia de un encargado de la seguridad denota la poca importancia que se le da a este tema.

Grupo de preguntas N°3: Con relación a la clasificación y control de activos informáticos.

Tabla N° 4: Políticas de Seguridad

Item	Pregunta	Si	Parcial	No	Puntos	Índice
a	¿Están clasificados los activos informáticos (hardware, software, servicios)?	19	39	41	77	38,89%
b	¿Cuenta esta clasificación, con un sistema de software que la automatice?	3	21	75	27	13,64%
c	¿Realizan periódicamente la actualización de su inventario de activos informáticos?	24	29	46	77	38,89%
d	¿Actualizan las etiquetas con nombres de contenidos, fechas, ubicación y versiones?	9	20	70	38	19,19%
e	¿Actualizan las etiquetas con nombres de los responsables de los activos informáticos?	5	7	87	17	8,59%
	Totales	60	116	319	236	23,84%

Análisis

Si bien existe un inventario de los activos, está desactualizado y no cuenta con información completa. La mayoría de los usuarios desconoce que tienen el carácter de activo informático, y lo relacionan con la asignación de activos fijos que se realiza institucionalmente. El nivel evaluado sigue siendo bajo: 23.84%.

Grupo de preguntas N°4: Con relación a las políticas del personal respecto a la seguridad Informática.

Tabla N° 5: Políticas de Seguridad

Item	Pregunta	Si	Parcial	No	Puntos	Índice
a	¿Están preparados los usuarios para reportar los incidentes de seguridad de los sistemas de información?	4	14	81	22	11,11%
b	¿La institución tiene acuerdos con el personal sobre la confidencialidad de la información?	16	13	70	45	22,73%
c	¿Reciben los usuarios capacitación actualizada en temas de seguridad de la información?	3	6	90	12	6,06%
d	¿Tienen procedimientos de respuesta a incidentes y anomalías en materia de seguridad informática para ser aplicados por los usuarios?	2	9	88	13	6,57%
e	¿Los empleados, contratistas y terceros tienen una guía que establezca expectativas de seguridad de su rol?	0	8	91	8	4,04%
	Totales	25	50	420	100	10,10%

Análisis

Este factor es uno de los más bajos en la evaluación, con 10,10%; representa un nivel crítico en lo relacionado a las políticas de seguridad que el personal debe conocer y debe cumplir, falta capacitación a todo nivel en este tema.

Grupo de preguntas N°5: Con relación a la seguridad física y ambiental de los sistemas de Información.

Tabla N° 6: Políticas de Seguridad

Item	Pregunta	Si	Parcial	No	Puntos	Índice
a	¿Tienen identificadas las áreas físicas seguras donde se encuentran los sistemas de información?	32	34	33	98	49,49%
b	¿Tienen controles de ingreso del personal a las áreas físicas donde se encuentran los sistemas de información?	34	39	26	107	54,04%
c	¿Tienen mecanismos de seguridad de la información para los equipos que ingresan y salen fuera del ámbito de la institución?	52	42	5	146	73,74%
d	¿Cuentan con mantenimiento periódico del hardware y software en los equipos informáticos?	31	34	34	96	48,48%
e	¿Se usan técnicas para que la información de dispositivos de almacenamiento con datos sensible no sea recuperable?	1	10	88	12	6,06%
	Totales	150	159	186	459	46,36%

Análisis

A pesar que el resultado general del factor no es tan bajo (46.36%); la seguridad de la que todos los usuarios están conscientes es la que dan los guardias (física) en la garita, y los controles que ahí se hacen; los cuales no son efectivos siempre.

Grupo de preguntas N°6:Con relación al uso de la red LAN.

Tabla N° 7: Políticas de Seguridad

Item	Pregunta	Si	Parcial	No	Puntos	Índice
a	¿Están preparados para mantener el correcto funcionamiento del cableado de datos en caso de alguna falla?	8	15	76	31	15,66%
b	¿Están preparados para mantener el correcto funcionamiento del suministro eléctrico en caso de alguna falla?	14	28	57	56	28,28%
c	¿Tienen un registro de fallas de las comunicaciones de datos?	1	6	92	8	4,04%
d	¿Tienen un control documentado de toda la información referida a la red de datos, es decir direcciones IP de las máquinas de los usuarios, distribución de las IP, diagrama de la red de datos, entre otros?	5	12	82	22	11,11%
e	¿Tienen establecidos controles de seguridad para el sistema de correo electrónico de la institución?	9	29	61	47	23,74%
	Totales	37	90	368	164	16,57%

Análisis

En lo que respecta a las redes de área local (LAN), se puede distinguir que el nivel de seguridad es bajo (16.57%) y sobre todo el grado de conocimiento sobre los controles que en esta área se dan son mínimos. No existe registro de fallas exclusivo relacionado a las comunicaciones de la red, sino cuando un usuario comunica de un incidente en la red. Sólo en el caso de los correos electrónicos existe una opción de contingencia para hacerlo vía web mail, pero no todos los funcionarios conocen de esa opción.

Grupo de preguntas N°7: Con relación a la gestión de las comunicaciones de datos y operaciones de los sistemas informáticos.

Tabla N° 8: Políticas de Seguridad

Item	Pregunta	Si	Parcial	No	Puntos	Índice
a	¿Cuentan con procedimientos y responsabilidades operativas del uso y acceso a los sistemas informáticos?	29	39	31	97	48,99%
b	¿Cuentan con documentación de los procedimientos operativos del uso y acceso de los sistemas informáticos?	22	27	50	71	35,86%
c	¿Tienen procedimientos para afrontar incidentes de las comunicaciones de datos y operaciones de los sistemas informáticos?	16	14	69	46	23,23%
d	¿Tienen establecidos controles en la red de datos contra software malicioso (antivirus, antispyware,etc)?	19	24	56	62	31,31%
e	¿Tienen un registro de acceso y uso de las aplicaciones y servicios de la red de datos del personal operativo?	12	26	61	50	25,25%
	Totales	98	130	267	326	32,93%

Análisis

El punto más débil está en la falta de registro de incidentes en lo relacionado al uso de aplicaciones con la red. Si bien se registran todos los incidentes mediante un sistema de mesa de ayuda, nunca se especifica o no existe nivel de detalle para almacenar este indicador.

Grupo de preguntas N°8:Con relación al control de acceso a los sistemas informáticos.

Tabla N° 9: Políticas de Seguridad

Item	Pregunta	Si	Parcial	No	Puntos	Índice
a	¿Tienen políticas de control de acceso a los sistemas informáticos de los usuarios en la red de datos?	9	18	72	36	18,18%
b	¿Cuentan con un registro permanente de acceso a los sistemas informáticos de los usuarios en la red de datos?	23	28	48	74	37,37%
c	¿Cuentan con una administración de las contraseñas de usuarios para los sistemas informáticos?	28	46	25	102	51,52%
d	¿Tienen políticas de uso de los servicios de la red de datos de su institución?	11	28	60	50	25,25%
e	¿Tienen establecido limitaciones de horario para la conexión a la red de datos?	0	31	68	31	15,66%
	Totales	71	151	273	293	29,60%

Análisis:

Existen controles en lo que respecta al acceso o registros de los sistemas existentes, sin embargo, la mayoría de los usuarios no conocen o están conscientes de la importancia que tienen para salvaguardar la información que manejan.

Grupo de preguntas N°9:Con relación al desarrollo y mantenimiento de sistemas informáticos.

Tabla N° 10: Políticas de Seguridad

Item	Pregunta	Si	Parcial	No	Puntos	Índice
a	¿Realiza el análisis y define especificaciones de los requerimientos de seguridad informática cuando desarrolla sistemas informáticos?	2	11	86	15	7,58%
b	¿Tienen mecanismos de validación de datos de entrada y de salida los sistemas de información?	1	9	89	11	5,56%
c	¿Tienen políticas de uso de los controles criptográficos en su red de datos?	0	2	97	2	1,01%
d	¿Tienen servicios de no repudio, es decir que el usuario no pueda negar las acciones realizadas en los sistemas informáticos?	2	5	92	9	4,55%
e	¿Tienen procedimientos de control de los cambios que se realizan en las aplicaciones software y el sistema operativo de los servidores o las estaciones de trabajo?	5	9	85	19	9,60%
	Totales	10	36	449	56	5,66%

Análisis

Sin duda, aquí se concentra el nivel más bajo en lo que a seguridades se refiere, y no solo es por desconocimiento o incomprensión de los usuarios ante la pregunta, sino que el desarrollo de aplicaciones no le da la importancia del caso a las aplicaciones que tiene en producción.

Grupo de preguntas N°10: Con relación a la gestión de incidentes de sistemas informáticos.

Tabla N° 11:Políticas de Seguridad

Item	Pregunta	Si	Parcial	No	Puntos	Índice
a	¿Usa algún sistema de registro de incidentes o software de Helpdesk?	37	38	24	112	56,57%
b	¿Realiza la clasificación de incidentes?	23	27	49	73	36,87%
c	¿Tienen elaborado un plan de respuesta ante incidentes?	9	15	75	33	16,67%
d	¿Investigan y recolectan evidencias sobre el incidente?	16	35	48	67	33,84%
e	¿Evalúan el daño y costo de las incidencias?	13	37	50	63	31,82%
	Totales	98	152	246	348	35,15%

Análisis

Este es el factor con el mejor nivel dentro de los evaluados, con 35% de cobertura de los indicadores medidos encuentra su justificativo en la existencia de un sistema de gestión de incidentes. Sin embargo, como se puede evidenciar en los resultados, no todos están al tanto de lo que permite ese sistema, ni de la importancia que tiene para solventar incidentes. Muchos lo ven como algo burocrático que solo evidencia daños; pero los técnicos si lo usan como un registro histórico de los problemas que puede haber tenido un usuario, un equipo o un servicio.

2.8. Procesamiento de la información obtenida mediante entrevistas y observación

2.8.1. Análisis de entrevista al director de TIC

La configuración predeterminada con la que llegan los sistemas se crea para maximizar las características disponibles y por lo general no se da importancia a la seguridad. Es importante utilizar equipos homologados e imágenes documentadas para mantener la uniformidad entre todos los equipos de escritorio y las terminales de trabajo. Esta uniformidad permitirá una mayor eficacia en la detección y paralización de ataques potenciales. Robustecer el servidor implica actualizar sistema operativo, aplicar los parches adecuados, reforzar las configuraciones y auditar el acceso y las vulnerabilidades de los sistemas.

Formalmente ninguno se ha estandarizado o exigido de manera general, en algunos casos se han bloqueado las pantallas con contraseñas, y los antivirus que se utilizan son en algunos casos los que permiten detección de software espía o malicioso.Se han establecido medidas de restricción mediante la implementación de un Datacenter, y otras medidas de seguridad física que incluyen en algunos casos cables de bloqueo para equipos portátiles, armarios o racks con llave para servidores/equipos de red y guardias de seguridad.

Debido a la existencia de un Datacenter los riesgos a este nivel están minimizados en este sentido, pues contempla las seguridades físicas respectivas mediante control de accesos biométricos, llaves en los rack y monitoreo en video. En este segmento se estudia las aplicaciones que son esenciales para el GADPE y las valora desde el punto de vista de la seguridad y disponibilidad, además se examinan tecnologías utilizadas para aumentar el índice de defensa en profundidad. De la información que posee GADPE no se requiere que terceros procesen la información, así mismo, los datos del cliente no se almacenan o procesan en un ambiente compartido.

El mecanismo utilizado para asegurar una alta disponibilidad de las aplicaciones es el soporte permanente mediante una mesa de ayuda a través de la intranet y un centro de llamadas. Los fabricantes independientes proporcionan periódicamente actualizaciones y parches de software como la documentación sobre los mecanismos de seguridad. El equipo

interno de desarrollo proporciona periódicamente actualizaciones y parches de software como la documentación sobre los mecanismos de seguridad debido a que conoce las vulnerabilidades de seguridad que existen para las aplicaciones de la intranet.

La actividad del GADPE se desarrollan en un ambiente de estrategia política, en el que el robo de material intelectual o el espionaje son temas de gran preocupación por lo que no está conectada la red corporativa a otras redes (ya sean de clientes, de socios o de terceros) mediante enlaces de red públicos o privados. Solo en caso de una unidad adscrita que es el Patronato se mantienen recursos compartidos como la red local y el soporte técnico.

No se han registrado incidentes que afecte a las aplicaciones o a las infraestructuras orientadas a los usuarios, tales como apagones o fallos de suministro eléctrico, pero no afectan significativamente las operaciones diarias. Algunos componentes de infraestructura y las aplicaciones del usuario dependen del acceso a recursos de su entorno, son pocos los casos en que los componentes de infraestructura y aplicaciones se comparten entre varios usuarios. Salvo el plan anual de rotación, no existen cambios en el personal técnico del departamento

Existen acuerdo de servicios establecidos como parte de los contratos con los proveedores de servicios subcontratados en el caso de internet, sistema de rastreo satelital, garantías de los equipos. No están definidos los que hacen referencia al sistema financiero y al sistema médico laboral. Existen siete servidores virtuales para los sistemas Olimpo, Médico Laboral, Intranet, Base de Datos, Proxy, Documental, Antivirus, Monitoreo CCTV, mismo que comprueba periódicamente el cortafuego para garantizar que funciona según lo previsto.

2.8.2. Análisis de entrevista al administrador de la red

No existe un modelo para asignar niveles de importancia a los componentes del entorno informático. Al asignar niveles de prioridad a los componentes, una empresa estará más preparada para centrar sus esfuerzos de seguridad en aquellos sistemas que necesitan acceso. Disponer de una lista de este tipo también asigna una prioridad para la recuperación cuando se producen apagones.No existen directivas para la regulación del

entorno informático, las directiva son reglas y prácticas que especifican cómo se puede utilizar de forma adecuada un entorno informático. Si no existen directivas, no existe mecanismo alguno para definir o hacer cumplir los controles dentro del entorno.

Existen directivas de seguridad de información para la regulación de la actividad relacionada con la seguridad del GADPE, pero solo a nivel de la dirección de TIC, es decir no existe una política corporativa aplicada al resto de la institución.La gestión de las cuentas de usuarios individuales no es compartida, tampoco hay un proceso documentado para la creación de servidores, ni pautas documentadas que indiquen qué protocolos y servicios están permitidos en la red corporativa

2.8.3. Análisis de entrevista al desarrollador sobre la gestión de actualizaciones y revisiones

Los procesos de gestión de cambios y configuraciones permiten asegurar que los cambios en el entorno de producción, se han probado y documentado exhaustivamente antes de utilizarse, a nivel institucional a modo de referencia.

Se prueba en la institución los cambios de configuración antes de aplicarlos a los sistemas de producción, pero no existe un proceso establecido para las directivas de actualización y revisión.No existe una directiva establecida por la que se regule la actualización de productos de detección basados en firmas. La aparición de nuevos virus es constante, por lo que resulta imprescindible mantener una lista actualizada de firmas de virus. Su solución antivirus será tan eficaz como lo permita su lista de firmas de virus.

Tampoco hay diagramas lógicos y documentación de configuración precisa para la infraestructura de red y los servidores, arquitectura y del flujo de datos de las aplicaciones principales.Los registros se almacenan en un servidor central de registros, los mismos que son revisados periódicamente según sea necesario. Se hacen copias de seguridad de todos los recursos críticos y confidenciales periódicamente ya que están definidas las directivas y procedimientos para el almacenamiento y la gestión de los dispositivos de copias de seguridad.

2.8.4. Análisis de la Observación

Se visualizaron en el sistema Olimpo los registros de todos los activos informáticos hardware: computadoras y periféricos, software, programas y aplicaciones). En los casos de activos en bodega se puede constatar el valor nominal registrado cuando fue adquirido y, según el caso, el valor invertido en el mismo.

Se pudo revisar el software instalado en los equipos de cómputo, con sus licencias en cada caso debidamente identificadas para cada estación de trabajo, servidores y equipo de redes que se utilizan.Se visitó el área donde se guarda el stock de partes y piezas utilizadas para una sustitución en caso de mantenimiento o reparación.

En la observación documental se pudo constatar la existencia de Políticas y planes de seguridad, base reglamentaria, Normas de control interno, seguridad Física y ambiental, así como el respaldo y el almacenaje de Información.

En la página web institucional también se pudo observar el acceso y uso de servicios: Correo electrónico, internet, sistemas, intranet, accesos remotos y sitio web. En las políticas de navegación aplicadas a nivel de Firewall de Software que se integre al controlador de dominio para restringir el acceso a páginas o recursos de Internet por IP y usuario y al mismo tiempo optimizar el uso del ancho de banda contratado del enlace y optimizar el tiempo de los empleados.

Mediante una consulta al servidor se pudo revisar el inventario de las direcciones IP internas así como las públicas que posee la institución, ya que, de no existir un control de esto, estas direcciones se convierten en una vulnerabilidad fuerte para la organización.

Existe un bitácora digital de acceso al área de servidores así como un sistema de monitoreo por medio de video con su respectiva bitácoras a cargo de los guardias de seguridad física. Existe un sistema de protección de descargas electros atmosféricos para el local de servidores así como una correcta distribución y ubicación de los Rack´s con el respectivo sistema de detección de incendios y protección contra intrusos.

La climatización del local de servidores se realiza mediante un aire acondicionado de alta precisión, existe un cableado estructurado en el 80% de las instalaciones del edificio principal. No se pudo verificar la existencia de mapas disponibles de los diferentes puntos de red y su uso, así como alguna bitácora de registro de limpieza del área de servidores y frecuencia.

2.9. FODA

2.9.1. Fortalezas

- Estructura organizacional de TIC consolidada y con funciones segregadas según cada proceso interno.
- Talento humano de la Dirección de TIC está capacitado técnicamente en la solución de problemas e incidentes.
- El nivel de eficiencia de la dirección es relativamente alto a nivel de entrega servicios, soporte técnico, atención al usuario y gestión de incidentes.
- Existencia de una Plan Informático en donde se contempla como un objetivo la gestión del riesgo
- Infraestructura tecnológica con tecnología de última generación (equipos de cómputo, servidores y data center)
- Presupuesto aprobado para invertir en equipos y licencias de seguridad informática.
- La Dirección de TIC está posicionado al más alto nivel y puede implementar e instaurar procesos para el gobierno de TI de manera formal y directa.

2.9.2 Debilidades

- Poco conocimiento sobre la gestión del riesgo informático en los miembros del departamento de TIC.
- Bajo nivel de concientización de los riesgos que existen por la falta de controles y seguridad a nivel de los funcionarios del GADPE.
- Subutilización de los servidores al no utilizar herramienta de monitoreo y control del tráfico de red.

- El seguimiento del cumplimiento de las pocas políticas de seguridad definidas no es periódico.
- Mal uso de la red por parte de la mayoría de funcionarios del GADPE.
- No existe una adecuada cultura digital por parte de la mayoría de funcionarios y usuarios de la intranet.
- Plan de contingencias ha sido elaborado en base al criterio de una sola persona sin considerar aspectos técnicos de cada subproceso.
- No hay el conocimiento necesario del tiempo y costo de los procesos de TI

2.9.3 Oportunidades

- Apoyo de la máxima autoridad para los proyectos de tecnología que generen eficiencia operacional y mejora continua.
- Las normas de control interno exigen la gestión del riesgo a todo nivel.
- Las metodologías y estándares internacionales se ajustan a la normativa vigente dictada para el sector público.
- La automatización de procesos internos en la institución obliga a valorar y estimar el riesgo informático existente.
- Existencia de software especializado como apoyo a la gestión de riesgos tanto para redes, infraestructura y sistemas.
- Buenas relaciones con los funcionarios del resto de departamentos que conforman la institución.
- Utilización frecuente de servicios que la dirección de TIC presta al del resto de direcciones
- El GADPE tiene entre sus objetivos brindar asistencia técnica a todos los GAD de la provincia en este tipo de procesos de administración y gobierno de TI.

2.9.4 Amenazas

- Las auditorías realizadas por contraloría pueden determinar errores administrativos y establecer responsabilidades, perono gestionar el riesgo.
- Percepción de desigualdad en el trato a los usuarios por parte de algunos empleados.
- Dificultad en el reconocimiento de problemas de TI por parte de los empleados.

- Bajo nivel de formación en informática por parte de los empleados.
- Al ser un gobierno, su naturaleza la expone a espionaje por parte de los sectores contrarios al proyecto político gobernante.
- Personal conspirador que busca acceder a información confidencial para scar provecho propio.
- El surgimiento de los virus informáticos puede ocasionar la para o demora de alguno de los procesos automatizados.
- La vertiginosa obsolescencia informática hace que muchos de los equipos de última generación tengan que ser repotenciados cada vez con más frecuencia.

2.10. Estrategias FA, FO, DO, DA

Tabla N° 12: Estrategias FODA

ESTRATEGIAS FO-FA-DO-DA	AMENAZAS	OPORTUNIDADES
FORTALEZAS	Comunicar a las instancias de Auditoría Interna y de Gestión de Calidad las fases del plan de gestión en que se realizará el evaluación y valoración de los activos informáticos y sus vulnerabilidades y riesgos.	Estructurar un plan integral de gestión del riesgo informático considerando el análisis de los responsables de cada subproceso y conociendo la relación e interdependencia que tienen los mismos con el resto de procesos institucionales
DEBILIDADES	Organizar talleres de capacitación para todos los funcionarios del GADPE sobre temas informáticos y tecnológicos de manera dinámica a través la articulación de equipos de trabajo multidisciplinarios que permitan conocer puntos de vista diferentes	Capacitar mediante cursos especializados y de alto nivel a todo el personal de la Dirección de TIC en temas de gestión de riesgo, encriptación, firmas electrónicas, seguridades físicas y lógicas, administración de Datacenter, redes y servidores, aplicaciones web, y el control interno informático.

2.11. Determinación del Problema Diagnóstico

El Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas, no cuenta con un Plan de Gestión de Riesgos que ayude a mitigar y a la vez identificar las distintas amenazas, vulnerabilidades y riesgos de los recursos de TI. Por lo que la entidad podría estar en un atraso en lo que es el desarrollo tecnológico, debido a que los procesos o procedimientos que existen actualmente en la gestión de servicios (riesgos) son antiguos por lo que no son gestionados, sino funcionan de una forma manual e informal que lo impide que se puedan optimizar recursos y mejorar el rendimiento laboral en la entidad.

Por tal motivo, se ha visto la necesidad de elaborar un plan para la gestión del riesgo informático, que optimice los recursos existentes bajo las normas legales ecuatorianas y basadas en las mejores prácticas a nivel internacional con el objetivo de garantizar la continuidad de las operaciones de esta institución que brinda servicios a toda la provincia en el marco de las competencias otorgadas por la ley.

CAPÍTULO III: PROPUESTA
PLAN DE CONTINGENCIAS PARA LA GESTION DE RIESGO INFORMÁTICO DEL GADPE 2016-2019

3.1. Introducción

El crecimiento tecnológico que ha tenido la institución, la rápida evolución de internet y la necesidad de estar conectados en todo momento como institución a requerir un alto nivel de fiabilidad y seguridad, de tal forma que se proteja la información institucional y esté disponible sin interrupciones o degradación del acceso, con el objetivo de no poner en peligro su normal funcionamiento,

Los datos almacenados, no son datos estáticos, están en constante movimiento, se interrelacionan unos con otros y dan como resultado nuevos datos. Su crecimiento es constante y ello implica no solo que deben estar protegidos mediante las medidas de seguridad adecuadas, sino también dotados de infraestructura tecnológica (Datacenter) acorde a las necesidades institucionales. Un Datacenter o centro de datos literalmente es una instalación especializada para brindar facilidades de hospedaje de aplicaciones y diversos servicios de comunicaciones.

Según las normas de control interno es necesario tener un Plan de gestión que contemple aspectos como las actividades previas al desastre (bitácora de operaciones), las actividades durante el desastre (plan de emergencias, entrenamiento) y por últimolas actividades después del desastre. Es indispensable designar un comité con roles específicos y nombre de los encargados de ejecutar las funciones de contingencia en caso de suscitarse una emergencia.

El plan de gestión de riesgos es un documento de carácter confidencial que describeuna vez definidos los activos informáticos contenga los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.

3.2. Objetivos

3.2.1. General:

Elaborar un plan de respuesta a los riesgos que incluya la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento.

3.2.2. Específicos:

- Evaluar los activos informáticos de la institución mediante el despliegue de una matriz de gestión de riesgo informático.
- Elaborar un plan de contingencias que mitigue los riesgos informáticos existentes en la institución.
- Socializar los resultados de la matriz y su respectivo plan de contingencias con los funcionarios usuarios de TIC del GADPE.

3.3. Metodología

3.3.1. Introducción

Inicialmente se utilizará la Matriz para el Análisis de Riesgo, en base a un taller de seguimiento al Plan Informático Institucional del GADPE en donde consta la estrategia 1.3 que tiene como objetivo: GARANTIZAR EL MANTENIMIENTO Y CONTROL DE LA INFRAESTRUCTURA TECNOLÓGICA.

Por lo que es clave analizar y determinar los riesgos en el manejo de los datos e información de la Institución. La matriz, por el momento es una hoja de cálculo, no dará un resultado detallado sobre los riesgos y peligros de cada recurso (elemento de información) de la institución, sino una mirada aproximada y generalizada de estos.

Hay que tomar en cuenta que el análisis de riesgo detallado, es un trabajo muy extenso y consumidor de tiempo, porque requiere que se compruebe todos los posibles daños de cada

recurso de una institución contra todas las posibles amenazas, es decir se termina con un sinnúmero de grafos de riesgo que se debe analizar y clasificar.

Por otro lado, hay que reconocer que la mayoría de los gobiernos autónomos descentralizados e instituciones públicas en Ecuador, no cumplen de manera óptima las normas de control interno relacionadas al Riesgo Informático, ni dedican mucho tiempo en preocuparse por la seguridad de la información que manejan y en muchas ocasiones tampoco por la formación adecuada de sus funcionarios en el manejo de las herramientas informáticas.

Entonces lo que se pretende con el enfoque de la Matriz es localizar y visualizar los recursos del GADPE, que están más en peligro de sufrir un daño por algún impacto negativo, para posteriormente ser capaz de tomar las decisiones y medidas adecuadas para la superación de las vulnerabilidades y la reducción de las amenazas.

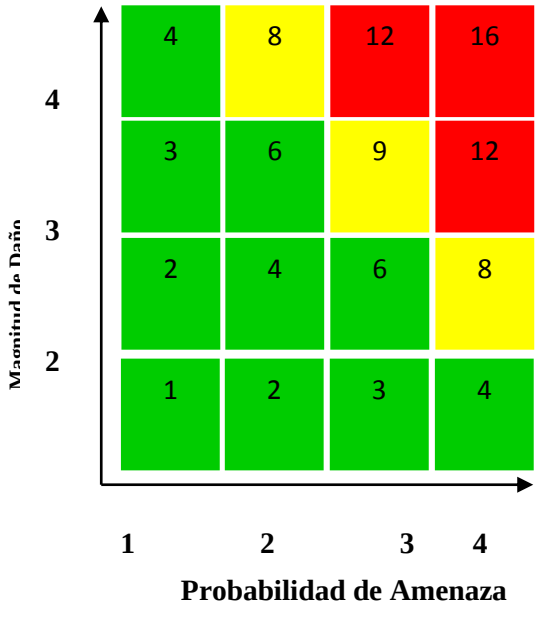
3.3.2. Fundamento de la Matriz

La Matriz se basó en el método de Análisis de Riesgo con un grafo de riesgo, usando la fórmula: **Riesgo= Probabilidad de Amenaza x Magnitud de Daño**

La Probabilidad de Amenaza y Magnitud de Daño pueden tomar los valores y condiciones respectivamente

- 1 = **Insignificante** (incluido Ninguna)
- 2 = **Baja**
- 3 = **Mediana**
- 4 = **Alta**

Figura N°6: Fundamento de la Matriz



El Riesgo, que es el producto de la multiplicación Probabilidad de Amenaza por Magnitud de Daño, está agrupado en tres rangos, y para su mejor visualización, se aplica diferentes colores.

- **Bajo Riesgo = 1 – 6 (verde)**
- **Medio Riesgo = 8 – 9 (amarillo)**
- **Alto Riesgo = 12 – 16 (rojo)**

3.3.3. Uso de la Matriz

La Matriz verdadera se basó en un archivo con varias hojas de cálculo que superan el tamaño de una simple pantalla de un monitor. Entonces por razones demostrativas, en las siguientes imágenes solo se muestra una fracción de ella.

La Matriz contiene una colección de diferentes Amenazas y Elementos de información. Para llenar la Matriz, se tendrá que estimar los valores de la Probabilidad de Amenaza por cada Amenaza y la Magnitud de Dañopor cada Elemento de Información.

Para la estimación de la Probabilidad de amenazas, se trabaja con un valor generalizado, que está relacionado con el recurso más vulnerable de los elementos de información, sin embargo es usado para todos los elementos. Si por ejemplo existe una gran probabilidad de que pueden robar documentos y equipos en la oficina, porque ya entraron varias veces y no cuenta todavía con una buena vigilancia nocturna de la oficina, no se distingue en este momento entre la probabilidad si robarán una portátil, que está en la oficina (con gran probabilidad se van a llevarla), o si robarán un documento que está encerrado en una caja fuerte escondido (es menos probable que se van a llevar este documento).

Este proceder obviamente introduce algunos resultados falsos respecto al grado de riesgo (algunos riesgos saldrán demasiado altos), algo que posteriormente tendrá que corregirlo. Sin embargo, excluir algunos resultados falsos todavía es mucho más rápido y barato, que hacer un análisis de riesgo detallado, sobre todo cuando el enfoque solo es combatir los riesgos más graves.

En el caso de que se determine los valores para la Probabilidad de Amenaza y Magnitud de Daño a través de un proceso participativo de trabajo en grupo, se recomienda primero llenar las fichas de apoyo para los Elementos de Información y Probabilidad de Amenaza, y una vez consolidado los datos, llenar la matriz. Dependiendo de los valores de la Probabilidad de Amenaza y la Magnitud de Daño, la Matriz calcula el producto de ambas variables y visualiza el grado de riesgo.

3.3.4. Elementos de la Matriz

La Matriz se basa en una hoja de cálculo (ver anexo N°14 a). Existe la versión en LIBRE OFFICE y MICROSOFT OFFICE y se recomienda usar el formato que corresponde con el sistema operativo donde se la usa, debido a algunos problemas de compatibilidad entre ambos formatos.

La Matriz está compuesta por 5 hojas

- **Datos (Ver ANEXO N° 14 a):** Es la hoja utilizada para valorar el riesgo para los Elementos de Información, para lo cual se debe establecer la magnitud de Daño y la Probabilidad de Amenaza conforme a sus valores estimados. Los valores de Probabilidad de Amenaza solo se aplica en está hoja, porque las demás hojas, hacen referencia a estos.

- **Sistemas (Ver ANEXO N° 14 b):**Se utiliza para valorar el riesgo para los Sistemas e Infraestructura. Hay que llenar solo los valores de Magnitud de Daño, debido a que los valores de Probabilidad de Amenaza están copiados automáticamente desde la hoja anteriormente referida.

- **Personal(Ver ANEXO N° 14 a):**Se utiliza para valorar el riesgo para elPersonal. Igual como en el anterior caso solo hay que llenar los valores de Magnitud de Daño.

- **Análisis Promedio**: Esta hoja contiene el promedio aritmético de los diferentes riesgos, en relación con los diferentes grupos de amenazas y daños. La idea de esta hoja es ilustrar en que grupo (combinación de Probabilidad de Amenaza y Magnitud de Daño) hay mayor o menor peligro. No hay nada que llenar en esta hoja.

- **Análisis Factores**: Esta hoja tiene el mismo propósito como la hoja anterior con la diferencia que esta vez el promedio aritmético de los grupos está mostrado en un grafo, dependiendo de la Probabilidad de Amenaza y Magnitud de daño. La línea amarilla muestra el traspaso de la zona Bajo Riesgo a Mediano Riesgo y la línea roja, el traspaso de Mediano riesgo a Alto Riesgo. La idea de esta hoja es ilustrar el nivel de peligro por grupo y la influencia de cada factor (Probabilidad de amenaza, Magnitud de Daño).

3.3.5. Adaptación de la Matriz a las necesidades individuales

La Matriz trabaja con una colección de diferentes Amenazas y Elementos de información. Ambas colecciones solo representan una aproximación a la situación común de una organización, pero no necesariamente reflejan la realidad de una organización específica. Entonces si hay necesidad de adaptar la Matriz a la situación real de una organización, solo hay que ajustar los valores de las Amenazas en la hoja Datos (solo en esta) y los Elementos de información en su hoja correspondiente. Es decir hay que insertar, quitar filas o columnas, se recomienda hacerlo con mucho cuidado, debido a que se corre el peligro de introducir errores en la presentación y el cálculo de los resultados.

Una vez aplicada la matriz de análisis de riesgo informático se pudo establecer que en los aspectos políticos e institucionales el riesgo es bajo, mientras que existe un riesgo medio o moderado en lo que respecta a la infraestructura física es decir a los activos informáticos tangibles, situación que debe ser gestionada mediante estrategias de recuperación o contingencias por parte de la Dirección de TIC

Para un mejor entendimiento de los resultados se anexa la matriz completa (Anexo N°14).

3.4. Gestión de contingencias

3.4.1. Presentación

El GADPE tiene en funcionamiento nueva INFRAESTRUCTURA TECNOLOGICA que mitigaría los riesgos de pérdida de datos e indisponibilidad de sistemas. Esta infraestructura está compuesta por:

Tabla N° 13: Infraestructura de riesgos

		Probabilidad de Amenaza		
		Criminalidad y Político	Sucesos de origen físico	Negligencia y Institucional
Magnitud de daño	Datos e información	6,3	7,1	6,1
	Sistemas e Infraestructura	6,9	7,8	6,8
	Personal	6,5	7,3	6,3

- DATA CENTER (VER ANEXO N° 9)
- 2 SERVIDORES BLADE (VER ANEXO N°10)
- UNIDAD DE ALMACENAMIENTO
- UNIDAD DE RESPALDO

El Data Center constituye el núcleo tecnológico de toda infraestructura TI, siendo así uno de los activos más importantes de las organizaciones. En este sentido, resulta vital comprender y diseñar al mismo como una unidad integraly no como un conjunto de partes aisladas.Actualmente, el Data Center resulta un actor vital para las empresas las cuales deben expandir y optimizar sus infraestructuras, asegurando la continuidad de los servicios de las organizaciones. Se da seguimiento a las últimas tendencias y los principales análisis, se decide como institución la adquisición de esta novedosa y necesaria infraestructura tecnológica.

3.4.2. DATA CENTER

El ambiente dentro del Datacenter está controlado las 24 horas del día y está formado por:

- El aire de precisión es usado para mantener la temperatura, generalmente en 20 grados Centígrados y 40% de humedad, esto es crucial ya que esta clase de equipo confinado en un cuarto sin ventilación no sobreviviría un periodo muy largo sin las condiciones ideales.
- Respaldo de energía: este recurso es 100% indispensable, cuenta con 2 UPS de torre y uno de rack para cubrir que los servidores no sufran apagones,
- Un piso falso que es adecuado para manejar todo el cableado interno de red y de electricidad.
- Sistema de detección de humedad y temperatura, y el de extinción para incendios es otro paso usado para contener los riegos de una catástrofe.
- Seguridad de acceso a través de reloj biométrico. Además, cuenta con cámaras de video vigilancia.
- Sistema de alarma visual y audible, sirena y una campana.
- Sistema de monitoreo y alarmas vía email.
- Cuenta con 2 rack, 1 para cableado y comunicación y el otro para servidores.

Todos estos complementos garantizan el normal y continuo funcionamiento de los servidores blade.

3.4.3. SERVIDORES BLADE

Los servidores blade están diseñados para aprovechar el espacio, reducir el consumo y simplificar su explotación. Cada servidor blade es una delgada "tarjeta" que contiene únicamente microprocesador, memoria y buses. Es decir, no son directamente utilizables ya que no disponen de fuente de alimentación ni tarjetas de comunicaciones.

Estos elementos más voluminosos se desplazan a un chasis que se monta en el bastidor. El chasis que adquirió el GADPE puede albergar hasta catorce "tarjetas" o servidores blade (IBM). El chasis lleva integrados los siguientes elementos, que son compartidos por todos los servidores:

- Fuente de alimentación: redundante
- Ventiladores o elementos de refrigeración.
- Conmutador de red redundante con el cableado.
- Interfaces de almacenamiento. En particular, es habitual el us

- Interfaces de almacenamiento. En particular, es habitual el uso de redes.
- Sistema de respaldo en cintas.
- Servidores.

Además, estos servidores suelen incluir utilidades software para su despliegue automático. Por ejemplo, son capaces de arrancar desde una imagen del sistema operativo almacenada en disco. Es posible arrancar una u otra imagen según la hora del día o la carga de trabajo, etc.

El GADPE cuenta con un Software de gestión de almacenamiento que automatiza las funciones de restauración y copia de seguridad. IBM Tivoli Storage Manager, producto de la familia de productos Tivoli, enfocada a la gestión de TI siguiendo las mejores prácticas recomendadas por ITIL.IBM Tivoli Storage Manager proporciona una gran variedad de funciones de gestión de almacenamiento desde un único punto de control, lo que permite al GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE ESMERALDAS aprovechar la gran cantidad de información de que dispone.

Permite proteger los datos de la organización de fallas y otros errores mediante copias de respaldo, archivado, administración del espacio del almacenamiento, así mismo, cumplir con regulaciones y planes de recuperación de desastres. Además, cabe indicar que el sistema de almacenamiento permite utilizar una parte para crear servidores virtuales y otra para respaldo. Finalmente, esta infraestructura cuenta con sistema de respaldo en cinta.

Las ventajas se listan a continuación:

- Son más baratos, ya que requiere menos electrónica y fuentes de alimentación para el mismo número de servidores. También consumen menos energía.
- Ocupan menos espacio, debido a que es posible ubicar catorce (14) servidores donde habitualmente solo caben cuatro.
- Son más simples de operar, ya que eliminan la complejidad del cableado y se pueden gestionar remotamente.
- Son menos propensos a fallos ya que cada servidor blade no contiene elementos mecánicos.

- Son más versátiles, debido a que es posible añadir y quitar servidores sin detener el servicio, es decir en caliente (como un disco duro).

3.4.4. INVENTARIO DE SISTEMAS

Tabla N° 14: Inventario de sistemas

Sistemas	Módulos	Procesos que soporta	Usuarios	Arquitectura
Olympo versión 7	Contabilidad	Registros y control contables, garantías, reportes, presupuesto, generación de archivos planos.	1.- María Lara 2.- Angela Murillo 3.- Bonnie Castro 4.- Andrea Mercado 5.- DeisyMenendez 6.- Daniela Santos 7.- Bertha Vasquez 8.- Duval Constantini	CLIENTE – SERVIDOR (BD SQL SERVER) (SERVIDOR HP PROLIANT ML300)
	Consolidación	Consolidar cuentas de las empresas contables	1.- María Lara 2.- Bonnie Castro	
	Roles	Registros y control de roles de pago, generación de archivos planos, reportes.	1.- Katty Bernal 2.- Jennifer Poveda	
	Inventario	Registro y control de bienes de consumo y de larga duración, reportes.	1.- Teresa Mejía 2.- Morenita Moreno 3.- Guillermo Ponce	
	Garantías	Registro y control de garantías, reportes	1.- Daniela Santos	
	Activos Fijos	Registro y control de activos fijos de la institución, generación de	1.- Lorena Zurita	

		etiquetas con códigos de barra.		
Sistema de ruta de archivos		Controla ruta de archivos	1.- Ines Meza 2.- Irma Gonzales	CLIENTE – SERVIDOR (BD MYSQL) (PC)
Intranet		Compartir aplicaciones y archivos.	Todos los funcionarios.	CLIENTE – SERVIDOR (BD MYSQL)
4 Relojes biométricos	2 Edificio Central	Registra y genera reportes de asistencia	1.- Sonia Bautista	Monousuario (BD ACCESS) (BIOSYSTEN B1)
	2 San Mateo	Registra y genera reportes de asistencia	1.- JhonyCordova	Monousuario (BD ACCESS) (BIOSYSTEN i360c)
Portal compras publicas		Registra y controla los procesos de contratación de bienes, servicios, obras, consultorías.	1.- Fabian Oleas 2.- Fanny Egas 3.- Sulay Valencia 4.- Marvi Corozo	WEB

3.4.5. ANÁLISIS DE RIESGOS Y SU CLASIFICACIÓN SEGÚN CRITICIDAD

En el siguiente cuadro se presentan las causas más representativas que originan cada uno de los escenarios propuestos en el Sistema de Contingencia para los Sistemas Informáticos del GADPE:

Tabla N° 15: Inventario de incidencias

CAUSAS	ESCENARIOS
o Fallas Corte de Cable UTP. o Fallas Tarjeta de RED. o Fallas IP asignado. o Fallas Punto de Switch. o Fallas Punto Pacht Panel.	I. No hay comunicación entre CLIENTE – SERVIDOR

○ Fallas Punto de Red. ○ Fallas corte del cable patchcord	
○ Fallas de Componentes de Hardware del Servidor. ○ Falta de UPS(Sin suministro eléctrico) ○ Ataque de Virus Informático. ○ Sobrepasar el límite de almacenamiento en Disco.	II. Falla de un Servidor
○ Accidente ○ Renuncia Intempestiva	III. Ausencia parcial o permanente del personal de Tecnología de la Información.
○ Corte General de Fluido Eléctrico	IV. Interrupción del Fluido Eléctrico durante la ejecución de los procesos.
○ Falla de equipos de comunicación: Switch, antenas, fibra óptica. ○ Fallas en el software de acceso a internet. ○ Perdida de comunicación con proveedores de Internet.	V. Pérdida de servicio de Internet.
○ Incendio. ○ Sabotaje. ○ Corto Circuito. ○ Terremoto. ○ Tsunami.	VI. Indisponibilidad de los Servidores que contienen almacenados los datos.

A continuación, se muestra la prioridad en que deberían recuperarse los sistemas en caso de que acontezca un desastre:

1.- Sistema Contable
2.- Portal de Compra Públicas
3.- Intranet y sus aplicaciones (Sistema de Ruta)
4.- Relojes Biométricos

3.4.6. SISTEMA DE CONTINGENCIA

Tabla N° 16: Sistema de contingencia

Escenario	Recursos de contingencia	Procedimiento	Responsable
I	* Cables de red * Tarjetas de red * Conectores de red * Testeadores de red, ponchadoras,	1.- Comprobar que la conexión física de la red entre cliente y servidor estén correctas, caso contrario reparar. 2.- No debe haber conflicto de ip 3.- El servidor y cliente deben estar en el mismo segmento de red con todos los permisos apropiados.	* Personal de sistemas Ing. Mendoza
II	*UPS (6-8 respaldo) *Servidores con sistema de almacenamiento. *Tener virtualizado el o los servidores.	1.- Ante la falla de un componente del servidor, reemplazar el componente con falla siempre que lo permita cambiar en caliente. 2.- Debe estar conectado a un UPS en caso de que se quede sin suministro eléctrico. 3.- Respaldar los servidores virtuales, para que en caso de fallas de uno de ellos se monte en otro servidor virtual.	* Personal de sistemas Ing. Mendoza Ing. Quevedo
III	*Plan de contingencia *Manuales de procedimientos.	1.-Ante la falta de presencia del personal responsable deben actuar los que han sido capacitados para cubrir dicha necesidad. 2.-Actuar de acuerdo a lo dispuesto en los manuales y planes de contingencia.	* Personal de sistemas Ing. Mendoza Ing. Loor Ing. Quevedo Ing. Constantini

IV	* UPS (6-8min respaldo full carga) que suministre energía a los equipos que trabajan con los sistemas. *Adquirir una planta generadora	1.-Ante un apagón automáticamente debe entrar el sistema alterno de energía de tal manera que no se interrumpa la energía a los equipos. 2.-Si el apagon supera el backup de energía del UPS comunicar a todos los usuarios que se van a detener los servicios y apagar los servidores.	* Personal de sistemas Ing. Constantini Ing. Loor
V	*Switch *Servidor Proxy virtualizado *1 ISP ADICIONAL.	1.-Comprobar que los equipos de conexión están funcionando correctamente, caso contrario reemplazarlo, ejm 1 switch, proxy. 2.-En caso de que se falle el servicio de internet con el ISP 1 Poner en funcionamiento el ISP 2.	* Personal de sistemas Ing. Mendoza Ing. Quevedo
VI	*Contrato con una empresa externa que garantice la seguridad de la información. *Mantener el DATA CENTER. *Administrar los servidores con sistemas de respaldo que garanticen la	1.-Realizar los respaldos en cinta de acuerdo a lo programado para cada sistema. 2.- Tener en stock dispositivos (cintas, discos duros) para unidades de respaldos y servidores. 3.- Realizar el servicio preventivo de los componentes del Datacenter en el tiempo oportuno. 4.- Realizar un constante monitoreo de los servicios de los servidores para garantizar su disponibilidad y corrección a tiempo de alguna falla. 3..- En caso que se activen todas las alarmas de detección	* Personal de sistemas Ing. Mendoza Ing. Quevedo Ing. Constantini Ing. Quevedo

	disponibilidad de los sistemas y su información. *Activación del sistema de extinción. * Mensajes recibidos en el email de ingreso al Datacenter en horarios no laborables.	de temperatura comprobar si hay fuego en la data center acelerar la expulsión del gas de extinción, aso contrario abortar dicha alarma. 4.- Revisar las alarmas y verificar la imagen de la o las personas que ingresan, de ser personal no autorizado comunicar inmediatamente a guardianía.	Ing. Estupiñán

3.4.7. RECUPERACIÓN

Con la implementación del sistema de almacenamiento y respaldo en cinta se garantiza la recuperación del 95-98 % de datos que hayan sido afectados en la contingencia.

Verificación de la pérdida de datos:

- Actividad que depende exclusivamente del usuario final del sistema que debe verificar que los movimientos del día no se hayan perdido, este procedimiento lo debe realizar el usuario de forma inmediata y reportar al área de soporte de sistemas de la perdida de datos, para analizarlos. A través del plan de restablecimiento se recupera la mayor cantidad de datos. Los datos que no se recuperen deben ser ingresados al sistema de inmediato por los usuarios del sistema.

- Si no se presentó pérdida de datos el área de soporte de Sistemas dará vía libre para comenzar la recuperación de datos de todos los registros manuales o documentos originales o copias que se diligenciaron o se recibieron por parte de un usuario durante el lapso de tiempo de la contingencia. Esta información se debe ingresar de forma inmediata y el usuario del sistema es responsable por la pérdida que se puede ocasionar por no actualizar los datos en el sistema.

3.4.8. COPIAS DE SEGURIDAD (BACKUP)

Al contar con la implementación del sistema de almacenamiento y respaldo en cinta la Institución mitigará los riesgos de pérdida de datos e indisponibilidad de sistemas.

Con la nueva infraestructura los respaldos se realizan de acuerdo a las siguientes políticas:

1.- DIARIO – cada día – caduca cada mes
2.- HORARIO – cada hora – caduca cada semana
3.- MENSUAL – cada mes - ∞

Tabla N° 17: Infraestructura de respaldos

Sistema	Tipo	Medio de almacenamiento	Política	Responsable
OLYMPO V7	Todas las BD SQL SERVER	Storage, cintas	2.- HORARIO	Ing. Mendoza
	Ejecutables	Storage, cintas	2.- HORARIO	
Reloj biométrico		CD-DVD	10:00 DE LUNES A VIERNES	Ing. Mendoza
Sistema de ruta de archivos	Todo el BD MYQL	Storage, cintas	2.- HORARIO	Ing. Quevedo

3.4.9.- CALENDARIO DE IMPLANTACIONES Y PUESTA EN MARCHA

Para poner en marcha el Sistema de Contingencia se deben adquirir recursos, ya que en la actualidad carece de ellos. Estos son:

- Independizar las conexiones eléctricas para los equipos que utilizan los sistemas.
- Planta generadora eléctrica
- Contratar otro ISP. Para tener redundancia en disponibilidad de internet.
- Dispositivos de red (switch, cables, conectores, etc) para migrar a cat. 6ª.

3.4.10. PLAN DE PRUEBAS Y SIMULACIONES

Las pruebas y simulaciones se la realizará una vez adquiridos los recursos de contingencias antes descritos, ya que se pone en riesgo la información, sin embargo para aquellos escenarios que no se necesita adquirir algún recurso se presenta el siguiente plan de pruebas.

Tabla N° 18: Plan de pruebas y simulaciones

Problema	Escenario	Acción de recuperación o alternativa	Fecha inicio	Fecha fin	Tiempo	Responsables
1.- disco duro, fuente de poder, mainboard, o memoria ram dañada		-Iniciar el servidor virtualizado en pc disponible (pc a cargo del responsable). -Reemplaza en caliente en el servidor blade el	1.- Jun-03-2016	1.- Jun-07-2016	1-4 horas	Ing. Darwin Mendoza
2.- Servidor caído.	I	disco duro quemado. -Restaurar la información del último	2.-Jun-17-2016	2.- Jun-17-2016	1-4 horas	Ing. Duval Quevedo
3.-Problemas del sistema operativo o sistema		backup -Levantar los servicios del servidor. -Coordinar con los	3.- Jul-18-2016	3.-Jul-18-2016	1-4 horas	

		usuarios el reingreso de información desde el backup hasta el suceso del problema				
1.- Perdida o daño del patchcord que conecta el servidor o el pc de un usuario al punto de red.	I	-Elaboración del patchcord y conectar el servidor o pc al punto de red. -comprobar conexión	1.- May-15-2016	1.- May-15-2016	5-10 min.	Ing. Darwin Mendoza Ing. Jean Loor
1.-Substracción, robo, o daño de 1 reloj biométrico	V	-Restaurar el backup de las huellas del reloj problema al otro reloj -Informar a los funcionarios de lo acontecido.	1.-Jun-11-2016	1.-Jun-11-2016	1 Hora	Ing. Darwin Mendoza
1.-Corte del fluido eléctrico de los	IV	-Entra a funcionar el sistema de respaldo de	1.- Abr-25-2016	1.- Abr-25-2016	1 min.	Ing. Darwin Mendoza

relojes biométricos		energía, ya que éstos equipos tiene una batería de 5 horas de respaldo.				
1.- Corte del fluido eléctrico a los servidores	VI	-Ubicar e instalar los servidores en un área con fluido eléctrico, (área de sistemas o contabilidad)	1.- Ago-13-2016	1.- Ago-13-2016	30 min	Ing. Darwin Mendoza

3.4.11. Bienes susceptibles (activo informático)

Se puede identificar los siguientes bienes afectos a riesgos:

a) Personal: 9 funcionarios
b) Hardware: 200 computadores personales.
c) Software y utilitario: 67 Licencias de Windows 10, 150 licencias de Office 365, CD instaladores del sistema operativo Server 2013.
d) Datos e información: BDD OLYMPO, sistema RUTA.
e) Documentación: archivos, manuales de usuario, de sistema, etc
f) Suministro de energía eléctrica:
g) Suministro de telecomunicaciones: 7 switches, 8 router inalámbricos
h) DATA CENTER. con sus componentes
i) Servidores tipo BLADE.
j) Unidad de almacenamiento
k) Unidad de respaldo.

3.4.12. Efectos

El primer escenario es la imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o humanas.

El segundo escenario es la imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, llámese por ejemplo, cambios de claves de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

3.4.13. Prioridades

La estimación de los daños en los bienes y su impacto, fija una prioridad en relación a la cantidad del tiempo y los recursos necesarios para la reposición de los Servicios que se pierden en el acontecimiento. Por lo tanto, los bienes de más alta prioridad serán los primeros a considerarse en el procedimiento de recuperación ante un evento de desastre.

3.4.14. Fuentes de daño

- Acceso no autorizado
- Por vulneración de los sistemas de seguridad en operación (Ingreso no autorizado a las instalaciones).
- Ruptura de las claves de acceso a los sistema computacionales

  a) Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (Virus, sabotaje).

  b) Intromisión no calificada a procesos y/o datos de los sistemas, ya sea por curiosidad o malas intenciones.

- Desastres Naturales

  a) Movimientos telúricos que afecten directa o indirectamente a las instalaciones físicas de soporte (edificios) y/o de operación (equipos computacionales).

  b) Inundaciones causados por falla en los suministros de agua.

  c) Fallas en los equipos de soporte:

    - Por fallas causadas por la agresividad del ambiente
    - Por fallas de la red de energía eléctrica pública por diferentes razones ajenas al manejo del edificio.
    - Por fallas de los equipos de acondicionamiento atmosféricos necesarios para una adecuada operación de los equipos computacionales más sensibles.
    - Por fallas de la comunicación.
    - Por fallas en el tendido físico de la red local.
    - Por fallas en las telecomunicaciones con instalaciones externas.
    - Por fallas de Central Telefónica.
    - Por fallas de líneas de fax.

- Fallas de Personal Clave

  a) Personal de Informática.

  b) Jefes, Directores

  c) Personal de Administración

    - Enfermedad
    - Accidentes
    - Renuncias.
    - Abandono de sus puestos de trabajo.
    - Otros imponderables.

- Fallas de Hardware

  a) Falla en el Servidor de Aplicaciones y Datos, tanto en su(s) disco(s) duro(s) como en el procesador central.

  b) Falla en el hardware de Red:

    - Falla en los Switches.
    - Falla en el cableado de la Red.

  c) Falla en el Router.

  d) Falla en el muro corta fuego

  e) Incendios

3.5. Medidas preventivas

3.5.1. Control de Accesos.-Se debe definir medidas efectivas para controlar los diferentes accesos a los activos computacionales:

a) Acceso físico de personas no autorizadas.

b) Acceso a la Red de computadoras y Servidor.

c) Acceso restringido a las librerías, programas, y

3.5.2. Previsión de desastres Naturales.-La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en el área del data center, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar mediante su caída y/o destrucción, la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, el tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, cintas, discos con información vital de respaldo de aquellos que se encuentren aun en las instalaciones de la institución.

3.5.3. Adecuado Soporte de Utilitarios.- Las fallas de los equipos de procesamiento de información pueden minimizarse mediante el uso de otros equipos, a los cuales también se les debe controlar periódicamente su buen funcionamiento, se refiere a:

a) UPS de respaldo de actual servidor de Red o de estaciones críticas
b) UPS de respaldo switches

3.5.4. Seguridad Física del Personal.- Se deberá tomar las medidas para recomendar, incentivar y lograr que el personal comparta sus conocimientos con sus colegas dentro de cada área, en lo referente a la utilización del software y elementos de soporte relevantes. Estas acciones permitirán mejorar los niveles de seguridad, permitiendo los reemplazos en caso de desastres, emergencias o períodos de ausencia ya sea por vacaciones o enfermedades.

3.5.5. Seguridad de la Información.- La información y programas de los Sistemas de Información que se encuentran en el Servidor, o de otras estaciones de trabajo críticas deben protegerse mediante claves de acceso y a través de un plan de respaldo adecuado.

3.6. Plan de respaldo y recuperación

El Plan de Respaldo trata de cómo se llevan a cabo las acciones críticas entre la pérdida de un servicio o recurso, y su recuperación o restablecimiento. Todos los nuevos diseños de Sistemas, Proyectos o ambientes, tendrán sus propios Planes

3.6.1. Objetivos

- Determinarpolíticas y procedimientos para respaldar las aplicaciones y datos.
- Planificar la reactivación dentro de las 24 horas de producido un desastre, todo el sistema de procesamiento y sus funciones asociadas.
- Aplicar el permanente mantenimiento y supervisión de los sistemas y aplicaciones.
- Establecer una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un desastre.

3.6.2. Alcance del Plan de Recuperación

El objetivo es restablecer en el menor tiempo posible el nivel de operación normal del centro de procesamiento de la información, basándose en los planes de emergencia y de respaldo a los niveles del Centro de Cómputos y de los demás niveles. La responsabilidad sobre el Plan de Recuperación es de la Dirección Tic, la cual debe considerar la combinación de todo su personal, equipos, datos, sistemas, comunicaciones y suministros.

3.6.3. Activación del Plan

Decisión.- La decisión queda a juicio del Comité Informático del Gobierno Autónomo Descentralizado de Esmeraldas para determinar la activación del Plan de Desastres, y además indicar el lugar alternativo de ejecución del Respaldo y/o operación de emergencia, basándose en las recomendaciones indicadas por éste.

Duración estimada.-Los especialistas de cada área determinarán la duración estimada de la interrupción del servicio, siendo un factor clave que podrá sugerir continuar el procesamiento en el lugar afectado o proceder al traslado del procesamiento a un lugar alternativo.

Responsabilidades

- Orden de Ejecución del Plan : Comité Informático GADPE, conformado por los 9 funcionarios de la Dirección de TI.
- Supervisión del Plan de Rec. : Especialista(s) de Área(s).
- Abastecimiento (HW, SW): Administración.
- Tareas de Recuperación: Personal de tareas afines.

CAPÍTULO IV: ANÁLISIS DE IMPACTOS

Se han establecido los aspectos positivos o negativos para la ejecución del proyecto de investigación provocando cambios en el ámbito tecnológico, organizacional, administrativo, legal, ético, económico y ambiental. Los mismos que para una mejor comprensión e interpretación se lo analiza sobre la base de una tabla matriz de impactos, para lo cual se sigue el siguiente procedimiento:

Para cada área o aspecto se determinó indicadores de impacto en la respectiva matriz. Los niveles de Impacto se califican numéricamente con la siguiente escala:

Tabla N°19 : Tabla de impactos

Niveles	Descripción
-3	Impacto negativo alto
-2	Impacto negativo medio
-1	Impacto negativo bajo
0	No hay impacto alguno
1	Impacto positivo bajo
2	Impacto positivo medio
3	Impacto positivo alto

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

4.1. Impacto tecnológico

Tabla N°20: Matriz de Impacto Tecnológico

Nivel de impactos / Indicadores	-3	-2	-1	0	1	2	3
1. Sistemas y Aplicaciones							X
2. Infraestructura tecnológica							X
3. Redes y comunicaciones							X
4. Servicios Web							X
TOTAL							**12**

$\sum = 12$

Nivel de Impacto $= \dfrac{\Sigma}{\textit{Numero de Indicadores}}$

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

Nivel de Impacto Tecnológico: Impacto Positivo Alto

Análisis

La Tecnología es la organización y aplicación de conocimientos para el logro de fines prácticos. Incluye manifestaciones físicas como las máquinas y herramientas, pero también técnicas intelectuales y procesos utilizados para resolver problemas y obtener resultados deseados. El uso de tecnologías ha cambiado la forma en que operan las organizaciones a través de su uso se logran importantes mejoras, puesto que automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y, lo más importantes, su implantación logra ventajas competitivas, el impacto tecnológico determinado en esta investigación es positivo alto, y la argumentación para cada indicador se detalla a continuación:

4.1.1. Los **Sistemas y aplicaciones**tienen un impacto positivo alto debido a que mediante este trabajo, se garantiza el desarrollo de software es seguro y optimiza el ciclo de vida del desarrollo de software. Además de mejorar el control de acceso al identificar la persona que desea acceder a las aplicaciones, sistemas y a sus datos, y al verificar la identidad de dicha persona.

4.1.2. En **Redes y comunicaciones** existe un impacto positivo alto debido al control de acceso a la red, la existencia de control de los accesos de los usuarios internos y externos tales como proveedores o invitados a la red institucional. Así como las conductas que causan la destrucción, desgaste, o deterioro del cableado y equipo de comunicación

4.1.3. La **Infraestructura tecnológica** tiene un impacto positivo debido a que incluye la apropiada protección y soporte en los distintos procesos involucrados, el proceso de gestión de incidentes se mejora cuando se da respuesta ante un incidente de seguridad. Comprende todas aquellas medidas dirigidas a evitar daños en el hardware o en el software, ya sea por factores externos (sismos, incendios, inundaciones) o internos (mal uso, sabotaje, negligencia).

4.1.4. En los **Servicios web** existe un impacto positivo alto debido a que la propuesta incluida en esta investigación mitiga el efecto y consecuencias que los ataques informáticos, fallas de equipos y catástrofes naturales, pueden generar en la prestación y continuidad de los servicios de TIC tanto mediante la página web, correo electrónico y los diversos módulos de la intranet institucional.

4.2. Impacto administrativo

Tabla N° 21: Matriz de Impacto Administrativo

Nivel de impactos / Indicadores	-3	-2	-1	0	1	2	3
1. Procesos de control interno							X
2. Mantenimiento de activo Informático							X
3. Seguridad Física							X
4. Control de bienes Informáticos							X
TOTAL							**12**

Nivel de Impacto $= \dfrac{\Sigma}{\textit{Numero de Indicadores}}$ $\sum = 12$

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

Nivel de Impacto Administrativo: Impacto Positivo Alto

Análisis

La administración hace referencia a los procesos con los que se gestionan los recursos institucionales utilizados en el cumplimiento de las competencias otorgadas por la ley a GADPE, Existe un impacto positivo alto de este trabajo sobre cada uno de estos procesos de gestión de los recursos tangibles (materiales, suministros, equipos) e intangibles (normas, procesos, procedimientos) de la administración pública que forman el activo informático y son parte de los bienes de larga duración. A continuación se detallan los argumentos considerados en cada indicador:

4.2.1. Los **Procesos de control interno** tienen un impacto positivo alto debido a que tanto la propuesta como los resultados de esta investigación fortalecen los controles existentes a través de una articulada serie de controles establecidos con las partes interesadas para una buena gestión de los activos de larga duración (computadoras, impresoras, sistemas, equipo de comunicación, sistemas y paquetes informáticos).

4.2.2. En **Mantenimiento de activo Informático** el impacto es positivo alto considerando que al tener un inventario de los activos informáticos clasificado por proceso, categoría, y sobre todo por la valoración de su nivel de riesgo facilita que otros planes existentes (mantenimiento, informático, operativo) tengan insumos reales tanto para su ejecución como para su actualización. Además de garantizar el normal funcionamiento y operación de cada activo.

4.2.3. La **Seguridad Física** tiene un impacto positivo alto debido a que tanto la matriz de riesgo establecida como los procedimientos planificados en la propuesta consideran los controles de accesos como el punto de partida de todo el sistema de seguridad de la institución a nivel no solo informático sino administrativo.

4.2.4. En el **Control de bienes Informáticos** se ha establecido un impacto positivo alto debido a que se incluyen estrategias para el control de los bienes de larga duración, y se basa en los procedimientos establecidos tanto por el área administrativa como por la contraloría general del estado para salvaguardar dicho patrimonio, estableciendo actividades, procedimientos, responsables y tiempos para cada categoría en un plan de gestión de riesgo informático.

4.3. Impacto organizacional

Tabla N° 22: Matriz de Impacto Organizacional

Nivel de impactos / Indicadores	-3	-2	-1	0	1	2	3
1. Planificación de estrategias							X
2. Gestión de cambios							X
3. Capacitación y adiestramiento							X
4. Monitorización de eventos							X
TOTAL							**12**

Nivel de Impacto = $\frac{\sum}{\textit{Numero de Indicadores}}$ $\sum = 12$

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

Nivel de Impacto Organizacional : Impacto Positivo Alto

Análisis

La organización hace referencia al orden y estructura que la institución tiene como modelo de gestión, la gestión de riesgos es reconocida como una parte integral de las buenas prácticas en una organización. Es un proceso iterativo que consta de pasos, los cuales, cuando son ejecutados en secuencia, posibilitan una mejora continua en el proceso de toma de decisiones por lo que el impacto establecido es positivo alto. A continuación se detallan los argumentos considerados en cada indicador:

4.3.1. **Planificación de estrategias** tienen un impacto positivo alto debido a que esta investigación incluye dentro del plan de gestión del riesgo informático políticas de continuidad de negocio, que van desde las amenazas leves hasta algún cambio significativo en la administración para la seguridad informática.

4.3.2. En la **Gestión de cambios** el impacto es positivo alto considerando la existencia de cambios regulatorios tanto legales como normativos en el sector público, sobre todo en el área informática a nivel de sistemas de información, gestión de archivos y aplicaciones documentales. Solo bajo un enfoque de optimización del riesgo es que gradualmente una organización del sector público como el GADPE, a través de la robustez de su estructura de control interno, así como la eficiencia y eficacia de ésta, alcanza el cumplimiento de sus objetivos, y por lo tanto generar impactos y efectos positivos sobre la población.

4.3.3. La **Capacitación y adiestramiento** tiene un impacto positivo alto debido a que Falta de formación y concienciación se ha considerado en la elaboración de la propuesta ante la necesidad de potenciar la formación en materia de seguridad de la información tanto al personal interno como a la máxima autoridad. El factor humano es de vital relevancia para prevenir los ciber ataques avanzados o el fraude electrónico.

4.3.4. En la **Monitorización de eventos** se ha establecido un impacto positivo alto debido a que esta investigación los procesos reactivos contemplados e incluidos en la propuesta permite a la administración medir correctamente la implementación de políticas y procedimientos informáticos.

4.4. Impacto ético

Tabla N° 23: Matriz de Impacto Ético

Indicadores \ Nivel de impactos	-3	-2	-1	0	1	2	3
1. Administración de accesos							X
2. Manejo de Información y almacenamiento							X
3. Utilización de computadoras e impresoras							X
4. Uso de Internet y correo electrónico							X
TOTAL							**12**

$\sum = 12$

Nivel de Impacto $= \dfrac{\Sigma}{\textit{Numero de Indicadores}}$

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

Nivel de Impacto Ético: Impacto Alto Positivo

Análisis

La Ética incita a que el los funcionarios tengan una conciencia social, relacionada con la tecnología informática y utilizar los ordenadores no solo con eficiencia y sino con criterios éticos. El objetivo es tomar decisiones sobre temas tecnológicos con la moral y los valores institucionales y los derechos humanos en general por lo que el impacto establecido es positivo alto. A continuación se detallan los argumentos considerados en cada indicador:

4.4.1. En la **Administración de accesos** tienen un impacto positivo alto debido a que esta investigación incluye dentro del plan de gestión del riesgo informático incluye políticas de control de accesos de manera que a nivel físico o lógico se mitigue el efecto que las amenazas pueden generar sobre las vulnerabilidades existentes en la institución.

4.4.2. En el **Manejo de Información y almacenamiento** el impacto es positivo alto considerando que se ha establecidos controles para evitar que personal sin estar

autorizado, se apodere, utilice o modifique datos reservados de carácter personal o institucional de otro que se hallen almacenados en archivos o plataformas informáticas, o cualquier otro tipo de archivo digital sea público o privado.

4.4.3. Con respecto a la **Utilización de computadoras e impresoras** tiene un impacto positivo alto debido a que se mantiene un inventario de activo informático actualizado sobre el cual se contemplan actividades de monitoreo y revisión periódicos que garanticen un buen uso. Evitando que se utilicen esos recursos para fines distintos al trabajo institucional. A nivel de suministros de impresión se ha incluido un software de gestión que controla los contadores, el rendimiento y el uso que los usuarios mantienen de manera diaria.

4.4.4. El **Uso de Internet y correo electrónico** se ha establecido un impacto positivo alto debido a que tanto a través de las políticas como de las estrategias incluidas en el plan de gestión de riesgos se contemplan seguridades en el servidor tanto para la navegación y acceso al internet como procedimientos de control para la asignación y actualización de los correos electrónicos de los funcionarios, de manera que algunas páginas identificadas como no permitidas, inseguras o no necesarias para cada tipo de usuario se encuentren bloqueadas.

4.5. Impacto legal

Tabla N° 24: Matriz de Impacto Legal

Indicadores / Nivel de impactos	-3	-2	-1	0	1	2	3
1. Derechos de información							X
2. Propiedad intelectual							X
3. Responsabilidad formal							X
4. Licenciamiento de aplicaciones							X
TOTAL							**12**

Nivel de Impacto $= \dfrac{\sum}{\textit{Numero de Indicadores}}$ $\sum = 12$

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

Nivel de Impacto Legal: Impacto Positivo Alto

Análisis

El aspecto legal tiene un impacto positivo alto debido a la importancia de la normativa legar en las instituciones públicas, considerando: el modelo de Gestión por Resultados implementado en el GADPE, el COOTAD, las leyes para la gestión de los bienes de larga duración, las normas de control interno de la Contraloría General del Estado, el Plan informático y el Manual de Procesos, Procedimientos y Puestos de trabajo de la institución. A continuación se exponen los argumentos considerados en cada indicador:

4.5.1. Los **Derechos de información** tienen un impacto positivo alto debido a que en esta investigación se consideran las amenazas y vulnerabilidades que de alguna manera pueden afectar la publicación de la información que la institución genera y por ley está obligada a publicar de manera periódica y en base a los formatos establecidos en la LOTAIP. Además de precautelar la confidencialidad de

información institucional o personal y la divulgación indebida de los datos contenido o almacenados en sistemas informáticos y recursos digitales.

4.5.2. En la**Propiedad intelectual** el impacto es positivo alto considerando que en esta investigación se incluyen estrategias de dirigidas a proteger y salvaguardar los derechos reservados primero de la institución y también de los propietarios de los sistemas y aplicaciones ante las conductas dirigidas a obtener datos, información o incluso software de manera ilegítima. Evitando así el fraude electrónico, la piratería informática, el plagio informático y la fuga de información confidencial. .

4.5.3. La **Responsabilidad formal** tiene un impacto positivo alto considerando los módulos o funciones al ser una característica de los sistemas y las instituciones, implican la definición y existencia de mecanismos para determinar quién realizo acciones y quien debe rendir cuentas sobre las mismas, es decir el establecimiento de responsabilidades sobre cada una de las actividades y procedimientos definidos.

4.5.4. El **Licenciamientode aplicaciones** genera un impacto positivo alto considerando a través de las políticas establecidas por la institución y las disposiciones contempladas en las resoluciones administrativas o en las mismas leyes se establece la legalización del software comercial.

4.6. Impacto económico

Tabla N° 24: Matriz de Impacto Económico

Nivel de impactos / Indicadores	-3	-2	-1	0	1	2	3
Vida útil del activo informático							X
Gasto de suministros							X
Gastos de mantenimiento					X		
Licenciamiento de aplicaciones			X				
TOTAL			**-1**		**1**		**6**

Nivel de Impacto $= \dfrac{\Sigma}{\textit{Numero de Indicadores}}$ $\sum = 6$

$$NI = \frac{6}{4} = 1{,}5$$

Nivel de Impacto Económico: Impacto Medio Positivo

Análisis

Existe un impacto económico positivo medio debido a la relación entre el rendimiento de las inversiones para mantener la vida útil de los equipos informáticos, el ahorro que la gestión del riesgo informático genera y los gastos incurridos en el licenciamiento, mantenimiento y suministros necesarios para la operación de la institución. A continuación se exponen los argumentos considerados en cada indicador:

4.6.1. Existe un impacto positivo alto en la **Vida útil del activo informático** considerando que con las medidas contempladas en el plan de gestión de riesgos se precautela el estado de cada uno de los bienes de larga duración alargando la vida útil y ahorrando recursos económicos en la adquisición de nuevos equipos o recursos de TIC para la institución. Además de contemplar las medidas a tomar en caso de desastres naturales como los sismos, inundaciones, o fallas eléctricas.

4.6.2. En el **Gasto de suministros** el impacto es positivo alto considerando que al definirse estrategias dentro del plan de gestión de riesgo informático orientados a la implementación de procedimientos de control y monitoreo para las impresoras y sus consumibles a través del registro automático de uso que dan

los usuarios, es decir mediante la focalización de impresión se reduce el riesgo de quedarse sin servicio de impresión y se ahorran recursos para la institución.

4.6.3. En lo concerniente a los **Gastos de mantenimiento** se tiene un impacto positivo bajo debido a que en esta investigación se incluyen estrategias que por un lado incrementan los costos de mantenimiento informático sobre todo preventivo, pero por otro lado es mucho más barato que realizar mantenimiento correctivo o peor aún comprar nuevos equipos, además de evitar paros en las actividades de los funcionarios o servicios de la institución.

4.6.4. El **Licenciamiento de aplicaciones** se ha establecido un impacto negativo bajo debido a que los costos son altos, a nivel de sistemas operativos, bases de datos, sistemas específicos, utilitarios, antivirus, aplicaciones de seguridad; sin embargo garantizan el correcto funcionamiento y operación de los servicios de TIC y por ende de la institución, y además de mitigar el riesgo de sufrir algún embargo o sanción por el uso de software pirata que generaría gastos innecesarios.

4.7. Impacto ambiental

Tabla N° 26: Matriz de Impacto Ambiental

Nivel de impactos / Indicadores	-3	-2	-1	0	1	2	3
1. Sistemas de alarma y monitoreo							X
2. Consumo de papel							X
3. Consumo de energía	X						
4. Reciclaje tecnológico							X
TOTAL	**-3**						**9**

$\sum = 6$

Nivel de Impacto $= \dfrac{\Sigma}{\textit{Numero de Indicadores}}$

$$NI = \frac{6}{4} = 1.5$$

Nivel de Impacto Ambiental: Impacto Positivo Medio

Análisis

Debido a la contaminación por parte de las computadoras se da con el desperdicio de energía: una computadora de escritorio promedio desperdicia casi la mitad de la energía que consume, por lo que se incrementa el costo en electricidad y la emisión de gases nocivos para el planeta. Este proceso se ha acelerado gracias a diseños que reducen la vida útil del artículo, lo cual acelera la fabricación así como la generación de los residuos electrónicos, sin embargo debido al plan de gestión de riesgo informático contemplado en esta investigación se establece un impacto positivo bajo.A continuación se exponen los argumentos de cada indicador:

4.7.1. Existe un impacto positivo alto al usar **Sistemas de alarma y monitoreo** tanto para el Datacenter como para las áreas estratégicas de las instalaciones, los sistemas contra incendio no solo permiten evitar daños mayores sino contaminar en menor grado el ambiente, además de dar la seguridad necesaria para los seres humanos que laboran en la institución.

4.7.2. En el **Consumo de papel** el impacto es positivo alto considerando que las acciones incluidas en la propuesta no solo que controlan la impresión y uso de papel sino que tienden a automatizar procesos y fomentan y garantiza el uso de información digital por parte de los funcionarios del GADPE.

4.7.3. Debido a que el **Consumo deenergía** y los costos de unidades de energía ininterrumpida son altos, a pesar que en la gestión de riesgo informático se consideran medidas de ahorro; el impacto determinado es negativo medio considerando el equipamiento y mantenimiento de activos como: el Datacenter, aires acondicionados, equipos de gran escala y el propio parque informático, se establece un impacto negativo alto.

4.7.4. Con el **Reciclaje tecnológico** se disminuyen los residuos electrónicos, mismos que contienen un alto grado de elementos tóxicos, y representan grandes riesgos al ambiente y a la salud pública. Al juntarlos con los demás desechos y llevarlos a los mismos tiraderos, éstos son altamente contaminantes por el tipo de materiales; al incluirse estrategias que fomentan el manejo ambiental de estos residuos dentro de plan de gestión de riesgo informático se genera un impacto positivo alto.

4.8. Impacto general

Tabla N° 26: Matriz de Impacto General

Nivel de impactos / Indicadores	-3	-2	-1	0	1	2	3
1. Impacto Tecnológico							X
2. Impacto Administrativo							X
3. Impacto Organizacional							X
4. Impacto Ético							X
5. Impacto Legal							X
6. Impacto Económico						X	
7. Impacto Ambiental						X	
TOTAL						**4**	**15**

$\sum = 19$

Nivel de Impacto $= \dfrac{\Sigma}{\textit{Numero de Indicadores}}$

$$NI = \frac{19}{6} = 2.71 \approx 3$$

Nivel de Impacto General: Impacto Positivo Alto

Análisis:

El presente proyecto genera en si un impacto en general **Alto 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

5.1. CONCLUSIONES

Las instituciones del sector público poseen un modelo de gestión por resultados en donde las tecnologías de información y comunicación son la plataforma base para automatizar procesos, gestionar información y alcanzar la eficiencia operacional en el cumplimiento de sus objetivos institucionales a través del cumplimiento de las normas de control interno de la Contraria General del Estado, independiente del giro de negocio o actividad que realicen.

La Gestión de Riesgo es la posibilidad de la ocurrencia de un hecho o suceso no deseado o la no ocurrencia de uno deseado, conformada por una combinación de circunstancias del entorno, donde hay posibilidad de pérdidas, por lo que la gestión de riesgo informático puede definirse como el efecto de una causa multiplicado por la frecuencia probable de ocurrencia dentro del entorno de las TIC.

El Gobierno Autónomo Descentralizado de la Provincia de Esmeradas para el ejercicio de sus competencias otorgadas por la constitución y reguladas por el COOTAD cuenta con un parque informático y con los recursos suficientes para alinear las TIC a los objetivos estratégicos institucionales pero necesitaba de un plan de Gestión de Riesgo Informático que minimice las debilidades y amenazas existentes y maximice las fortalezas y oportunidades con las que cuentan.

El avance de la tecnología y la aparición de muchas metodologías para la gestión de riesgos ha permitido establecer un proceso de valoración y priorización de los riesgos con base en la información institucional a través de matrices elaboradas en la etapa de identificación, con el fin de clasificar un riesgos y proveer información real para establecer el nivel de riesgo y las acciones que se deben implementar por parte del personal de TIC.

La metodología utilizada es aplicable a cualquier situación donde un resultado no deseado o inesperado pueda ser significativo o donde se identifiquen oportunidades de mejora, asociado al conjunto de pasos secuenciales, lógicos y sistemáticos que se deben seguir para identificar, valorar y manejar los riesgos asociados a los procesos de TIC de cualquier institución, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados minimizando las pérdidas o maximizando las oportunidades de mejora.

La inseguridad es una propiedad inherente a los recursos informáticos y la gestión del riesgo o informático es la única forma de medirla y aminorarla por lo que los recursos financieros de una organización deben invertirse de la mejor manera mirando siempre el retorno de inversión.

La forma de conseguir el mayor beneficio en seguridad de la información es contar con una adecuada evaluación de riesgos, que oriente las inversiones, que minimicen el impacto en casos de incidentes en casos de incidentes, sin importar la metodología que se selecciones.

5.2. RECOMENDACIONES

El plan de contingencias debe ser aprobado, luego difundido entre el personal responsable de su ejecución y deberá ser sometido a pruebas, entrenamientos y evaluaciones periódicas, o cuando se haya efectuado algún cambio en la configuración de los equipos o el esquema de procesamiento.

Se debe considerar en el Plan de continuidad de las operaciones la puesta en marcha de un centro de cómputo alterno propio o de uso compartido en un Datacenter Estatal, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos.

La seguridad de la información no debe ser una responsabilidad únicamente del área de tecnología, debe fluir desde la alta gerencia hacia todos los procesos de negocios. Si la seguridad de la información depende únicamente de TI entonces la probabilidad es del 100% de que no se implemente.

Se debe conformar el comité de seguridad de la información compuesto por cada director departamental debido a que genera más compromiso para hacer cumplir las políticas de seguridad de la información.

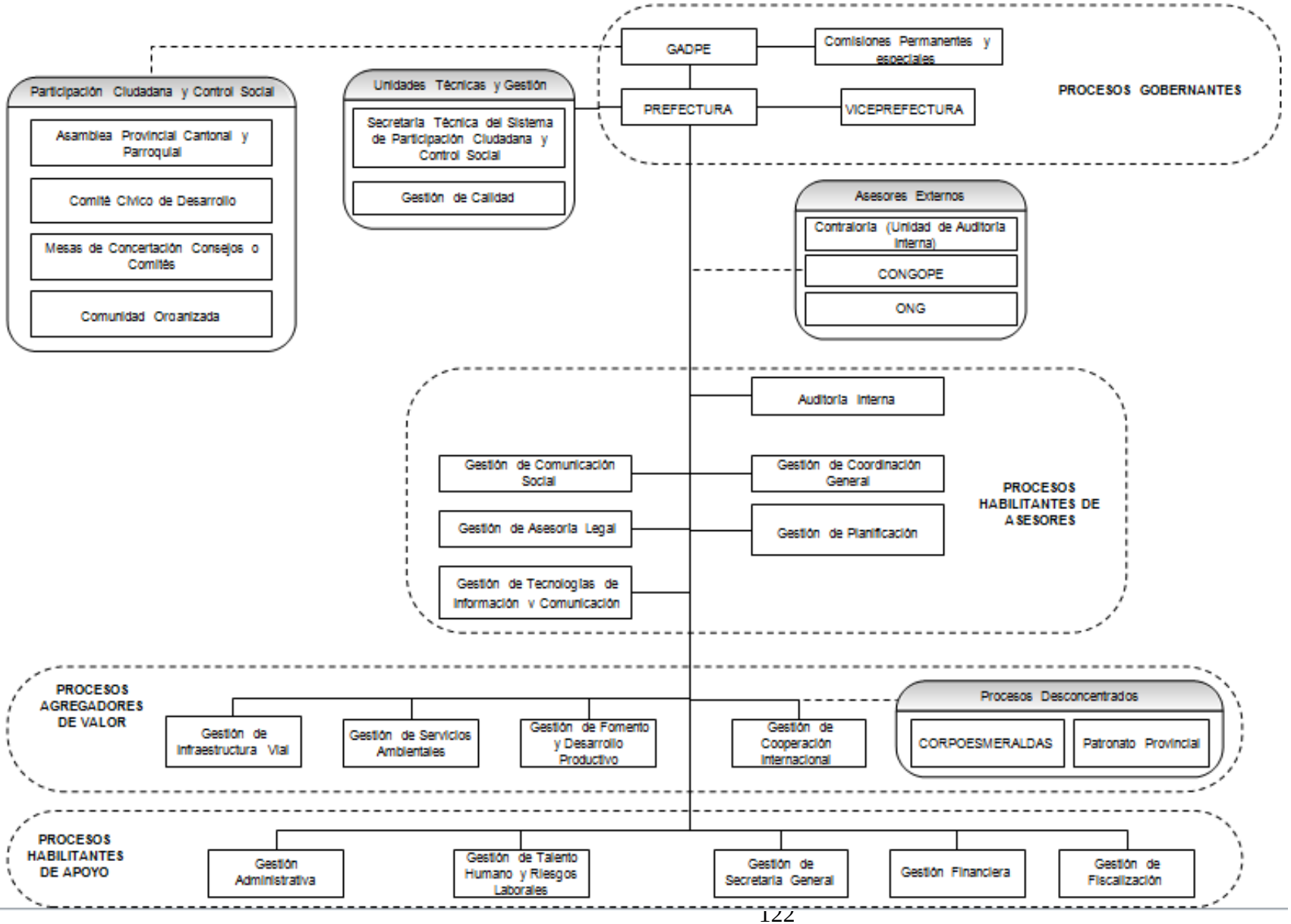
BIBLIOGRAFÍA

- Ambruster T (2014). *Aplicación de HACCP en la validación de procesos farmacéuticos*. Pharmaceutycal Technology, Edición Argentina #49. Buenos Aires.
- 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.
- Coopers y Lybrand (2007). *Los nuevos conceptos del control interno.* Informe COSO, Ediciones Díaz de Santos, Madrid, tomo I, 3-16p, 2007.
- GADPE. (2014). *Politicas, Procesos y Procedimientos de TIC.* Gobierno Autonomo Descentralizado de Esmeraldas - Direccion de TIC. Obtenido de: www.prefecturadeesmeraldas.gob.ec/mpptic.htm.
- ICONTEC (2011). *Estándar Internacional ISO/IEC 27005:2011* Information technology — Security techniques — Information security risk management second edition.
- 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

- Luhmann Nikla (2000). *Technology, Environment, and Social Risk: A System Perspective*.: Industrial Crisis Quaterly, 4, S: 223-231.
- 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
- Quirós, M.C.(2013*). Administración del riesgo y auditoria interna*. Universidad de costa Rica. Contraloría Universitaria. Boletín 1, Articulo 9. [en línea septiembre 2003]. Disponible en: http://ucu.ucr.ac.cr/boletin1-2003.articulo9.htm.
- 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

ANEXOS

ANEXO N°1: Organigrama Estructural



ANEXO N°2: Encuestas CHECKLIST aplicadas a usuarios

3.2.1 Oficina primitiva, oficina industrial o burótica	Sí	Parc	No
Cuenta su oficina con procesamiento electrónico de datos generalizado?			
Se mide la productividad de la oficina mas por la calidad que por la cantidad?			
La Contabilidad es de diseño moderno y cuenta con rutinas gerenciales?			
Su oficina está comunicada con el exterior con medios teleinformáticos?			
Se han informatizado las funciones telefónicas internas y externas?			

3.2.2 Orientación al trabajo en red	Sí	Parc	No
Opera la organización con sistemas informáticos en red?			
Es concebida la Contabilidad como un concentrador último de información?			
Compartiendo información, se han adoptado normas de confidencialidad ?			
Operando en red, cuenta la empresa con un administrador interno de la red ?			
Aprovechan los niveles de Staff rutinariamente las ventajas de la red ?			

3.2.3 Oficina y flujo de información	Sí	Parc	No
Existe un adecuado flujo de información interna a través de la red ?			
Existe un adecuado flujo de información con el exterior a través de la red ?			
La información es dosificada por niveles a través de normas de acceso ?			
Se filtra debidamente la información que fluye al Staff bajo normas de rutina ?			
Se considera al Centro de Cómputos como un proveedor interno ?			

3.2.4 Auditoría de sistemas	Sí	Parc	No
Se cuenta con un Plan Maestro de Auditoría, Contable y de Sistemas ?			
Prevé el Plan de Auditoría controles contables, administrativos y sistémicos ?			
Se cuenta con informes periódicos de auditoría externa ?			
Se investigan debidamente las salvedades que emergen de los informes ?			
Está informada la firma sobre la existencia de Paquetes de Auditoría ?			

3.2.5 Capacitación en TICs	Sí	Parc	No
Se capacita a la gente en el manejo del equipamiento de hardware ?			
Se capacita a la gente en el manejo de las aplicaciones existentes ?			
Se capacita a la gente en el manejo de aplicaciones standard (Office, etc.) ?			
Se capacita a la gente en el manejo de las comunicaciones en red ?			
Se capacita a la gente en el dominio de Internet ?			

3.2.6 Aprovisionamiento de equipos informáticos	Sí	Parc	No
Al adquirir hardware se toman en cuenta factores extra precios ?			
Se cuenta con proveedores estables de hardware de reconocida idoneidad ?			
Se han centralizado las compras de hardware en personal idóneo ?			
Al instalar nuevo hardware se tiene en cuenta la seguridad física ?			
La recepción de nuevo hardware está a cargo de personal idóneo ?			

3.2.7 Soporte técnico del hardware	Sí	Parc	No
Se cuenta con soporte técnico interno para el manejo del hardware ?			
Se cuenta con soporte técnico externo para el manejo del hardware ?			
Se ha contratado regularmente el mantenimiento del hardware ?			
Es satisfactorio el comportamiento del mantenimiento del hardware ?			
Está previsto el mantenimiento de equipos, instalaciones y periféricos ?			

3.2.8 Obsolescencia del hardware	Sí	Parc	No
Es razonablemente moderno el nivel del hardware existente ?			
Se avanza razonablemente en la reposición de equipos de avanzada ?			
Se ha superado la obsolescencia en el rubro de impresoras ?			
Se cuenta con los más avanzados equipos de seguridad ?			
Se cuenta con documentación al día en materia de posible obsolescencia ?			

3.2.9 Plan maestro de equipamiento del hardware	Sí	Parc	No
Se cuenta con un Plan Maestro de reequipamiento de computadoras ?			
Se cuenta con un Plan Maestro de reequipamiento de impresoras ?			
Se cuenta con un Plan maestro de ampliación de la red ?			
Se destinan partidas presupuestarias para cumplir con el reequipamiento ?			

Se considera el reequipamiento informático como un factor crítico del éxito ?			

3.2.10 Prevención de desastres en el hardware	Sí	Parc	No
Se plantean reacciones frente a hipotéticos casos de desastre en hardware ?			
Se cuenta con equipamiento muleto a la medida de las necesidades reales ?			
Se verifican apropiadamente y con asiduidad las instalaciones eléctricas ?			
Se prevén acciones de emergencia frente al caso concreto de un desastre ?			
Hay seguridad en materia de posibles robos o daños intencionales ?			

3.2.11 Integración de los sistemas	Sí	Parc	No
Los sistemas instalados cuentan con un aceptable grado de integración ?			
Ventas, clientes, contabilidad y stocks se hallan realmente integrados ?			
Compras, proveedores, stocks, contabilidad, se hallan realmente integrados ?			
Surgen de los sistemas elementales rutinas de Tablero de Comando ?			
Se conoce adecuadamente la oferta de sistemas contables enlatados ?			

3.2.12 Proyección general del software	Sí	Parc	No
Está todo el software en uso orientado a rutinas de uso gerencial ?			
Demandan los gerentes disponer de rutinas para la toma de decisiones ?			
Se procura disponer de aplicaciones gerenciales basadas en utilitarios ?			
La búsqueda de nuevo software tiene en cuenta necesidades gerenciales ?			
El perfil del responsable de sistemas apunta al nivel de un C.I.O. ?			

3.2.13 Obsolescencia del software	Sí	Parc	No
El criterio de obsolescencia verifica el apoyo a la toma de decisiones ?			
El software contable administrativo está a salvo de la obsolescencia ?			
El software de utilitarios es de ultima generación ?			
Se cuenta con soporte interno para desarrollar aplicaciones simples ?			
Se cuenta con soporte externo para desarrollar aplicaciones complejas ?			

3.2.14 Soporte técnico del software	Sí	Parc	No
Se cuenta con soporte técnico interno relacionado con el software ?			
Se cuenta con soporte técnico externo relacionado con el software ?			
Se ha contratado regularmente el mantenimiento del software ?			
Es satisfactorio el comportamiento del mantenimiento del software ?			
Se cuenta con documentación al día en materia de posible obsolescencia ?			

3.2.15 Prevención de desastres en el software	Sí	Parc	No
Se cuenta con aplicaciones antivirus de ultima generación ?			
Se han instalado procesos antivirus preventivos automáticos ?			
Se cuenta con radicaciones paralelas de software para caso de desastres ?			
Se cuenta con instalaciones de software OK en propiedad intelectual ?			
Hay seguridad en materia de posibles robos o daños intencionales ?			

SUMA DE LOS PUNTOS PARCIALES .....

PROMEDIO .....

ANEXO N°3: Modelo de Entrevista aplicada al Director de TIC

1. ¿El GADPE configura los sistemas o esta tarea la efectúan otros proveedores o distribuidores de hardware?

2. ¿Cuáles de los siguientes elementos se han creado basándose en una configuración documentada o en una homologación formal?

- **Pc estación de trabajo**
- **Servidores**
- Ninguno

2.1. ¿Esta configuración incluye procedimientos para robustecer el servidor?

- **Sí**
- No
- No lo sé

3. ¿Cuáles de las soluciones siguientes se han instalado en las terminales de trabajo y los equipos portátiles de los empleados?

- software de firewall personal
- software de detección y eliminación de spyware
- software de encriptación de discos
- software de administración/control remoto
- protector de pantalla protegido por contraseña
- **Ninguno**

4. ¿Se ha aplicado controles de seguridad físico para garantizar la seguridad de la propiedad de la institución?

- **Sí**
- No
- No lo sé

4.1. ¿Cuál de los siguientes controles de seguridad utiliza?

- **Sistema de alarma para detectar e informar las intrusiones.**
- **Equipos de red (conmutadores, cableado, conexiones a Internet) en lugares cerrados con llaves y con acceso restringido.**
- **Los equipos de red se encuentran además en un armario o rack que se pueda cerrar con llave.**
- **Los servidores se encuentran en un lugar cerrado con llave y conacceso restringido.**
- **Los servidores se encuentran además en un armario o rack que se pueda cerrar con llave.**

- Las terminales de trabajo se protegen con cables de seguridad.
- Los materiales impresos confidenciales se guardan en armarios cerrados con llave

5. En los procedimientos del GADPE, ¿se requiere que terceros procesen la información?

- Sí
- **No**
- No lo sé

6. ¿Los datos del cliente se almacenan o procesan en un ambiente compartido con recursos corporativos?

- Sí
- **No**
- No lo sé

7. ¿Recurre a fabricantes independientes de software para complementar la oferta de servicios de desarrollo?

- **Sí**
- No
- No lo sé

8. ¿El GADPE recibe ingresos por ofrecer servicios de procesamiento o minería de datos?

- Sí
- **No**
- No lo sé

9. Los datos que procesa el GADPE ¿son considerados sensibles o críticos para las operaciones comerciales de sus clientes?

- Sí
- No
- No lo sé

10. ¿Se ofrecen aplicaciones críticas a través de Internet?

- Sí
- **No**
- No lo sé

11. ¿Qué mecanismos tiene el GADPE para asegurar una alta disponibilidad de las aplicaciones?

- Equilibrio de carga
- Clústeres
- Pruebas periódicas de recuperación de aplicaciones y datos
- **Soporte permanente**
- Ninguno

12. ¿Fabricantes de software han desarrollado algunas aplicaciones de la intranet?

- **Sí**
- No
- No lo sé

12.1. ¿Los fabricantes independientes proporcionan periódicamente actualizaciones y parches de software como la documentación sobre los mecanismos de seguridad? (se mantiene soportada)

- **Sí**
- No
- No lo sé

13. ¿El equipo interno de desarrollo ha creado algunas de las aplicaciones clave de la intranet?

- **Sí**
- No
- No lo sé

13.1. ¿El equipo interno de desarrollo proporcionan periódicamente actualizaciones y parches de software como la documentación sobre los mecanismos de seguridad? (se mantiene soportada)

- Sí
- **No**
- No lo sé

14. ¿El GADPE conoce las vulnerabilidades de seguridad que existen para las aplicaciones de la intranet?

- **Sí**
- No
- No lo sé

En caso de responder Sí:

14.1. ¿Cuenta con los procedimientos para abordar dichas vulnerabilidades?

- Sí
- **No**

ANEXO N°4: Modelo de Entrevista sobre el entorno aplicada al responsable de seguridad

1. ¿La actividad del GADPE se desarrollan en un ambiente de estrategia política, en el que el robo de material intelectual o el espionaje son temas de gran preocupación?

- **Sí**
- No

2. ¿Está conectada su red corporativa a otras redes (ya sean de clientes, de socios o de terceros) mediante enlaces de red públicos o privados?

- **Sí, Patronato**
- No
- No lo sé

3. ¿Obtiene el GADPE ingresos por servicios basados en el almacenamiento o la distribución electrónica de datos, como por ejemplo, archivos de medios o documentación?

- Sí
- **No**
- No lo sé

4. En los últimos seis meses, ¿se ha sustituido radicalmente algún componente tecnológico de gran importancia?

- Sí
- **No**

5. Un incidente que afecte a las aplicaciones o a las infraestructuras orientadas a los usuarios, como un apagón o el fallo de una aplicación o hardware, ¿afectaría significativamente las operaciones diarios?

- **Sí**
- No
- No lo sé

6. Los componentes de infraestructura y las aplicaciones del usuario, ¿dependen del acceso a recursos de su entorno?

- **Sí**
- No
- No lo sé

7. ¿Comparte la institución los componentes de infraestructura y aplicaciones entre varios usuarios?

- **Sí**
- No
- No lo sé

8. ¿Cambia muy a menudo el personal técnico en su departamento?

- Sí
- **No**

9. ¿Utiliza versiones obsoletas de software que ya no cuenten con el servicio técnico del fabricante?

- Sí
- **No**
- No lo sé

10. ¿Adquiere el GADPE software de fabricantes o proveedores conocidos y fiables?

- **Sí**
- No
- No lo sé

11. ¿Es la institución la que gestiona el entorno o se contrata los servicios de un tercero?

- La empresa gestiona el entorno
- La empresa subcontrata la gestión

11.1. ¿Tiene la empresa acuerdo de servicios establecidos como parte de los contratos con los proveedores de servicios subcontratados?

- Sí
- **No**

11.2. ¿Se han incluido cláusulas específicas sobre seguridades los acuerdos de servicios (SLA)?

- Sí
- **No**

12. ¿Utiliza la empresa servidores de gestión dedicados a la administración segura de los sistemas y dispositivos del entorno?

- **Sí**
- No
- No lo sé

12.1. Seleccione los sistemas para los que existen servidores de gestión dedicados:

- Dispositivos de red
- **Servidores**

13. ¿Se utilizan cuentas de registro individuales para las actividades normales en contraposición con las actividades administrativas o de gestión?

- Sí
- **No**
- No lo sé

14. ¿Garantiza la empresa a los usuarios el acceso administrativo a sus estaciones de trabajo y equipos portátiles?

- **Sí**
- No
- No lo sé

15. ¿Se comprueba periódicamente el cortafuego para garantizar que funciona según lo previsto?

- Sí
- **No**
- No lo sé

ANEXO N°5: Modelo de Entrevista al administrador de la red

1. ¿Existe un modelo para asignar niveles de importancia a los componentes del entorno informático?

- Sí
- **No**
- No lo sé

2. ¿Existen directivas para la regulación del entorno informático?

- **Sí**
- No
- No lo sé

2.1. ¿Existen directivas de seguridad de información para la regulación de la actividad relacionada con la seguridad del GADPE?

- **Sí**
- No
- No lo sé

2.1.1. Indique quién desarrolló la directiva:

- **Sólo la Dirección de TIC**
- Sólo la Dirección Administrativa
- El departamento de TI y la Dirección Administrativa
- Otro

2.2. ¿Hay una directiva corporativa para el uso aceptable?

- Sí
- **No**
- No lo sé

2.3. ¿Hay directivas para la gestión de las cuentas de usuarios individuales?

- Sí
- **No**
- No lo sé

2.3.1. Seleccione cuáles de las siguientes directivas se aplican a la gestión de las cuentas de usuarios individuales:

- **Cuentas de usuarios individuales (no compartidas)**
- Cuentas sin y con privilegios para administradores
- Hacer cumplir la calidad de las contraseñas

- Cuando un empleado deja su trabajo, se desactivas sus cuentas?

3. ¿Hay un proceso documentado para la creación de servidores? Si la respuesta es afirmativa, ¿de qué tipo? (¿Para qué tipos de host hay un proceso de creación documentado?)

- Dispositivos de infraestructura
- **Servidores**
- Estaciones de trabajo y portátiles
- Ninguno

4. ¿Hay pautas documentadas que indiquen qué protocolos y servicios están permitidos en la red corporativa? Seleccione la opción adecuada:

- Sí
- **No**
- No lo sé

ANEXO N°6: Modelo de Entrevista aplicada al desarrollador sobre la gestión de actualizaciones y revisiones

1. ¿Hay un proceso de gestión para las configuraciones y los cambios?

- **Sí**
- No
- No lo sé

Los procesos de gestión de cambios y configuraciones permiten asegurar que los cambios en el entorno de producción, se han probado y documentado exhaustivamente antes de utilizarse.

1.1. ¿Dispone el GADPE de configuraciones documentadas a modo de referencia?

- **Sí**
- No
- No lo sé

2. ¿Prueba la institución los cambios de configuración antes de aplicarlos a los sistemas de producción?

- **Sí**
- No
- No lo sé

2.1. ¿Se comprueba y se garantiza de forma centralizada la compatibilidad con las configuraciones (por ejemplo, mediante directivas de grupos)?

- Sí
- **No**
- No lo sé

3. ¿Existe un proceso establecido para las directivas de actualización y revisión?

- **Sí**
- No
- No lo sé

3.1. Seleccione los componentes para los que existan estos procesos:

- **Sistemas operativos**
- Aplicaciones
- Tanto los sistemas operativos como las aplicaciones

4. ¿Prueba el GADPE las actualizaciones y revisiones antes de aplicarlas?

- **Sí**
- No
- No lo sé

4.1. Indique cuáles de los siguientes elementos se utilizan para aplicar y gestionar las actualizaciones:

- Actualización automática de Windows
- Sitio Web de Windows Update

- Servicios de actualización de Windows Server
- **Otras soluciones de gestión de actualizaciones**

4.2. ¿En qué tipos de hosts se utiliza la gestión automática de actualizaciones?
- Estaciones de trabajo
- **Servidores**

5. ¿Existe una directiva establecida por la que se regule la actualización de productos de detección basados en firmas?
- Antivirus
- Sistema de detección de intrusiones (IDS)
- **Ninguno**

Análisis:
La aparición de nuevos virus es constante, por lo que resulta imprescindible mantener una lista actualizada de firmas de virus. Su solución antivirus será tan eficaz como lo permita su lista de firmas de virus.

6. ¿Hay diagramas lógicos y documentación de configuración precisa para la infraestructura de red y los hosts?
- Sí
- **No ó han caducado**
- No lo sé

7. ¿Existen diagramas exactos de la arquitectura y del flujo de datos de las aplicaciones principales?
- **Sí**
- No
- No lo sé

7.1. Seleccione los tipos de aplicaciones de las que existen diagramas
- Sólo aplicaciones externas
- **Sólo aplicaciones internas**
- Tanto las aplicaciones internas como externas

ANEXO N°7: Modelo de Entrevista al encargado de los servidores sobre copias de seguridad y recuperación

1. ¿Está activado en el entorno el registro de los eventos producidos en los hosts y los dispositivos?

- Sí
- No
- No lo sé

2. ¿Toma medidas la institución para proteger la información incluida en los registros?

- El sistema operativo y las aplicaciones están configuradas para no sobrescribir eventos.
- Los archivos de registro se rotan con frecuencia para asegurarse de que hay suficiente espacio disponible.
- El acceso a los archivos de registro está restringido a las cuentas de tipo administrador.
- **Los registros se almacenan en un servidor central de registros**
- Ninguno

3. ¿Revisa el GADPE periódicamente los archivos de registro?

- **Sí**
- No
- No lo sé

3.1. ¿Con qué frecuencia se revisan los registros?

- Diariamente
- Semanalmente
- Mensualmente
- **Según sea necesario**
- No lo sé

4. ¿Se hacen copias de seguridad de todos los recursos críticos y confidenciales periódicamente?

- **Sí**
- No
- No lo sé

4.1. ¿Existen directivas y procedimientos para el almacenamiento y la gestión de los dispositivos de copias de seguridad?

- **Sí**
- No
- No lo sé

4.1.1. ¿Cuáles de las directivas y procedimientos siguientes se cumplen?

- Almacenamiento fuera de las instalaciones
- Almacenamiento en armarios cerrados, a prueba de fuego
- **Acceso limitado a dispositivos de copias de seguridad**
- Rotación y duración de los dispositivos de copias de seguridad

5. ¿Existen directivas para la comprobación periódica de los procedimientos de copias de seguridad y restauración? Estas directivas, ¿están documentadas?

- Sí, y están documentados
- **Sí, pero no están documentados**
- No
- No lo sé

ANEXO N°8: Ficha de Observación

Lugar: **Fecha:**
Responsable: **Hora:**

Aspectos a observar:

- hardware: Las computadoras y de sus periféricos; Software. Programas y aplicaciones; Información almacenada.
- Software instalado dentro de sus equipos de cómputo
- Información esencial en cada servidor o equipo que debe ser respaldada para garantizar la continuidad las operaciones.
- Stock para una sustitución
- Políticas y planes de seguridad
- Base reglamentaria: normas de control interno
- Seguridad Física y ambiental
- Uso y asignación de recursos de TI de la institución.
- Respaldo y almacenaje de Información.
- Copias de seguridad y su almacenaje.
- Normas para el acceso y uso de servicios: Correo electrónico, internet, sistemas, intranet, accesos remoto y sitio web.
- Mantenimiento Preventivo, adquisición, modernización y baja técnica de equipos.
- Inventario de las direcciones IP públicas que posee la empresa
- Políticas de navegación aplicadas a nivel de Firewall de Software
- Utilizar de herramientas de monitoreo de red y detección de vulnerabilidades.
- Productos antivirus
- Bitácoras de Video.
- Temperatura ambiente del área de servidores.
- Ubicación, distribución de los Rack y propósito del rack.
- Sistemas detección de incendios y protección contra intrusos.
- Climatización del local de servidores.
- Rack independiente para equipos activos y pasivos de Voz, Datos, Video.

Descripción / observación / detalle:

_____

ANEXO N°9: Datacenter

ANEXO N°10: Servidores Blade

ANEXO N°11: Sistema contraincendios

ANEXO N°12: Unidades de Energía Ininterrumpida

ANEXO N°13: Sistemas de monitoreo

ANEXO N°14 a: Matriz de gestión del riesgo informático - DATOS

ANEXO N°14 b: Matriz de gestión del riesgo informáticoSISTEMAS

ANEXO N°14 c: Matriz de gestión del riesgo informático PERSONAL

ANEXO N°15: Curvas de representación del riesgo informático en el GADPE