VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TEMA "PROPUESTA METODOLÓGICA DE GESTIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN (TIC) PARA ENTIDADES PÚBLICAS CONFORME NORMATIVA NTE INEN ISO/IEC 27005"

AUTOR: PATIÑO ROSADO, SUSANA GABRIELA

DIRECTOR: ING. SOLÍS ACOSTA, EDGAR FERNANDO MGT.

SANGOLQUÍ

2018

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "***PROPUESTA METODOLÓGICA DE GESTIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN (TIC) PARA ENTIDADES PÚBLICAS CONFORME NORMATIVA NTE INEN ISO/IEC 27005***" fue realizado por la señora ***Patiño Rosado, Susana Gabriela*** el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 1 de noviembre de 2017

Firma:

.....

Ing. Fernando Solís Mgt.

C.C.: 1803005071

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORÍA DE RESPONSABILIDAD

Yo, ***Patiño Rosado, Susana Gabriela***, con cédula de ciudadanía n°0802119016, declaro que el contenido, ideas y criterios del trabajo de titulación: ***"PROPUESTA METODOLÓGICA DE GESTIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN (TIC) PARA ENTIDADES PÚBLICAS CONFORME NORMATIVA NTE INEN ISO/IEC 27005"*** es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 1 de noviembre de 2017

Firma

.....

Susana Gabriela Patiño Rosado

C.C.: 0802119016

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN

Yo, **Patiño Rosado, Susana Gabriela**, con C. C. nº0802119016 autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"PROPUESTA METODOLÓGICA DE GESTIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN (TIC) PARA ENTIDADES PÚBLICAS CONFORME NORMATIVA NTE INEN ISO/IEC 27005"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 1 de noviembre de 2017

Firma

.....

Susana Gabriela Patiño Rosado

C.C.: 0802119016

DEDICATORIA

A Daniel, Didier y Danna,
porque son la fuente de mi fuerza.

Sue.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

En el Ecuador, la Secretaría Nacional de Administración Pública determinó la implementación de la norma ISO/IEC 27001:2005, en respuesta a los continuos ataques y delitos informáticos presentados. Sin embargo, la normativa solo establece directrices para la gestión de riesgo en la seguridad de la información, mas no una guía paso a paso de cómo llevar a cabo un análisis y evaluación de riesgo. Debido a lo anterior, se establece en el presente trabajo elaborar una guía metodológica práctica para la gestión de riesgo de TIC en entidades del sector público conforme normativa NTE INEN ISO/IEC 27005 para mejorar la administración de la seguridad de la información. Para lograr el objetivo fue necesario conocer la normativa ISO/IEC 27005 y determinar el nivel con el cual se administran los riesgos tecnológicos en entidades públicas, por lo cual se realizó un estudio cuali-cuantitativo de alcance descriptivo y se consideró un muestreo no probabilístico. Se aplicó la técnica encuesta, a través de un cuestionario a 18 jefes de área de tecnología de las entidades públicas ubicadas en la ciudad de Esmeraldas. Obteniendo principalmente que, a pesar de la incorporación de la normativa internacional es todavía complejo el proceso debido a que los estándares fueron creados para empresas desarrolladas en otro contexto. En respuesta, se propone la guía detallada en la cual se desarrolla cada etapa con su conjunto de actividades, y su aplicación en una entidad del sector público con la finalidad de validar cada una de las etapas previamente definidas.

Palabras claves:

- **GESTIÓN DE RIESGO TECNOLÓGICO**
- **CULTURA DE ADMINISTRACIÓN DE RIESGOS TECNOLÓGICOS**
- **SEGURIDAD DE LA INFORMACIÓN.**

ABSTRACT

In Ecuador, through the National Secretariat of Public Administration, the implementation of ISO / IEC 27001: 2005 was determined in response to the continuous attacks and computer crimes presented. However, the regulation only establishes guidelines for risk management in information security, but not a step-by-step guide on how to carry out risk analysis and evaluation. Due to the above, it is established in the present work to elaborate a practical guide for the management of ICT risk in entities of the public sector according to NTE INEN ISO / IEC 27005 regulation to improve the administration of information security. In order to achieve the objective, it was first necessary to know the ISO / IEC 27005 standard and then to determine the level at which the technological risks are managed in public sector entities, for which a qualitative and quantitative study was carried out, and a non-probabilistic sampling. The survey technique was applied, through a questionnaire to 18 heads of technology area of the public entities located in the city of Esmeraldas. Obtaining mainly that, despite the incorporation of international regulations, the process is still complex because the standards were created for companies developed in another context. In response, the detailed guide is proposed in which each stage is developed with its set of activities, and its application in a public sector entity in order to validate each of the previously defined stages.

Keywords:

- **TECHNOLOGICAL RISK MANAGEMENT**
- **CULTURE OF TECHNOLOGY RISK MANAGEMENT**
- **SECURITY OF THE INFORMATION**

CAPÍTULO I: INTRODUCCIÓN

1.1 Antecedente

Actualmente las empresas orientadas al servicio público adoptan normativas internacionales para mejorar la administración de sus procesos estratégicos y por consiguiente los servicios que brindan a sus usuarios. Uno de los estándares de mayor aceptación es la familia de normas ISO/IEC 27000.

Debido a que es una serie de estándares relacionados con los Sistemas de Gestión de Seguridad de la Información, siendo adaptada en varios países para su implementación obligatoria en las diferentes entidades del sector público.

En América del sur, Colombia se ha sumado al resguardo de la información, mediante resolución Nº 1332 firmada el 4 de septiembre de 2014 por la Dirección General del Consejo Profesional Nacional de Ingeniería (COPNIA) de la República de Colombia, acuerda la adopción de la norma NTC- ISO 27001, acorde a la infraestructura y recursos del COPNIA. (Consejo Profesional Nacional de Ingeniería de la República de Colombia, 2014)

De acuerdo con Resolución Ministerial Nº004-2016PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática del Perú. (Presidencia del Consejo de Ministros de la República del Perú, 2016)

En el año 2011 el Instituto Ecuatoriano de Normalización, realiza una traducción idéntica de la Norma Internacional ISO/IEC 27001:2005, la cual se adopta para el Ecuador como NTE INEN –ISO/IEC 27001:2011 para uso obligatorio en la entidades de la Administración Pública Central y las que dependan de la Función Ejecutiva según Acuerdo Nº166,proporcionando un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información. (Instituto Ecuatoriano de Normalización, 2012)

La Secretaría Nacional de la Administración Pública (SNAP) del Ecuador es “una entidad de derecho público dotada de autonomía presupuestaria, financiera, económica y administrativa, encargada de establecer las políticas, metodologías de gestión e innovación institucional y herramientas necesarias para el mejoramiento de la eficiencia y calidad de la gestión en las entidades y organismos de la Función Ejecutiva”. (Secretaria Nacional de Administración Pública, 2011)

La SNAP creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información (CSITIC) y dentro de sus atribuciones tiene la de establecer lineamientos de seguridad informática, así como la protección de la infraestructura computacional. (Secretaria Nacional de Administración Pública, 2011)

La CSITIC en su informe final, describe las amenazas más frecuentes que las entidades gubernamentales han experimentado en los últimos años, destacando que los sistemas informáticos o portales web no cumplen con estándares para la seguridad informática o no se les otorga la importancia del caso a los mismos. Asimismo, los delitos por mal uso de contraseñas de parte de ciertos funcionarios han provocado estafas y desfalco de dinero público, evidenciando la falta de controles en algunos sistemas gubernamentales (Comisión para la Seguridad Informática y de las Tecnologías de la Información, 2011)

En respuesta, la CSITIC planteó la adopción y adaptación de un estándar internacional para salvaguardar la información en las organizaciones gubernamentales, por lo cual la SNAP mediante Acuerdo ministerial Nº166 determinó la implementación de un Sistema de Gestión de Seguridad de Información (SGSI) basado en la de la Norma ISO/IEC 27001:2005, para uso obligatorio en las entidades de la Administración Pública Central y las que dependan de la Función Ejecutiva. (Secretaria Nacional de Administración Pública, 2011)

Por otra parte, el artículo 7 del mismo acuerdo determina que: “Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/IEC 27005 Gestión del Riesgo en la Seguridad de la Información.” (Secretaria Nacional de Administración Pública, 2011)

Además, Gómez (2013) determina al proceso de análisis de riesgos como “una etapa de evaluación previa de los riesgos del sistema informático, que se debe realizar con rigor y objetividad para que cumpla su función con garantías” (p.59). Es decir, las entidades públicas están obligadas a realizar un proceso de administración de riesgo, el cual es un análisis profundo de los incidentes que puedan afectar negativamente la continuidad de las actividades de la organización.

Por otra parte, la Contraloría General del Estado Ecuatoriano, ente regulatorio de las normas de control interno, en el apartado *Tecnologías de la Información en la sección 410* de las “Normas de Control Interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos”, determina en varios artículos la necesidad de implementar el proceso de gestión de riesgo que permita identificar las vulnerabilidades y amenazas. (Contraloría General del Estado Ecuatoriano, 2009)

En particular en el apartado *410-10 Seguridad de tecnología de información*, recomienda el establecimiento de mecanismos que protejan y salvaguarden contra las pérdidas y fugas de los medios físicos y la información que se procesa mediante sistemas informáticos. Igualmente, indica que se debe implementar acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados. (Contraloría General del Estado Ecuatoriano, 2009)

1.2 Justificación e Importancia

La justificación principal del proyecto es el aporte a las entidades públicas a través de un mejor entendimiento de la norma ISO 27001 e ISO 27005, la cual es de obligatoriedad en el Ecuador y en algunos países de Latinoamérica y Europa, considerando la inexistencia de una guía que se alinea a los directrices de la normativa internacional bajo el contexto de las entidades públicas del Ecuador.

Asimismo, al ser implementada la presente guía permitirá optimizar la administración del riesgo tecnológico de acuerdo con los criterios de información de los activos: disponibilidad, integridad y confidencialidad, los cuales soportan los servicios tecnológicos.

Por otra parte, se crearía la cultura de administración de los riesgos en el personal del departamento de tecnología de las entidades públicas, proporcionando mayor conocimiento de las posibles amenazas y una conciencia de las consecuencias que podrían producirse al no ser tratadas.

Además, aportará a mejorar el control interno en los servicios tecnológicos produciendo mayor eficiencia en las actividades realizadas por los servidores públicos induciendo en la ciudadanía mayor confianza en los servicios recibidos.

1.3 Planteamiento del problema

Con el continuo surgimiento de nuevas tecnologías aparecen nuevas amenazas que atentan contra la seguridad de los servicios tecnológicos, provocando la interrupción de las actividades normales en las organizaciones.

De igual manera, el personal responsable de la administración de los sistemas de información no tiene la predisposición o en ciertos casos la preparación para realizar un análisis profundo de las vulnerabilidades existentes lo que convierte a la entidad pública en un blanco fácil para el desarrollo de delitos informáticos por mal uso de los recursos tecnológicos, así como por falta de controles eficientes.

Asimismo, la identificación de riesgos tecnológicos no es un proceso rápido y mucho menos barato, debido a que demanda la contratación de personal experto que guíe y cree una cultura de seguridad de la información en el personal de la empresa.

Por otra parte, es necesario aplicar un método sistemático de gestión de riesgo que oriente en la identificación de vulnerabilidades para posteriormente establecer correctamente los mecanismos que salvaguarden la información. Sin embargo, la norma ISO/IEC 27005 solo provee directrices para la gestión de riesgo en la seguridad de la información en una organización, mas no una guía paso a paso de cómo llevar a cabo un análisis y evaluación de riesgo.

Debido a la necesidad de mitigar las nuevas amenazas es necesario el diseño de una guía metodológica para la gestión de riesgo en el área de tecnología de información de entidades públicas, que facilite la identificación de las vulnerabilidades a través de un conjunto de etapas específicas, cumpliendo con las directrices propuestas por NTE INEN-ISO/IEC 27005.

1.4 Formulación del problema

Problema general

¿La elaboración de una guía metodológica para la gestión de riesgo de TIC mejorará la administración de la seguridad de la información en entidades del sector público?

Problemas específicos

- ¿Cuál es la normativa ecuatoriana aplicada en la seguridad de la información en entidades del sector público en Ecuador?
- ¿Cuál es el grado de administración de los riesgos de TIC en entidades del sector público?
- ¿Existe una guía metodológica diseñada para la ejecución de Análisis de Riesgo de TIC en entidades del sector público?

1.5 Hipótesis

La elaboración de una guía metodológica para la gestión de riesgo de TIC mejorará la administración de la seguridad de la información en entidades del sector público.

1.6 Objetivo general

Elaborar una guía metodológica para la gestión de riesgo de TIC en entidades del sector público conforme normativa NTE INEN ISO/IEC 27005 para mejorar la administración de la seguridad de la información.

1.7 Objetivos específicos

- Investigar las normas INEC ISO/IEC 27001:2013 e INEC ISO/IEC 27005:2008

- Determinar el grado con el cual se administran los riesgos tecnológicos en entidades del sector público; mediante la aplicación de una encuesta al responsable del área de tecnología.

- Aplicar la guía metodológica de gestión de riesgos de TIC basada en la normativa ISO 27005 en una entidad del sector público.

CAPÍTULO II: MARCO TEÓRICO

2

2.1 Marco teórico relacionado con la Gestión de Riesgo de TIC

De acuerdo con Álvaro Gómez en su libro *Enciclopedia de la Seguridad Informática* comprende al Análisis y Gestión de riesgo en un sistema informático como una etapa de evaluación previa de los riesgos el cual definirá un plan para la implantación de salvaguardias, que permita disminuir la probabilidad de que se materialice una amenaza y por consiguiente el impacto en la organización (Gómez Vieites, 2013).

Asimismo, la evaluación de riesgo es la identificación de los riesgos, la cual permite cuantificar su probabilidad e impacto, analizando medidas que logren disminuir la ocurrencia de los hechos o mitiguen su impacto (Piattini Velthuis & del Peso Navarro, 2000).

Además, un punto importante a considerar son los recursos que posee la organización para comprometerse de manera adecuada a un proceso de gestión del riesgo y otro es el motivo por el cual la organización decide implementar una metodología. Según el contexto, puede ser por un gran número de incidentes relacionados con la seguridad de la información, para la preparación de un plan de continuidad de las actividades, por aspectos legales o requisito para la creación de un Sistema de Gestión de Seguridad de Información (Carpentier, 2016).

2.2 Antecedentes del estado del arte

Existen diferentes trabajos de investigación que abordan desde diferentes perspectivas la seguridad de la información, asimismo la gestión de riesgo y la salvaguarda de los activos basado en la familia ISO 27000. Los más importantes se mencionan a continuación:

En la investigación Calidad de la gestión en la seguridad de la información basada en la norma ISO/IEC 27001, en instituciones públicas, en la ciudad de QUITO D.M, desarrollado por Luis Pazmiño, mide el nivel de calidad de gestión en la seguridad de la información, para ello desarrolló una metodología de evaluación basada en la norma NTE INEN-ISO/IEC 27001:2011.

Luis Pazmiño previamente ha realizado un análisis de los fundamentos teóricos, alcances y objetivos de las normas NTE INEN-ISO/IEC 27001:2011 para determinar la normativa ecuatoriana para gestionar la seguridad de la información.

Existen varias investigaciones que proponen el proceso Gestión de Riesgos, entre las cuales destaca el artículo científico presentado por Alexandra Ramírez Castro, Zulima Ortiz Bayona denominado *Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios*, presenta una metodología para gestionar riesgos tecnológicos cuya base son los estándares ISO 31000 e ISO/IEC 27005. Además, incluye recomendaciones y buenas prácticas de otros estándares y guías internacionales para manejo de riesgos, seguridad y gestión de servicios. (Ramírez & Ortiz, 2010).

Asimismo, en el artículo *Evaluación de Seguridad de la Información basada en ISO/IEC 27000* de Vallejo, Vivanco, Velásquez y Castro. Tiene como objetivo evaluar la seguridad de la información del proceso de admisión de estudiantes de pregrado en la Universidad Tecnológica Equinoccial basado en la norma internacional ISO/IEC 27000 para determinar el nivel de seguridad y posteriormente elaborar un plan de tratamiento de riesgos. El desarrollo del trabajo establece los pasos a seguir y las actividades a realizar en cada etapa del proceso hasta obtener los resultados finales sobre la brecha de seguridad y así posteriormente el plan de tratamiento que mitiguen los riesgos priorizados acorde a los criterios de aceptación definidos por el Rector de la UTE (Ricardo, Edwin, Nancy, & Fidel, 2014).

Por lo tanto, se evidencia la inexistencia de una guía metodológica para la gestión de riesgo de TIC en el sector público, como se propone en la presente investigación.

2.3 Marco conceptual

2.3.1 Activo

Es “cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste” (Instituto Nacional de Cibeseguridad de España, 2017).

Además, el activo dependerá de la empresa y del o los riesgos que pueden estar asociados al mismo. En las nuevas normas se denomina “fuente de riesgo” debido a que puede originar uno o varios riesgos en la empresa.

2.3.2 Amenaza

Es la “circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor” (Instituto Nacional de Cibeseguridad de España, 2017).

En las nuevas normas se denomina “suceso”.

2.3.3 Vulnerabilidad

Es la “debilidad que presentan los activos y que facilita la materialización de las amenazas” (Instituto Nacional de Cibeseguridad de España, 2017).

Además, al materializarse puede provocar un impacto, es decir un servicio podría verse comprometido por la explotación de sus vulnerabilidades. Es necesario asegurarse de tener una comprensión real de los sistemas vulnerables.

2.3.4 Impacto

“Impacto o consecuencia de la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad” (Instituto Nacional de Cibeseguridad de España, 2017).

El impacto describe las consecuencias de un riesgo detectado. Para permitir la evaluación de riesgos y el establecimiento de prioridades, el impacto debe especificar el efecto negativo que la realización de un riesgo implicaría. Es decir, pérdidas esperadas u objetivos de negocio no alcanzados como resultado del impacto

En las nuevas normas es el resultado de un suceso que afecta a los objetivos.

2.3.5 Probabilidad

"La posibilidad de ocurrencia de un hecho, suceso o acontecimiento. La frecuencia de ocurrencia implícita se corresponde con la amenaza" (Instituto Nacional de Cibeseguridad de España, 2017).

2.3.6 Riesgo

"Es el potencial que tiene una determinada amenaza para explotar las vulnerabilidades de un activo o grupo de activos y por consiguiente causar daño a la organización" (ISO/IEC 27005:2008,2008).

El nivel de riesgo es una estimación de lo que puede ocurrir y se valora de forma cuantitativa y cualitativa. De forma cuantitativa como el producto del impacto (consecuencia), asociado a una amenaza (suceso) por la probabilidad de la misma.

2.3.7 Gestión de Riesgo

"Las actividades cuyo objetivo es mantener el riesgo por debajo del umbral fijado se engloban" (Instituto Nacional de Cibeseguridad de España, 2017).

Dos etapas principales son: Análisis de Riesgo y Tratamiento de Riesgos.

2.3.8 Análisis de Riesgo

"Que consiste en averiguar el nivel de riesgo que la empresa está soportando. Para ello, tradicionalmente las metodologías proponen que se realice un inventario de activos, se determinan las amenazas, las probabilidades de que ocurran y los posibles impactos" (Instituto Nacional de Cibeseguridad de España, 2017).

2.3.9 Tratamiento de Riesgo

"Para aquellos riesgos cuyo nivel está por encima del umbral deseado la empresa debe decidir cuál es el mejor tratamiento que permitan disminuirlos" (Instituto Nacional de Cibeseguridad de España, 2017).

Asimismo, se determinan los riesgos que serán disminuidos considerando que el coste de tratamiento no sea mayor al costo de riesgo disminuido.

Un riesgo puede ser tratado de diferentes formas:

Evitar o eliminar el riesgo. El activo es reemplazado por otro que no se ve afectado por la amenaza.

Reducirlo o mitigarlo Tomando las medidas oportunas para que el nivel de riesgo se sitúe por debajo del umbral. Se puede reducir la probabilidad implementando medidas preventivas o el impacto estableciendo controles para las amenazas.

Transferirlo, compartirlo o asignarlo a terceros. En ocasiones la empresa no tiene la capacidad de tratamiento y precisa la contratación de un tercero con capacidad para reducir y gestionar el riesgo dejándolo por debajo del umbral.

Aceptarlo. Se asume el riesgo, bien porque está debajo del umbral aceptable de riesgo bien en situaciones en las que los costes de su tratamiento son elevados y aun siendo riesgos de impacto alto su probabilidad de ocurrencia es baja o porque aun a pesar del riesgo la empresa no quiere dejar de aprovechar la oportunidad que para su negocio supone esa actividad arriesgada (Instituto Nacional de Cibeseguridad de España, 2017).

2.3.10 Etapas del Proceso Gestión de Riesgo

De acuerdo con Instituto Nacional de Ciberseguridad de España (2015) son las siguientes:

Comunicación. Durante todo el proceso es necesario la comunicación entre el personal involucrado de la empresa, principalmente la dirección.

Estableciendo el contexto de seguridad de la información. Se determina criterios como determinar si el enfoque es global o detallado.

Valorando los riesgos de la seguridad de la información. Se realiza la identificación de los activos de información. Luego se estiman los riesgos permitiendo medir las consecuencias o impacto bajo los criterios de confidencialidad, integridad y disponibilidad de los activos. Finalmente se valora las consecuencias o impactos y la probabilidad de los incidentes para los activos del ámbito elegido, se ha de realizar el producto de ambos para calcular los riesgos. Los resultados obtenidos se compararon con los criterios de aceptación de riesgo**.**

Tratando y aceptando riesgos de seguridad de la información. En esta fase se seleccionarán la opción de tratamiento adecuada (evitar, reducir o mitigar, transferir o aceptar) para cada uno de los riesgos de la lista.

Monitorizando los riesgos de seguridad de la información. Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios. Los riesgos no son estáticos y pueden cambiar de forma radical sin previo aviso.

CAPÍTULO III: NORMATIVA ECUATORIANA DE GESTIÓN DE RIESGO DE SI.

3

3.1 Esquema Gubernamental de Seguridad de Información

La Secretaria Nacional de Administración Pública considera las TIC como herramientas imprescindibles para el desempeño de la organización, por lo cual creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación.

La comisión realizó un análisis de la situación respecto de la gestión de la Seguridad de la Información en las Instituciones de la Administración Pública Central, Dependiente e Institucional, determinando la necesidad de implementar y aplicar normas para la seguridad de la información. Debido a ello, se crea el documento Esquema Gubernamental de Seguridad de Información (EGSI) basado en la norma INEN ISO/IEC 27002.

El EGSI establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información e inicia un proceso de mejora continua, considerando que el EGSI no reemplaza la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices.

3.1.1 Política de seguridad de la información

La política de seguridad tiene como objetivo proporcionar dirección y apoyo gerencial para brindar seguridad de la información a través de toda la organización, mediante una comunicación según corresponda.

De acuerdo con el EGSI, la política de seguridad de la información tiene como referencia:

“Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema

Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera" (Secretaria Nacional de Administración Pública, 2013).

3.1.2 Organización de la seguridad de la información

Se debe administrar la seguridad para administrar y controlar la implementación de un Sistema de Información en la organización y mantener la seguridad en el acceso a terceros.

3.1.3 Gestión de los activos

Se debe mantener adecuada protección de los activos de la organización, designar propietarios, clasificar la información para asegurar un adecuado nivel de protección.

3.1.4 Seguridad de los recursos humanos

Reducir los riesgos de error humano, robo, fraude o uso inadecuado de instalaciones. Las responsabilidades en materia deben ser: explicadas en la etapa de reclutamiento, incluida en los contratos y monitoreadas durante el desempeño como empleado.

Los empleados deben firmar habitualmente un acuerdo de confidencialidad como parte de sus términos y condiciones iniciales de empleo.

El personal ocasional y los usuarios externos aun no contemplados en un contrato formalizado (que contenga el acuerdo de confidencialidad) deberán firmar el acuerdo mencionado antes de otorgarles acceso a las instalaciones de procesamiento de información.

Los acuerdos de confidencialidad deben ser revisados cuando se identifican cambios en los términos y condiciones del empleo o contrato.

Además, se debe garantizar que los usuarios están al corriente de las amenazas con respecto a la seguridad de la información, y están capacitados para respaldar la política de seguridad de la organización en el transcurso de sus actividades normales.

Algunas consideraciones para tener en cuenta en el proceso de concienciación:

- Involucrar a todo el personal de la organización.
- Auspiciado por la alta gerencia.
- Asegurar su permanencia a largo plazo.
- Definir medidas en caso de que algún miembro del personal deje la organización.

3.1.5 Seguridad física y del entorno

Prevenir accesos físicos no autorizados, información crítica o sensible en áreas seguras. El equipamiento debe estar protegido de amenazas físicas y de medio ambiente. Se debe proteger principalmente las sedes, instalaciones y documentos impresos.

3.1.6 Gestión de comunicaciones y operaciones

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de operación. Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todas las instalaciones de procesamiento de información. Además, se debe implementar la separación de funciones cuando corresponda.

3.1.7 Control de acceso

Las reglas y derechos del control de accesos, para cada usuario o grupo de usuarios, deben ser claramente establecidos en una declaración de política de accesos:

- Requerimientos de seguridad de cada una de las aplicaciones comerciales.
- Identificación de toda información relacionada con las aplicaciones comerciales.
- Políticas de divulgación y autorización de información.

- Coherencia entre las políticas de control de acceso y la clasificación de información de los diferentes sistemas y redes.
- Legislación aplicable y obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
- Perfil de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
- Administración de derechos de acceso.

3.1.8 Adquisición, desarrollo y mantenimiento de sistemas de información

Verificar que la seguridad es incorporada a los sistemas de información. Los requerimientos de seguridad deben ser identificados y aprobados antes del desarrollo de los sistemas de información.

Se debe considerar los controles automáticos a incorporar al sistema y la necesidad de controles manuales de apoyo. Los controles introducidos en la etapa de diseño son significativamente baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

3.1.9 Gestión de los incidentes de la seguridad de la información

Minimizar el daño producido por incidentes y anomalías en materia de seguridad, monitorear dichos incidentes y aprender de los mismos. Los incidentes que afectan la seguridad deben ser comunicados mediante canales gerenciales. Se debe concienciar a todos los empleados y contratistas acerca de los procedimientos de comunicación de los diferentes tipos de incidentes. La organización debe establecer un proceso disciplinario formal para ocuparse de los empleados que perpetren violaciones de la seguridad. Además, se debe establecer un procedimiento formal de comunicación y los incidentes presentados deben ser utilizados en la capacitación con el objetivo de crear conciencia de seguridad en el usuario.

3.1.10 Gestión de la continuidad del negocio

Contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los negocios de los efectos de fallas significativas o desastres. Tiene como principales etapas:

- Clasificación de los distintos escenarios de desastres.
- Evaluación de impacto en el negocio.
- Desarrollo de una estrategia de recupero.
- Implementación de la estrategia.
- Documentación del plan de recupero.
- Testeo y mantenimiento del plan.

3.1.11 Cumplimiento

Se debe realizar el cumplimiento de requisitos legales para impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

El diseño, operación, uso y administración de los sistemas de información pueden estar sujetos a requisitos de seguridad legal, normativa y contractual.

Se debe procurar asesoramiento sobre requisitos legales específicos por parte de los asesores jurídicos de la organización, o de abogados convenientemente calificados. Se deben definir y documentar claramente todos los requisitos legales, normativos y contractuales pertinentes para cada sistema de información.

También se debe garantizar la compatibilidad de los sistemas con las políticas y estándares de seguridad de la organización.

3.2 Norma INEC ISO/IEC 27001:2017

El Servicio Ecuatoriano de Normalización (INEN) adopta la norma internacional ISO/IEC 27001 versión 2017. Es una norma que proporciona los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información. El sistema de gestión de la seguridad de la información se basa en salvaguardar la integridad, disponibilidad y confiabilidad de la información en una organización (INEN ISO/IEC 27001, 2017).

3.2.1 Acciones para abordar los riesgos y las oportunidades

Para planificar un sistema de gestión de la seguridad, las empresas deben considerar: los asuntos externos e internos importantes que afecten la capacidad de lograr los objetivos de la seguridad de la información y se debe comprender las necesidades y expectativas de las partes interesadas los cuales puede incluir requerimientos legales (INEN ISO/IEC 27001, 2017).

Además, al determinar los riesgos deben ser cubiertos para:

- Asegurar el sistema de gestión de seguridad de la información pueda alcanzar los resultados esperados.
- Evitar o disminuir efectos no deseados.
- Lograr una mejora continua.

La organización debe definir y aplicar un proceso de evaluación de riesgo de la seguridad de la información, que permita:

- Establecer y mantener los criterios de riesgo de la seguridad de la información tales como: los criterios de aceptación del riesgo y los criterios para realizar las evaluaciones de riesgo de la seguridad de la información.

- Asegurar los resultados consistentes, válidos y comparables que producen las evaluaciones de riesgo una y otra vez.

- Identificar los riesgos asociados a la perdida de la confidencialidad, integridad y disponibilidad para la información dentro del alcance del sistema de gestión de la seguridad de la información, así como los propietarios del riesgo.

- Analizar los riesgos a través de la evaluación de las posibles consecuencias que podrían resultar si los riesgos identificados se hicieran realidad, también la probabilidad realista de la ocurrencia y determinar el nivel del riesgo.

- Evaluar los riesgos, comparando los resultados del análisis de riesgo con los criterios de riesgos definidos y priorizar los riesgos analizados para el tratamiento de riesgo.

Además, la organización debe conservar la información documentada acerca del proceso de evaluación de riesgo de la seguridad de la información (INEN ISO/IEC 27001, 2017).

La organización además debe definir un proceso de tratamiento de riesgo para: (INEN ISO/IEC 27001, 2017)

- Seleccionar las opciones apropiadas de tratamiento de riesgo considerando los resultados de la evaluación de riesgo.

- Determinar los controles necesarios para implementar las opciones de tratamiento de riesgo. Las organizaciones pueden diseñar controles, según sea necesario o identificarlos de cualquier fuente.

- Comparar los controles definidos con los propuestos por la ISO 27002 y verificar que ningún control necesario fue omitido.

- Generar una Declaración de Aplicabilidad que contenga los controles necesarios y la justificación de inclusión y exclusión de los controles propuestos por la norma.

- Formular un plan de tratamiento del riesgo de seguridad de la información.
- Obtener la aprobación del propietario del riesgo del plan de tratamiento del riesgo de la seguridad de la información.

3.2.2 Objetivos de seguridad de la información

La organización debe establecer los objetivos de seguridad de la información cumpliendo que sean consistente con la política de seguridad de la información, si es posible puedan ser medidos, comunicados y actualizados (INEN ISO/IEC 27001, 2017).

3.2.3 Apoyo

La organización debe proporcionar los recursos necesarios para el establecimiento, implementación y mejora del sistema de gestión de seguridad de información (INEN ISO/IEC 27001, 2017).

Un recurso principal es el humano, por lo cual la norma nos sugiere determinar las competencias necesarias de los empleados que afectaría el desempeño en la seguridad de la información. Para lograrlo es necesario una preparación profesional adecuada, pero si no se las tiene será necesario adquirirlas a través de la capacitación y evaluar posteriormente la efectividad de las acciones tomadas. Asimismo, es primordial guardar información adecuada como evidencia de competencia.

Es primordial conocer la política de seguridad de la información, la contribución a la eficacia del sistema de gestión de seguridad de información y las implicaciones de no cumplir con los requisitos propuestos en el sistema antes mencionado.

Otro punto de apoyo es la comunicación tanto interna como externa, que incluya: que comunicar, cuando, con quien, quien debe comunicarlo y los procesos que serán afectados por la comunicación.

Asimismo, debe almacenarse la información necesaria para la norma y definido por la organización para la eficiencia del sistema de gestión de seguridad de información.

Por otra parte, la magnitud de la información documentada puede variar debido al tamaño de la organización y su tipo de actividades, procesos, productos y servicios, así como la complejidad de sus procesos y la competencia de las personas.

3.2.4 Operación

La organización debe realizar evaluaciones de riesgo de la seguridad de la información, en intervalos planificados o cuando se propongan u ocurran cambios significativos considerando los criterios establecidos en la política de seguridad de información. Además, la organización debe almacenar la información documentada de las evaluaciones de riesgo, así del tratamiento del mismo. (INEN ISO/IEC 27001, 2017)

3.3 Norma ISO/IEC 27005:2011

Esta norma provee las directrices para la gestión del riesgo en la seguridad de la información. Además, brinda soporte a los conceptos generales que se especifican en la norma ISO/IEC 27001 y en ISO/IEC 27002 para la total comprensión de la norma. Se puede aplicar a todo tipo de organizaciones que pretenden gestionar los riesgos que podrían comprender la seguridad de la información de la organización (ISO/IEC 27005, 2011).

Asimismo, el proceso de gestión del riesgo se puede aplicar a la organización en su totalidad, a una parte separada de la organización a cualquier sistema de información, existente o planificado, o aspectos particulares del control (ISO/IEC 27005, 2011).

3.3.1 Visión general de la gestión de la evaluación del riesgo

Todas las actividades para la gestión del riesgo en la seguridad en la información se presentan en la figura 1 se ilustra cómo el proceso puede ser iterativo para las actividades de valoración de riesgo y/o tratamiento de riesgo. El contexto es valorado primero, luego se realiza la valoración de los riesgos, si se suministra información suficiente para determinar las acciones

que se necesitan para modificar los riesgos hasta un nivel aceptable, entonces finalmente se sigue el tratamiento de riesgo. Si la información no es suficiente, se realiza otra iteración con un contexto revisado. La eficacia del tratamiento del riesgo depende de los resultados de la valoración del riesgo. Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual. Es este caso si es necesario otra iteración de la valoración de riesgo con cambios en los parámetros del contexto (ISO/IEC 27005, 2011).

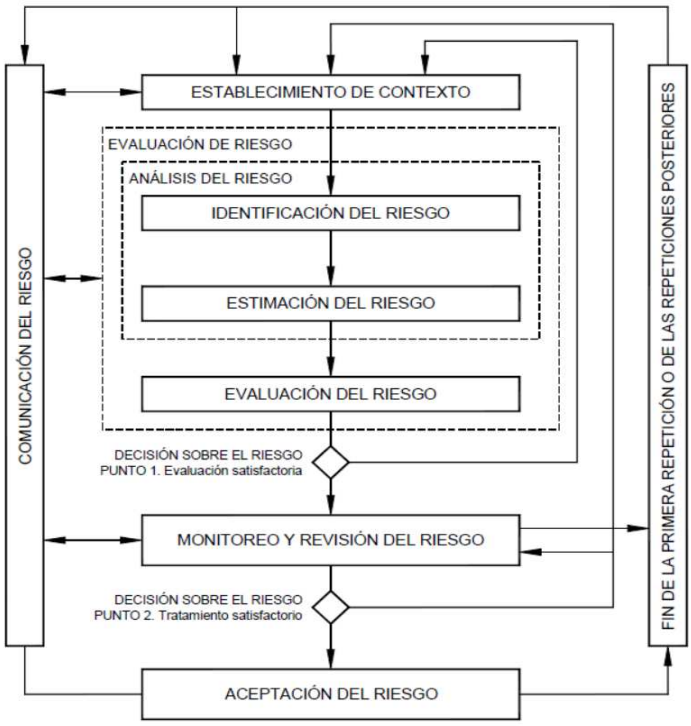

Figura 1: Proceso de gestión del riesgo en la seguridad de la información

Fuente *(ISO/IEC 27005, 2011)*

La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la organización, es esencial si los controles requieren un financiamiento fuerte y es necesario postergar su implementación. Es importante durante todo el proceso la comunicación y documentación tanto de los riesgos como de su tratamiento (ISO/IEC 27005, 2011).

3.3.2 Contexto de la Gestión de Riesgo

Para establecer el contexto es necesario identificar toda la información pertinente para establecer el contexto de la gestión del riesgo en la seguridad de la información. Se debe especificar los criterios básicos, alcance y limite, así como la organización del proceso de gestión del riesgo. Se aconseja seleccionar un enfoque que aborde: criterios de evaluación de riesgo, criterios de impacto y criterios de aceptación del riesgo. (ISO/IEC 27005, 2011)

Se recomienda desarrollar criterios para la evaluación del riesgo, se debe tener en cuenta aspectos como criticidad de los activos de información involucrados, requisitos legales y reglamentarios, así como las expectativas y percepciones de las partes interesadas y sus consecuencias para la empresa.

En relación con los criterios de impacto del riesgo, la norma específica que se debe desarrollar el criterio en base al grado de daño o de los costos para la organización considerando el nivel de clasificación de los activos, operaciones deterioradas, incumplimiento legal, daños para la reputación entre otros.

Por otro lado, los criterios de aceptación dependen con frecuencia de las políticas, metas, objetivos de la organización y las partes interesadas. La organización debería definir sus propias escalas para los niveles de aceptación del riesgo.

Una correcta organización para la gestión del riesgo requiere desarrollar el proceso de gestión del riesgo más adecuado para la organización, así como la aprobación por los directores correspondientes de la entidad. (ISO/IEC 27005, 2011)

3.3.3 Evaluación del riesgo en la seguridad de la información

Los riesgos se deberían identificar, describir cuantitativa o cualitativamente y priorizar frente a los criterios de evaluación del riesgo y los objetivos relevantes para la organización.

Un riesgo es una combinación de las consecuencias que se presentarían después de la ocurrencia de un evento y de su probabilidad de ocurrencia. La valoración del riesgo cuantifica o

describe cualitativamente el riesgo y permite a los directores priorizar los riesgos de acuerdo con su gravedad u otros criterios establecidos.

La valoración del riesgo determina el valor de los activos de información; identifica las amenazas y vulnerabilidades aplicables que existen o que podrían existir, identifica los controles existentes y sus efectos en el riesgo identificado, determina las consecuencias potenciales y, finalmente, prioriza los riesgos derivados y los clasifica frente a los criterios de evaluación del riesgo determinados en el contexto establecido. Con frecuencia, la valoración del riesgo se lleva a cabo en dos o más iteraciones. En primer lugar, se realiza una valoración general para identificar riesgos potencialmente altos que ameriten posterior valoración. La siguiente iteración puede implicar una consideración adicional en profundidad de los riesgos potencialmente altos revelados en la iteración inicial (ISO/IEC 27005, 2011).

Depende de la organización seleccionar su propio enfoque para la valoración del riesgo con base en los objetivos y la meta de esta valoración.

3.3.4 Análisis del riesgo

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida. Los pasos se describen a continuación para la actividad de estimación del riesgo:

a) *Identificación de los activos* se debe llevar a cabo con un nivel adecuado de detalle, que proporcione información suficiente para la valoración del riesgo. Además, se debe identificar al propietario de cada activo, para asignarle la responsabilidad. El propietario con frecuencia es la persona más idónea para determinar el valor del activo (ISO/IEC 27005, 2011).

b) *Identificación de las amenazas* se debe identificar las amenazas y sus orígenes. Una amenaza puede tener su origen dentro o fuera de la organización. Las amenazas se deben identificar genéricamente y por tipo y, cuando sea adecuado, las amenazas individuales dentro de la clase genérica identificada. Una amenaza puede afectar a más de un activo,

en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados. La información de las amenazas puede ser obtenido de los propietarios de los activos, usuarios, personal de recurso humanos, especialistas en seguridad de la información, experto en seguridad física, etc. Además, también es posible considerar los incidentes anteriores, así como catálogos de amenazas para completar la lista de amenazas genéricas y que están disponibles en organismos industriales, del gobierno general, organizaciones legales, etc. (ISO/IEC 27005, 2011).

c) *Identificación de los controles existentes*, se debe identificar los controles existentes y los planificados considerando como entrada documento de los controles y planes para la implementación del tratamiento del riesgo. Se debería realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, además es recomendable revisar el funcionamiento de los controles existentes, debido a que, si el control no funciona, puede causar vulnerabilidades. Una forma de estimar el efecto del control es analizar la manera en que reduce la probabilidad de ocurrencia de la amenaza y la facilitad de explotar la vulnerabilidad, o el impacto del incidente. Las revisiones por parte de la dirección y los reportes de auditoria también suministran información acerca de la eficacia de los controles existentes (ISO/IEC 27005, 2011).

d) *Identificación de las vulnerabilidades*, un control que se utiliza de modo incorrecto podría por si solo ser una vulnerabilidad. Un control puede ser eficaz o ineficaz dependiendo del ambiente en el cual funciona. Por el contrario, una amenaza que no tiene una vulnerabilidad puede no resultar en un riesgo. Las vulnerabilidades pueden estar relacionadas con las propiedades de los activos que se pueden usar de una manera, o para un propósito, diferente del previsto cuando se adquirió o se elaboró el activo (ISO/IEC 27005, 2011).

e) *Identificación de las consecuencias*, una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, perdidas de negocio, reputación, daño, etc. Las consecuencias pueden ser causadas por un escenario de incidente. Un escenario de incidente es la descripción de una amenaza que explota una vulnerabilidad determinada o

> un conjunto de vulnerabilidades en un incidente de seguridad de la información. El impacto de los escenarios de incidente puede afectar a uno o más activos, considerando que los activos tengan asignados un costo financiero, así como por la consecuencia si se ven comprometidos (ISO/IEC 27005, 2011).

El análisis de riesgo se puede realizar con diferentes grados de detalle dependiendo de la criticidad de los activos, la amplitud de las vulnerabilidades conocidas y los incidentes anteriores que implicaron a la organización.

Una metodología puede ser cuantitativa o cualitativa o una combinación de ambas. En la práctica generalmente se utiliza la estimación cualitativa para obtener de primeramente una indicación del nivel de riesgo, y así encontrar los de mayor impacto.

La forma del análisis debe ser consistente con los criterios de evaluación de riesgo desarrollado en el contexto.

La *estimación cualitativa* utiliza una escala de atributos calificativos para describir la magnitud de las consecuencias potenciales y la probabilidad de que ocurran dichas consecuencias. Una ventaja es su facilidad de comprensión, mientras que una desventaja es la dependencia en la selección subjetiva de la escala. Las escalas pueden ajustarse para satisfacer las circunstancias. Preferiblemente para el análisis cualitativo se debe utilizar información basada en hechos.

La *estimación cuantitativa* utiliza una escala con valores numéricos tanto para las consecuencias como para la probabilidad. La calidad de los datos depende de la exactitud de los valores numéricos y la validez de los modelos utilizados.

Se debe evaluar el impacto en la organización provocado por incidentes posibles o reales, teniendo en cuenta la brecha existente en la seguridad de la información, por ejemplo, la perdida de confidencialidad, integridad o disponibilidad en los activos. El valor del impacto se puede expresar cualitativa o cuantitativa, sin embargo, cualquier método para proveer un valor monetario en general suministra más información.

Las consecuencias se pueden expresar en términos monetarios, técnico o de impacto humano, cualquier otro pertinente para la organización (ISO/IEC 27005, 2011).

Después de identificar los escenarios de los incidentes, es necesario evaluar la probabilidad de cada escenario y el impacto de que ocurra, utilizando técnicas de estimación cualitativas o cuantitativas. Se debe tomar en consideración la frecuencia con la que ocurren las amenazas y la facilidad con la que las vulnerabilidades pueden ser explotadas, teniendo en cuenta:

- La experiencia y las estadísticas aplicables para la probabilidad de la amenaza.
- Para fuentes de amenazas deliberada: la motivación y las capacidades, las cuales cambiarán con el tiempo, y los recursos disponibles para los posibles atacantes, así como la percepción de atracción y vulnerabilidad de los activos para un posible atacante.
- Vulnerabilidades, tanto individuales como en grupo.
- Controles existentes y su eficacia.

La estimación del riesgo asigna valores a la probabilidad y las consecuencias de un riesgo. Estos valores pueden ser cuantitativos o cualitativos. La estimación del riesgo se basa en las consecuencias evaluadas y la probabilidad. El riesgo estimado es una combinación de la probabilidad de un escenario de incidente y sus consecuencias. (ISO/IEC 27005, 2011)

3.3.5 Evaluación del riesgo

Para evaluar los riesgos, las organizaciones deben comparar los riesgos estimados con los criterios de evaluación que se definieron en el establecimiento del contexto, así como los objetivos de la organización, punto de vista de las partes interesadas, etc. Las decisiones se tomarán de acuerdo con el nivel de aceptación del riesgo, sin embargo, es importante analizar la agrupación de múltiples riesgos bajos o medios que pudieran provocar riesgos globales muchos más altos.

3.3.6 Tratamiento del riesgo

Se deben seleccionar controles para reducir, retener, evitar o transferir los riesgos, con relación a los escenarios de incidentes que llevan a tales riesgos.

En la figura 2 se ilustra el tratamiento del riesgo dentro de los procesos de la gestión de riesgo. Las opciones para el tratamiento del riesgo se deberían seleccionar con base en el resultado de la evaluación de riesgo, el costo esperado para implementar estas opciones y los beneficios esperados.

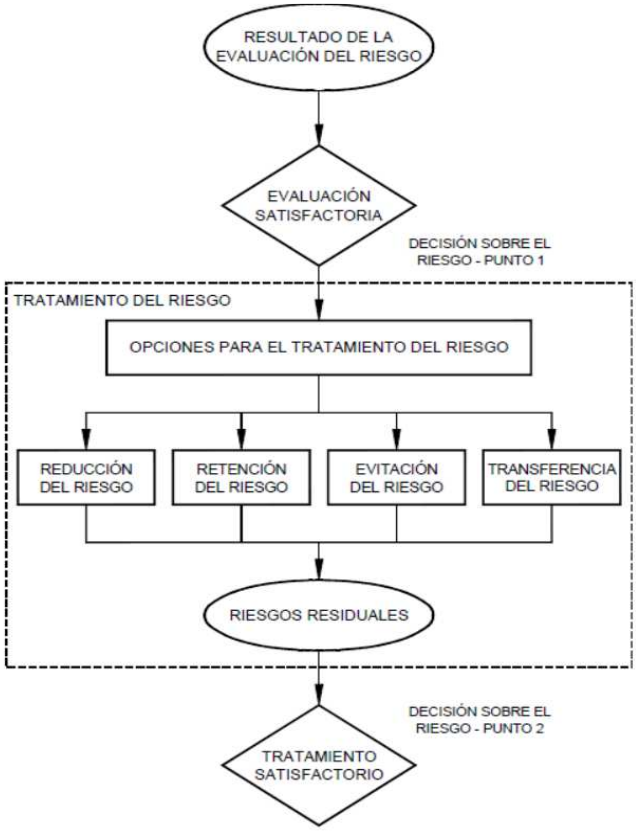

Figura 2: Actividad para el tratamiento del riesgo

Fuente (ISO/IEC 27005, 2011)

Las cuatro opciones para el tratamiento no se excluyen mutuamente, sin embargo, es necesario realizar un análisis de los costos de implementación debido a que las mejoras pueden no ser económicas y es necesario estudiarlas para determinar si se justifican o no.

Sin embargo, puede haber tratamientos eficaces para más de un riesgo, por cual es conveniente determinar un plan de tratamiento del riesgo que identifique con claridad el orden de prioridad en el cual se deberían implementar los tratamientos individuales.

Las opciones para el tratamiento del riesgo se deberían considerar teniendo en cuenta:

- Como perciben el riesgo las partes interesadas.
- La forma más adecuada de comunicación con dichas partes.

Una vez definido el plan para el tratamiento de riesgo, es necesario determinar los riesgos residuales. Esto implica una actualización de la evaluación del riesgo, considerando los efectos esperados del tratamiento propuesto para el riesgo. Si el riesgo residual aun no satisface los criterios de aceptación, puede ser necesario otra repetición del tratamiento del riesgo antes de proceder con la aceptación del riesgo.

3.3.7 Reducción del riesgo

A nivel de riesgo puede reducir mediante la selección de controles, de manera tal que el riesgo residual se puede revaluar como aceptable.

Es importante resaltar que existen muchas restricciones que pueden afectar las selecciones de controles. Las restricciones técnicas tales como los requisitos de desempeño, el manejo y los aspectos de compatibilidad pueden dificultar el uso de algunos controles o podrían inducir error humano bien sea anulando el control, dando una falsa sensación de seguridad o incluso aumentando el riesgo de modo que no haya control (ISO/IEC 27005, 2011).

3.3.8 Retención del riesgo

La decisión sobre la retención del riesgo sin acción posterior se debería tomar dependiendo de la evaluación del riesgo. Si el nivel de riesgo satisface los criterios para su aceptación, no es necesario implementar controles adicionales y el riesgo se puede retener (ISO/IEC 27005, 2011).

3.3.9 Evitación del riesgo

Se debe evitar la actividad o la acción que da origen al riesgo particular. Cuando los riesgos identificados se consideran muy altos, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar una decisión para evitar por completo el riesgo, mediante el retiro de una actividad o un conjunto de actividades planificadas o existentes, o mediante el cambio en las condiciones bajo las cuales se efectúa tal actividad (ISO/IEC 27005, 2011).

3.3.10 Transferencia del riesgo

El riesgo se debe transferir a otra parte que pueda manejar eficazmente el riesgo particular dependiendo de la evaluación del riesgo.

La transferencia puede involucrar compartir algunos riesgos con las pares externas. La transferencia puede crear riesgos nuevos o modificar los riesgos identificados existentes. Por lo tanto, puede ser necesario el tratamiento adicional para el riesgo (ISO/IEC 27005, 2011).

3.3.11 Aceptación del riesgo en la seguridad de la información

Se debe tomar la decisión de aceptar los riesgos y las responsabilidades de la decisión y registrarla de manera formal.

Los planes de tratamiento de riesgo deberían describir la forma en que los riesgos evaluados se deben tratar, con el fin de satisfacer los criterios de aceptación del riesgo. Es importante que los directores responsables revisen y aprueben los planes propuestos para el

tratamiento del riesgo y los riesgos residuales resultantes, y que registren todas las condiciones asociadas a tal aprobación (ISO/IEC 27005, 2011).

3.3.12 Comunicación de los riesgos para la seguridad de la información

La comunicación de los riesgos es una actividad para lograr un acuerdo sobre la manera de gestionar los riesgos al intercambiar y/o compartir información acerca de los riesgos, entre quienes toman las decisiones y las otras partes involucradas. La comunicación garantizará que aquellos con derechos de adquiridos comprenden las bases sobre las cuales toman las decisiones y por qué se requieren acciones particulares (ISO/IEC 27005, 2011).

CAPÍTULO IV: CULTURA DE ADMINISTRACIÓN DE RIESGO DE TIC

4

4.1 Tipo de investigación

La investigación realizada asumió un enfoque mixto (cualitativo- cuantitativo). Como parte del estudio se recopiló información cuantitativa mediante la administración del cuestionario para la evaluación del riesgo tecnológico (Fernández Matute & Monteros Montenegro, 2014) al personal responsable de la gestión de riesgo informático a una muestra intencional de entidades del sector público de la ciudad de Esmeraldas, en Ecuador.

La investigación se caracterizó por la recopilación de la información en el periodo comprendido en los meses de abril y mayo de 2017 en las propias entidades seleccionadas sin que mediara una manipulación de variables que pudiera influir en la respuesta de los encuestados, por lo que se encuadra en la tipología de las investigaciones transeccionales y de campo.

En correspondencia con el objetivo del proyecto, centrado en el diagnóstico de las variables que caracterizan el proceso de gestión de riesgo tecnológico en las entidades del sector público la investigación alcanza un nivel de profundidad descriptivo.

4.2 Población y muestra

La población en estudio está constituida por las entidades del sector público de la ciudad de Esmeraldas que tienen implementado servicios tecnológicos.

La unidad de análisis es el responsable o responsables del área tecnológica de las entidades públicas.

La muestra fue seleccionada mediante un muestreo intencional de la población. Inicialmente fueron contactados 24 centros de las cuales accedieron 18 a participar en el estudio. Se encuentran listadas en la siguiente tabla:

Tabla 1

Entidades del sector público de la ciudad de Esmeraldas

	NOMBRE
1	Gobierno Autónomo Descentralizado de Municipalidad de Esmeraldas
2	Gobierno Autónomo Descentralizado de la Prefectura de Esmeraldas
3	Jefatura de Tránsito Esmeraldas
4	IESS Esmeraldas
5	IESS Hospital de Esmeraldas
6	Dirección Provincial de Educación de Esmeraldas
7	Empresa de Agua Potable
8	Corporación Nacional Eléctrica Empresa pública Esmeraldas
9	Registro Civil Esmeraldas
10	Ministerio de Inclusión Económica y Social Esmeraldas
11	Superintendencia de Telecomunicaciones Esmeraldas
12	Dirección Provincial del Consejo Judicatura de Esmeraldas
13	Unidad Judicial Especializada de la Familia Mujer Niñez y Adolescencia
14	Agencia Nacional de Tránsito
15	Policía Nacional del Ecuador
16	Flota Petrolera Empresa Pública
17	Celec TermoEsmeraldas
18	PetroEcuador Empresa Pública

4.3 Modalidad de la Investigación

El objetivo de la presente investigación científica fue realizar un diagnóstico para analizar el proceso de la gestión de riesgo en las entidades del sector público, con la finalidad de conocer la situación actual del proceso en las organizaciones desde la percepción del representante de TIC.

Para determinar el nivel de madurez de un proceso existen varias metodologías, de las cuales se considera para el estudio Cobit debido a que es un marco que proporciona métricas y modelos de madurez en los procesos a fin de medir el logro de los diferentes objetivos.

Cobit presenta una escala de 0 a 5 en su modelo de madurez para el tratamiento de la gestión de riesgo de TI, la misma que se detalla a continuación:

- Madurez Nivel 0: No existe ningún proceso de evaluación del riesgo de TI.

- Madurez Nivel 1: Los riesgos de TI se consideran de una forma ad-hoc. A veces se hace evaluación de los riesgos.

- Madurez Nivel 2: Repetible pero intuitiva. Solo en proyectos importantes o cuando se detectan problemas.

- Madurez Nivel 3: Proceso definido y documentado. Existe un procedimiento documentado que establece cuando y como se debe realizar la evaluación del riesgo de TI.

- Madurez Nivel 4: Medido y gestionado. No sólo existen procedimientos de identificación y gestión del riesgo, sino que se efectúan medidas y se controlan resultados.

- Madurez Nivel 5: Optimización.

A partir de la escala anterior Fernández y Monteros (2014) establecieron la siguiente escala para el estudio, como se muestra en la siguiente tabla:

Tabla 2
Escala de nivel de madurez

NIVEL	DEFINICIÓN
0	No dispone
1	No se piensa en ello de manera esencial
2	Ocasional y/o solo en ciertos proyectos
3	Procedimientos definidos y documentados
4	Medido y gestionado
5	Optimizado

Fuente: (Fernández Matute & Monteros Montenegro, 2014)

De igual manera, los ejes que fueron evaluados corresponden a los cinco aspectos que The Ernst & Young Business Risk Resport (2010) en su publicación “The top 10 risks for global business”, considera representativo:

- Políticas y práctica de gerencia de riesgos.

- Comunicación efectiva.

- Amenazas y riesgos.

- Herramientas y tecnologías.
- Gobierno y control.

4.4 Instrumento

Se usó un cuestionario de 25 preguntas desarrollada por Fernández y Montero (2014) ajustándolo de acuerdo con el ámbito de la población de estudio.

Las preguntas están organizadas para medir 5 ejes de nivel de madurez: políticas y prácticas de gerencia de riesgos, comunicación efectiva, amenazas latentes, herramientas tecnológicas y gobierno de seguridad (Anexo 1).

4.4.1 Atributos demográficos del cuestionario:

Información empresarial. - Es la información de la empresa y aspectos principales del área de Tecnología de Información.

Nombre. -Razón social de la empresa pública.

Tipo de organización. - Determina si la empresa es proveedora o usuario de servicio tecnológicos.

Presupuesto anual de TI.-Ubica en un rango determinado el monto presupuestado en dólares para la adquisición de infraestructura o servicios tecnológicos en la organización en el último año.

4.4.2 Ejes de nivel de madurez

Políticas y prácticas de gerencia de riesgos

Política general de seguridad. - Es el grado de implantación de una política de seguridad en la empresa.

Mapa de Riesgo. - Es el nivel de implantación de un mapa de riesgo en la organización.

Proceso de administración de riesgos. - Es el nivel de adopción de un proceso de administración de riesgos en la organización.

Marco de referencia. - Identifica el nivel de implantación de un marco referencia, estándares o modelos de Administración de riesgo tecnológico en la empresa.

Auditoría informática. - Explora el nivel de ejecución del proceso de auditoría informática en la organización.

Relación entre la administración de riesgo y la función de auditoría. - Indaga sobre la relación que existe entre la administración de riesgo y la función de auditoría.

Relación entre la administración de riesgos y el control interno. - Indaga hasta qué punto está involucrada la administración de riesgos en el trabajo de control interno realizado para cumplir con los requerimientos regulatorios.

Comunicación

Comunicación de políticas y acciones de riesgo. - Explora el nivel en el que la organización comunica a sus políticas y acciones de administración de riesgos.

Revelación de riesgos en reportes de información. - Identifica el nivel en el que la entidad pública revela sus riesgos en el reporte de información (reporte anual, documentos de referencia, etc.).

Revelación de programas de seguros en reportes financieros. – Indica el nivel en qué la entidad pública revela sus programas de seguros en su reporte de información financiera.

Política de seguridad de la información. - Explora el nivel en el cual la organización tiene una política de seguridad de la información, considerando su estado de implementación, es decir si se mantiene en constante evaluación y actualización.

Comunicación de políticas de seguridad de la información. - Indica el nivel de comunicación de la política de seguridad de la información, es decir si la organización difunde las políticas de seguridad de la información satisfactoriamente al personal en general

Conocimiento del incumplimiento de la normativa de seguridad por parte del personal. - Es el grado de conocimiento de las consecuencias que puede derivarse del incumplimiento de la normativa de seguridad por parte del personal.

Amenazas y riesgos

Recursos para identificar amenazas cambiantes. - Evalúa el nivel de inversión de la empresa en recursos para lograr identificar riesgos y amenazas.

Nivel de riesgo por uso de redes sociales, computo en la nube y dispositivos personales. – Identifica el nivel de percepción de cambio en el ambiente de riesgo producido a partir de nuevas tecnologías, es decir por el uso de redes sociales, cómputo en la nube y dispositivos personales móviles en la organización.

Administración de riesgos de TI.- Evalúa el nivel de implantación de un programa de administración de riesgos de TI establecido que maneje los riesgos derivados del uso de las redes sociales, cómputo en nube y dispositivos personales móviles

Herramientas y tecnológicas

Tecnología para el proceso de administración de riesgo. - Identifica el nivel de implementación de tecnología para la administración de riesgo.

Tecnología de virtualización. - Identifica el nivel de implantación de tecnologías de virtualización.

Mecanismo para el control de administración de accesos. - Identifica el nivel de implementación de un software o control específico de administración de accesos e identidades que mitigue los riesgos asociados con los derechos de acceso a sus datos y sistemas.

Gobierno y control

Implementación de un sistema de gestión de seguridad de información. – Identifica el nivel de implementación del sistema de gestión de seguridad de información en organización.

Comité de seguridad de la información. -Es el nivel de implementación de un comité de seguridad de la información en la entidad pública.

Nivel de implementación de un plan de respuesta. -Identifica el nivel de implementación de un plan de respuesta en la organización para el tratamiento de incidentes de seguridad.

Nivel de ejecución de evaluación de riesgos tecnológicos. – Identifica el nivel de ejecución de evaluaciones periódicamente de riesgos tecnológicos que realiza la entidad pública.

Contratación de póliza de delitos informáticos. – Evalúa el nivel de contratación de póliza de delitos informáticos.

Nivel de implementación de un plan de contingencia y/o continuidad de negocios. – Identifica el nivel de implementación de un plan de contingencia y/o continuidad de negocios, así como si el proceso está optimizado y evaluado constantemente.

4.5 Confiabilidad

La confiabilidad del cuestionario en correspondencia a la escala 1 a 5 puntos empleada para la medición de cada elemento del cuestionario fue establecida mediante el cálculo de la consistencia interna del cuestionario mediante el coeficiente alfa de Cronbach en una muestra de tamaño 18, lo que generó un coeficiente de 0,929 considerado adecuado para cualquier uso en la investigación y toma de decisiones según criterio de (Morales Vallejo, 2007) al tiempo que indica la conveniencia del uso de la medida que resulta al sumar los puntajes de cada uno de los elementos para caracterizar el nivel alcanzado en la variable que se mide, en este caso la madurez del proceso de percepción de riesgo informático en las instituciones del sector público encuestadas.

4.6 Técnica de Análisis de datos

La información al ser procesada obtuvo estadísticos descriptivos como frecuencias, porcentajes y un diagrama de radar para analizar la madurez del proceso correspondiendo cada dominio como eje de evaluación.

4.7 Análisis de resultados

El estudio investigativo refleja principalmente que:

- El 72% de las entidades públicas encuestadas indicaron tener implementado un proceso de administración de riesgos, sin embargo, apenas el 44% tiene implementado un marco de referencia para el control interno como COBIT, COSO, etc.

- A penas el 44% de las entidades públicas se encuentran certificadas y tienen implementado un SGSI, asimismo, se evidencia que la mayoría de entidades cuenta con una política de seguridad de información 83%, de igual manera el personal conoce sobre la política de la seguridad de la información 78%.

- Además, poco más de la mitad el 56% manifiesta que se tiene los recursos para lograr identificar los riesgos y amenazas, indiferentemente del presupuesto asignado a TI.

- Sin embargo, el 16% que expone no tener los recursos para identificar cambios se encuentra en el grupo de entidades con un presupuesto menor a 50.000 dólares.

- Por otro lado, el 61% manifestaron poseer a la fecha un programa de administración de riesgo de TI que maneja los riesgos derivados del uso de redes sociales, cómputo en la nube y dispositivos personales móviles.

- El 94% de las empresas encuestadas cuenta con un software o control especifico de administración de acceso e identidades el cual se implementó con el fin de mitigar riesgos asociados con los derechos de acceso a datos. Lo cual demuestra una mayor

responsabilidad en salvaguardar la información considerando que el 83% de las entidades tiene tecnología de virtualización implementada.

- Por otra parte, el 78% tiene completamente optimizado y evaluado un plan de respuestas a incidentes de seguridad.

Tabla 3

Nivel de Madurez de los dominios

Dominio 1 **Políticas y prácticas de gerencia de riesgos**	Nivel de Madurez (/5)	*Promedio (/5)*
Política general de seguridad	4,06	***3,28***
Mapa de Riesgo	2,78	
Proceso de administración de riesgos	3,33	
Marco de referencia	2,28	
Auditoría informática	3,00	
Relación entre la administración de riesgo y la función de auditoría	3,50	
Relación entre la administración de riesgos y el control interno	4,00	
Dominio 2 **Comunicación**	**Nivel de Madurez (/5)**	***Promedio (/5)***
Comunicación de políticas y acciones de riesgo	2,66	***3,20***
Revelación de riesgos en reportes de información	3,72	
Revelación de programas de seguros en reportes financieros	3,56	
Política de seguridad de la información	4,11	
Comunicación de políticas de seguridad de la información	4,00	
Conocimiento del incumplimiento de la normativa de seguridad por parte del personal	4,33	
Dominio 3 **Amenazas y riesgos**	**Nivel de Madurez (/5)**	***Promedio (/5)***
Recursos para identificar amenazas cambiantes	3,67	***3,56***
Nivel de riesgo por uso de redes sociales, computo en la nube y dispositivos personales	3,39	
Administración de riesgos de TI	3,61	
Dominio 4 **Herramientas tecnológicas**	**Nivel de Madurez (/5)**	***Promedio (/5)***
Tecnología para el proceso de administración de riesgo	3,89	***4,33***
Tecnología de virtualización	4,17	
Mecanismo para el control de administración de accesos	4,94	
Dominio 5 **Gobierno y control**	**Nivel de Madurez (/5)**	***Promedio (/5)***
Implementación de un sistema de gestión de seguridad de información	3,83	***3,36***
Comité de seguridad de la información	3,17	
Nivel de implementación de un plan de respuesta	3,94	
Nivel de ejecución de evaluación de riesgos tecnológicos	3,78	
Contratación de póliza de delitos informáticos	1,44	
Nivel de implementación de un plan de contingencia y/o continuidad de negocios	4	

En la Tabla 3, se detalla el promedio de madurez de cada dominio, valores que son resultado de la aplicación de la encuesta.

Además, en la Tabla 4 se encuentra la consolidación de los resultados, mostrando el promedio general por dominio.

Se evidencia que existe mayor implementación de herramientas tecnológicas para el control de acceso en comparación con el proceso de planificación y administración de los riesgos, lo que demuestra que el personal de tecnología se encuentra mayormente involucrado o preparado en la implementación de tecnología que en la elaboración de planificaciones.

Tabla 4
Consolidación de resultados

N	DOMINIO	Pro medio (/5)
1	Políticas y prácticas de gerencia de riesgos	3,28
2	Comunicación	3,20
3	Amenazas y riesgos	3,56
4	Herramientas tecnológicas	4,33
5	Gobierno y control	3,36

En la figura 3 se muestran los resultados en el diagrama de radar, donde cada dominio corresponde a un eje de evaluación. El mayor nivel de madurez de todos los ejes es *Herramientas tecnológicas* debido a que en los últimos años el estado ecuatoriano se ha preocupado por incorporar tecnología como herramienta para la prestación de los servicios públicos.

Sin embargo, el eje *Gobierno y control* se encuentra en un nivel en el cual sus procedimientos se encuentran definidos, pero es necesario que sean correctamente medidos y gestionados.

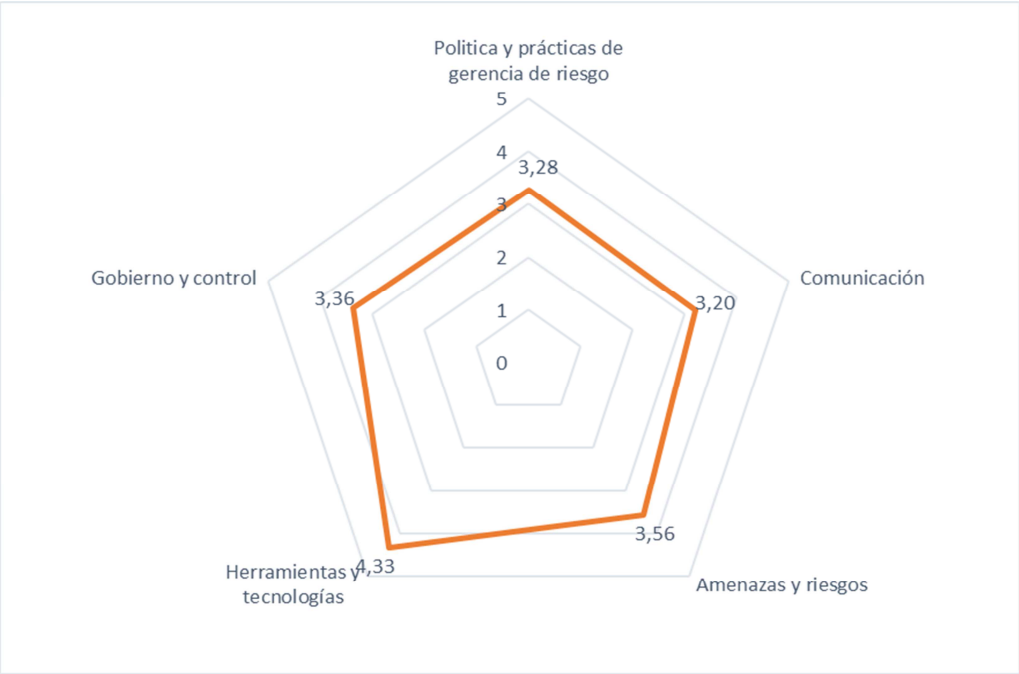

Figura 3: Nivel de madurez del riesgo en entidades públicas de la ciudad de Esmeraldas.

En función a los resultados obtenidos en cada dominio se determinó que el proceso gestión de riesgo tecnológico en las entidades públicas se ubica en el nivel 3, es decir los procedimientos se encuentran definidos y documentados como lo indica la Tabla 1.

CAPÍTULO V: GUÍA METODOLÓGICA DE GESTIÓN DE RIESGO DE TIC

5

5.1 Descripción general

En base a las directrices de la normativa para la gestión del riesgo, se presenta la siguiente guía metodológica de gestión de riesgo de TI.

Figura 4: Ciclo de la Gestión del Riesgo

La guía metodológica se basa en el ciclo del proceso de Gestión de riesgo, el cual tiene varias etapas que se realizan en bucle hasta que todos los riesgos sean evaluados y tratados de acuerdo con el contexto previamente establecido por las autoridades de la organización.

El núcleo e inicio del ciclo es el establecimiento del contexto en el cual se define los procesos críticos dependientes directamente de la tecnología. Luego se identifican los riesgos asociados a los principales activos de los procesos. Posteriormente se realiza el cálculo del riesgo considerando la valoración de la probabilidad de ocurrencia de las amenazas y la valoración del impacto cuando una vulnerabilidad es aprovechada por la amenaza.

En la evaluación del riesgo se establecen los riesgos que son inaceptables y que requieren un tratamiento mediante la selección de un control. Si el control es eficiente termina, caso contrario se realiza la estimación nuevamente para determinar su valoración y evaluación del riesgo.

La Figura 5 muestra gráficamente el esquema a seguir por la guía:

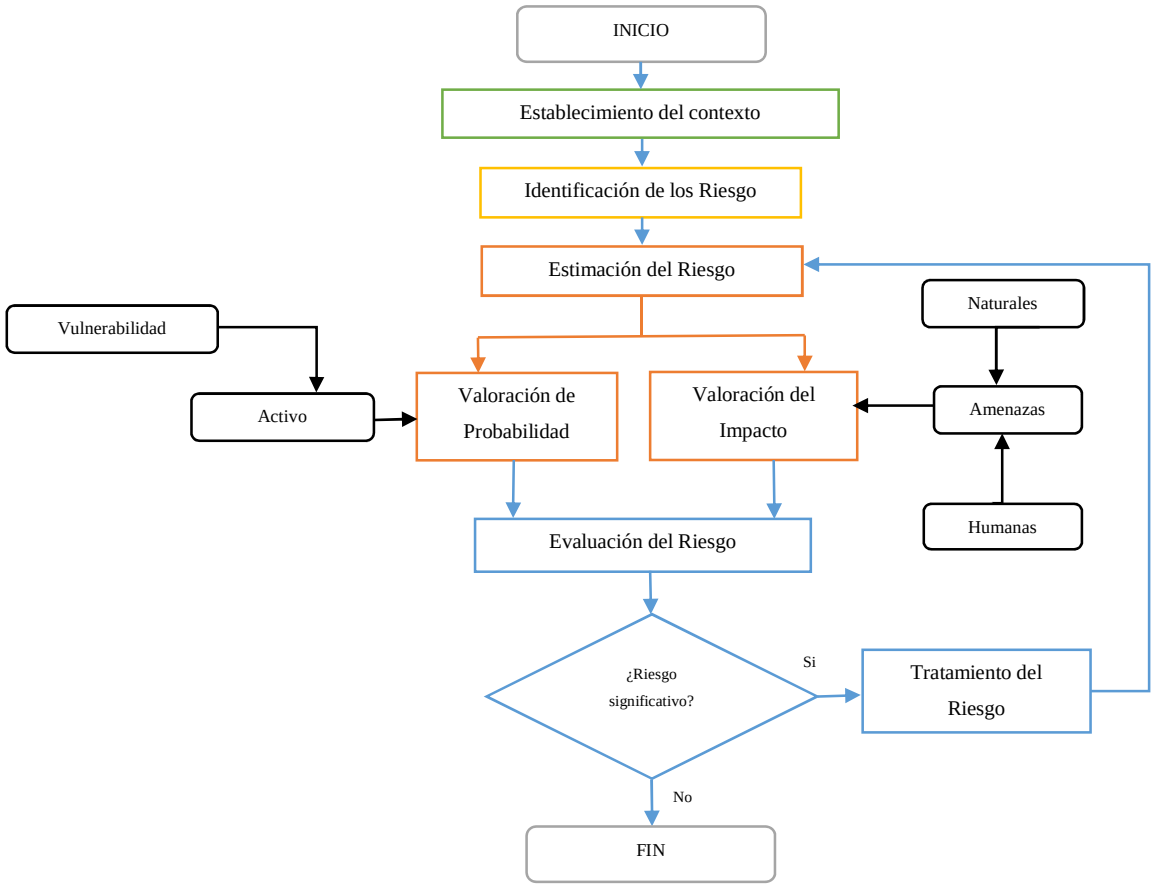

Figura 5: Esquema de la guía metodológica propuesta de gestión del Riesgo de TI

5.2 Proceso vs Propuesta metodológica de Gestión del Riesgo de TI

Desarrolla las principales etapas del proceso de Gestión del Riesgo de la norma ISO/IEC 27005: 2008. En la figura 8 se detalla la relación entre ambos.

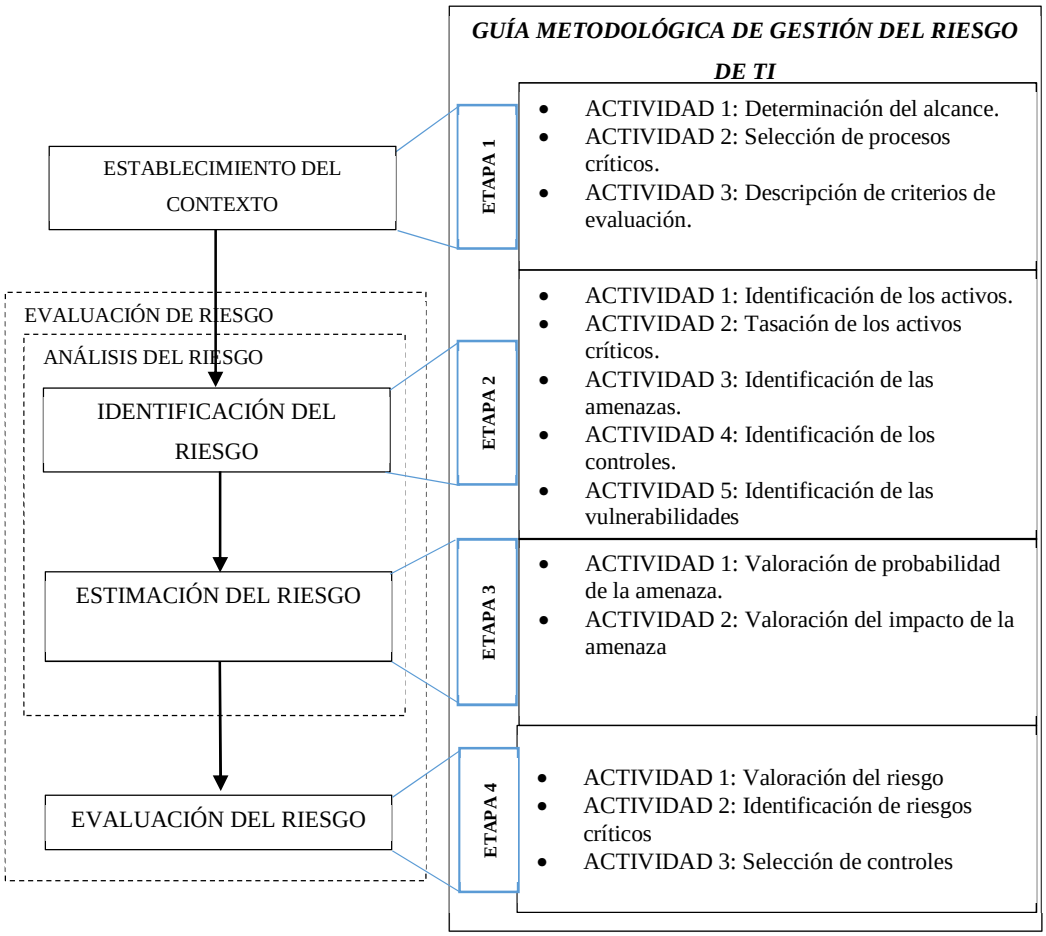

Figura 6: Proceso de Gestión de Riesgo vs Guía metodológica propuesta

5.3 Estructura

La metodológica propone una guía práctica de 4 etapas para Gestión del Riesgo de TI, cada una produce documentos que serán la entrada para la siguiente etapa.

Cada etapa tiene actividades que deben ser desarrolladas para lograr una adecuada gestión del riesgo de TIC como se muestra en la siguiente tabla:

Tabla 5
Estructura de la Guía Metodológica Práctica de Gestión del Riesgo de TI

ETAPA	ACTIVIDAD
Establecimiento del contexto	1. Determinación del alcance. 2. Selección de procesos críticos. 3. Descripción de criterios de evaluación.
Identificación del riesgo	1. Identificación de los activos. 2. Tasación de los activos críticos. 3. Identificación de las amenazas. 4. Identificación de los controles. 5. Identificación de las vulnerabilidades.
Estimación del riesgo	1. Valoración de probabilidad de la amenaza. 2. Valoración del impacto de la amenaza.
Evaluación del riesgo	1. Valoración del riesgo 2. Identificación de riesgos críticos 3. Selección de controles

5.4 Etapa 1: Establecimiento del contexto

Es esencial que la gestión de riesgos se integre tanto con el resto de áreas de la entidad pública como con su entorno externo. Por tanto, hay que determinar los condicionantes tanto internos como externos que definen el marco de trabajo.

A nivel interno se tendrán en cuenta: la cultura, recursos, procesos y objetivos del negocio. A nivel externo se consideran diferentes aspectos relativos al entorno social, económico o legislativo.

5.4.1 Actividad 1: Determinación del alcance

Debe ser en relación con las características de la empresa, la organización, su ubicación, bienes y tecnología. El alcance tiene que estar definido y completo.

El alcance para la gestión del riesgo comprende todos los procesos o ciertos procesos críticos que son esenciales para el cumplimiento de los objetivos estratégicos.

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

5.4.2 Actividad 2: Selección de procesos críticos

Para iniciar es importante tener en cuenta la información y documentación de la organización relacionada con la planeación estratégica y procesos existentes; por lo que es indispensable la participación del personal de la organización que se logra a través de encuestas, entrevistas, visita a las instalaciones y demás actividades que permitan recolectar la información necesaria.

5.4.3 Actividad 3: Descripción de los criterios de evaluación

Se establece como metodología para la estimación del riesgo, el tipo cualitativa.

La estimación cualitativa utiliza la siguiente escala de atributos calificativos para describir la magnitud de las consecuencias potenciales:

Para evaluar el impacto en el negocio de la organización, es necesario determinar las consecuencias que puede provocar la pérdida de la confidencialidad, integridad o disponibilidad de los activos.

El impacto nos indica las consecuencias de la materialización de una amenaza. El nivel de riesgo es una estimación de lo que puede ocurrir y se valora, de forma cuantitativa, como el

producto del impacto, (consecuencia), asociado a una amenaza (suceso), por la probabilidad de la misma: Riesgo=Impacto x Probabilidad

Tabla 6

Escala de nivel de probabilidad de ocurrencia de una amenaza

Nivel	Valor	Descripción
Altamente improbable	1	Ocurre solamente en circunstancias excepcionales. Los controles de seguridad existentes son seguros y hasta el momento han suministrado un adecuado nivel de protección.
Improbable	2	Podría ocurrir en algún momento. Los controles de seguridad existentes son moderados y en general han suministrado un adecuado nivel de protección.
Eventual	3	Es posible la ocurrencia de nuevos incidentes, pero no muy probable.
Probable	4	Ocurre normalmente. Existe una gran probabilidad de que haya incidentes así en el futuro.
Altamente probable	5	Se espera que ocurra en la mayoría de las circunstancias. Los controles de seguridad existentes son bajos o ineficaces.

En la Tabla 7 se mantiene el mismo enfoque utilizado para la probabilidad de la amenaza.

Tabla 7

Escala de nivel de impacto de la amenaza al explotar la vulnerabilidad

Nivel	Valor	Descripción
Insignificante	1	Pérdida económica que no pone en riesgo los intereses de la compañía y no afecta el flujo normal de los procesos.
Menor	2	Pérdida económicamente asumible por la compañía sin consecuencias ni esfuerzos adicionales que afecten notablemente su situación financiera y no afecta los procesos de manera considerable.
Serio	3	Perdida económicamente mediana, respaldable por la compañía y puede afectar el flujo normal de algún proceso de la compañía.
Desastroso	4	Pérdida económica importante, que implica esfuerzos adicionales no planeados por la compañía y se puede presentar una interrupción parcial en los procesos.
Catastrófico	5	Pérdida económica que compromete seriamente el patrimonio y la estabilidad de la compañía y se interrumpe el proceso normal de las operaciones de manera indefinida.

En la Tabla 8 se detalla los rangos producidos por la multiplicación de los valores del impacto y la probabilidad. Se califica dentro de distintos grupos considerando a los dos de mayor numeración como riesgos no aceptables. Si bien es posible, y en ocasiones necesario, realizar un análisis cualitativo, trabajar con cantidades económicas facilita a las organizaciones establecer el llamado umbral de riesgo, también llamado apetito al riesgo: el nivel máximo de riesgo que la empresa está dispuesta o se atreve a soportar. La gestión de riesgos debe mantener el nivel de riesgo siempre por debajo del umbral.

Tabla 8

Escala de nivel de riesgo

Impacto x Probabilidad	**Nivel de Riesgo**
1-2	Muy Bajo
3-4	Bajo
5-6-8-9	Medio
10-12-15-16	Alto
20-25	Muy Alto

Definidos los rangos, se puede definir una matriz/mapa de riesgos base para el estudio como se detallada a continuación:

Tabla 9

Representación de los riesgos en el mapa de calor

IMPACTO	5.- Muy Alto	5	10	15	20	25
	4.- Alto	4	8	12	16	20
	3.- Medio	3	6	9	12	15
	2.-Bajo	2	4	6	8	10
	1.- Muy Bajo	1	2	3	4	5
MAPA/ MATRIZ DE RIESGOS		1. Altamente Improbable	2.Improbable	3. Eventual	4. Probable	5 Altamente Probable
		FRECUENCIA				

Fuente **(Jaramillo, 2013)**

5.5 Etapa 2: Identificación del riesgo

Luego de determinar el contexto y determinar los criterios de evaluación, la siguiente etapa es la identificación de todos los activos dentro del alcance para así posteriormente identificar las vulnerabilidades y amenaza que pueden afectarlos.

5.5.1 Actividad 1: Identificación de los activos

Primeramente, un activo es aquel que tiene valor en la organización. Los activos pueden ser documentos en papel o en formato electrónico, aplicaciones y bases de datos, personas, equipos de TI, infraestructura y servicios externos o procesos externalizados.

La información almacenada en los activos puede ser afectada por los riesgos, comprometiendo sus tres principales características:

- **Confidencialidad**: la información solo tiene que ser accesible o divulgada a aquellos que están autorizados.
- **Integridad**: la información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.
- **Disponibilidad**: la información debe estar siempre accesible para aquellos que estén autorizados.

Se debe identificar el conjunto de activos de la información, entendiendo un activo como cualquier elemento que represente valor para la organización. Estos activos serán aquellos que queden enmarcados dentro de los procesos seleccionados previamente en el alcance.

La mayoría de activos de información son elementos de configuración dentro de la infraestructura tecnológica, si se agrupa de acuerdo con sus características principales se tendrían 7 categorías como se muestra en la siguiente figura:

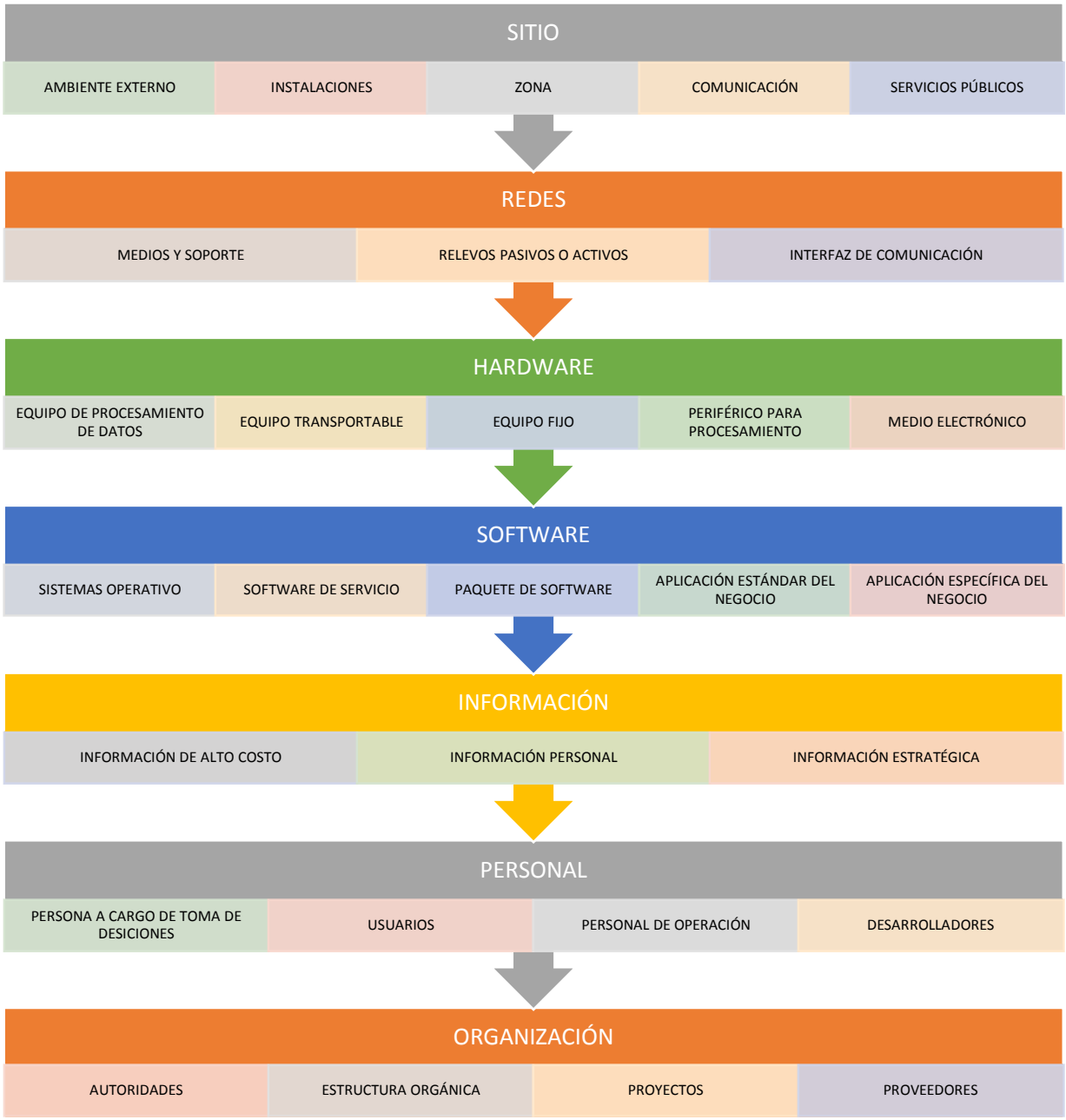

Figura 7: Categoría general y específica de Activos

Al identificar los activos también es necesario identificar a sus propietarios: la persona o unidad organizativa responsable de cada activo. Por lo tanto, en esta actividad se debe identificar

los activos, la categoría general, categoría específica y el propietario del activo de los procesos críticos previamente identificados en la actividad 2 de la etapa anterior.

5.5.2 Actividad 2: Tasación de los activos críticos

Para realizar la tasación de los activos, los propietarios de los activos calificarán las tres dimensiones de la información de acuerdo con el nivel de impacto en una escala de 1 a 5, siendo 5 la calificación más alta (mayor impacto) mientras que 1 la calificación más baja (menor impacto).

Para evaluar el impacto del activo en relación con la Confidencialidad (C), se realiza la siguiente pregunta ¿Qué nivel de confidencialidad tiene la información almacenada en el activo x?, considerando como respuesta lo detallado en la siguiente tabla:

Tabla 10
Escala del nivel de confidencialidad

NIVEL	DESCRIPCIÓN
Nada-1	Es de conocimiento público.
Poco-2	Puede ser de conocimiento público.
Algo-3	Es de conocimiento solo dentro de la organización
Bastante-4	Debe controlarse su difusión dentro de la organización.
Mucho-5	Debe ser accesible solo por aquellos que están autorizados.

Al calificar la Integridad (I), debe responderse a la pregunta: ¿Qué nivel de integridad tiene la información almacenada en el Activo?, considerando la tabla siguiente:

Tabla 11
Escala del nivel de integridad

NIVEL	DESCRIPCIÓN
Nada-1	No afecta a la organización si la información es dañada o destruida.
Poco-2	Afecta parcialmente a la organización por daño o destrucción de la información.
Algo-3	Paraliza parcialmente a la organización por daño o pérdida de la información.
Bastante-4	Paraliza los servicios críticos temporalmente por pérdida de la información
Mucho-5	Paraliza a la organización indefinidamente si la información es manipulaciones por terceros o dañada.

Para evaluar la Disponibilidad (D), debe responderse a la pregunta: ¿Qué nivel de disponibilidad tiene la información almacenada en el activo?, considerando:

Tabla 12

Escala del nivel de disponibilidad

NIVEL	DESCRIPCIÓN
Nada-1	No afecta a la organización si la información no está accesible.
Poco-2	Afecta parcialmente a la organización la falta de accesibilidad de la información.
Algo-3	Paraliza parcialmente a la organización por la falta de accesibilidad de la información.
Bastante-4	Paraliza los servicios críticos temporalmente por la falta de accesibilidad de la información.
Mucho-5	Paraliza a toda la organización indefinidamente si la información no es accesible para aquellos que estén autorizados.

La tasación de activos se realizará por cada activo del proceso crítico, detallando todos los activos involucrados, identificando al propietario y la categoría específica a la cual pertenece.

Las calificaciones se promedian y se obtiene una calificación única por activo, como se ejemplifica en la Tabla 13:

Tabla 13

Tasación de activos de un proceso crítico

Tasación de activos								
Proceso	**N**	**Activos**	**Categoría Específica**	**Propietario**	**Nivel de Impacto (1-5)**			
					C	**I**	**D**	**P**

Luego se selecciona solo los activos que promedien más 3.00, considerando que son críticos para la organización, es decir, al ser afectado negativamente podría impedir el correcto funcionamiento de las actividades de la empresa.

5.5.3 Actividad 3: Identificación de las amenazas

Es necesario analizar la existencia de amenazas que puedan explotar las vulnerabilidades de los activos identificados, así como el tipo de amenaza y el origen

El tipo de amenaza varía dependiendo de la naturaleza del activo.

Se considera el listado de la Tabla 14 como posibles vulnerabilidades y amenazas de acuerdo con la categoría general y específica del activo, considerando el contexto de las entidades del sector público.

Tabla 14

Lista de vulnerabilidades y amenazas de activos

CATEGORÍA GENERAL	CATEGORÍA ESPECÍFICA	AMENAZA	VULNERABILIDAD
Hardware	Equipo fijo	Errores de mantenimiento	Mantenimiento inadecuado
Hardware	Equipo fijo	Deterioro de soportes	Mantenimiento insuficiente
Hardware	Equipo fijo	Sustracción de información	Puertos USB habilitados
Hardware	Equipo fijo	Interrupción del suministro eléctrico	Susceptibilidad del equipamiento a alteraciones en el voltaje
Hardware	Equipo fijo	Contaminación	Susceptibilidad del equipamiento a la humedad y a la contaminación
Hardware	Equipo fijo	Descarga de un rayo	Susceptibilidad del equipamiento a la temperatura
Hardware	Equipo fijo	Fallas en equipos	Uso de equipamiento obsoleto
Hardware	Equipo transportable	Robo	Equipamiento móvil proclive para robar
Información	Información de alto costo	Código malicioso	Bases de datos con protección desactualizada contra códigos maliciosos
Información	Información de alto costo	Acceso no autorizado al sistema de información	Claves criptográficas accesibles a personas no autorizadas
Información	Información de alto costo	Uso no autorizado de materiales patentados	Copiado sin control
Información	Información de alto costo	Sustracción de información	Eliminación de soportes de almacenamiento sin borrado de datos
Información	Información estratégica	Sustracción de información	Información disponible para personas no autorizadas
Información	Información de alto costo	Destrucción de registros	Única copia, sólo una copia de la información
Información	Información estratégica	Sustracción de información	Nivel de confidencialidad no definido con claridad
Información	Información estratégica	Sustracción de información	Reglas criptográficas no definidas con claridad
Información	Información estratégica	Repudio o duplicidad de actividades	Reglas organizacionales no definidas con claridad
Información	Información estratégica	Acceso no autorizado al sistema de información	Reglas para control de acceso no definidos con claridad

Continúa

Información	Información estratégica	Sustracción de información	Reglas para trabajo afuera de las instalaciones no definidas con claridad
Información	Información estratégica	Incumplimiento en el mantenimiento del sistema de información	Requisitos para desarrollo de software no definidos con claridad
Organización	Autoridades	Incumplimiento de leyes	Inadecuada o falta de implementación de auditoría interna
Personal	Personal de operación	Huelgas	Empleados desmotivados o desconformes
Personal	Personal de operación	Fallas en equipos	Inadecuada capacidad de gestión
Personal	Personal de operación	Falla en los vínculos de comunicación	Inadecuada gestión de redes
Personal	Personal de operación	Fraudes	Inadecuada separación de tareas
Organización	Proveedores	Incumplimiento de relaciones contractuales	Inadecuada supervisión de proveedores externos
Personal	Personal de operación	Espionaje industrial	Inadecuada supervisión del trabajo de los empleados
Personal	Usuarios	Ingeniería social	Inadecuado nivel de conocimiento y/o concienciación de empleados
Personal	Usuarios	Fraudes	Inadecuados derechos de usuario
Redes	Medios y soportes	Escuchas encubiertas	Colocación de cables
Redes	Medios y soportes	Acceso no autorizado a la red	Redes accesibles a personas no autorizadas
Hardware	Equipo transportable	Interceptación de información	Conexiones de red pública sin protección
Sitio	Ambiente externo	Incendio	Ubicación susceptible a desastres naturales
Sitio	Servicios públicos	Inundación	Ubicación susceptible a pérdidas de agua
Sitio	Zona	Acceso físico no autorizado	Acceso no autorizado a instalaciones
Software	Aplicación específica del negocio	Revelación de contraseñas	Cuentas de usuario generadas por sistema en las que las contraseñas permanecen sin modificación
Software	Aplicación específica del negocio	Errores de aplicaciones	Elección inadecuada de datos de prueba
Software	Aplicación específica del negocio	Uso erróneo de sistemas de información	Falta de control en datos de entrada y salida
Software	Aplicación específica del negocio	Modificación accidental de datos del sistema de información.	Falta de separación de entornos de prueba y operativos
Software	Aplicación específica del negocio	Uso de códigos no autorizados o no probados	Falta de validación de datos procesados
Software	Aplicación específica del	Errores de aplicaciones	Inadecuado control de cambios

Continúa

	negocio		
Software	Aplicación específica del negocio	Modificación accidental de datos del sistema de información	Interfaz de usuario complicada
Software	Aplicación específica del negocio	Identidad de usuario camuflada	Sesiones activas después del horario laboral
Software	Aplicación específica del negocio	Deterioro de soportes	Sobre dependencia en un dispositivo o sistema
Software	Aplicación específica del negocio	Error de usuario	Software no documentado
Software	Aplicación específica del negocio	Fuga o revelación de información	Uso no controlado de sistemas de información
Software	Paquete de software	Contagio de virus	Falta de antivirus con licencia
Software	Paquete de software	Instalación no autorizada de software	Falta de inventario de licencias instaladas
Software	Sistema operativo	Sustracción de información	Contraseñas inseguras
Software	Sistema operativo	Daños provocados por actividades de terceros	Falta de desactivación de cuentas de usuario luego de finalizado el empleo
Software	Sistema operativo	Uso no autorizado de software	Sistemas desprotegidos ante acceso no autorizado
Software	Software de servicio	Contagio de virus	Descargas de Internet sin control

De acuerdo con el listado anterior, se elabora una lista de chequeo para ser aplicada en entrevistas al personal responsable de cada activo con el propósito de identificar los incidentes producidos por los activos vulnerables en el pasado. A continuación, un ejemplo de la Lista de Chequeo para registrar las vulnerabilidades encontradas.

Tabla 15

Lista de chequeo de vulnerabilidad y amenaza del activo

Lista de Chequeo				
Fecha				
Proceso				
Responsable				
Categoría General	Categoría Específica	Activo	Amenaza	Vulnerabilidad

5.5.4 Actividad 4: Identificación de los controles

Una o varias amenazas pueden ser neutralizadas con una correcta implementación de controles. Un control es un mecanismo manual o automático que permite mitigar el riesgo.

Se debe realizar el análisis de los controles implementados, por lo cual se realiza una lista de chequeo de controles.

La lista de chequeo se aplicará a los servidores públicos responsables de los activos a través de la entrevista y observación con el fin de identificar los eventos que podrían amenazar la continuidad de las actividades en la organización.

Es esencial mantener actualizadas las listas de chequeo para reflejar cambios en el ambiente de control de una organización.

La lista de chequeo detallada en la Tabla 16 se propone para identificar el estado del control: ineficaz, insuficiente e injustificado, para posteriormente considerar su reemplazo o eliminación. Además, se analiza el porcentaje de implementación.

Tabla 16

Lista de chequeo de controles existentes

Lista de Chequeo de Controles Existentes						
Fecha						
Proceso						
Activo						
Vulnerabilidad	Amenaza	Control Existente-% de Implementación	Estado			Observación
			Ineficaz	Insuficiente	Injustificado	

Además, es necesario conocer la evidencia y el porcentaje de implementación del control para las posteriores revisiones.

Una manera de ubicar y establecer el nivel de madurez que tiene un control o salvaguarda es a través de la clasificación que propone el Centro Criptológico Nacional del Manual de Usuario PILAR versión 4.3 como se detalla a continuación:

Tabla 17
Niveles de madurez de las salvaguardias

Nivel de madurez	Código	Descripción del nivel de madurez	Valoración numérica
Inexistente	L0	*Procedimiento:* No se realiza. *Elemento:* No se tiene. *Documento:* No se tiene.	0%
Inicial	L1	*Procedimiento:* Se está empezando a hacer, o sólo lo hacen algunas personas. *Elemento:* Se tiene, pero no se usa apenas. *Documento:* Se está preparando su elaboración.	10%
Reproducible pero intuitivo	L2	*Procedimiento:* Todos lo hacen igual, pero no está documentado. *Elemento:* Se tiene, pero se está terminando de afinar. *Documento:* Se está elaborando.	50%
Proceso Definido	L3	*Procedimiento:* Todos lo hacen igual y está documentado. *Elemento:* Se tiene y funciona correctamente. *Documento:* Se tiene.	90%
Gestionado y Medible	L4	*Procedimiento:* Se obtienen indicadores. *Elemento:* Se obtienen indicadores. *Documento:* Se obtienen indicadores.	95%
Optimizado	L5	*Procedimiento:* Se revisa el mismo y los indicadores, se proponen mejoras y se aplican. *Elemento:* Se revisa el mismo y los indicadores, se proponen mejoras y se aplican. *Documento:* Se revisa el mismo y los indicadores, se proponen mejoras y se aplican.	100%

Fuente: (Centro Criptológico Nacional, Guía de la seguridad de TIC, 2008)

5.5.5 Actividad 5: Identificación de las vulnerabilidades

Luego de identificada la lista de amenazas conocidas, la lista de activos y los controles existentes, se procede a identificar las vulnerabilidades que pueden ser explotadas por las amenazas A continuación, el formato de una lista de vulnerabilidades con relación a los activos y las amenazas.

Tabla 18
Lista de vulnerabilidades de los activos

Fecha				
Proceso				
Responsable				
Activo	**Categoría General**	**Categoría Específica**	**Amenaza**	**Vulnerabilidad**

. La lista de identificación de controles debe tener los estándares básicos de seguridad y ser utilizada para evaluar e identificar sistemáticamente las vulnerabilidades asociadas a los activos. Es importante identificar las vulnerabilidades que no tienen amenaza, debido a que puede cambiar su ambiente y surgir posteriormente amenazas no consideradas, por lo tanto, es importante el monitoreo constante.

5.6 Etapa 3: Estimación del riesgo

En esta etapa se valora la probabilidad de ocurrencia del riesgo y el impacto que puede producir.

5.6.1 Actividad 1: Valoración de la probabilidad de la amenaza

Se califica la probabilidad de que la amenaza explote la vulnerabilidad a través de un valor numérico comprendido en la escala definida en la Tabla 6. Además, es primordial considerar la existencia y eficiencia de controles que puedan mitigar la amenaza.

La siguiente tabla es parte del documento Evaluación de Riesgo de los Activos Críticos (Formato en Anexo 2) a continuación, se muestra una parte como ejemplo:

Tabla 19

Valoración de la probabilidad de la amenaza

ACTIVO DE INFORMACIÓN	VULNERABILIDAD	AMENAZA	PROBABILIDAD DE LA AMENAZA
Servidor Windows	Falta de antivirus	Contagio de virus	5

5.6.2 Actividad 2: Valoración del impacto de materializarse la amenaza

Considerando el previo análisis realizado a los activos con relación a los criterios. Se procede a calificar el impacto de la materialización de la amenaza en la organización de acuerdo con la escala de la Tabla 7, considerando las consecuencias que puede ocasionar en la institución.

A continuación, un fragmento del documento Evaluación de Riesgo de los Activos Críticos (Anexo 2), en el cual se califica el impacto.

Tabla 20
Valoración del impacto de materializarse la amenaza

ACTIVO DE INFORMACIÓN	PROBABILIDAD DE LA AMENAZA	IMPACTO DE MATERIALIZARSE LA AMENAZA
Servidor Windows	5	4

5.7 Etapa 4: Evaluación del riesgo

5.7.1 Actividad 1: Valoración del riesgo

Una vez valorado el impacto y la probabilidad de los incidentes, se realiza el producto de ambos para calcular el riesgo.

Es necesaria la actualización periódicamente del documento Evaluación de Riesgo de los Activos Críticos (Anexo 2), debido a la posible aparición de nuevos riesgos, así como el cambio en las actividades operativas, la realización de nuevas y la eliminación de otras.

Es importante que la valoración se realice cada 6 meses para mantener actualizado los riesgos tecnológicos de la institución.

A continuación, en la Tabla 21 se muestra parte del documento Evaluación de Riesgo de los Activos Críticos (Anexo 2), como ejemplo:

Tabla 21
Cálculo de riesgo

ACTIVO DE INFORMACIÓN	PROBABILIDAD DE LA AMENAZA	IMPACTO DE MATERIALIZARSE LA AMENAZA	NIVEL DEL RIESGO
Servidor Windows	5	4	20=MUY ALTO

5.7.2 Actividad 2: Identificación de riesgos críticos

Considerando el contexto de las entidades públicas se estipuló que se tratarán los riesgos considerados como Alto y Muy Alto.

5.7.3 Actividad 3: Selección de controles

El objetivo de implementar el control es la disminución de la probabilidad de la amenaza, por lo cual debe seleccionarse la opción más apropiada.

La organización deberá decidir sobre la implementación de las acciones a desarrollar. A continuación, se presenta en la Tabla 22 cuatro opciones de tratamiento de riesgos de acuerdo con la ubicación del riesgo en el mapa de calor, con el fin de facilitar la toma de decisiones. Las opciones de tratamiento que se le da a un riesgo son: mitigar, aceptar, evitar y transferir a un tercero.

Se identifica una opción de tratamiento de riesgos para cada uno de los riesgos considerados como inaceptables. A continuación, la tabla con los criterios para el tratamiento de riesgo, considerando el costo y beneficio del control. La actividad de selección de los controles requiere la participación de los dueños de la información de la entidad pública.

Tabla 22

Tratamiento del riesgo

Tratamiento	Descripción	Costo-Beneficio
Mitigar	A través de la implementación de controles eficientes.	El coste del tratamiento es adecuado a los beneficios.
Transferir	Compartir a través de la asociación con alguien	El coste del tratamiento por terceros es más beneficioso que el tratamiento directo.
Aceptar	Reconocer formalmente la existencia del riesgo	El nivel de riesgo está muy alejado del nivel de tolerancia.
Evitar	Eliminar el origen del riesgo, y así el riesgo	El coste del tratamiento es muy superior a los beneficios.

CAPÍTULO VI: VERIFICACIÓN DE LA GUÍA METODOLÓGICA PROPUESTA

6

6.1 Introducción

En el presente capítulo se implementa la guía metodológica propuesta de gestión de riesgo de TIC en una entidad pública de la ciudad de Esmeraldas con la finalidad validar cada una de las etapas definidas en el capítulo anterior. De acuerdo con las políticas de confidencialidad que posee la entidad colaboradora, no se permite la revelación del nombre de la organización, así como, los nombres de los responsables que participaron en el proyecto.

6.2 Etapa 1: Establecimiento del contexto

6.2.1 Actividad 1: Determinación del alcance

a) Estudio de la organización

Visión- La entidad del sector público tiene como visión liderar los procesos de desarrollo de la provincia, mediante la eficiente ejecución de sus competencias, con un amplio sentido de responsabilidad social y de respeto a la biodiversidad y pluriculturalidad presentes en su territorio.

Misión - Por otra parte, la misión es fomentar el desarrollo socio- económico de la provincia a través de servicios de calidad, la participación 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.

Objetivos:

- Impulsar procesos periódicos de fortalecimiento institucional y de mejoramiento de las capacidades administrativas, financieras y operativas.

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

b) Estudio del Área de TIC

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

Visión - La Dirección de Tecnologías de la Información se posicionará como referente nacional de calidad y mejora continua a través de la implementación del Gobierno Electrónico, creación de valor y conocimiento de la información para las autoridades y funcionarios que tienen que tomar decisiones y apoyar la gestión institucional.

Procesos y servicios

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

c) Alcance de la Gestión de Riesgo de TIC

De acuerdo con el ambiente público en el cual se desarrolla la entidad, se plantea el alcance del proceso de Gestión de riesgo de TIC como la evaluación de los procesos críticos que podrían detener la continuidad de los servicios públicos ofrecidos a la ciudadanía.

El proceso involucra:

- A todo el personal del área de TIC:
- Documentación presente en los procesos críticos.
- Infraestructura tecnológica que soporta los procesos críticos.
- Información generada a través de la infraestructura tecnológica.

d) Restricciones del alcance

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

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

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

6.2.2 Actividad 2: Selección de procesos críticos

Se consideró al proceso tecnológico al *Desarrollo e Integración de Sistemas* como el más crítico en el departamento de TIC, debido a que es fundamental para la continuidad de las actividades de la organización.

6.2.3 Actividad 3: Descripción de los criterios de evaluación

a) Criterios de evaluación de la probabilidad de ocurrencia de una amenaza

La estimación cualitativa utiliza la Tabla 6 como escala de atributos calificativos para describir la magnitud de las consecuencias potenciales.

b) Criterio de evaluación del impacto de la materialización de la amenaza

Para evaluar el impacto en el negocio de la organización, es necesario determinar las consecuencias que puede provocar la pérdida de la confidencialidad, integridad o disponibilidad de los activos. En la Tabla 7 se mantiene el mismo enfoque utilizado para la probabilidad de la amenaza.

El impacto nos indica las consecuencias de la materialización de una amenaza. El nivel de riesgo es una estimación de lo que puede ocurrir y se valora, de forma cuantitativa, como el producto del impacto, (consecuencia), asociado a una amenaza (suceso), por la probabilidad de la misma:

Riesgo=Impacto x Probabilidad

Los rangos de tolerancia al riesgo basados en la ponderación son los siguientes:

- Muy Bajo: Rango [1-2]
- Bajo: Rango [3-4]
- Medio: Rango [5-6-8-9]
- Alto: Rango [10-12-15-16]
- Muy Alto: Rango [20-25]

c) Criterio de apetito al riesgo

En la presente guía metodológica de gestión del riesgo de TI se estima como apetito al riesgo, aquellos riesgos que obtengan como resultado hasta el número 9, para los demás riesgos se consideraron no aceptable por lo tanto deben ser tratados a través de la implementación de un control.

6.3 Etapa 2: Identificación del riesgo

6.3.1 Actividad 1: Identificación de los activos

Se realizó la identificación de todos los activos dentro del proceso crítico; es decir, todos los activos que podrían ser afectados en los criterios de información: confidencialidad, integridad y disponibilidad. Se consideró activos como documentos en papel o en formato electrónico, aplicaciones y bases de datos, personas, equipos de TI e infraestructura. También se identificó a los propietarios.

6.3.2 Actividad 2: Tasación de los activos

A través de la entrevista realizada al responsable del proceso, se efectuó la calificación de los activos de acuerdo con los tres criterios de la información. Obteniendo una lista de los activos, a los cuales se le ejecutará el análisis de riesgos. La tasación de los activos se encuentra en la Tabla 23.

6.3.3 Actividad 3: Identificación de las amenazas.

Luego de identificar los activos, se establece de forma general las amenazas, el tipo de amenaza y su origen, de acuerdo con la Tabla 14 del capítulo anterior. El listado se encuentra en la Tabla 24.

6.3.4 Actividad 4: Identificación de los controles

Mediante la entrevista y observación se identificó los controles existentes para las amenazas. Se formularon las preguntas basándose en los controles propuestos por el EGSI. En base a la Tabla 17 y Tabla 16 se determinó el nivel de madurez que tiene el control implementado actualmente, así como su estado y una breve observación. Se realizó una lista de chequeo por cada activo para revisar los controles, la información se encuentra desde la Tabla 25 hasta la Tabla 38.

6.3.5 Actividad 5: Identificación de las vulnerabilidades

Luego de evaluar los controles se identificó las vulnerabilidades, la elaboración se encuentra en la Tabla 39.

Tabla 23
Resultado de la tasación de activos

Proceso	N	Activos	Categoría Específica	Propietario
Desarrollo y mantenimiento de software	A001	Data Center	Ambiente externo	Analista de Sistemas
	A002	Código ejecutable de sistema en producción	Código ejecutable	Analista de Sistemas
	A003	Código fuente de sistemas en producción	Código fuente	Analista de Sistemas
	A004	Copias de Respaldo de Base de datos	Copias de respaldo	Analista de Sistemas
	A005	Módulo de Administración de usuarios	Credenciales	Analista de Sistemas
	A006	Base de datos de prueba	Datos de prueba	Analista de Sistemas
	A007	Aplicaciones Desarrolladas	Desarrollo propio	Analista de Sistemas
	A008	Servidor Blade – IBM	Equipo fijo	Analista de Sistemas
	A009	Computador personal de desarrollo	Equipo fijo	Analista de Sistemas
	A010	Desarrollador de aplicaciones	Personal de operación	Analista de Sistemas
	A011	Contrato de Redes y Telecomunicaciones	Proveedores	Jefe de TIC
	A012	Registros de actividad de base de datos de producción	Registro de actividad	Analista de Sistemas
	A013	S.O. Windows Server 2003	Sistema operativo	Analista de Sistemas
	A014	Usuarios del Sistema integral	Usuarios	Analista de Sistemas

Tabla 24

Listado de activos con las amenazas generales

Fecha		**4 de septiembre de 2017**				
Proceso		Desarrollo y mantenimiento de software				
Responsable		Departamento de TIC				
Activo		**Categoría General**	**Categoría Específica**	**Amenaza**		**Tipo**
A001	Data Center	Sitio	Ambiente externo	**AM001**	Terremoto	Natural
				AM002	Acceso no autorizado a instalaciones	Humano
A002	Código ejecutable de sistema en producción	Datos	Código ejecutable	**AM003**	Errores de aplicaciones	Humano
A003	Código Fuente de sistemas en producción	Datos	Código fuente	**AM004**	Errores de aplicaciones	Humano
				AM005	Instalación no autorizada de software	Humano
A004	Copias de Respaldo de Base de datos	Datos	Copia de respaldo	**AM006**	Destrucción de registros	Humano/ Natural
				AM007	Sustracción de información	Humano
A005	Módulo de Administración de usuarios	Datos	Credenciales	**AM008**	Sustracción de información	Humano
				AM009	Acceso no autorizado al sistema de información	Humano
A006	Base de datos de Prueba	Datos	Base de datos de prueba	**AM010**	Destrucción de registros	Humano/Natural
				AM011	Errores de aplicaciones	Humano
				AM012	Sustracción de información	Humano
A007	Aplicaciones Desarrolladas	Software	Desarrollo propio	**AM013**	Sustracción de información	Humano
				AM014	Modificación accidental de datos del sistema de información.	Humano
				AM015	Uso erróneo de sistemas de información	Humano
				AM016	Revelación de contraseñas	Humano
				AM017	Errores de aplicaciones	Humano
				AM018	Error de usuario	Humano
				AM019	Incumplimiento en el mantenimiento del sistema de información	Humano
A008	Servidor tipo Blade-IBM	Hardware	Equipo fijo	**AM020**	Mantenimiento insuficiente	Humano
				AM021	Puertos USB habilitados	Humano

Continúa

				AM022	Susceptibilidad del equipamiento a la humedad y a la contaminación	Humano/Natural
				AM023	Uso de equipamiento obsoleto	Humano
A009	Computador personal de desarrollo	Hardware	Equipo fijo	**AM024**	Mantenimiento insuficiente	Humano
				AM025	Puertos USB habilitados	Humano
				AM026	Susceptibilidad del equipamiento a la humedad y a la contaminación	Humano/Natural
				AM027	Uso de equipamiento obsoleto	Humano
A010	Desarrollador de aplicaciones	Personal	Personal de operación	**AM028**	Fraudes	Humano
A011	Contrato de Adquisición de software	Personal	Proveedores	**AM029**	Incumplimiento de relaciones contractuales	Humano
A012	Registros de actividad de base de datos de producción	Datos	Registro de actividad	**AM030**	Errores de monitorización	Humano
A013	Windows-Server 2003	Software	Sistema operativo	**AM031**	Falta de desactivación de cuentas de usuario luego de finalizado el empleo	Humano
				AM032	Sistemas desprotegidos ante acceso no autorizado	Humano
				AM033	Contagio de virus	Humano
A014	Usuarios del Sistema integral	Personal	Usuarios	**AM034**	Fraudes	Humano

Tabla 25

Lista de chequeo de control del activo datacenter

Fecha	**5 de septiembre de 2017**								
Proceso	Desarrollo y mantenimiento de software								
Activo	A001 - Data Center								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V001	Ubicación susceptible a desastres naturales	AM001	Terremoto	¿Existe un centro alterno para el levantamiento de los procesos críticos?	0%	N/A	N/A	N/A	Presenta daños en las paredes del datacenter después del terremoto del 16 de abril de 2016. El personal no laboró en las instalaciones durante 8 meses hasta que el edificio se encontrara en un estado seguro para el personal.
V002	Acceso físico no autorizado	AM002	Acceso no autorizado a instalaciones	¿Existe un control de acceso físico al centro de datos?	50%	SI	NO	NO	El centro de datos tiene un sistema de acceso de mecanismo biométrico, el cual registra el acceso del personal, adicional la cámara ubicada frente a la puerta envía una fotografía al momento de apertura de la puerta y envía la información al correo del jefe de TIC. Sin embargo, no se pudo evidenciar el registro debido a que el responsable no recordaba la contraseña.

Tabla 26

Lista de chequeo de control del activo código ejecutable

Fecha	**5 de septiembre de 2017**								
Proceso	Desarrollo y mantenimiento de software								
Activo	A002 - Código ejecutable de sistemas en producción								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V003	Inadecuado control de cambios	AM003	Errores de aplicaciones	¿Existe un control de versiones para todas las actualizaciones de software?	0%	N/A	N/A	N/A	No se tiene

Tabla 27

Lista de chequeo de control del activo código fuente

Fecha	**5 de septiembre de 2017**								
Proceso	Desarrollo y mantenimiento de software								
Activo	A003-Código Fuente de sistemas en producción								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V004	Inadecuado control de cambios	AM004	Errores de aplicaciones	¿Existe evidencia de que los cambios se aplican a una copia y no directamente en el software original?	90%	SI	SI	SI	Se tiene y funciona correctamente. Sin embargo, el ambiente de prueba se encuentra en la computadora portátil del desarrollador.
V005	Única copia, sólo una copia de la información	AM004	Errores de aplicaciones	¿Existe almacenamiento seguro de las versiones del código	0%	N/A	N/A	N/A	No se tiene, se realiza un cambio sobre la última copia. Y el código

Continúa

				fuente como medida de contingencia?					fuente es guardado en la portátil del desarrollador y cada año saca un respaldo de su máquina. El respaldo es guardado en la maleta donde guarda el computador portátil.
V006	Falta de inventario de código fuente	AM005	Instalación no autorizada de software	¿Existe un único programa fuente relacionado a un programa objeto o ejecutable?	90%	NO	SI	NO	Existen 2 aplicaciones desarrolladas en el ambiente de prueba y varios archivos ejecutables en el ambiente de producción. Aunque el desarrollador dijo que se tenía una por cada aplicación en desarrollo.

Tabla 28

Lista de chequeo de activo copia de respaldo

Fecha	**5 de septiembre de 2017**								
Proceso	Desarrollo y mantenimiento de software								
Activo	A004 - Copias de Respaldo de Base de datos								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V007	Única copia, sólo una copia de la información	AM006	Destrucción de registros	¿Existe almacenamiento seguro de las copias de respaldo fuera de las instalaciones?	50%	NO	SI	NO	Se tiene, pero no se realiza una revisión de periódica para determinar si la copia esta correcta.
V008	Información disponible para personas no autorizadas	AM007	Sustracción de información	¿Existe solicitudes formales autorizadas por cada copia de seguridad del ambiente de producción?	0%	N/A	N/A	N/A	No se tiene, las copias se realizan sin un proceso formal.

Tabla 29

Lista de chequeo de activo módulo de administración de usuario

Fecha	**5 de septiembre de 2017**								
Proceso	Desarrollo y mantenimiento de software								
Activo	A005- Módulo de Administración de usuarios								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V009	Reglas criptográficas no definidas con claridad	AM008	Sustracción de información	¿Existen controles criptográficos para proteger las claves de acceso a los datos, sistemas y	0%	N/A	N/A	N/A	No se tiene

Continúa

				servicios?					
V010	Contraseñas inseguras	AM008	Sustracción de información	¿Existe un cifrado de las claves en la base de datos y/o archivos de parámetros?	90%	NO	NO	NO	Las claves almacenadas en la tabla de credenciales tienen encriptación.
V011	Claves criptográficas accesibles a personas no autorizadas	AM009	Acceso no autorizado al sistema de información	¿Existe un procedimiento para la administración de claves?	0%	N/A	N/A	N/A	No se tiene, el desarrollador desconoce la existencia del documento
V012	Reglas para control de acceso no definidos con claridad	AM009	Acceso no autorizado al sistema de información	¿Existen políticas sobre la administración de claves?	0%	N/A	N/A	N/A	No se tiene, el desarrollador desconoce la existencia del documento

Tabla 30

Lista de chequeo de activo base de datos ambiente prueba

Fecha	**5 de septiembre de 2017**								
Proceso	Desarrollo y mantenimiento de software								
Activo	A006-Base de datos de Prueba								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V013	Única copia, sólo una copia de la información	AM010	Destrucción de registros	¿Existe copias de seguridad de los datos de pruebas?	0%	N/A	N/A	N/A	No se tiene
V014	Elección inadecuada de datos de prueba	AM011	Errores de aplicaciones	¿Existe modificación o eliminación de los datos críticos extraídos del ambiente de	0%	N/A	N/A	N/A	No se tiene

Continúa

				producción al ambiente de prueba?					
V015	Información disponible para personas no autorizadas	AM012	Sustracción de información	¿Existe una revisión de datos de pruebas para utilizarse en los sistemas informáticos en desarrollo?	0%	N/A	N/A	N/A	No se tiene

Tabla 31

Lista de chequeo de activo aplicaciones desarrolladas

Lista de Chequeo de Controles Existentes									
Fecha	5 de septiembre de 2017								
Proceso	Desarrollo y mantenimiento de software								
Activo	A007- Aplicaciones Desarrolladas								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V016	Información disponible para personas no autorizadas	AM013	Sustracción de información	¿Existe un control de acceso físico y lógico al ambiente de producción?	90%	SI	NO	NO	El centro de datos tiene un sistema de acceso de mecanismo biométrico. Los sistemas operativos cuentan con clave y la base de datos también. El desarrollador realiza todo el proceso y paso
				¿Existe un control de acceso para el personal de desarrollo en el ambiente de producción?	0%	N/A	N/A	N/A	
				¿Existe control de acceso al entorno de desarrollo?	90%	SI	SI	NO	

Continúa

									a producción. El control de acceso es mediante usuario y contraseña sin embargo el ambiente de desarrollo está en la portátil del desarrollador
V017	Reglas criptográficas no definidas con claridad	AM013	Sustracción de información	¿Existen controles criptográficos en el envío de mensajes que contienen información reservada o confidencial? ¿Existen políticas sobre el uso de controles criptográficos?	0% 0%	N/A N/A	N/A N/A	N/A N/A	No se tiene No se tiene
V018	Contraseñas inseguras	AM013	Sustracción de información	¿Existen nuevas contraseñas en el ambiente de pruebas diferentes del ambiente de producción?	90%	N/A	N/A	N/A	Se tiene, pero no existe un política que permita controlar su cambio.
V019	Falta de separación de entornos de prueba y operativos	AM014	Modificación accidental de datos del sistema de información.	¿Existe un ambiente de prueba idéntico al ambiente de producción? ¿Existe un proceso para el paso a producción para los sistemas?	0% 0%	N/A N/A	N/A N/A	N/A N/A	No se tiene, El ambiente de prueba se encuentra en la portátil del desarrollador. No se tiene

Continúa

				¿Existe informe de paso a producción? ¿Existe informes de paso a pruebas previas? ¿Existe en el informe de producción un plan de contingencia?	0% 0%	N/A N/A	N/A N/A	N/A N/A	No se tiene No se tiene No se tiene
V020	Falta de control en datos de entrada y salida	AM015	Uso erróneo de sistemas de información	¿Existe protección en los datos utilizados en el ambiente de producción?	0%	N/A	N/A	N/A	No se tiene
V021	Cuentas de usuario generadas por sistema en las que las contraseñas permanecen sin modificación	AM016	Revelación de contraseñas	¿Existe funcionalidad en los sistemas para cambiar o actualizar claves, así como los usuarios que la utilizarán? ¿Existe funcionalidad en los sistemas para administrar las claves perdidas por parte de los usuarios?	90% 90%	NO NO	NO NO	NO NO	Existe el proceso de recuperación de clave, y también de generación de nueva contraseña, pero el segundo se realiza por medio de una solicitud al departamento de sistemas
V022	Inadecuado control de cambios	AM017	Errores de aplicaciones	¿Existe solicitudes de cambios por usuarios autorizados? ¿Existe notificación a los usuarios sobre los cambios realizados? ¿Existe revisión de	95% 95% 0%	NO NO N/A	SI SI N/A	NO NO N/A	A través del sistema de tickets Help Desk sin embargo, no se revisan los indicadores. La solicitud se imprime y es

Continúa

				los controles de integridad antes de realizar los cambios? ¿Existe un control de versiones para todas las actualizaciones de software?	0% 0%	N/A N/A	N/A N/A	N/A N/A	firmada por el usuario cuando se cierra, luego se archiva en una carpeta. No se tiene. No se tiene No se tiene
V023	Software no documentado	AM018	Error de usuario	¿Existe actualización en los manuales de usuario, así como en la operativa después de realizar un cambio?	0%	N/A	N/A	N/A	No se tiene
V024	Requisitos para desarrollo de software no definidos con claridad	AM019	Incumplimiento en el mantenimiento del sistema de información	¿Existe requisitos de seguridad que están incluidos en los requerimientos? ¿Existen políticas para el desarrollo seguro?	0% 0%	N/A N/A	N/A N/A	N/A N/A	No se tiene No se tiene

Tabla 32
Lista de chequeo de activo servidor IBM

Fecha	**5 de septiembre de 2017**								
Proceso	Desarrollo y mantenimiento de software								
Activo	A008- Servidor IBM								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V025	Deterioro de soportes	AM020	Mantenimiento insuficiente	¿Se realiza mantenimiento correctivo de los equipos de modo que asegure la continuidad de las actividades?	50%	NO	SI	NO	Se realiza mantenimiento de los proveedores de los equipos cada 2 años.
V026	Sustracción de información	AM021	Puertos USB habilitados	¿Existe un procedimiento para el manejo de medios removibles?	0%	N/A	N/A	N/A	No se tiene
V027	Interrupción del suministro eléctrico	AM022	Susceptibilidad del equipamiento a la humedad y a la contaminación	¿Se tiene implementado protecciones contra cortes de suministro de energía?	50%	NO	NO	NO	Si se tiene un sistema de energía que provee 4 horas si existe un corte de energía.
V028	Contaminación	AM022	Susceptibilidad del equipamiento a la humedad y a la contaminación	¿Se tiene implementado protecciones contra contaminación?	90%	NO	NO	NO	En el centro de datos se tiene un sistema contra incendio de gas adecuado para equipos electrónico.
V029	Descarga de un	AM022	Susceptibilidad del	¿Se tiene	90%	NO	SI	NO	En el centro de

Continúa

	rayo		equipamiento a la humedad y a la contaminación	implementado protecciones contra temperaturas altas?					datos se realizó una limpieza debido a los escombros del 16 de abril de 2016. Sin embargo, se evidencia daño en la infraestructura.
V030	Fallas en equipos	AM023	Uso de equipamiento obsoleto	¿Se realiza mantenimiento preventivo de los equipos de modo que asegure la continuidad de las actividades?	90%	NO	SI	NO	Se tiene un sistema de registro de incidentes que es manejado por el personal de operación.

Tabla 33

Lista de chequeo de activo computador de desarrollo

Fecha	**5 de septiembre de 2017**								
Proceso	Desarrollo y mantenimiento de software								
Activo	A009- Computador personal de desarrollo								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V031	Deterioro de soportes	AM024	Mantenimiento insuficiente	¿Se realiza mantenimiento correctivo de los equipos de modo que asegure la continuidad de las actividades?	90%	NO	SI	NO	Se realiza el mantenimiento por el personal del departamento.
V032	Sustracción de	AM025	Puertos USB	¿Existe un	0%	N/A	N/A	N/A	No se tiene

Continúa

	información		habilitados	procedimiento para el manejo de medios removibles?					
V033	Interrupción del suministro eléctrico	AM026	Susceptibilidad del equipamiento a la humedad y a la contaminación	¿Se tiene implementado protecciones contra cortes de suministro de energía?	50%	NO	SI	NO	Se tiene equipo UPS
V034	Contaminación	AM026	Susceptibilidad del equipamiento a la humedad y a la contaminación	¿Se tiene implementado protecciones contra contaminación?	0%	N/A	N/A	N/A	No se tiene
V035	Descarga de un rayo	AM026	Susceptibilidad del equipamiento a la humedad y a la contaminación	¿Se tiene implementado protecciones contra temperaturas altas?	0%	N/A	N/A	N/A	No se tiene
V036	Fallas en equipos	AM027	Uso de equipamiento obsoleto	¿Se realiza mantenimiento preventivo de los equipos de modo que asegure la continuidad de las actividades?	90%	NO	SI	NO	Se realiza el mantenimiento por el personal del departamento.

Tabla 34
Lista de chequeo de activo desarrollador

Fecha	**5 de septiembre de 2017**								
Proceso	Desarrollo y mantenimiento de software								
Activo	A010- Desarrollador de aplicaciones								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V037	Inadecuada separación de tareas	AM028	Fraudes	¿Existe un responsable de la implementación de cambios en el ambiente de producción que no pertenece al área de desarrollo o mantenimiento?	0%	N/A	N/A	N/A	No se tiene
				¿Existe un administrador de programas fuentes que no pertenece al área de desarrollo/mantenimiento?	0%	N/A	N/A	N/A	No se tiene

Tabla 35
Lista de chequeo de activo contrato de adquisición de software

Fecha	**5 de septiembre de 2017**								
Proceso	Desarrollo y mantenimiento de software								
Activo	A011- Contrato de Adquisición de software								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V038	Inadecuada supervisión de proveedores	AM029	Incumplimiento de relaciones contractuales	¿Existe acuerdos de licencia, acuerdos de uso, propiedad de código y derechos sobre software	0%	N/A	N/A	N/A	No se tiene
				desarrollado externamente?	0%	N/A	N/A	N/A	No se tiene
				¿Existe documentación donde se especifique los requerimientos contractuales?	0%	N/A	N/A	N/A	No se tiene
				¿Existe una verificación del cumplimiento de los requerimientos de seguridad de software?	0%	N/A	N/A	N/A	No se tiene

Tabla 36

Lista de chequeo de activo registro de actividad

Fecha	**5 de septiembre de 2017**								
Proceso	Desarrollo y mantenimiento de software								
Activo	A012- Registros de actividad de base de datos de producción								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V039	Inadecuada o falta de implementación de auditoría interna	AM030	Errores de monitorización	¿Existe registros de auditoria incorporados en la base de datos con un responsable de monitoreo?	0%	N/A	N/A	N/A	No se tiene

Tabla 37

Lista de chequeo de activo sistema operativo

Fecha	**5 de septiembre de 2017**								
Proceso	Desarrollo y mantenimiento de software								
Activo	A013- Windows-Server 2003								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V040	Daños provocados por actividades de terceros	AM031	Falta de desactivación de cuentas de usuario luego de finalizado el empleo	¿Existen políticas de administración de cuentas de usuario de las personas de operación?	0%	N/A	N/A	N/A	No se tiene
V041	Uso no autorizado de software	AM032	Sistemas desprotegidos ante acceso no autorizado	¿Existe cuentas de usuario en el sistema operativo?	90%	NO	SI	NO	Se tiene
V042	Descargas de Internet sin control	AM033	Contagio de virus	¿Existe sistema de antivirus licenciado y actualizado?	90%	NO	SI	NO	Si se tiene y se encuentra actualizado

Tabla 38
Lista de chequeo de activo usuario

Fecha	**5 de septiembre de 2017**								
Proceso	Desarrollo y mantenimiento de software								
Activo	A014- Usuarios del Sistema integral								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V043	Inadecuados derechos de usuario	AM034	Fraudes	¿Existe políticas para controlar los perfiles de sistemas asignados al personal?	0%	N/A	N/A	N/A	No se tiene

Tabla 39

Listado de vulnerabilidades del proceso

Fecha		**4 de septiembre de 2017**					
Proceso		Desarrollo y mantenimiento de software					
Responsable		Departamento de TIC					
Activo		**Categoría General**	**Categoría Específica**	**Amenaza**		**Vulnerabilidad**	
A001	Data Center	Sitio	Ambiente externo	**AM001**	Terremoto	**V001**	Ubicación susceptible a desastres naturales
				AM002	Acceso no autorizado a instalaciones	**V002**	Acceso físico no autorizado
A002	Código ejecutable de sistema en producción	Datos	Código ejecutable	**AM003**	Errores de aplicaciones	**V003**	Inadecuado control de cambios
A003	Código Fuente de sistemas en producción	Datos	Código fuente	**AM004**	Errores de aplicaciones	**V004**	Inadecuado control de cambios
						V005	Única copia, sólo una copia de la información
				AM005	Instalación no autorizada de software	**V006**	Falta de inventario de código fuente
A004	Copias de Respaldo de Base de datos	Datos	Copia de respaldo	**AM006**	Destrucción de registros	**V007**	Única copia, sólo una copia de la información
				AM007	Sustracción de información	**V008**	Información disponible para personas no autorizadas
A005	Módulo de Administración de usuarios	Datos	Credenciales	**AM008**	Sustracción de información	**V009**	Reglas criptográficas no definidas con claridad
						V010	Contraseñas inseguras
				AM009	Acceso no autorizado al sistema de información	**V011**	Claves criptográficas accesibles a personas no autorizadas
						V012	Reglas para control de acceso no definidos con claridad
A006	Base de datos de Prueba	Datos	Datos de datos de prueba	**AM010**	Destrucción de registros	**V013**	Única copia, sólo una copia de la información
				AM011	Errores de aplicaciones	**V014**	Elección inadecuada de datos de prueba
				AM012	Sustracción de información	**V015**	Información disponible para personas no autorizadas
A007	Aplicaciones	Software	Desarrollo	**AM013**	Sustracción de información	**V016**	Información disponible para

Continúa

	Desarrolladas		propio				personas no autorizadas
						V017	Reglas criptográficas no definidas con claridad
						V018	Contraseñas inseguras
				AM014	Modificación accidental de datos del sistema de información.	**V019**	Falta de separación de entornos de prueba y operativos
				AM015	Uso erróneo de sistemas de información	**V020**	Falta de control en datos de entrada y salida
				AM016	Revelación de contraseñas	**V021**	Cuentas de usuario generadas por sistema en las que las contraseñas permanecen sin modificación
				AM017	Errores de aplicaciones	**V022**	Inadecuado control de cambios
				AM018	Error de usuario	**V023**	Software no documentado
				AM019	Incumplimiento en el mantenimiento del sistema de información	**V024**	Requisitos para desarrollo de software no definidos con claridad
A008	Servidor tipo Blade-IBM	Hardware	Equipo fijo	**AM020**	Mantenimiento insuficiente	**V025**	Deterioro de soportes
				AM021	Puertos USB habilitados	**V026**	Sustracción de información
				AM022	Susceptibilidad del equipamiento a la humedad y a la contaminación	**V027**	Interrupción del suministro eléctrico
						V028	Contaminación
						V029	Descarga de un rayo
				AM023	Uso de equipamiento obsoleto	**V030**	Fallas en equipos
A009	Computador personal de desarrollo	Hardware	Equipo fijo	**AM024**	Mantenimiento insuficiente	**V031**	Deterioro de soportes
				AM025	Puertos USB habilitados	**V032**	Sustracción de información
				AM026	Susceptibilidad del equipamiento a la humedad y a la contaminación	**V033**	Interrupción del suministro eléctrico
						V034	Contaminación
						V035	Descarga de un rayo
				AM027	Uso de equipamiento obsoleto	**V036**	Fallas en equipos
A010	Desarrollador de aplicaciones	Personal	Personal de operación	**AM028**	Fraudes	**V037**	Inadecuada separación de tareas

A011	Contrato de Redes y Telecomunicaciones	Personal	Proveedores	**AM029**	Incumplimiento de relaciones contractuales	**V038**	Inadecuada supervisión de proveedores
A012	Registros de actividad de base de datos de producción	Datos	Registro de actividad	**AM030**	Errores de monitorización	**V039**	Inadecuada implementa interna
A013	Windows-Server 2003	Software	Sistema operativo	**AM031**	Falta de desactivación de cuentas de usuario luego de finalizado el empleo	**V040**	Daños provocados por actividades de terceros
				AM032	Sistemas desprotegidos ante acceso no autorizado	**V041**	Uso no autorizado de software
				AM033	Contagio de virus	**V042**	Descargas de Internet sin control
A014	Usuarios del Sistema integral	Personal	Usuarios	**AM034**	Fraudes	**V043**	Inadecuados derechos de usuario

Continúa

6.4 Etapa 3: Estimación del Riesgo

6.4.1 Actividad 1: Valoración de la probabilidad de la amenaza

Previamente, la organización determinó los criterios para aceptar los riesgos, así como las escalas en la actividad 3 de la etapa 1. Una vez identificado las amenazas, se evaluó las consecuencias para cada combinación de amenazas y vulnerabilidades de un activo específico.

Al tener un conocimiento de los controles existentes y las vulnerabilidades de los activos se procedió a calificar el riesgo de acuerdo con los criterios de evaluación desarrollados en el establecimiento del contexto.

6.4.2 Actividad 2: Valoración del impacto de materializarse la amenaza

Posteriormente se realizó la calificación del impacto y las consecuencias que pudieran surgir de la materialización de la amenaza. Se evaluó de acuerdo con la escala de la Tabla 6.

6.5 Etapa 4: Evaluación del Riesgo

6.5.1 Actividad 1: Valoración del riesgo

La valoración de los riesgos es el producto del impacto de la materialización de la amenaza y la probabilidad de que ocurra en la organización.

En la Tabla 40 se muestra el resultado de la evaluación del riesgo de los activos, de acuerdo con el cálculo cada riesgo se ubica en uno de los cinco grupos siguientes:

Resultado [1-2]: Muy Bajo

Resultado [3-4]: Bajo

Resultado [5-6-8-9]: Medio

Resultado [10-12-15-16]: Alto

Resultado [20-25]: Muy Alto

Tabla 40
Evaluación de riesgos de los activos

FECHA	**4 de septiembre de 2017**								
PROCESO	Desarrollo y mantenimiento de software								
RESPONSABLE	Departamento de TIC								
TIPIFICACIÓN RIESGO	**ACTIVO**		**VULNERABILIDAD**		**AMENAZA**		**PROBABILIDAD QUE LA AMENAZA EXPLOTE LA VULNERABILIDAD**	**IMPACTO DE MATERIALIZARSE LA AMENAZA**	**RIESGO DEL ACTIVO**
R1	**A001**	Data Center	V001	Ubicación susceptible a desastres naturales	AM001	Terremoto	3.0	5.0	15=Alto
R2			V002	Acceso físico no autorizado	AM002	Acceso no autorizado a instalaciones	1.0	3.0	3=Bajo
R3	**A002**	Código ejecutable de sistema en producción	V003	Inadecuado control de cambios	AM003	Errores de aplicaciones	5.0	5.0	25=Muy alto
R4	**A003**	Código Fuente de sistemas en producción	V004	Inadecuado control de cambios	AM004	Errores de aplicaciones	5.0	5.0	25= Muy alto
R5			V005	Única copia, sólo una copia de la información	AM004	Errores de aplicaciones	5.0	5.0	25= Muy alto
R6			V006	Falta de inventario de código fuente	AM005	Instalación no autorizada de software	2.0	3.0	6=Medio
R7	**A004**	Copias de Respaldo de Base de datos	V007	Única copia, sólo una copia de la información	AM006	Destrucción de registros	2.0	5.0	10=Alto
R8			V008	Información disponible para personas no autorizadas	AM007	Sustracción de información	2.0	3.0	6=Medio
R9	**A005**	Módulo de Administración de usuarios	V009	Reglas criptográficas no definidas con claridad	AM008	Sustracción de información	2.0	3.0	6=Medio
R10			V010	Contraseñas inseguras	AM008	Sustracción de información	3.0	5.0	15=Alto
R11			V011	Claves criptográficas accesibles a personas no autorizadas	AM009	Acceso no autorizado al sistema de información	3.0	3.0	9=Medio
R12			V012	Reglas para control de acceso no definidos con claridad	AM009	Acceso no autorizado al sistema de información	3.0	5.0	15=Alto
R13	**A006**	Base de datos de Prueba	V013	Única copia, sólo una copia de la información	AM010	Destrucción de registros	3.0	3.0	9=Medio
R14			V014	Elección inadecuada de datos de prueba	AM011	Errores de aplicaciones	3.0	1.0	3=Bajo
R15			V015	Información disponible para personas no autorizadas	AM012	Sustracción de información	3.0	5.0	15=Alto
R16	**A007**	Aplicaciones Desarrolladas	V016	Información disponible para personas no autorizadas	AM013	Sustracción de información	1.0	3.0	3=Bajo
R17			V017	Reglas criptográficas no definidas con claridad	AM013	Sustracción de información	5.0	3.0	15=Alto
R18			V018	Contraseñas inseguras	AM013	Sustracción de información	1.0	3.0	3=Bajo
R19			V019	Falta de separación de entornos de prueba y operativos	AM014	Modificación accidental de datos del sistema de información.	5.0	5.0	25=Muy Alto
R20			V020	Falta de control en datos de entrada y salida	AM015	Uso erróneo de sistemas de información	5.0	3.0	15=Alto
R21			V021	Cuentas de usuario generadas por sistema en las que las contraseñas permanecen sin modificación	AM016	Revelación de contraseñas	1.0	3.0	3=Bajo
R22			V022	Inadecuado control de cambios	AM017	Errores de aplicaciones	3.0	4.0	12=Alto
R23			V023	Software no documentado	AM018	Error de usuario	5.0	3.0	15=Alto
R24			V024	Requisitos para desarrollo de software no definidos con claridad	AM019	Incumplimiento en el mantenimiento del sistema de información	5.0	3.0	15=Alto
R25	**A008**	Servidor tipo Blade-IBM	V025	Deterioro de soportes	AM020	Mantenimiento insuficiente	2.0	3.0	6=Medio
R26			V026	Sustracción de información	AM021	Puertos USB habilitados	2.0	3.0	6=Medio

Continúa

R27			V027	Interrupción del suministro eléctrico	AM022	Susceptibilidad del equipamiento a la humedad y a la contaminación	1.0
R28			V028	Contaminación	AM023	Susceptibilidad del equipamiento a la humedad y a la contaminación	3.0
R29			V029	Descarga de un rayo	AM024	Susceptibilidad del equipamiento a la humedad y a la contaminación	1.0
R30			V030	Fallas en equipos	AM023	Uso de equipamiento obsoleto	1.0
R31	**A009**	Computador personal de desarrollo	V031	Deterioro de soportes	AM024	Mantenimiento insuficiente	1.0
R32			V032	Sustracción de información	AM025	Puertos USB habilitados	3.0
R33			V033	Interrupción del suministro eléctrico	AM026	Susceptibilidad del equipamiento a la humedad y a la contaminación	3.0
R34			V034	Contaminación	AM027	Susceptibilidad del equipamiento a la humedad y a la contaminación	1.0
R35			V035	Descarga de un rayo	AM028	Susceptibilidad del equipamiento a la humedad y a la contaminación	1.0
R36			V036	Fallas en equipos	AM027	Uso de equipamiento obsoleto	1.0
R37	**A010**	Desarrollador de aplicaciones	V037	Inadecuada separación de tareas	AM028	Fraudes	3.0
R38	**A011**	Contrato de Redes y Telecomunicaciones	V038	Inadecuada supervisión de proveedores	AM029	Incumplimiento de relaciones contractuales	3.0
R39	**A012**	Registros de actividad de base de datos de producción	V039	Inadecuada o falta de implementación de auditoría interna	AM030	Errores de monitorización	3.0
R40	**A013**	Windows-Server 2003	V040	Daños provocados por actividades de terceros	AM031	Falta de desactivación de cuentas de usuario luego de finalizado el empleo	3.0
R41			V041	Uso no autorizado de software	AM032	Sistemas desprotegidos ante acceso no autorizado	1.0
R42			V042	Descargas de Internet sin control	AM033	Contagio de virus	1.0
R43	**A014**	Usuarios del Sistema integral	V043	Inadecuados derechos de usuario	AM034	Fraudes	3.0

6.5.2 Actividad 2: Identificación de riesgos críticos

Para lograr identificar los riesgos críticos se priorizó aquellos que después de realizarse el cálculo se valorizaran en el grupo de Alto y Muy Alto, considerando que son riesgos que requieren de un tratamiento inmediato. En la siguiente figura se ubica cada riesgo de acuerdo con su evaluación.

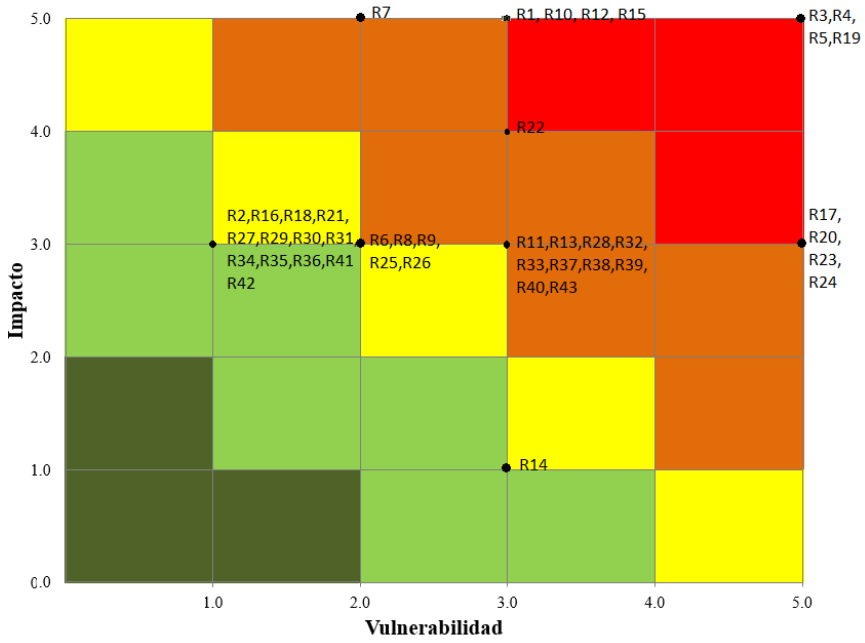

Figura 8: Mapa de calor de riesgos

De acuerdo con el apetito de riesgo establecido, se seleccionaron los siguientes riesgos:

- Muy altos: R3, R4, R5, R19
- Altos: R1, R10, R12, R15, R17, R20, R22, R23, R24

6.5.3 Actividad 3: Selección de controles

En virtud de lo expuesto se considera que existen varios riesgos relacionados a la falta de políticas, procedimientos y control en la gestión, que pueden afectar la efectividad, eficiencia, confidencialidad, integridad, disponibilidad y confiabilidad de la información que se procesa. Por

tanto, se sugiere trabajar en la implementación de controles que minimicen el riesgo de que se materialicen las vulnerabilidades anteriormente citadas. A continuación, se proponen los siguientes controles de acuerdo con el EGSI, el cual está basado en ISO 27002.

- Para asegurar la continuidad de las operaciones, se debe implementar adecuadamente un esquema y políticas de respaldos de información con los recursos que actualmente se disponen; con el fin de minimizar el impacto sobre la pérdida sustancial de información; a la vez empezar con la elaboración del Plan de Contingencias y Continuidad (R1).

- Se sugiere empezar a trabajar de manera urgente en un procedimiento formal de administración de cambios de sistemas, a fin de minimizar el riesgo de cambios no autorizados a los datos en el ambiente de producción (R3, R4, R22).

- Con el propósito de mejorar el control de respaldos, se recomiendan las siguientes acciones: establecer políticas de seguridad sobre los respaldos de información considerando cual es la información crítica que será respaldada, implementar un procedimiento para verificar la integridad de la información cuando se obtienen los respaldos, además llevar un registro de los respaldos obtenidos especificando el tipo de respaldo, la frecuencia, las fechas de respaldo y la ubicación de los mismo (R5, R10, R15).

- Para evitar la pérdida del código fuente de las aplicaciones desarrolladas, se recomienda implementar una metodología de desarrollo de software que tenga las fases mínimas: definición de necesidades, análisis y diseño de sistemas, desarrollo, pruebas, implantación y revisión posterior a la implantación. Las fases deben incluir: procedimientos de aprobación por parte de los usuarios, estándares de programación, políticas de entrenamiento a usuarios y procedimiento de paso a producción de las aplicaciones desarrolladas que contemple la implementación de un ambiente de prueba similar al ambiente de producción en los servidores del centro de datos. Además, se debe elaborar y archivar la correspondiente documentación (R12, R17, R19, R20, R23, R24).

CAPÍTULO VII: CONCLUSIONES Y RECOMENDACIONES

7

7.1 Conclusiones

- La familia ISO 27001 proporciona los requisitos para establecer, implementar, mantener y mejorar un SGSI basado en los criterios: integridad, disponibilidad y confiabilidad de la información en una organización. Por otro lado, la norma ISO 27005 dispone las directrices para realizar un análisis de riesgo más no una guía de implementación.

- Se evidenció que la incorporación de la normativa internacional en entidades públicas encuestadas. Sin embargo, todavía es un reto debido a que los estándares fueron creados para empresas de otro contexto. Por otro lado, existe el compromiso por parte de las entidades públicas en implementar controles y planes de seguridad para salvaguardar la información.

- La guía de gestión de riesgos de TIC propuesta está basada en la normativa ISO 27005 y aporta en detalle con múltiples formatos y escalas de evaluación para facilitar la identificación de los activos, sus vulnerabilidades, amenazas y controles.

- Se realizó la comprobación de la hipótesis, siendo positiva debido a, que la elaboración e implementación de la guía metodológica permitió mejorar la administración de la seguridad de la información en la entidad del sector público, porque permitió la identificación de controles que posteriormente serán implementados de acuerdo con los recursos disponibles en la institución.

7.2 Recomendaciones

- Es recomendable que las entidades públicas adopten la guía metodológica y la establezcan formalmente como un proceso del departamento tecnológico con la finalidad de mejorar continuamente.

- Debido al impacto cultural en el personal del área tecnológica que puede producirse al implementar la guía metodológica de gestión de riesgo de TIC, se recomienda la participación de los mismos durante las diferentes etapas, así como contar con la correspondiente comunicación de las medidas de tratamiento del riesgo a ser implementadas.

- Es recomendable que las organizaciones que adopten la guía, luego de realizar la correspondiente evaluación se realice un análisis de factibilidad tanto técnica como económica y así priorice en un plan de tratamiento de riesgos los controles a implantarse en corto, mediano y largo plazo, debido a la inversión económica que puede ser necesaria para mantener la seguridad de la información.

BIBLIOGRAFÍA

Carpentier, J.-F. (2016). *La seguridad informática en la PYME - Situación actual y mejores prácticas.* ENI. Recuperado el 10 de diciembre de 2016

Centro Criptológico Nacional, Guía de la seguridad de TIC. (2008). *Manual de Usuario PILAR versión 4.3.* Madrid: Centro Criptológico Nacional.

Comisión para la Seguridad Informática y de las Tecnologías de la Información. (2011). *Informe Final.* Quito. Obtenido de https://www.educarecuador.gob.ec/anexos/correo/Acuerdo_166.pdf

Consejo Profesional Nacional de Ingeniería de la República de Colombia. (4 de septiembre de 2014). *Consejo Profesional Nacional de Ingeniería Colombia de la República de Colombia.* Obtenido de Consejo Profesional Nacional de Ingeniería Colombia de la República de Colombia: https://copnia.gov.co/uploads/filebrowser/DCALIDAD/Normatividad/1.4%20POLITICA%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N.pdf

Contraloría General del Estado Ecuatoriano. (2009). *Contraloría General del Estado Ecuatoriano.* Recuperado el 1 de 11 de 2016, de Contraloría General del Estado Ecuatoriano: http://www.contraloria.gob.ec/documentos/informes/RendicionCuentas2013/index.html

Fernández Matute, R., & Monteros Montenegro, N. (2014). *Propuesta Metodológica para la gestión de riesgos tecnológicos en empresas proveedoras de servicios de telecomunicaciones.*

Gago González , L. (2 de marzo de 2006). *Aula TIC-PYMEs de la USC.* Obtenido de http://www.usc.es/atpemes/Guia-de-Autodiagnostico-para-Pymes

Gómez Vieites, Á. (2013). *Enciclopedia de la Seguridad Informática* (Segunda ed.). México D.F.: Alfaomega Grupo Editor. Recuperado el 2 de diciembre de 2016

INEN ISO/IEC 27001. (2017). *Tecnología de la Información-Técnicas de seguridad - Sistemas de gestión de la seguridad de la información- Requisitos.*

Instituto Ecuatoriano de Normalización. (2012). Recuperado el 5 de 11 de 2016, de Instituto Ecuatoriano de Normalización.

Instituto Nacional de Cibeseguridad de España. (14 de febrero de 2017). *INCIBE*. Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_0.pdf

ISO/IEC 27005. (2011). *Tecnología de la Información-Técnicas de Seguridad-Gestión de Riesgo en la Seguridad de la Información.*

Jaramillo, A. J. (2013). *"Propuesta de Gestión del Riesgo de Infraestructura Tecnológica Basada en COBIT, para la empresa SOFT WAREHOUSE S.A."*. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/6247/T-PUCE-6426.pdf?sequence=1&isAllowed=y

Morales Vallejo, P. (18 de Septiembre de 2007). *La fiabilidad de los tests y escalas.* Obtenido de https://matcris5.files.wordpress.com/2014/04/fiabilidad-tests-y-escalas-morales-2007.pdf

Piattini Velthuis, M. G., & del Peso Navarro, E. (2000). *Auditoría Informática: Un enfoque práctico.* Ra-Ma. Recuperado el 30 de noviembre de 2016

Prada Hernández, N. (2010). *Diseño de un sistema de gestión de seguridad de la información, alineado con la norma ISO/IEC 27002, para el área de tecnología de una empresa del sector financiero.* Pontificia Universidad Javeriana, Bogotá. Obtenido de http://pegasus.javeriana.edu.co/~CIS0830IS12/

Presidencia del Consejo de Ministros de la República del Perú. (8 de Enero de 2016). *Presidencia del Consejo de Ministros de la República del Perú.* Obtenido de Presidencia del Consejo de Ministros de la República del Perú: http://www.pcm.gob.pe/wp-content/uploads/2016/01/RM_N_04-2016-PCM.pdf

R. V., E. V., N. V., & F. C. (2014). *Repositorio Institucional de la Universidad de las Fuerzas Armadas ESPE.* Recuperado el 2 de noviembre de 2016, de Repositorio Institucional de la Universidad de las Fuerzas Armadas ESPE: http://repositorio.espe.edu.ec/bitstream/21000/9025/1/AC-MEAST-ESPE-048284.pdf

Secretaria Nacional de Administración Pública. (Septiembre de 2011). *Acuerdo Interiministeria 804.* Recuperado el 10 de Enero de 2017

Secretaria Nacional de Administración Pública. (2011). *Acuerdo Ministerial 166.* Obtenido de http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2015/04/PROYECTO-IMPLEMENTACION-CONTROL-Y-SEGUIMIENTO.pdf

Secretaria Nacional de Administración Pública. (Septiembre de 2013). Recuperado el 10 de Enero de 2017

Secretaria Nacional de la Administración Pública del Ecuador. (2014). *Proyecto: Implementación, control y seguimiento de la seguridad de la información en entidades de la administración pública central e institucional.* Quito. Recuperado el 04 de enero de 2017, de http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2015/04/PROYECTO-IMPLEMENTACION-CONTROL-Y-SEGUIMIENTO.pdf

Secretaria Nacional de Planificación y Desarrollo. (2013). *Empreasa Públicas y Planificación: Su rol en la transformación social y productiva.* Quito. Recuperado el 20 de febrero de 2017, de http://www.planificacion.gob.ec/wp-content/uploads/downloads/2014/02/Libro-Empresas-P%C3%BAblicas-web.pdf

ANEXOS

ANEXO 1 Encuesta para entidades del sector público

ANEXO 2 Formato de evaluación de riesgo de activos