UNIDAD ACADÉMICA:

DEPARTAMENTO DE INVESTIGACIÓN Y POSTGRADOS

TEMA:

DESARROLLO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN LAS NORMAS ISO 27002 PARA UNA COORDINACIÓN ZONAL DEL INEC

Proyecto de Investigación y Desarrollo de grado previo a la obtención del título de Magister en Gerencia Informática

Línea de Investigación, Innovación y Desarrollo principal:

Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus aplicaciones.

Caracterización técnica del trabajo:

Desarrollo

Autor:

Dorys Natalia Ledezma Espin

Director:

Mg. José Marcelo Balseca Manzano

Ambato – Ecuador

Diciembre 2015

Desarrollo de políticas de seguridad de la información basadas en las Normas ISO 27002 para una Coordinación Zonal del INEC

Informe de Trabajo de Titulación

presentado ante la

Pontificia Universidad Católica del Ecuador

Sede Ambato

Por:

Dorys Natalia Ledezma Espin

En cumplimiento parcial de los requisitos para el Grado de

Magister en Gerencia Informática

Departamento de Investigación y Postgrados

Diciembre 2015

Desarrollo de políticas de seguridad de la información basadas en las Normas ISO 27002 para una Coordinación Zonal del INEC

Aprobado por:

Varna Hernández Junco, PhD
Presidente del Comité Calificador
Director DIP

Enrique Garcés, Mg
Miembro Calificador

José Marcelo Balseca Manzano, Mg
Director de Proyecto

Dr. Hugo Altamirano Villaroel
Secretario General

Zandra Altamirano, Mg
Miembro Calificador

Fecha de aprobación:
Diciembre 2015

Ficha Técnica

Programa: Magister en Gerencia Informática

Tema: Desarrollo de políticas de seguridad de la información basadas en las Normas ISO 27002 para una Coordinación Zonal del INEC.

Tipo de trabajo: Proyecto de Investigación y Desarrollo

Clasificación técnica del trabajo: Desarrollo

Autor: Dorys Natalia Ledezma Espin

Director: Mg. José Marcelo Balseca Manzano

Líneas de Investigación, Innovación y Desarrollo

Principal: Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus aplicaciones.

Resumen Ejecutivo

Las instituciones que procesan grandes cantidades de información y comunicación, requieren de toda la seguridad posible para el cumplimiento de su gestión institucional y de servicio a la comunidad logrando la eficiencia, e integridad de la información y que ésta no sea modificada, dañada o eliminada por parte de terceras personas que acceden a la misma.

El objetivo principal del presente trabajo consiste en desarrollar políticas de seguridad de la información basadas en las normas ISO 27002 para una Coordinación Zonal del INEC, de manera que se permita garantizar la adecuada aplicación de las políticas, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información. El presente trabajo se enfocó en analizar los requerimientos necesarios sobre cómo se encuentra la información actual de la institución, para lo cual se realizaron entrevistas personales a personeros de la Coordinación Zonal 3 del INEC y luego se aplicó la metodología en cascada, que es la que más se adapta al presente trabajo de titulación.

Declaración de Originalidad y Responsabilidad

Yo, Dorys Natalia Ledezma Espin, portadora de la cédula de ciudadanía y/o pasaporte No. 0201814902, declaro que los resultados obtenidos en el proyecto de titulación y presentados en el informe final, previo a la obtención del título de Magister en Gerencia Informática, son absolutamente originales y personales. En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto, y luego de la redacción de este documento, son y serán de mi sola y exclusiva responsabilidad legal y académica.

Dorys Natalia Ledezma Espin
0201814902

Dedicatoria

Al culminar esta etapa de mi vida profesional la dedico con grata satisfacción a Dios por haberme dado vida y sabiduría.

A mis padres, mis abuelitos, mis tíos y todas las personas que de una u otra manera estuvieron presentes en mi formación académica, ya que han sido la fuente y base primordial de todo mi empeño y dedicación para seguir siempre hacia adelante.

Reconocimiento

Con pleitesía extiendo mi alta consideración y estima a la **PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO,** sus autoridades y docentes que con su paciencia, sabiduría y entusiasmo me permitieron adquirir nuevos conocimientos.

A mi Director de tesis el Mg. José Marcelo Balseca por su orientación y apoyo incondicional para poder desarrollar la presente investigación.

A mi familia de quienes siempre recibí apoyo e incentivación para culminar con éxito esta etapa de mi vida.

Resumen

En el presente trabajo de desarrollo, se identificó el problema relacionado con la inseguridad que existe en la Coordinación Zonal 3 del INEC, debido al fácil acceso de terceras personas a la información confidencial, no solo de la zonal sino también en el INEC a nivel nacional, lo que provoca que la información pueda ser cambiada o adulterada, causando grandes problemas económicos, administrativos y afectación a la sociedad en general. El objetivo principal del presente trabajo consistió en desarrollar Políticas de Seguridad de la Información Basadas en las Normas ISO 27002 para una Coordinación Zonal del INEC, de manera que se permita garantizar la adecuada aplicación de las normas y procedimientos, sobre las plataformas tecnológicas y los sistemas de información. La investigación se enfocó en analizar los requerimientos necesarios sobre cómo se encuentra la información actual de la institución, para lo cual se realizaron entrevistas personales a personeros de la Coordinación Zonal 3 del INEC y luego se aplicó la metodología de cascada, ya que es la que más se adapta al presente trabajo de titulación. El desarrollo de las políticas de seguridad de la información basadas en la norma ISO 27002 pretende asegurar la fidelidad de la información institucional y con la gestión de las Tecnologías de Información y Comunicación lograr que la institución pueda entregar información precisa, confiable y concisa a los usuarios internos y externos de la sociedad.

Palabras clave: Información, seguridad, políticas, normas, informática, tecnología, comunicación, desarrollo.

Abstract

In this development project a problem was identified with insecurity in the Zonal Coordinating Office 3 of INEC due to the easy access of third parties to confidential information, not only within the zone but also at a national level. Because of this, the information can be changed or altered, thus causing great financial and administrative problems as well as affecting the community in general. The main objective of this study was to develop information security policies based on ISO 27002 standards for the Zonal Coordinating Office of INEC so that it will be able to guarantee the adequate application of the standards and procedures regarding the technological platforms and information systems. The research focused on analyzing the necessary requirements for how the current information of the institution is found. For this reason, personal interviews were conducted with officials from the Zonal Coordinating Office 3 of INEC and later the waterfall methodology was applied since it best adapts to this thesis project. The development of information security policies based on ISO 27002 standards expects to ensure accuracy of the institution's information and together with the management of information and communication technologies achieve that the institution can issue precise, reliable and concise information to the internal and external users from the community.

Keywords: information, security, policies, standards, computer science, technology, communication, development.

Tabla de Contenidos

Lista de Tablas

Lista de Figuras

Capítulo 1

Introducción

El tema "Desarrollo de políticas de seguridad de la información basadas en las Normas ISO 27002 para una Coordinación Zonal del INEC", es un tema muy actual debido al auge de la tecnología y la información. En el Capítulo 1 se da un enfoque acerca del contenido de este tema y cuáles son las expectativas que se tuvieron para afrontar y solucionar el problema que se presentó en lo relacionado a la seguridad de la información, en el Capítulo 2 se trata sobre el planteamiento de la propuesta del trabajo, con una descripción del mismo, se formulan: la meta y los objetivos de la investigación, además la delimitación funcional, en el Capítulo 3 se realiza todo el marco teórico que sustenta toda la investigación, en el Capítulo 4 se establece la metodología usada en la investigación, aquí constan las entrevistas realizadas a personeros del departamento de tecnologías de información y comunicación, en el Capítulo 5 se determinan los resultados de la investigación y de manera especial el diseño de las políticas de seguridad de la información basadas en la norma ISO 27002 en las áreas que existe vulnerabilidad, en el Capítulo 6 se trata sobre las conclusiones y recomendaciones, para finalizar con los Apéndices, las Referencias Bibliográficas y el Resumen Final.

1.1. Presentación del trabajo

Dentro de las instituciones se producen grandes cantidades de información y comunicación, las cuales son herramientas imprescindibles para el cumplimiento de la gestión institucional e interinstitucional, por lo tanto éstas, deben cumplir con estándares de seguridad, que permitan la eficiencia, e integridad de la información y que ésta no sea modificada, dañada o eliminada por parte de terceras personas que acceden a la misma. La seguridad debe ser preservada dando cumplimiento a las políticas de seguridad de la información, las cuales fueron establecidas para resguardar la misma.

Lo que se pretende hacer es desarrollar políticas de seguridad de la información en la Coordinación Zonal 3 del INEC basadas en las normas ISO 27002, las cuales contemplan mejores prácticas en la

gestión de la institución, se podrá tener una adecuada protección de los activos físicos, información, software, recurso humano, identificar las amenazas, evaluar la vulnerabilidad, el posible impacto, satisfacer el conjunto de requisitos legales, estatuarios, regulatorios y contractuales para dar cumplimiento a los principios, objetivos y requisitos de la Institución, además se establecerán indicadores para determinar la adecuación de los controles y el logro de los objetivos de seguridad para dar cumplimiento de la norma ISO 27002 [1].

De acuerdo a investigaciones realizadas en relación al presente tema de investigación las políticas de seguridad que se implementan basadas en las normas ISO 27002, pretenden lograr la mayor seguridad posible para la información que es parte importante en muchas instituciones estudiadas, de manera que estas investigaciones dan luz a otro tipo de soluciones que se pretenden implantar con esta investigación.

La Coordinación Zonal 3 del INEC, como una institución encargada de procesar mucha información importante requiere cada vez más de las políticas de seguridad de la información, basadas en las normas ISO 27002, de manera que resulta bastante significativo el presente estudio a desarrollarse.

1.2. Descripción del documento

El Capítulo 1 es la Introducción a la presente investigación, en el Capítulo 2 se plantea la propuesta de trabajo. En el Capítulo 3 se aborda el Marco Teórico; en particular, la Sección 3.1 está dedicada a definiciones y conceptos, en tanto que la Sección 3.2 permite establecer el estado del arte. En el Capítulo 4 se presenta la Metodología; partiendo en (4.1.) con la etapa de Diagnóstico, en el (4.2.) se da a conocer los Métodos particulares aplicados, para llegar al punto (4.3.) sobre los materiales y herramientas usados en la investigación. El Capítulo 5 está dedicado a la Presentación y Análisis de los Resultados del trabajo. Las Conclusiones y Recomendaciones son materia del Capítulo 6.

El trabajo está complementado con los Apéndices y las referencias contenidas en el trabajo investigativo.

[1] ISO 27002. (2009). "Código de Práctica para la Gestión de la Seguridad de Información".

Capítulo 2

Planteamiento de la Propuesta de Trabajo

2.1. Información técnica básica

Tema: Desarrollo de políticas de seguridad de la información basadas en las Normas ISO 27002 para una Coordinación Zonal del INEC

Tipo de trabajo: Proyecto de Investigación y Desarrollo

Clasificación técnica del trabajo: Desarrollo

Líneas de Investigación, Innovación y Desarrollo

Principal: Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus aplicaciones.

2.2. Descripción del problema

Debido al fácil acceso de terceras personas a la información confidencial de instituciones gubernamentales como el INEC, se presta para que los datos informativos sean cambiados o adulterados provocando variaciones en la información, lo que causa, a su vez, problemas económicos y administrativos, incluso la sociedad en general puede ser afectada.

Por esta razón el Instituto Nacional de Estadística y Censos Coordinación Zonal 3 (INEC), como parte del órgano rector de la estadística nacional, es la institución responsable de resguardar todos los datos que genera. Es primordial mencionar que hasta la actualidad no se han establecido políticas ligadas a la seguridad de los sistemas informáticos, ambiente tecnológico, seguridad física de los equipos informáticos y recurso humano, en base al Acuerdo 166 de la Secretaria de Administración

Pública[2], por lo que el presente proyecto tiene como finalidad establecer las Políticas de Seguridad de Información según las normas ISO 27002.

2.3. Preguntas básicas

¿Por qué se origina? El fácil acceso de los usuarios a la información.

¿Qué lo origina? El fácil acceso a información confidencial de las instituciones gubernamentales por parte de personas que no están autorizadas a manejar este tipo de información, así como la no aplicación de las políticas de seguridad de la información que han sido establecidas para el efecto.

2.4. Formulación de meta

Desarrollar políticas de seguridad de la información basadas en las normas ISO 27002 para una Coordinación Zonal 3 del INEC, que garanticen la emisión de datos confiables y seguros.

2.5. Objetivos

2.5.1. Objetivo general

Desarrollar políticas de seguridad de la información basadas en las normas ISO 27002 para una Coordinación Zonal 3 del INEC.

2.5.2. Objetivos específicos

1. Analizar los requerimientos necesarios en base a cómo se encuentra la información actual.

[2] Publicado en el Registro Oficial Suplemento 88 de 25-sep-2013

2. Aplicar políticas de seguridad de información basadas en normas técnicas ecuatorianas INEN ISO/IEC 27002.

3. Garantizar la adecuada aplicación de las políticas, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

2.6. Delimitación funcional

Pregunta 1. ¿Qué será capaz de hacer el producto final del proyecto de titulación?

1. Definir políticas de seguridad de información que permitan controlar la gestión de la seguridad de la información.

2. Minimizar los riesgos y amenazas a las cuales se encuentra inmersa la institución mediante las Normas Técnicas Ecuatorianas ISO 27002.

3. Mejora de los procesos y procedimientos de gestión de la información.

4. Determinar las políticas de seguridad para gestión de incidentes en las actividades administrativas por eventos adversos.

Pregunta 2. ¿Qué no será capaz de hacer el producto final del proyecto de titulación?

1. Los usuarios no podrán modificar o agregar nuevas políticas al proceso sin previa autorización del comité técnico.

2. Esta normativa se aplica únicamente a empresas o instituciones que manejen volúmenes altos de información, es decir lo que se denomina *Big Data*, (Datos masivos). "Por la simple denominación usada se entiende que se trata de grandes volúmenes de información que no es sencillo tratar con las herramientas y

procedimientos tradicionales. Encierra esta idea el tratamiento de información que hace evolucionar los métodos y recursos habituales para hacerse cargo de grandes volúmenes de datos (de *terabytes* pasamos a *zetabytes*)".[3]

[3] Carrillo, A. y otros. "Big Data en los entornos de Defensa y Seguridad". Instituto Español de Estudios estratégicos. (IEEE). España. (p. 7).

Capítulo 3

Marco Teórico

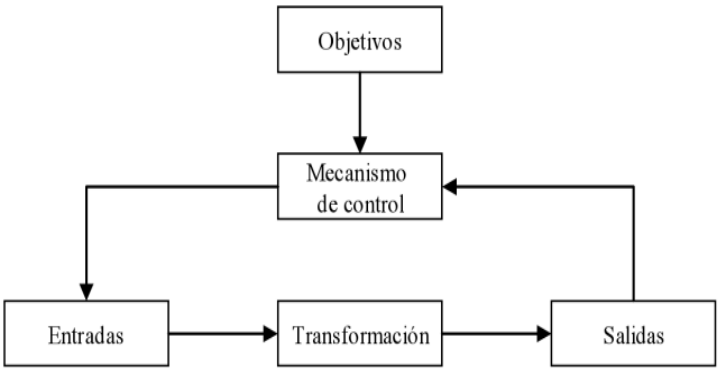
3.1. Definiciones y conceptos

3.1.1. Sistema

Para entrar en el estudio de los sistemas informáticos, se requiere primeramente definir lo que es un sistema, para lo cual se toma en cuenta la siguiente referencia:

> Un *sistema* es un conjunto de componentes que interaccionan entre sí para lograr un objetivo común. Aunque existe una gran variedad de sistemas, la mayoría de ellos pueden representarse a través de un modelo formado por cinco bloques básicos: elementos de entrada, elementos de salida, sección de transformación, mecanismos de control y objetivos. Tal y como muestra la figura 1.1, los recursos acceden al sistema a través de los elementos de entrada para ser modificados en la sección de transformación, Este proceso es controlado por el mecanismo de control con el fin de lograr el objetivo marcado. (Fernández, V., 2006, p. 11).

1: Modelo general de un sistema



Fuente: Fernández, V., 2006 (p. 11)

El avance de la tecnología contribuye de manera importante en la evolución y desarrollo de la información y la comunicación, los cuales al ser manejados por el potencial humano forman parte de los sistemas que los procesan así que estos sistemas también evolucionan posibilitando el desarrollo de las empresas.

3.1.1.1. Sistemas informáticos

Los sistemas de información también conocidos como sistemas informáticos, deben estar debidamente organizados y controlados para lograr el objetivo principal de la Coordinación Zonal 3 del INEC que es el de entregar información lo más clara posible. Al respecto, se afirma que:

> Un sistema de información será eficaz si facilita la información necesaria para la organización, y será eficiente si lo realiza con los menores recursos tecnológicos, humanos y económicos posibles, y en el momento oportuno.
>
> Por otro lado, el sistema informático de la empresa es un subsistema dentro del sistema de información de la misma, y está formado por todos los recursos necesarios para dar respuesta a un tratamiento automático de la información y aquellos otros que posibiliten la comunicación de la misma. En definitiva, por tecnologías de la información y de las comunicaciones (TIC).
>
> Por medio de la comunicación se transforman los hechos y acontecimientos del entorno o del ámbito interno de la empresa en información. (Heredero, C. y otros, 2006, p. 34).

3.1.1.2. Evolución de los Sistemas informáticos

En instituciones que generan grandes cantidades de información como lo es la Coordinación Zonal 3 del INEC, debe adaptarse a la evolución de los sistemas informáticos. Para comprender mejor esta evolución se hace referencia a lo siguiente:

> La segunda cualidad, la evolución tecnológica, debe asegurar que el sistema sea capaz de evitar que las modificaciones que se produzcan debido a los avances tecnológicos sean incompatibles con la estructura existente, asegurando de este modo que actualizar y mejorar componentes del sistema sea posible sin variar la estructura lógica. Por ejemplo, reemplazar un componente

> de almacenamiento de información por otro más moderno, sin que ello implique tener que modificar la información. La capacidad de evolución no se refiere solamente a los dispositivos físicos, sino también a los elementos lógicos, permitiendo cambiar los requisitos de información de acuerdo a las necesidades. La idea básica es la reusabilidad de partes, separando la gestión y control del sistema lógico dc su implementación física para aislar los impactos de cualquier cambio. (Sánchez, J., 2003, p. 27)

Actualmente los sistemas informáticos y en sí la información y comunicación se hallan en etapas de madurez, lo que les permite adaptarse más eficientemente a los constantes cambios tecnológicos actuales. Este desarrollo se da igualmente en los componentes de los sistemas de información.

3.1.1.3. El sistema informático y el potencial humano

Uno de los componentes más importantes dentro de un sistema informático es el potencial humano es decir las personas que son quienes deben asegurar el procesamiento de dicha información, en relación a lo mencionado, se dice que:

El primer componente que se analiza, que es el más importante, es el formado por las personas Según Whitten, Bentley y Dittmam (2004) todos los individuos que pueden y deben participar en el desarrollo de un sistema de información se pueden clasificar en función de la visión que tienen de un sistema de información. En este caso, la clasificación está formada por cinco grandes grupos: Propietarios, usuarios, diseñadores, constructores y Analistas (Fernández, V., 2006, pp. 15-20).

Los sistemas informáticos, como parte fundamental de la Coordinación Zonal 3 del INEC, deben ser precautelados en relación a los riesgos a los que puedan estar expuestos y con ello provocar graves pérdidas de información importante.

3.1.2. Riesgos de los Sistemas Informáticos

Como ya se ha mencionado, los sistemas informáticos de las instituciones encargadas de proveer información, como lo es la Coordinación Zonal 3 del INEC, están siendo susceptibles de ser afectados

por varios tipos de amenazas, es por esto que se trata a continuación sobre los riesgos que corren estos sistemas:

> En función de lo anterior, podemos aseverar que los riesgos informáticos se refieren a la incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos como por ejemplo los equipos informáticos, periféricos, instalaciones, proyectos, programas de cómputo, archivos, información, datos confidenciales, responsabilidad civil que éstos ocasionan frente a terceros por la prestación de un servido informático, etcétera. (Téllez, J., 1988, p.33)

3.1.2.1. Tipos de riesgos

Existen algunos tipos de riesgos que corren los sistemas informáticos y para los cuales los responsables del manejo de la información deben tomar acciones para corregirlos, los riesgos se pueden clasificar de la siguiente manera: "Respecto a los equipos, respecto a los programas, respecto a las personas, y respecto a los trabajos" (Téllez, J., 1988, p. 35).

3.1.2.2. Definición

Vale la pena definir los riesgos que corren los sistemas informáticos con la idea de conocer a fondo su origen y así poder eliminarlos, para garantizar la recepción de datos informativos de la mejor manera posible, al respecto se menciona que: "Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma" (Aguilera, P., 2010, p. 14).

Así mismo es la responsabilidad de los directores de la Coordinación Zonal 3 del INEC, tomar en cuenta la aparición de estos riesgos y actuar al respecto, de esta manera: "Ante un determinado riesgo, una organización puede optar por tres alternativas distintas:

1. Asumirlo sin hacer nada. Esto solamente resulta lógico cuando el perjuicio esperado no tiene valor alguno o cuando el coste de aplicación de medidas superaría al de la reparación del daño.
2. Aplicar medidas para disminuirlo o anularlo.
3. Transferirlo (por ejemplo, contratando un seguro)". (Aguilera, P., 2010, p. 14).

Existen varios mecanismos de cómo afrontar estos riesgos y uno de los más importantes es la implementación de políticas de seguridad que reduzcan o anulen estas amenazas para la información.

Los riesgos tiene relación con acontecimientos como son las vulnerabilidades, los ataques a la información, la materialización de las amenazas, que todo esto puede ser: "directo o indirecto, si se produce desde el atacante al elemento 'víctima' directamente, o a través de recursos o personas intermediarias" (Aguilera, P., 2010, p. 14).

Como se mencionó antes, dentro de los riesgos que corren los sistemas informáticos de la Coordinación Zonal 3 del INEC, es necesario referirse a lo que son las amenazas para los mismos.

3.1.2.3. Amenazas

Las amenazas siempre estarán presentes en los sistemas informáticos debido a la fragilidad que muchos de éstos presentan y se lo puede definir de la siguiente manera:

> En sistemas de información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que — de tener la oportunidad — atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad. Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde las físicas como cortes eléctricos, fallos del hardware o riesgos ambientales hasta los errores intencionados o no de los usuarios, la entrada de software malicioso (virus, troyanos, gusanos) o el robo, destrucción o modificación de la información. (Aguilera, P., 2010, p. 13).

3.1.2.4. Impactos

Al respecto de lo que son los impactos y las consecuencias que puede ocasionar, se puede mencionar que: “Son la consecuencia de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema o, dicho de otra manera, el daño causado. Los impactos pueden ser cuantitativos, si los perjuicios pueden cuantificarse económicamente, o cualitativos, si suponen daños no cuantificables, como los causados contra los derechos fundamentales de las personas” (Aguilera, P., 2010, p. 15).

Todos los riesgos mencionados pueden suceder dentro de los sistemas informáticos de la Coordinación Zonal 3 del INEC, por lo que se deben tomar las respectivas precauciones para proteger la información.

3.1.3. Gestión de riesgos

> El análisis y gestión de riesgos es un método formal para investigar los riesgos de un SI y recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos. A su vez es una salvaguarda preventiva que intenta buscar ordenadamente otras salvaguardas para proteger el SI.
>
> El análisis de riesgos introduce un enfoque riguroso y consecuente para la investigación de los factores que contribuyen a los riesgos. En general implica la evaluación del impacto que una violación de la seguridad tendría en la empresa; señala los riesgos existentes, identificando las amenazas que afectan al sistema informático; y la determinación de la vulnerabilidad del sistema a dichas amenazas. Su objetivo es proporcionar una medida de las posibles amenazas y vulnerabilidades del sistema de manera que los medios de seguridad puedan ser seleccionados y distribuidos eficazmente para reducir al mínimo las posibles pérdidas. (Heredero, Carmen de P. y otros, 2006, p. 180).

La gestión de riesgos, como se manifiesta es el método más adecuado para enfrentar ciertas amenazas y por lo tanto es imprescindible que la institución siga lineamientos de medidas preventivas con el fin de llegar a proteger la información en la Coordinación Zonal 3 del INEC.

3.1.4. Seguridad de los Sistemas Informáticos

La seguridad en los sistemas informáticos, debe ser encaminada a garantizar la efectividad en la entrega de la correcta información por parte de la Coordinación Zonal 3 del INEC al usuario final. Se clarifica la definición de la seguridad en los sistemas informáticos en la siguiente referencia:

> Las definiciones clásicas sobre seguridad informática tienden a alinearse en dos direcciones, una más instrumental y otra más funcional. Tomando acepciones literales, una definición más bien instrumental sería «conjunto de técnicas y procedimientos que garantizan tanto el rendimiento como la eficacia de un sistema informático»; mientras que otra definición más funcional sería «propiedad del sistema de información que permite que los usuarios pongan una confianza justificada en la calidad del servicio que les ofrece» (Heredero, C., 2006, p.172).

Las técnicas y procedimientos que se señala en la cita son efectivas, siempre y cuando, se las ponga en práctica, por lo tanto es necesario analizar cómo se las puede aplicar, para lo cual es importante referirse a las prácticas de seguridad de los sistemas informáticos.

3.1.5. Prácticas de seguridad de los Sistemas Informáticos

Las prácticas de seguridad de los sistemas informáticos, como su nombre lo indica son actividades permanentes encaminadas a mantener la seguridad de la información dentro de la Coordinación Zonal 3 del INEC, es por esto que se hace referencia a los siguientes lineamientos: "los aspectos importantes en materia de prevención, radica en configurar el sistema operativo para hacerlo más seguro. Entre las buenas prácticas que se pueden tener en cuenta se encuentran:

- ✓ Deshabilitar las carpetas compartidas.
- ✓ Utilizar contraseñas fuertes.
- ✓ Crear un perfil de usuario con privilegios restringidos.
- ✓ Deshabilitar la ejecución automática de dispositivos USB.
- ✓ De ser posible, migrar hacia plataformas (sistemas operativos) modernas.

- ✓ Configurar la visualización de archivos ocultos ya que la mayoría de los códigos maliciosos se esconden en el sistema con este tipo de atributos.
- ✓ Configurar la visualización de las extensiones de archivos para poder identificar las extensiones de los archivos descargados y no ser víctimas de técnicas como la doble extensión" (Mieres, J., 2009, p. 5).

Las prácticas de seguridad que ejerza la Coordinación Zonal 3 del INEC, serán aún más efectivas al estar inmersos dentro de la gestión de seguridad de los Sistemas Informáticos.

3.1.6. Gestión de seguridad de los Sistemas Informáticos

Dentro de la gestión de seguridad de los Sistemas Informáticos, se deben establecer ciertas herramientas que ayudaron a que la Coordinación Zonal 3 del INEC tenga mejores resultados, en la gestión de seguridad, se puede establecer:

1. Política de seguridad
2. Auditoría
3. Plan de contingencias

El plan de contingencias consta de tres subplanes independientes:

- ✓ Plan de respaldo.
- ✓ Plan de emergencia.
- ✓ Plan de recuperación.

4. Modelos de seguridad

En relación a las funciones u operaciones sobre las que se ejerce mayor control se puede clasificar los modelos de seguridad en tres grandes grupos;

- ✓ ***Matriz de acceso.*** Este modelo considera tres elementos básicos; sujeto, objeto y tipo de acceso.

- ✓ ***Acceso basado en funciones de control (RBAC –Role Access Base Control–).*** Puede considerarse una modalidad del de matriz de acceso, pero, en este caso, el acceso no se define en función de quién es el sujeto, sino de qué función tiene.

- ✓ ***Multinivel.*** Este modelo se basa en la jerarquización de los datos (todos los datos son importantes pero unos son más privados que otros. (Aguilera, P., 2010, pp. 21-24).

El componente principal de los sistemas informáticos es la información, la cual debe ser manejada responsablemente por todos involucrados en este proceso, es por lo tanto necesario el análisis respectivo de la misma.

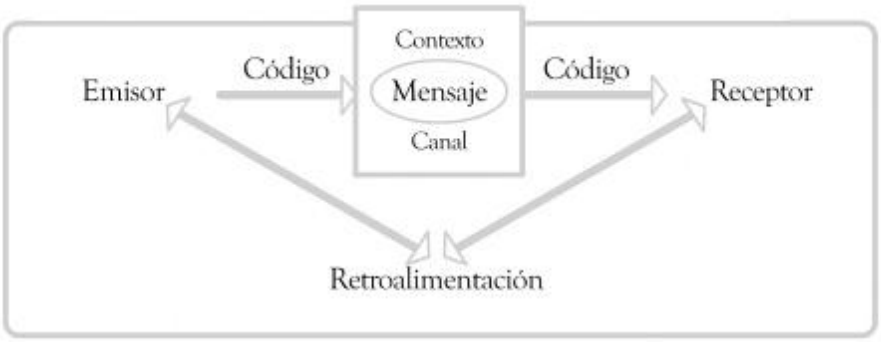
3.1.7. Información

Las instituciones que manejan grandes volúmenes de información deben tener en cuenta que esta debe ser lo más clara posible ya que permiten a los usuarios de los sistemas la correcta toma de decisiones, es así que la Coordinación Zonal 3 del INEC debe procurar el mejor manejo de la información, al respecto, se menciona que:

> Por otra parte, la tecnología de la información, también llamada informática, es la ciencia que estudia las técnicas y procesos automatizados que actúan sobre los datos y la información. La palabra "informática" proviene de la fusión de los términos "información" y "automática", lo que originalmente significaba la realización de tareas de producción o de gestión por medio de máquinas (autómatas). (Suárez y Alonso, R., 2007, p. 3).

El proceso por el cual el mensaje o la información son transmitidos entre el emisor y el receptor, se refleja en el siguiente gráfico:

2: Proceso de la información



Fuente: (Suárez y Alonso, R., 2007, p. 3).

3.1.7.1. Definición de información

"Información es la medida de la probabilidad de intercambio de mensajes entre emisores y receptores humanos en el ámbito social, dado el condicionamiento de la realidad social a la infraestructura material y técnica". (Monsalve, A., 2003, p. 52).

La información que se maneja en la Coordinación Zonal 3 del INEC está relacionada con la realidad social de los receptores, por lo que es necesario tratar sobre la seguridad de la información.

3.1.8. Seguridad de la información

Tomando en cuenta la importancia que tiene la información para instituciones como la Coordinación Zonal 3 del INEC, hay que referirse a la seguridad que debe tener la información para garantizar su confiabilidad, es por esto que:

> La seguridad informática, o de forma más global, la seguridad en los sistemas de información, representa el conjunto de medios y técnicas implementados para asegurar la integridad y que no se difundan involuntariamente los datos que recorren el sistema de información, entendiendo como tal al conjunto de datos y de recursos (físicos, lógicos y humanos) que permiten almacenar y que circule la información que contiene. También representa la red de

actores que intervienen sobre éste, que intercambian datos, acceden a ellos y los usan. (Agé, M. y otros, 2013, p. 19).

La seguridad de la información depende de la forma como se manejen los datos y los equipos, y es ahí donde radica la importancia que tiene dentro de la institución las normas de seguridad que se establezcan. Existen ciertos tipos de seguridad, que se detalla a continuación.

3.1.8.1 Tipos de seguridad

Al respecto se menciona que existe dos tipos de seguridad de la información, como sigue: **"Activa:** Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema. **Pasiva:** Está formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema" (Aguilera, P., 2010, p. 10).

La seguridad es requerida principalmente para proteger todos los datos informativos emanados por instituciones como la Coordinación Zonal 3 del INEC, es necesario que la información sea lo más fiable posible, ya que está al servicio de la colectividad.

3.1.8.2 Importancia de la seguridad de la información

El desarrollo de las políticas de seguridad de la información, basadas en las Normas ISO 27002 para una Coordinación Zonal 3 del INEC, lleva a considerar la importancia de la aplicabilidad de seguridades de la información, de esta manera:

> Con el famoso 'todo disponible para todos y a la vez', el transporte de datos fuera de casa o de la empresa es una realidad en la que vale la pena cuestionar la seguridad de las transmisiones para no comprometer al sistema de información.
>
> Ya sea a nivel de empresa, de multinacional, de un usuario privado o incluso dc un país, la seguridad de un sistema de información adquiere una importancia proporcional al valor de los datos que contiene.

> En el despliegue de una red, no sólo hay que enfrentarse con el problema del aumento de la cantidad, sino también, y sobre todo, con la importancia de los datos que la recorren. (Agé, M. y otros, 2013, p. 19).

Además de los criterios expresados por el autor antes citado, se toma en cuenta otros criterios relacionados con la importancia de la seguridad de la información:

> Como casi siempre en el mundo de la Seguridad de la Información, la solución a los problemas planteados no podemos basarla en una herramienta o tecnología a utilizar, sino en una serie de políticas, procedimientos y buenas prácticas que, apoyándose en las distintas tecnologías, nos permita mejorar el nivel de protección de nuestra información sensible, sin olvidar que toda esta gestión se apoya también en el eslabón humano.
>
> Una vez más, llegamos a la conclusión de que la Seguridad de la Información es un proceso en el que debemos combinar distintas medidas de seguridad para conseguir nuestro objetivo. (Berciano J., 2010, p. 1).

La mejor manera de asegurar la información procesada por la Coordinación Zonal 3 del INEC es aplicar responsablemente políticas, procedimientos y buenas prácticas, no solo de los directores y administradores de la institución, sino de todos los usuarios de los sistemas de información.

3.1.8.3 Objetivos de la seguridad de la información

A nivel general se puede decir que: "El objetivo de un servicio de seguridad es mejorar la seguridad de los sistemas de procesamiento de datos y la transferencia de información en las organizaciones. Los servicios de seguridad están diseñados para contrarrestar los ataques a la seguridad y hacen uso de uno o más mecanismos de seguridad para proporcionar el servicio" (Segunda Cohorte del Doctorado en Seguridad Estratégica, 2014, pp. 105 – 106).

Los objetivos de la seguridad de la información son los que a continuación se mencionan de acuerdo a la siguiente referencia:

1. Disponibilidad y accesibilidad de los sistemas y datos, sólo para su uso autorizado.

2. Integridad.

- ✓ Integridad de datos. Es la propiedad de que los datos no hayan sido alterados de forma no autorizada, mientras se almacenan, procesan o transmiten.
- ✓ Integridad del sistema. Es la cualidad que posee un sistema cuando realiza la función deseada, de manera no deteriorada y libre de manipulación no autorizada. La integridad, normalmente, es el objetivo de seguridad más importante después de la disponibilidad.

3. Confidencialidad de datos y de la información del sistema.

4. Responsabilidad a nivel individual (registros de auditoría).

5. Confiabilidad (aseguramiento)". (Areitio, J., 2008, p. 3).

De acuerdo al mismo autor, quién menciona otro tipo de objetivos que persigue la seguridad de la información, los cuales merecen ser tomados en cuenta.

- ✓ Conocer todos los riesgos de seguridad asociados a una empresa u organización.
- ✓ Establecer un conjunto equilibrado de requisitos de seguridad dc acuerdo con los riesgos identificados, para satisfacer las necesidades de un determinado proceso de negocio.
- ✓ Transformar las necesidades de seguridad en una guía de seguridad, para integrarla en las actividades de otras disciplinas implicadas en un proyecto y en unos descriptores de configuración u operación de un sistema.
- ✓ Establecer la confianza o garantía en la corrección y efectividad de los mecanismos de seguridad.
- ✓ Determinar que los impactos operacionales debidos a las vulnerabilidades de seguridad residuales de un sistema o su operación, sean tolerables, es decir, que los riesgos sean aceptables.
- ✓ Integrar los esfuerzos de todas las disciplinas de ingeniería y especialidades en un entendimiento combinado de la confianza fidedigna de un sistema. (Areitio, J., 2008, pp. 3 – 4).

Todos estos objetivos mencionados están encaminados a la consecución de la seguridad de la información de las instituciones que procesan información muy importante para la sociedad, se puede mencionar también lo que se refiere a los pilares de la seguridad de la información.

3.1.8.4 Necesidad de la seguridad de la información

Como se afirmó antes la existencia de varias razones obliga a que sea muy necesaria la implementación de seguridades de la información en la Coordinación Zonal 3 del INEC. La necesidad de seguridad de la información es primordialmente para proteger la información manejada y además la importancia de la formación del personal que debe diseñar, implementar, usar y administrar los sistemas. (Jaime Gutiérrez, J., Tena, J., 2004, p. 14).

Debido a la importancia y la necesidad de asegurar la información en los tiempos actuales se debe buscar las maneras de lograr esta seguridad que puede ser a través de la implementación de políticas.

3.1.9. Políticas de seguridad informática

En relación a la aplicación de las políticas de seguridad informática, se toma en cuenta el siguiente criterio:

> Lo primero que hemos de hacer es un análisis de las posibles amenazas que puede sufrir el sistema informático, una estimación de las pérdidas que esas amenazas podrían suponer y un estudio de las probabilidades de que ocurran.
>
> A partir de este análisis habrá que diseñar una política de seguridad en la que se establezcan las responsabilidades y reglas a seguir para evitar esas amenazas o minimizar los efectos si se llegan a producir. (Segunda Cohorte del Doctorado en Seguridad Estratégica, 2014, p. 45).

3: Política de seguridad

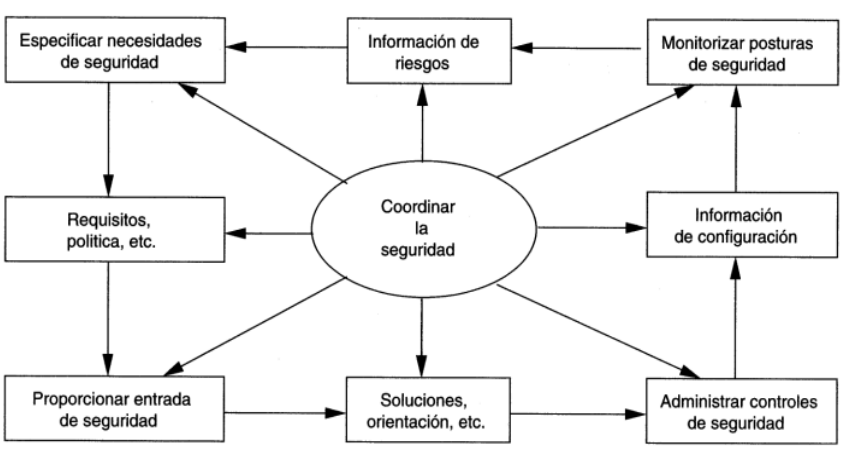
Fuente: Mifsud, E. (2012).

3.1.9.1. Objetivos de las políticas de seguridad informática

En cuanto a los objetivos que tienen las políticas de seguridad informática, se manifiesta lo siguiente: "El objetivo de la Política de Seguridad de Información de una organización es, por un lado, mostrar el posicionamiento de la organización con relación a la seguridad, y por otro lado servir de base para desarrollar los procedimientos concretos de seguridad. Las políticas deben contener claramente las prácticas que serán adoptadas por la compañía. Y estas políticas deben ser revisadas, y si es necesario actualizadas, periódicamente" (Mifsud, E., 2012, p. 1).

Con el siguiente gráfico se detalla el objetivo principal de las políticas de seguridad informática.

4: Objetivo principal de las políticas de seguridad informática



Fuente: Areitio, J., 2008, p. 46

3.1.9.2. Importancia de las políticas de seguridad informática

Es necesario recalcar sobre la importancia que tienen las políticas de seguridad de la información y su debida aplicación en instituciones de abundante procesamiento de información como es la Coordinación Zonal 3 del INEC.

> Antes de implementar y distribuir la política de seguridad a todos los empleados, debe revisarse para no dejar ninguna laguna legal. Asimismo, hay que asegurarse que la política es clara, concisa y consistente.
>
> También debe establecerse de forma firme la validez de la política de seguridad, que debe observar las leyes establecidas por ésta, para evitar complicaciones legales.
>
> Para que una organización mantenga un nivel suficiente de seguridad, su política de seguridad de la información debe evolucionar para la detección de nuevos tipos de amenazas, para lo que debe revisarse constantemente. De lo contrario, la política dejaría de ser útil. (Areitio, J., 2008, p. 47).

Las políticas de seguridad de la información tienen su guía o complemento en los estándares o normas de seguridad.

3.1.10. Estándares o normas de seguridad

En la actualidad se menciona frecuentemente los estándares o normas de seguridad, y es así que se toma en cuenta que:

> Un estándar es un documento con un contenido de tipo técnico-legal que establece un modelo o norma que refiriere lineamientos a seguir para cumplir una actividad o procedimientos. Su uso se ha popularizado en la actualidad debido a que se busca que los procesos y actividades de organizaciones y sus personas sean repetibles, organizados, y estructurados. (Borbón, J., 2011, pp. 14-16).

Es por lo citado que instituciones como la Coordinación Zonal 3 del INEC, pueden aplicar este tipo de normas de seguridad, con el propósito de precautelar la información que se procesa y que se pone a disposición de la sociedad. Se puede mencionar otro tipo de normas de seguridad resumidas en la siguiente tabla:

1: Normas de seguridad

Estándares	Detalles
CoBIT	Este documento establece un marco de trabajo basado en dominios y procesos, a través del cual se ofrecen unas buenas prácticas enfocadas a optimizar la inversión de recursos en áreas de IT
ITIL	Este compendio de documentos, conocido como la Biblioteca de Infraestructura de Tecnologías de Información, aborda recursos orientados a la correcta gestión de los servicios de IT
NIST SP 800-30	Este documento fue creado en el año 2002 y ofrece pautas para la gestión del riesgo buscando su evaluación, gestión, control y mitigación.
BS 259999	Este estándar de origen británico, aborda los lineamientos que deben contemplarse para la administración de la continuidad del negocio.

Fuente: (Borbón, J., 2011, p. 16)

3.1.10.1. Norma ISO

> ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización. Esta entidad es una organización no gubernamental constituida por más de 160 países y otras organizaciones, así como es la mayor en el desarrollo y publicación de estándares internacionales con más de 18.500 estándares publicados en la actualidad. (FUNIVSCYL, 2012, p. 85).

Los estándares de seguridad de la información se basan firmemente en las normas internacionales establecidas como es el caso de la Organización Internacional de Normalización (ISO), que es la base de todas las normas que se aplican en el país.

3.1.10.1.1. Referencia histórica de la norma ISO

Luego de la Segunda Guerra Mundial, bajo el amparo de las Naciones Unidas se fueron creando organizaciones para distintos propósitos, como por ejemplo la UNESCO, que tenían como finalidad el entendimiento entre los países y es así que:

> En este contexto, el 14 de octubre de 1946 se reunieron en Londres 25 países que deseaban establecer un organismo oficial para definir las normas que hicieran posible el intercambio de productos, repuestos, equipos y maquinaria. Ellos acordaron fundar la Organización Internacional para la Normalización. En inglés es la *International Organization for the Standardization*, sus siglas serían IOS, pero los creadores eligieron la palabra ISO porque en griego significa igualdad, bastante analógico con el propósito de la naciente organización. (Esponda, A., y otros, 2001, p. 19)

La Norma Internacional ISO comenzó su funcionamiento en el año 1947, cuya sede inicial fue en Ginebra, Suiza, ha publicado más de 13.000 normas en más de 50 años y la integran más de 150 países. (Esponda, A., y otros, 2001, p. 19).

La organización ISO que desarrolla y publica los Estándares Internacionales también se encuentra en el Ecuador, por lo tanto es aplicable en la Coordinación Zonal 3 del INEC como medida para precautelar la información.

3.1.11. Normas ISO 27000

La Norma ISO 27000 es un conjunto de normas tendientes a normalizar las técnicas, actividades y medidas a considerar para que se pueda implementar Sistemas de Gestión de Seguridad de la Información, esta norma es considerada como un hito fundamental para la seguridad de los sistemas de información del siglo XXI. (Corletti, A. 2011, p. 510)

3.1.11.1. Estándares que componen la norma ISO 27000

"La organización ISO ha reservado recientemente su serie 27000 para ternas relacionados con la seguridad de la información". (Heredero, C., y otros, 2006, p. 181).

El conjunto de estándares que aportan información de la familia ISO-27xxx son:

2: Estándares que componen la norma ISO 27000

Norma ISO 27000	**DETALLES**
ISO/IFC 27000	Es una visión general de las normas que componen la serie 27000
ISO/IEC 27001	Sistema de Gestión de la Seguridad de la Información. Publicada en octubre de 2005.
ISO/IEC 27002	Código o Guía de buenas prácticas para la Seguridad de la Información, fue publicado el 15 de junio del 2005 y detallados 133 controles reunidos en 11 grupos, más 39 Objetivos de control.
ISO/IEC 27003	Guía de Implementación. Describe los aspectos a tener en cuenta para la implantación de un SGSI. (2009).
ISO/SEC 27004	Es la norma que describe todos los aspectos de métricas, indicadores y mediciones que deben realizarse sobre un SCSI. (2009)
ISO/IEC 27005	Trata los aspectos relacionados a la Gestión de Riesgos tema de suma importancia en toda esta familia, (2008).
ISO/IEC 27006	Especifica los requisitos que debe reunir cualquier organización que desee acreditarse como entidad certificadora de ISO 27001. (2007).
ISO/IEC 27007	(Borrador) Guía para auditoria de un SGSI
ISO/IEC 27008	(Borrador) Guía para auditoria de los controles de un SGSI.
ISO/IEC 27010	(Borrador) Guía para la gestión de la seguridad de Sistemas de Información entre organizaciones.
ISO/IEC 27011	Guía de implementación de un SGSI para el sector de Telecomunicaciones (2008).
ISO/IEC 27012	(Borrador) SGSI para el sector de e-administración.
ISO/IEC 27013	(Borrador) Integración con ISO-20000.
ISO/IEC 27014	(Borrador) Gobierno corporativo de un SGSI.
ISO/IEC 27015	(Borrador) Sector financiero.
ISO/IEC 27016	(Borrador) Relacionado a finanzas en las organizaciones.
ISO/IEC 27031	Directrices para la preparación de las TIC en la Continuidad de Negocio, de reciente publicación.
ISO/IEC 27032	(Borrador) Ciberseguridad.
ISO/IEC 27033	Seguridad en redes

ISO/IEC 27034	(Borrador) Guías de seguridad para aplicaciones informáticas.
ISO/IEC 27035	(Borrador) Guía para la gestión: reincidentes de seguridad.
ISO/IEC 27036	(Borrador) Guía de seguridad para externalización de prestaciones.
ISO/IEC 27037	(Borrador) Relacionada a evidencias digitales.
ISO/IEC 27038	(Borrador) Redacción digital.
ISO/IEC 27039	(Borrador) Sistemas de detección de intrusiones (IDSs).
ISO/IEC 27040	(Borrador) Seguridad en almacenamiento de información.
ISO 27799	Está orientada a la aplicación de un SGSI en el ámbito sanitario. Publicada en el 2008.

Fuente: (Corletti, A. 2011, pp. 510-512)

3.1.12. Norma ISO 27002

La Norma ISO 27002 proporciona una guía de buenas prácticas para la seguridad de la información, con lineamientos básicos y diferentes alternativas para el tratamiento de los mismos. Permitiendo identificar las acciones apropiadas para minimizar los riesgos y vulnerabilidades a los que está expuesta la información, por lo tanto se la considera la más adecuada como referencia para diseñar las políticas de seguridad que necesita la Coordinación Zonal 3 del INEC.

> Se trata de una guía de buenas prácticas a partir de objetivos de control y controles recomendables a nivel de seguridad de la información. A diferencia de ISO 27001, no es un estándar certificable. Cuenta con 39 objetivos de control y 133 controles agrupados en 11 dominios, abordando más controles y dominios que los establecidos en el estándar certificable ISO 27001.
>
> A través de este documento se puede identificar un marco de trabajo más amplio para una organización cuando se desea implementar políticas de seguridad, establecer un sistema de gestión de la seguridad de la información y con la madurez adecuada lograr la certificación ISO 27001 que evalúa menos dominios. (Borbón, J., 2011, pp. 14-16)

Además se puede manifestar que las normas están actualizándose de manera permanente de acuerdo al avance de la tecnología y por ende mayores posibilidades de riesgo “La norma publicó su primera edición en el año 2000 y actualizada en junio de 2005. Se puede clasificar como las mejores prácticas

actuales en materia de sistemas de gestión de seguridad de la información. La BS 7799 original fue revisada y reeditada en septiembre de 2002" (Governance Institute, 2008, p. 17).

3.1.13. Acuerdo 166 de la Secretaria de Administración Pública

El acuerdo 166 de la Secretaria de Administración Pública, fue publicado en el Registro Oficial Suplemento 88 de 25-sep-2013, cuyo anexo No. 1 contempla el ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION (EGSI), el cual debe ser aplicado obligatoriamente por las entidades de la Administración Pública Central Dependiente e Institucional del Ecuador, como lo establece en el Artículo 1 del EGSI.

Art. 1.- Disponer a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.

3.2. Estado del Arte

La norma ISO 27002 es conocida en la informática por ser un estándar como se destaca en (Franco, D. y Guerrero, C., 2013), la misma que permite en el país estandarizar en varias empresas privadas y entidades gubernamentales un ejemplo claro de esto es (Romo, D. y Valarezo, J. 2012), en donde se destaca que gracias a la correcta aplicación de la normativa se pudo detectar que la Universidad Politécnica Salesiana sede Guayaquil es vulnerable ataques de colaboradores internos o externos.

Así también se evidencia en (Romero, C. y Castillo, J. 2011), donde se crea un patrón que aplica varios estándares que permiten mejorar la administración de la información en el Centro de Cómputo de la Facultad de Ingeniería en Electricidad y Computación de la escuela Superior Politécnica del Litoral.

La normativa ISO 27002 según (Amaya, C., 2013), busca mitigar el impacto o la posibilidad de ocurrencia de los diferentes riesgos a los cuales pueden estar expuestas las organizaciones así como implementar buenas prácticas para gestionar la seguridad de la información teniendo como guía de

aplicación (ISO27000, 2011), en donde mediante un análisis exhaustivo se determinará cuáles son los controles que se debe realizar.

En el trabajo realizado en (Montes, K. 2014), se evidencia que al aplicar normas dentro de la institución permite valorar las amenazas, vulnerabilidades, control, riesgo neto y riesgo residual permitiendo tener un alcance real de la situación y tomar medidas correctivas para proteger la información.

En la Seguridad de la Información el objetivo de la protección son los datos mismos y trata de evitar su perdida y modificación no-autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo existen más requisitos como por ejemplo la autenticidad entre otros. El motivo o el motor para implementar medidas de protección, que responden a la Seguridad de la Información, es el propio interés de la institución o persona que maneja los datos, porque la pérdida o modificación de los datos, le puede causar un daño (material o inmaterial). (ISO 27002, 2009).

> El objetivo del estándar ISO 27002 es brindar información a los responsables de la implementación de seguridad de la información de una organización. Puede ser visto como una buena práctica para desarrollar y mantener normas de seguridad y prácticas de gestión en una organización para mejorar la fiabilidad en la seguridad de la información en las relaciones interorganizacionales. En él se definen las estrategias de 133 controles de seguridad organizados bajo 11 dominios. La norma subraya la importancia de la gestión del riesgo y deja claro que no es necesario aplicar cada parte, sino sólo aquellas que sean relevantes. (Markus, E., 2008).

La seguridad en la información no recibe la atención adecuada y al no implementarse medidas de protección las instituciones están expuestas a sufrir serias complicaciones en la integridad y preservación de la información.

Capítulo 4

Metodología

4.1. Diagnóstico

Se realizaron entrevistas al Director Administrativo de la Coordinación Zonal 3 INEC Ing. Klever Villa y al Director de Tecnologías de la Información (TI) Ing. Sergio Abata. Entrevista No. 1 (Apéndice C) y la entrevista No. 2 (Apéndice D).

Análisis

De acuerdo a las entrevistas realizadas a personeros de la Coordinación Zonal 3 INEC, se ha podido notar que no existen políticas de seguridad de información aplicadas a la institución, que las personas involucradas en la Dirección de Tecnologías de la Información y Comunicación (DTIC), no tienen claros los roles de cada uno en la gestión de procesos y de seguridad. Lo que ocasiona que la institución está expuesta a vulnerabilidades como:

- ✓ Fácil acceso a información con acceso restringido.
- ✓ En seguridad de información están expuestos a que los usuarios puedan añadir programas no autorizados lo que podría generar pérdidas de información por efecto de virus o monitoreo remoto con troyanos.
- ✓ Se puede realizar copias no autorizadas, adulteración, revelación de información confidencial, sabotaje, vandalismo, etc.
- ✓ No existe una metodología para hacer los respaldos de información.

4.2. Método(s) aplicado(s)

Se aplicó la Metodología de Cascada, la cual es la que más se adapta al presente trabajo de titulación, aplicado a una Coordinación Zonal 3 del INEC. Se lo puede definir de la siguiente manera:

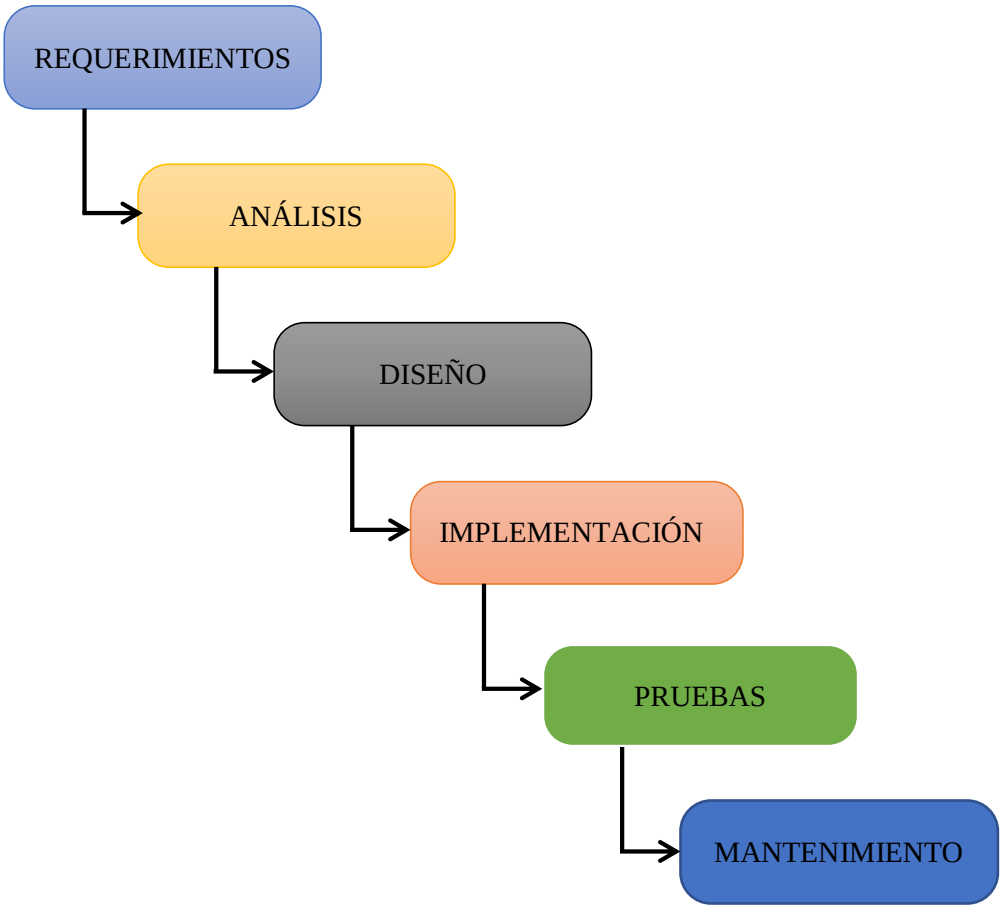
> Modelo lineal o en cascada: donde no se inicia una etapa o fase hasta que se completa la anterior. Cada vez que finaliza una etapa se obtiene un documento o producto final, que revisado, validado y aprobado, sirve como aproximación y documentación de partida para la siguiente. Es el más extendido y utilizado, en proyectos de gestión, medianos y grandes. (Barranco de Areba, J., 2001, p. 44).

La metodología de Cascada se denomina así por la posición de los pasos o fases para su desarrollo, que tiene la forma de cascada, de manera que el final de la primera fase permite el comienzo de la segunda y así hasta terminar todo el proceso.

Cada una de las fases permite ser revisada para determinar si esta lista para ser terminada y avanzar a la próxima. Este es un proceso lineal y secuencial muy adecuado para el desarrollo de sistemas y en este caso en el proceso de elaboración de políticas de seguridad de la información.

Una de las mayores ventajas de esta metodología es el orden y la organización del mismo, de manera que las fases no se mezclan permitiendo la agilidad necesaria para desarrollar todo el proceso sin problemas.

5: Metodología de Cascada



Elaboración propia

- ✓ **Requerimientos.-** Se estableció los requerimientos necesarios en base a cómo se encuentra la información actual.

- ✓ **Análisis.-** Con los requerimientos se determinó y evaluó las amenazas y vulnerabilidades en la información.

- ✓ **Diseño.-** Se desarrollaron las políticas de seguridad de información, que permitan corregir las vulnerabilidades existentes en el proceso actual.

- ✓ **Implementación.-** Aplicar las políticas de seguridad de información en base a la norma ISO 27002 para el Departamento de TI.

- ✓ **Pruebas.-** Se verificara la aplicación de las políticas de seguridad y su correcta implementación.

- ✓ **Mantenimiento.-** Actualización de políticas o mejoras en los procesos de gestión, en el caso de existir.

4.3. Materiales y herramientas

Las herramientas usadas fueron:

- ✓ Entrevistas personales realizadas a personeros de la Coordinación Zonal 3 del INEC, elaboradas de acuerdo a las necesidades de la institución. (Ver Apéndices A y B).

Capítulo 5

Resultados

5.1. Producto final del proyecto de titulación

Se determinó cual es la situación actual de la Coordinación Zonal 3 del INEC acerca de la aplicación de las políticas de seguridad de la información.

Se realizaron los análisis respectivos de las políticas a ser aplicadas en la Coordinación Zonal 3 del INEC, con el fin de establecer cuáles son las que deben ser aplicadas para lograr la mayor seguridad de la información.

Se elaboró el cuestionario de preguntas para entrevistar a los personeros de la institución, con el objetivo de establecer la situación actual de la institución y realizar los correctivos que sean necesarios para garantizar la seguridad de la información, la cual sirvió de beneficio para toda la colectividad que requiera de la misma.

5.2. Antecedentes

Según el Acuerdo 166 de la Secretaría de Administración Pública, es responsabilidad de empresas como la Coordinación Zonal 3 del INEC aplicar las políticas ligadas a la seguridad de los sistemas informáticos, el ambiente tecnológico, seguridad física de los equipos informáticos y recurso humano, aplicando el Esquema Gubernamental de Seguridad de la Información (EGSI) basado en la norma NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.

De acuerdo al análisis respectivo de las normas de seguridad de la información de la serie 27000, se estableció que la norma más adecuada para aplicar son las políticas indicadas en la norma ISO 27002, debido a que ésta es una guía de buenas prácticas a partir de objetivos de control y controles recomendables a nivel de seguridad de la información, Cuenta con 39 objetivos de control y 133

controles agrupados en 11 dominios, abordando más controles y dominios que los establecidos en el estándar certificable ISO 27001.

5.3. Aplicación de la metodología

De acuerdo a la metodología de cascada aplicada en el presente trabajo se desarrolló el producto final de la siguiente manera:

5.3.1 Requerimientos

La Coordinación Zonal 3 del INEC requirió lo más pronto posible poner en práctica los correctivos necesarios para la implementación de medidas de seguridad debido a la clara evidencia de vulnerabilidades que afectan la seguridad de la información, ya que, de acuerdo a las entrevistas realizadas, no se cuenta con las seguridades necesarias para el respaldo de información.

5.3.2 Análisis

Debido a los requerimientos de seguridad de la información, con el análisis respectivo de la situación actual de la institución, se ha determinado la existencia de amenazas y vulnerabilidades que ponen en peligro la seguridad de la información de la Coordinación Zonal 3 del INEC, por lo tanto es responsabilidad de la Dirección tomar en cuenta la propuesta de solución al problema presentado.

5.3.3 Diseño

A continuación se presenta el diseño de las políticas de seguridad de la información basadas en la norma ISO 27002.

5.3.3.1 Desarrollo de políticas de seguridad de la información basadas en la norma ISO 27002.

Propósito

Fortalecer la seguridad de la información institucional referente a la gestión de tecnologías de la información y comunicación, ya que las políticas son guías que aseguran la protección e integridad de la información permitiendo el cumpliendo de las disposiciones gubernamentales alineadas a las buenas prácticas para la gestión tecnológica de acuerdo a la Norma ISO 27002 y el Acuerdo No. 166 del Registro Oficial del Ecuador, donde se especifica el esquema gubernamental de seguridad de la información.

5.3.3.1.1 Uso correcto de los equipos

3: Uso correcto de los equipos

Políticas de seguridad de la información basadas en la norma ISO 27002	
Institución	Coordinación zonal del INEC - Ambato
Política	Política para el uso correcto de los equipos
Objetivo	Asegurar la operación correcta y segura de los servicios de procesamiento de información.
Responsables	
Cargo	**Responsabilidad**
1. Director de Tecnologías de la Información y Comunicación.	✓ Liderar la gestión tecnológica de manera eficiente y proactiva. ✓ Gestionar el cumplimiento de las políticas y procedimientos, entre otros documentos oficiales aprobados y relacionados con la seguridad de información.
2. Responsable de Seguridad de la Información en el Departamento de Tecnologías de Información y	✓ Implementar controles de seguridad de la información en los servicios tecnológicos que son administrados por el DTIC, de acuerdo a como se

Comunicación (DTIC)	encuentra dispuesto en el Esquema Gubernamental de Seguridad de la Información (EGSI). ✓ Vigilar que el equipo de cómputo se use bajo las condiciones especificadas por el proveedor
3. Técnico del DTIC	✓ Asesorar a los usuarios, referente al correcto uso de los servicios tecnológicos. ✓ Atender los requerimientos de los usuarios en el ámbito de su competencia y respetando las directrices vigentes. ✓ Cumplir y hacer cumplir las políticas y procedimientos relacionados con la seguridad de información.
4. Funcionarios Coordinación Zonal	✓ Cumplir con las directrices respecto al correcto uso de los servicios tecnológicos proporcionados por DTIC. ✓ Recurrir al personal del DTIC o la documentación vigente relacionada con los requerimientos informáticos.

Elaboración propia

I. Introducción

La política para el uso correcto de los equipos presenta las diferentes acciones que deberán seguirse para asegurar la operación correcta y segura de los servicios de procesamiento de información, bajo la supervisión permanente de la dirección de la Coordinación Zonal 3 del INEC.

II. Alcance

La presente política está orientada a los usuarios de los equipos dentro de las instalaciones de la institución.

III. Disposiciones generales

1. Se deberían establecer todas las responsabilidades y los procedimientos para la gestión y operación de todos los servicios de procesamiento de información. Esto incluye el desarrollo de procedimientos operativos apropiados.

2. Cuando sea conveniente, se debería implementar la separación de funciones para reducir el riesgo de uso inadecuado deliberado o negligente del sistema.

3. Los procedimientos de operación se deberían documentar, mantener y estar disponibles para todos los usuarios que los necesiten.

IV. Acciones

4: Acciones del uso correcto de equipos

Cargo	**Norma 27002 – (Numeral 10.1.1) Documentación de los procedimientos de operación**	**Política**
1. Director de Tecnologías de la Información y Comunicación.	Se deben establecer todas las responsabilidades y los procedimientos para la gestión y operación de todos los servicios de procesamiento de información.	✓ La responsabilidad de la seguridad fisica de los equipos informáticos corresponde al custodio. ✓ En el caso de equipos informáticos portátiles asignados, se debe evitar su exposición a sitios inseguros, públicos y de alto riesgo; de igual forma. DTIC implementará y socializará controles para la seguridad de la información en estos equipos, que tienen riesgos adicionales.
2. Responsable de Seguridad de la Información de la (DTIC)	Los procedimientos operativos, y los procedimientos documentados para las actividades del sistema, se deberían tratar como documentos formales y sus cambios deberían ser autorizados por la dirección.	✓ Todos los servicios tecnológicos del INEC, administrados y soportados por la DTIC y brindados a los funcionarios deben utilizarse con fines exclusivamente institucionales y relacionados con el desempeño de las actividades de trabajo. ✓ No podrán ser utilizados para uso personal, privado o comercial, además de que estos servicios se encuentran monitoreados y sus accesos se encuentran sometidos a controles que se estiman pertinentes para la seguridad informática respectiva.

3. Técnico del DTIC	Instrucciones para el manejo de errores y otras condiciones excepcionales que se pueden presentar durante la ejecución del trabajo, incluyendo las restricciones al uso de las utilidades del sistema.	✓ Cualquier duda sobre la utilización de los equipos informáticos, deberá ser resuelta por la DTIC, previa consulta del funcionario, siendo esta unidad administrativa la única autorizada para realizar chequeos, revisiones, reparaciones o mejoras de carácter preventivo o correctivo de los equipos informáticos, en caso de averías o anomalías en su funcionamiento y la responsable por la administración del componente tecnológico en la institución. ✓ Si por cuestiones estrictamente institucionales, fuera necesaria la instalación de algún programa o cualquier otro servicio tecnológico distinto a los disponibles para los funcionarios del INEC, deben hacer una petición al Director de TI.
4. Funcionarios Coordinación Zonal 3	Procesamiento y manejo de información	✓ El custodio y/o usuario, debe cuidar y dar un uso apropiado y correcto, a los equipos informáticos asignados, evitando su deterioro e incorrecta utilización. ✓ El uso del equipamiento y en general, de los servicios tecnológicos, debe ser exclusivamente para actividades laborales autorizadas en el ámbito de competencia correspondiente. ✓ Así en el caso de movilización del equipo se deben obedecer los procedimientos y

		directrices establecidos por la Dirección Administrativa Financiera de la institución con cumplimiento obligatorio a la presente política
	Copias de respaldo	✓ Toda la información de trabajo generada o utilizada por el funcionario, incluyendo el correo electrónico institucional, es de su responsabilidad exclusiva, la realización de respaldo y seguridad de la misma. La información institucional que genere debe encontrarse en el directorio "Mis Documentos" de la cuenta de usuario y respaldada en la partición secundaria que posee el disco duro en el directorio: "Respaldo Mis Documentos, evitando que su pantalla posea iconos innecesarios DTIC determinará el método de cifrado con el que será protegida la información sensible. ✓ Adicionalmente el Director de área tiene acceso a una carpeta compartida de la dirección y tiene la potestad de colocar, solicitar permisos de lectura y escritura a DTIC para sus miembros de equipo, a fin de que la información institucional colocada en dicho directorio sea respaldada periódicamente en los servidores de respaldos existentes.

Elaboración propia

Norma 27002 – (Numeral 11.2.3) Gestión de contraseñas para usuarios	**Política**
a) se debería exigir a los usuarios la firma de una declaración para mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de éste; esta declaración firmada se podría incluir en los términos y condiciones laborales (véase el numeral 8.1.3); b) cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debería suministrar una contraseña temporal segura (véase el numeral 11.3.1) que estén forzados a cambiar inmediatamente; h) las contraseñas predeterminadas por el proveedor se deberían cambiar inmediatamente después de la instalación de los sistemas o del software.	Toda cuenta de usuario tiene asociada una contraseña que debe cumplir con los siguientes requisitos: 1. Debe ser cambiada en el primer inicio de sesión. 2. Debe ser definida con una longitud mínima de 6 caracteres. 3. No debe ser en blanco, deben combinar letras y números sin un significado evidente. 4. Cambiarse obligatoriamente en un periodo máximo de 30 días, para lo cual el sistema notifica automáticamente 5. Ser distinta, de por lo menos, las últimas 3 contraseñas cambiadas 6. En sistemas desarrollados: el cambio, caducidad y control de claves se lo realizará de acuerdo a requerimientos
c) establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle una contraseña temporal, de reemplazo o nueva;	✓ Toda cuenta de usuario que haya intentado el acceso al sistema en forma fallida y consecutiva tres veces es automáticamente bloqueada y en este caso, el usuario debe solicitar et desbloqueo a la DTIC. ✓ La nomenclatura estándar de las cuentas de usuario

	personales se obtiene a partir del primer nombre completo, seguido del símbolo y el apellido completo y el dominio institucional (inec.gob.ec); por ejemplo: maria_garcia@inec.gob.ec. ✓ En caso de haber coincidencia con otro usuario, esta cuenta es creada con el segundo nombre de la persona. ✓ Las contraseñas son personales e intransferibles; queda terminantemente prohibida la compartición o divulgación a otras personas de las claves de acceso por cualquier medio, por lo tanto, cualquier acción realizada con la cuenta de usuario asignada es responsabilidad exclusiva de su propietario, salvo el caso en que demuestre que le ha sido usurpada.
d) las contraseñas temporales se deberían suministrar de forma segura a los usuarios; se recomienda evitar mensajes de correo electrónico de terceras partes o sin protección (texto claro); e) las contraseñas temporales deberían ser únicas para un individuo y no ser descifrables; f) los usuarios deberían confirmar la entrega de las contraseñas; g) las contraseñas nunca se deberían almacenar en sistemas de computador en un formato no protegido;	✓ Los cambios de contraseña por olvido o el desbloqueo de la respectiva cuenta, deben ser solicitados por el funcionario al responsable de este servicio en la DTIC; a fin de que la contraseña sea cambiada en el siguiente inicio de sesión por el usuario. ✓ Toda cuenta de usuario que no haya accedido al sistema por 30 días será bloqueada, en este caso, el usuario debe solicitar el desbloqueo a la DTIC.

Norma 27002 – (Numeral 11.4.1) Política de uso de los servicios en red.

Los usuarios sólo deberían tener acceso a los servicios para cuyo uso están específicamente autorizados.

Se debería formular una política con respecto al uso de las redes y los servicios de red. Esta política debería abarcar:

a) las redes y los servicios de red a los cuales se permite el acceso;
b) los procedimientos de autorización para determinar a quién se le permite el acceso a qué redes y qué servicios en red;
c) los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y los servicios de red;
d) los medios utilizados para el acceso a las redes y los servicios de red (por ejemplo las condiciones para permitir el acceso a la marcación a un proveedor de servicios de Internet o a un sistema remoto).

La política sobre el uso de los servicios de red debería ser consistente con la política de control de acceso de la organización (véase el numeral 11.1).

INTERNET

a. El usuario se abstendrá de utilizar este servicio con fines o efectos ilícitos, lesivos de los derechos e intereses de terceros, o que de cualquier forma puedan dañar, inutilizar, sobrecargar o deteriorar los servicios, los equipos informáticos de otros usuarios del Internet (*hardware* y *software*)
b. Si por motivos estrictamente profesionales o por necesidad institucional, fuere preciso el acceso hacia algún contenido bloqueado, el funcionario deberá solicitar autorización.
c. Se puede utilizar el internet para fines personales. siempre que dicho uso sea corto y que el funcionario deba realizar algún tipo de gestión por este medio, para evitar que se ausente de su lugar de trabajo, tales como trámites bancarios, IESS, SRI, etc., o consultas relacionadas con las actividades que realiza en el INEC.

d. EI INEC tiene potestad exclusiva respecto a la utilización y administración del servicio de internet institucional; en consecuencia, los funcionarios deben justificar los accesos realizados a este servicio, si así lo requiere la institución.
e. EI uso del servicio de Internet es monitoreado siempre y auditado cuando fuere necesario y por disposición o solicitud de las autoridades competentes.
f. Se prohíbe al usuario el acceder a páginas web, cuyo contenido sea ofensivo, inapropiado, pornográfico, erótico o discriminatorio por razones de género, etnia, opción sexual, discapacidad o cualquier otra circunstancia personal o social. La DTIC se reserva la facultad de implementar los mecanismos técnicos necesarios para impedir el acceso a los contenidos señalados anteriormente
g. Se prohíbe al usuario el uso de "*proxys*" anónimos, enmascaramiento o cualquier técnica de desbloqueo u ocultamiento de navegación.
h. El hecho de que la DTIC no haya bloqueado el acceso a una determinada página web o contenido anteriormente definido, no implica que el acceso a la misma esté autorizado.
i. Si durante el proceso de búsqueda de una determinada dirección o información a través de la red de Internet, se accede por desconocimiento o por error, a una dirección cuyo contenido resulte contrario a lo dispuesto en la presente política, el funcionario deberá abandonar dicha dirección inmediatamente e informar a la DTIC para su filtrado. De no producirse el abandono inmediato de la página, se considerara que la conexión ha sido intencional.
j. Se prohíbe al usuario el acceso a sistemas de mensajería instantánea (*chats*), únicamente está permitido el sistema local denominado *Spark*.

INTRANET

a. El usuario se abstendrá de utilizar este servicio con fines o efectos ilícitos, lesivos de los derechos e intereses de terceros, o que de cualquier forma puedan dañar, inutilizar, sobrecargar o deteriorar los servicios, los equipos informáticos de otros usuarios de Internet (*hardware* y *software*) así como los documentos, archivos y toda clase de contenidos almacenados en sus equipos informáticos, o impedir la normal utilización o disfrute de dichos servicios, equipos informáticos y documentos, archivos y contenidos por parte de los otros usuarios de la Comunidad de Internet.

b. Los niveles de acceso concedidos para el uso de los servicios de intranet deben respetarse conforme han sido dispuestos y son exclusivamente para uso interno institucional.
c. Está prohibido conectarse a la red con equipos que no sean de propiedad de la institución, sin la autorización establecida por el jefe inmediato del funcionario requirente y de la DTIC.
d. Será sancionado todo daño que se produzca, de manera intencionada, a los componentes de la red alámbrica e inalámbrica que se encuentran localizados en las dependencias de la institución.

CORREO ELECTRÓNICO

a. No se realizan copias de seguridad de los buzones de correo de los usuarios, siendo responsabilidad de éstos guardar una copia local en caso de almacenar los mensajes en el servidor.
b. Cada usuario de correo electrónico es responsable de depurar su buzón frecuentemente, para lo cual dispone de un tamaño máximo en el mismo. Existen 3 tipos de buzones de correo electrónico configurados en el servidor (interfaz web de correo electrónico-OWA) por su capacidad máxima:

   Uso común: 160 MB
   Intermedios: 500 MB
   Avanzados: 4 GB

   En caso de requerir mayor capacidad de almacenamiento en correo electrónico, los funcionarios deberán solicitar autorización.

c. El usuario está en la obligación de leer diaria y periódicamente durante la jornada de trabajo el buzón asignado desde el computador que le ha sido asignado.
d. Todo usuario es responsable por la destrucción de todo mensaje cuyo origen es desconocido, y asume la responsabilidad por las consecuencias que puede ocasionar la ejecución y envió del cualquier archivo adjunto. En estos casos, no se deben contestar dichos mensajes y debe ser enviada una copia al administrador del servicio para que efectúe las tareas de seguimiento e investigación necesarias.

e. La cuenta de correo electrónico es personal e intransferible. El usuario se compromete a hacer un uso diligente de la cuenta y a mantener su contraseña en secreto. Asimismo, el usuario se compromete a notificar a la DTIC, de manera inmediata, la pérdida de su contraseña o acceso no autorizado por parte de terceros a su cuenta.

5.3.3.1.2 Intercambio de información

5: Intercambio de información

Políticas de seguridad de la información basadas en la norma ISO 27002	
Institución	Coordinación zonal del INEC - Ambato
Política	Política para el intercambio de información
Objetivo	Mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.
Responsables	
Cargo	**Responsabilidad**
1. Director de Tecnologías de la Información y Comunicación.	✓ Liderar la gestión tecnológica de manera eficiente y proactiva. ✓ Gestionar el cumplimiento de las políticas y procedimientos, entre otros documentos oficiales aprobados y relacionados con la seguridad de información.
2. Responsable de Seguridad de la Información de la (DTIC)	✓ Implementar controles de seguridad de la información en los servicios tecnológicos que son administrados por el DTIC, de acuerdo a como se encuentra dispuesto en el EGSI.
3. Técnico de la DTIC	✓ Asesorar a los usuarios, referente al correcto uso de los servicios tecnológicos. ✓ Atender los requerimientos de los usuarios en el ámbito de su competencia y respetando las directrices vigentes.

	✓ Cumplir y hacer cumplir las políticas y procedimientos relacionados con la seguridad de información.
4. Funcionarios Coordinación Zonal	✓ Cumplir con las directrices respecto al correcto uso de los servicios tecnológicos proporcionados por DTIC. ✓ Recurrir al personal del DTIC o la documentación vigente relacionada con los requerimientos informáticos.

Elaboración propia

I. Introducción

De acuerdo a los del Acuerdo No. 166 del Registro Oficial del Ecuador, es mandatorio que la Coordinación zonal del INEC disponga de una política que regule el intercambio de información a fin de garantizar la confidencialidad, integridad y disponibilidad de la misma.

II. Alcance

La presente política está orientada a todo el personal de la Coordinación Zonal 3 del INEC que administra los servicios tecnológicos que permiten el intercambio de información a fin de que apliquen todas las acciones correspondientes.

III. Disposiciones generales

1. Toda salida de información (en soportes informáticos o por correo electrónico) sólo podrá ser realizada por personal autorizado y será necesaria la autorización formal del responsable del área del que proviene.
2. Además, en la salida de datos especialmente protegidos (como son los datos de carácter personal para los que se requiere medidas de seguridad de nivel alto), se deberán cifrar los mismos o utilizar cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada durante su transporte.

IV. Acciones

6: Acciones del intercambio de información

Cargo	Acción Norma 27002 – (Numeral 10.8) Intercambio de la información	Política
1. Director de Tecnologías de la Información y Comunicación.	Los intercambios de información y de software entre las organizaciones se deberían basar en una política formal de intercambio, ejecutar según los acuerdos de intercambio y cumplir la legislación correspondiente (véase la sección 15).	a. Todo documento generado debe llevar su respectivo control de cambios versionamiento y demás caracteristicas que aseguren la calidad y el mantenimiento respectivo a lo largo del tiempo. b. Realizar informes, adjuntando medios de verificación, que contengan la medición periódica de las métricas que se deben contemplar para monitoreo de la gestion de Intercambio de Información.
2. Responsable de Seguridad de la Información en la	**Norma 27002 – (Numeral 10.8.2) Acuerdos para el intercambio** a) responsabilidades de la dirección para controlar y notificar la transmisión, el despacho y la recepción;	Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificará el grado de sensibilidad de la información del organismo involucrado y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

(DTIC)	b) procedimientos para notificar a quien envía la transmisión, el despacho y la recepción; c) responsabilidades y deberes en caso de incidentes de la seguridad de la información, como la pérdida de datos; h) uso de sistemas acordados de etiquetado de la información sensible o crítica, garantizando que el significado de las etiquetas se entienda inmediatamente y que la información está protegida adecuadamente;	✓ Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones. ✓ Procedimientos de notificación de emisión, transmisión, envió y recepción. ✓ Responsabilidades y obligaciones en caso de pérdida de datos. ✓ Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida. ✓ Términos y condiciones de la licencia bajo la cual se suministra el software. ✓ Información sobre la propiedad de la información suministrada y las condiciones de su uso.
3. Técnico del DTIC	**Norma 27002 – (Numeral 10.8.1) Políticas y procedimientos para el intercambio de información** El intercambio de información se puede producir a través de la utilización de diferentes tipos de servicios de comunicación, incluyendo correo electrónico, voz, fax y video.	a) El intercambio de información física sólo debe utilizar los servicios de correos autorizados en el INEC, en forma certificada para controlar su trazabilidad. Adicionalmente ésta debe ser entregada personalmente al destinatario en un sobre sellado y su entrega debe quedar registrada en el Acta de Entrega - Recepción respectiva. b) Toda la información remitida mediante el servicio de correo electrónico institucional debe incluir pie de página, una advertencia en cuanto a su uso y autorizaciones al respecto, quedando bajo responsabilidad del receptor el cuidado

	El intercambio de software se puede dar a través de diferentes medios, incluyendo descargas desde Internet y adquiridas de vendedores de productos de mostrador. El negocio debería considerar las implicaciones legales y de la seguridad, asociadas con el intercambio electrónico de datos, el comercio electrónico y las comunicaciones electrónicas, así como los requisitos para los controles. La información podría verse amenazada debido a la falta de conciencia, de políticas o procedimientos sobre el uso de los servicios de intercambio de información, por ejemplo por la escucha en un teléfono móvil en un lugar público, la dirección incorrecta de un mensaje de correo electrónico, la escucha de los contestadores automáticos, el acceso no autorizado a sistemas de correo de voz de marcación o el envío accidental de facsímiles al equipo errado de fax. Las operaciones del negocio podrían ser	y resguardo de la información. Además esta información deberá ser encriptada para proteger el contenido de la misma. c) Toda información que se transmita mediante el servicio de correo electrónico o sea descargada de algún medio externo debe ser escaneada por el *software* de antivirus, *firewall*, *antispam* y otros mecanismos para protección contra código malicioso o mecanismos de ingeniería social.

	afectadas y la información podría ser comprometida si los servicios de comunicación fallan, se sobrecargan o interrumpen (véase el numeral 10.3 y el numeral 14). La información se vería comprometida por el acceso de usuarios no autorizados (véase el numeral 11).	
4. Funcionarios Coordinación Zonal 3	**Norma 27002 – (Numeral 10.8.3) Medios físicos en tránsito** Los medios que contienen información se deberían proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización. Se recomienda tener en cuenta las siguientes directrices para la protección de los medios que se transportan entre los lugares: a) se recomienda utilizar transporte confiable o servicios de mensajería; b) se debería acordar con la dirección una lista de servicios de mensajería;	Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar al menos: ✓ La utilización de medios de transporte o servicios de mensajería confiables. El Propietario de la Información a transportar determinará qué servicio de mensajería se utilizará conforme la entidad de la información a transmitir y de acuerdo a los disponibles en el INEC. ✓ Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores. La adopción de controles especiales. cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas, Entre los ejemplos se incluyen:

	c) se deberían desarrollar procedimientos para verificar la identificación de los servicios de mensajería; d) el embalaje debería ser suficiente para proteger el contenido contra cualquier daño físico potencial que se pueda producir durante el transporte, y estar acorde con las especificaciones del fabricante. e) Cuando sea necesario, se deberían adoptar controles para proteger la información sensible contra divulgación o modificación no autorizada; algunos ejemplos incluyen; 1) uso de contenedores cerrados con llave; 2) entrega personal; 3) embalajes con sello de la seguridad (que revelan cualquier intento de acceso); 4) en casos excepcionales, división de la remesa en más de una entrega y despacho por rutas	1- Uso de recipientes cerrados 2- Entrega en mano. 3- Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso). 4- En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes ruta.

	diferentes. Información adicional La información puede ser vulnerable al acceso no autorizado, al uso inadecuado o a la corrupción durante el transporte físico, es el caso de los envíos de medios a través de servicios postales o de mensajería.	
5. Funcionarios Coordinación Zonal 3	**Norma 27002 – (Numeral 10.8.4) Mensajería electrónica** La información contenida en la mensajería electrónica debería tener la protección adecuada. Guía de implementación Las consideraciones de la seguridad para la mensajería electrónica deberían incluir las siguientes: a) proteger los mensajes contra acceso no autorizado, modificación o negación de los servicios;	Es obligatorio el disponer de una solución contra correo no deseado (SPAM), en el que se incluyan filtros y reglas tales como: Bloqueo de direcciones, filtrado de contenido, filtros heurísticos, reputación de direcciones IP, soporte a TLS, seguimiento de conversaciones y más.

	b) garantizar que la dirección y el transporte del mensaje son correctos; c) confiabilidad general y disponibilidad del servicio; d) consideraciones legales como, por ejemplo, los requisitos para las firmas electrónicas; e) obtención de aprobación antes de utilizar servicios públicos externos como la mensajería instantánea o el compartir archivos;	✓ Es obligatorio el disponer de una solución de antivirus corporativo que escanee y filtre el tráfico de mensajería tanto de entrada como de salida. ✓ Es obligatorio el disponer de una solución que impida los accesos no autorizados, modificación o denegación de los servicios a fin de que la transmisión de la mensajería electrónica sea integra. ✓ Se debe monitoreara diariamente el flujo de mensajería electrónica a fin de controlar la calidad del servicio y asegurando la integridad y confidencialidad de la misma, mediante la implementación de controles criptográficos en los servicios correspondientes así como el uso de firmas electrónicas.
	f) niveles más sólidos de autenticación que controlen el acceso desde redes accesibles al público. La mensajería electrónica como, por ejemplo, el correo electrónico, el intercambio de datos electrónicos (EDI) y la mensajería instantánea tienen una función cada vez más creciente en las comunicaciones de los negocios. La mensajería electrónica tiene riesgos diferentes que las comunicaciones en papel.	Las firmas electrónicas y certificados digitales que se utilicen en la institución deben cumplir con la "Ley Ecuatoriana de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos" dispuesta por el Gobierno Nacional y DTIC debe velar por el cumplimiento a esta ley.

Elaboración propia

5.3.3.1.3 Control de acceso

7: Control de acceso

Políticas de seguridad de la información basadas en la norma ISO 27002	
Institución	Coordinación zonal del INEC - Ambato
Política	Política para el Control de acceso a la información
Objetivo	Controlar el acceso a la información.
Responsables	
Cargo	**Responsabilidad**
1. Director o Jefe de área requirente de respaldo de la información.	✓ Realizar los respaldos necesarios al directorio asignado a su dirección de toda la información institucional.
2. Director de Tecnologías de la Información y Comunicación.	✓ Liderar la gestión tecnológica de manera eficiente y proactiva. ✓ Gestionar el cumplimiento de las políticas y procedimientos, entre otros documentos oficiales aprobados y relacionados con la seguridad de información.
3. Responsable de Seguridad de la Información en el Departamento de Tecnologías de Información y Comunicación (DTIC)	✓ Implementar controles de seguridad de la información en los servicios tecnológicos que son administrados por el DTIC, de acuerdo a como se encuentra dispuesto en el EGSI.
4. Técnico del DTIC	✓ Asesorar a los usuarios, referente al correcto uso de los servicios tecnológicos. ✓ Atender los requerimientos de los usuarios en el ámbito de su competencia y respetando las directrices vigentes. ✓ Cumplir y hacer cumplir las políticas y procedimientos relacionados con la seguridad de información.

5. Funcionarios Coordinación Zonal	✓ Cumplir con las directrices respecto al correcto uso de los servicios tecnológicos proporcionados por DTIC. ✓ Recurrir al personal del DTIC o la documentación vigente relacionada con los requerimientos informáticos.

Elaboración propia

I. Introducción

La presente política pretende los lineamientos que permitan una adecuada implementación de los controles de acceso de manera que se pueda contar con una mejor seguridad en la información.

II. Alcance

La presente política pretende ser aplicada a todos los funcionarios de la institución, sean estos aAdministradores o usuarios que tengan derechos de acceso a la información, ya sea que esta se encuentre almacenada o sea generada dentro de la institución. Esta política tiene aplicación obligatoria a los servicios tecnológicos, que se encuentran bajo administración DTIC, como el "*datacenter*", el equipo informático, la red local y el acceso remoto.

III. Disposiciones generales

Sólo al personal autorizado le está permitido el acceso a las instalaciones donde se almacena la información confidencial

Sólo bajo la vigilancia de personal autorizado, puede el personal externo entrar en las instalaciones donde se almacena la información confidencial, y durante un período de tiempo justificado.

IV. Acciones

8: Acciones del Control de acceso

Cargo	Acción Norma 27002 – (Numeral 11.1) Requisitos del negocio para el control del acceso	Política
1. Director o Jefe de área requirente de respaldo de la información.	El acceso a la información, a los servicios de procesamiento de información y a los procesos del negocio se debería controlar con base en los requisitos de la seguridad y del negocio. Las reglas para el control del acceso deberán tener en cuenta las políticas de distribución y autorización de la información.	✓ Fortalecer la seguridad de la información institucional en lo que atañe a la gestión de tecnologías de la información y comunicaciones en el ambito de competencia de DTIC con el rnejoramento, monitoceo y seguimiento del control de acceso a los servicios tecnológicos. ✓ Cumplir con disposiciones gubernamentales alineadas a las buenas prácticas para gestión tecnológica, tales como: Normas de Control Interno de Ia Contralorla General del Estado; Acuerdo No. 166 del Registro Oficial del Ecuador, donde se especifica el Esquema Gubernamental de Seguridad de Ia Información (EGSI). ✓ Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados a la seguridad de la Información.
2. Director o Jefe de área requirente de respaldo de la	Las reglas y los derechos para el control del acceso para cada usuario o grupo de usuarios se deberían establecer con claridad en una política de control del acceso. Los controles del acceso son	✓ Cada funcionario es responsable de mantener la confidencialidad sobre las claves de acceso asignadas a él para uso a los servicios tecnológicos; por lo cual deberá mantenerlas de forma confidencial e intransferible, ✓ Todos los usuarios deberán autenticarse por los mecanismos de control de acceso

información	tanto lógicos como físicos (véase la sección 9) y se deberían considerar en conjunto. A los usuarios y a) los proveedores de servicios se les debería brindar una declaración clara de los requisitos del negocio que deben cumplir los controles del acceso.	provistos por la DTIC antes de poder usar la infraestructura tecnológica del INEC. ✓ Los usuarios no deben proporcionar información a personal externo o interno no autorizado, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del INEC, ✓ La Dirección de Tecnologías de la información y comunicación no es responsable por incidentes producidos debido al no cumplimiento de estas políticas de seguridad.
3. Técnico del DTIC	El acceso a la información, a los servicios de procesamiento de información y a los procesos del negocio se debería controlar con base en los requisitos de la seguridad y del negocio. Las reglas para el control del acceso deberían tener en cuenta las políticas de distribución y autorización de la información.	✓ La gestión de acceso al datacenter estará a cargo de la DTIC. ✓ Todo acceso físico al datacenter será restringido debiéndose gestionar y documentar, lo cual consta en el Procedimiento para acceso a los servicios tecnológicos ✓ El acceso al *datacenter* y *racks* de redes de TI están restringidos y sólo pueden ingresar los administradores de los servicios tecnológicos respectivos ✓ Todo acceso autorizado al *datacenter* será asentado en un registro de ingreso a éste. el mismo que consta en el procedimiento del Acceso a los servicios tecnológicos de DTIC ✓ Para el ingreso será indispensable hacerlo solamente con tarjetas de control de acceso.
4. Funcionarios Coordinación Zonal 3	a) diferenciación entre reglas que siempre se deben hacer cumplir y directrices que son opcionales o condicionales;	✓ Cada funcionario es responsable de mantener la confidencialidad sobre las claves de acceso asignadas a él para uso a los servicios tecnológicos; por lo cual deberá mantenerlas de forma confidencial e intransferible.

	b) establecimiento de reglas basadas en la premisa "En general, todo está prohibido, a menos que esté expresamente permitido" y no en la regla más débil de " En general, todo está permitido, a menos que esté expresamente prohibido"; c) cambios en las etiquetas de la información (véase el numeral 7.2) que son iniciados automáticamente por los servicios de procesamiento de información y aquellos iniciados a discreción del usuario; d) cambios en los permisos de usuario que son iniciados automáticamente por los servicios de procesamiento de información y aquellos iniciados por un administrador.	✓ Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la DTIC antes de poder usar la infraestructura tecnológica del INEC. ✓ Los usuarios no deben proporcionar información a personal externo o interno no autorizado, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del INEC. ✓ La Dirección de Tecnologías de la Información y comunicación no es responsable por incidentes producidos debido al no cumplimiento de estas políticas de seguridad.

Elaboración propia

5.3.3.1.4 Gestión de la continuidad del negocio

9: Gestión de la continuidad del negocio

Políticas de seguridad de la información basadas en la norma ISO 27002	
Institución	Coordinación zonal del INEC - Ambato
Política	Política para la Gestión de la continuidad del negocio
Objetivo	Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.
Responsables	
Cargo	**Responsabilidad**
1. Personal del Departamento de Tecnologías de Información y Comunicación (DTIC)	✓ Revisar constantemente los planes que estén bajo su responsabilidad, para identificar cambios en las disposiciones relativas a las actividades del DTIC aún no reflejadas en los planes de continuidad. ✓ Verificar el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.
2. Responsable de Seguridad de la Información en el Departamento de Tecnologías de Información y Comunicación (DTIC)	✓ Implementar controles de seguridad de la información en los servicios tecnológicos que son administrados por el DTIC, de acuerdo a como se encuentra dispuesto en el EGSI. ✓ Estar en constante participación en las definiciones, documentación, pruebas y actualizaciones de los planes de contingencia. ✓ Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o actividades del DTIC. ✓ Realizar evaluaciones contantes de los riesgos para determinar el impacto de esas interrupciones.

	✓ Identificar controles preventivos y correctivos. ✓ Desarrollar un plan estratégico tecnológico para asegurar la continuidad de las actividades del DTIC.
3. Coordinador de la Continuidad de TI	✓ Identificar y priorizar procesos, activos involucrados en procesos críticos del DTIC. ✓ Establecer el grado de criticidad de los procesos identificados conjuntamente con las personas involucradas en los servicios tecnológicos.
4. Comité de seguridad de la información institucional	✓ Coordinar la administración de continuidad operatoria de los sistemas de tratamiento de información frente a interrupciones imprevistas.

Elaboración propia

I. Introducción

El presente documento se dicta en cumplimiento de las disposiciones legales vigentes y establece los lineamientos que deben seguirse para gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico que son administrados y ofrecidos por la Dirección de Coordinación Zonal 3 del INEC.

II. Alcance

Esta política se aplica en todos los ámbitos relacionados con los procesos críticos, ya sean internos o externos vinculados a través de contratos o acuerdos con terceros.

III. Disposiciones generales

Se debería implementar un proceso de gestión de la continuidad del negocio para minimizar el impacto y la recuperación por la pérdida de activos de información en la organización (la cual puede ser el resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación. En este proceso es conveniente identificar los procesos críticos para el negocio e

integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones.

Las consecuencias de desastres, fallas de la seguridad, pérdida del servicio y disponibilidad del servicio se deberían someter a un análisis del impacto en el negocio. Se deberían desarrollar e implementar planes de continuidad del negocio para garantizar la restauración oportuna de las operaciones esenciales. La seguridad de la información debería ser una parte integral de todo el proceso de continuidad del negocio y de otros procesos de gestión en la organización.

La gestión de la continuidad del negocio debería incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, limitar las consecuencias de los incidentes dañinos y garantizar la disponibilidad de la información requerida para los procesos del negocio.

IV. Acciones

10: Acciones de la gestión de la continuidad del negocio

Cargo	Acción Norma 27002 – (Numeral 14) Gestión de la continuidad del negocio	Política
1. Personal del Departamento de la (DTIC).	**Norma 27002 – (Numeral 14.1.1) Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio** Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de la seguridad de la información necesarios para la continuidad del negocio de la organización.	✓ Todos los planes de continuidad deberán ser difundidos a través de medios audiovisuales e impresos a fin de crear conciencia de la importancia de conocer que hacer en caso de haber una interrupción de un servicio critico. ✓ En el caso de ausencia del Coordinador de Continuidad de los servicios tecnológicos, deberá designarse un delegado responsable de cumplir con las actividades a cargo. ✓ Al momento de implementar un nuevo sistema en la DTIC, se deberá realizar el análisis de la criticidad del mismo para posteriormente considerar la elaboración del plan de continuidad respectivo.
2. Responsable de Seguridad de la Información en la (DTIC)	**Norma 27002 – (Numeral 14.1.2) Continuidad del negocio y evaluación de riesgos**	Con el propósito de tener un plan estratégico y determinar un enfoque global con el que se abordará la continuidad de las actividades de DTIC se determina que se debe: a) Mantener los documentos de los procesos actualizados, utilizando la gestión de cambios.

	Los aspectos de la seguridad de la información en la continuidad del negocio se deberían basar en la identificación de los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos del negocio de la organización, por ejemplo fallas de los equipos, errores humanos, robo, desastres naturales y actos terroristas. Se debería continuar con una evaluación de riesgos para determinar la probabilidad y el impacto de tales interrupciones, en términos de tiempo, escala de daño y periodo de recuperación.	b) Crear procedimientos de respuesta a los incidentes. c) Definir los calendarios de pruebas e informes. d) Definir los acuerdos de niveles de servicios internos y con proveedores. e) Definir los contratos para servicios de recuperación, si fuera el caso. f) Definir las condiciones para activar los planes que describen el proceso a seguir antes de activar cada plan, así como sus responsabilidades g) Describir los procedimientos de respaldo para desplazar las actividades esenciales de los servicios tecnológicos o los servicios de soporte a lugares temporales alternos, y para devolver la operatividad de los procesos en los plazos establecidos. h) Describir los procedimientos de reanudación con las acciones a realizar para que las operaciones de los equipos y servicios vuelvan a la normalidad. i) Definir los activos y recursos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación de tos servicios. j) Distribuir la política, estrategias, procesos y planes generados.
3. Coordinador de la Continuidad de TI	**Norma 27002 – (Numeral 14.1.4) Estructura para la planificación de la continuidad del negocio** Cada plan debería tener un responsable específico. Los procedimientos de emergencia, los planes de recursos de emergencia manuales y de reanudación	EI personal de DTIC, con la asistencia del Coordinador de Continuidad, elaborará los planes de continuidad necesarios para garantizar la continuidad de Las actividades de DTIC. El proceso de planificación de la continuidad TI de las actividades considerará los siguientes puntos: a) Definir los equipos para la ejecución del plan, donde se destacan las funciones claves que serán realizadas por los responsables:

	deberían ser responsabilidad de los responsables de los recursos o procesos apropiados del negocio involucrados. Las disposiciones de respaldo para los servicios técnicos alternos, como servicios de procesamiento de información y comunicaciones, usualmente deberían ser responsabilidad de los proveedores del servicio.	i. Responsables de respuestas e incidentes: analizan el impacto de incidente; ii. Logística: responsable de reunir todos los medios para ayudar a la puesta en operación de las actividades; iii. Recuperación: puesta en servicio de la infraestructura. b) Desarrollar los procedimientos indicando el objetivo y el alcance, considerando las actividades y los tiempos de recuperación. c) Difundir y capacitar al personal responsable en los conceptos que contemplan la continuidad de los servicios tecnológicos. d) Definir las Estrategias: i. Seleccionar los sitios alternos y de almacenamiento externo; ii. Duplicado de los registros tanto físicos como electrónicos; iii. Métodos, procedimientos y procesos para la recuperación de los servicios. iv. Duplicar el suministro eléctrico; v. Estrategia de reinicio de las actividades: vi. Contratos de mantenimiento preventivo y correctivo: vii Estrategia adecuada de respaldos; viii. Seguros para los activos.
4. Comité de seguridad de la información institucional	**Norma 27002 – (Numeral 14.1.5) Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio**	Con el fin de establecer los planes de continuidad de los servicios tecnológicos identificados, el Coordinador conjuntamente con todos los involucrados deberán: a) Definir las actividades de los servicios y de las aplicaciones. b) Entender y establecer las complejidades e interrelaciones existentes entre:

	Las pruebas del plan de continuidad del negocio deberían asegurar que todos los miembros del equipo de recuperación y otro personal pertinente son conscientes de los planes y sus responsabilidades para la continuidad del negocio y la seguridad de la información, y conocen su función cuando se ejecuta un plan.	equipos, personas, tareas y departamentos, mecanismos de comunicación y relaciones con proveedores externos, los cuales pueden prestar servicios críticos que deben ser considerados. c) Identificar y valorar el impacto de las interrupciones de los procesos, aplicaciones y servicios tecnológicos, para cuantificar y calificar los impactos, además de conocer sus efectos. d) Identificar el tiempo máximo de interrupción permitida para cada servicio o aplicación critica. e) Analizar los riesgos, identificando las amenazas sobre los activos y su probabilidad de ocurrencia. f) Analizar las vulnerabilidades asociadas a cada activo y el impacto que puedan provocar sobre la disponibilidad g) Obtener un mapa de riesgos que permita identificar y priorizar aquellos que pueden provocar una paralización de las actividades de la institución. h) Crear una estrategia de gestión de control de riesgos y los planes de acción respectivos.

Elaboración propia

5.3.3.1.5 Respaldo y restauración de la información

11: Respaldo y restauración de la información

Políticas de seguridad de la información basadas en la norma ISO 27002	
Institución	Coordinación zonal del INEC - Ambato
Política	Política para el Respaldo y restauración de la información
Objetivo	Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.
Responsables	
Cargo	**Responsabilidad**
1. Director o Jefe de Área	Solicitar copia de respaldo o restauración de información.
2. Director de DTIC	✓ Decidir si aprueba o rechaza la solicitud de respaldo o restauración de información del requirente con su justificación. ✓ Solicitar informes mensuales con el responsable de las copias y restauración de información.
3. Jefe de TIC Zonal	✓ Supervisar labor del Administrador de respaldos ✓ Solicitar informes mensuales al Administrador de las copias y restauración de información. ✓ Responder al área solicitante el informe del administrador de respaldos acerca de las tareas cumplidas.
4. Administrador de respaldos	✓ Gestionar la realización de las copias de respaldo. ✓ Administrar el almacenamiento y medios requeridos para las copias de respaldo. ✓ Gestionar la verificación de los respaldos juntos con el responsable de seguridad de la información ✓ Controlar los periodos de tiempo de retención de las copias de respaldo y la rotación de los medios de almacenamientos. ✓ Informar al jefe de TIC zonal acerca de las tareas de administración de respaldos realizadas con informes mensuales con indicadores acerca de su labor.

5. Responsable de Seguridad de la Información del DTIC	✓ Verificar la restauración de las copias de respaldo de la información junto con el administrador de los respaldos. ✓ Validar e informar al director del DTIC y al oficial de seguridad de la información respecto a los cumplimientos del respaldo y restauración de información.
6. Oficial de seguridad de la información institucional	✓ Auditar, asesorar y monitorear el cumplimiento de los controles de seguridad de la información institucional mediante el seguimiento de la gestión del responsable de seguridad de la información del DTIC

Elaboración propia

I. Introducción

En vista de la necesidad de resguardar la información, es fundamental contar con el respectivo procedimiento de respaldos y su restauración en forma permanente en la institución. Esta es una buena manera de asegurar y mantener la continuidad la información.

II. Alcance

La aplicación de esta política contempla principalmente al Administrador de respaldos quién es el responsable de la aplicación de las acciones correspondientes

También tiene su alcance a las áreas responsables de realizar todos los respaldos que sean necesarios para garantizar la seguridad de la información de la Coordinación zonal del INEC.

III. Disposiciones generales

Se deben establecer procedimientos de rutina para implementar la política y la estrategia de respaldo acordada para hacer copias de la seguridad de los datos y probar sus tiempos de restauración.

IV. Acciones

12: Acciones del respaldo y restauración de la información

Cargo	Acción Norma 27002 – (Numeral 10.5) Respaldo	Política
1. Director o Jefe de Área	**Norma 27002 – (Numeral 10.5.1) Respaldo de la información** Se deberían hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.	Solicita mediante correo electrónico dirigido al Director de DTIC o Jefe de TIC zonales el requerimiento de respaldo o restauración de la información.
2. Director de DTIC	Es conveniente disponer de servicios de respaldo adecuados para garantizar que la información y el software esenciales se recuperan después de un desastre o una falla de los medios.	1. Analiza la viabilidad del requerimiento y responde el correo con la aprobación o rechazo justificado. 2. En caso de ser aprobado el requerimiento, remite al correo con autorización al Administrador de Respaldos (TIC Zonal).
3. Jefe de TIC Zonal	**10.6.1 Controles de las redes** Las redes se deberían mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.	1. Revisa, valida y aprueba los informes mensuales del Administrador de Respaldos. 2. Monitorea los indicadores reportados en los informes mensuales.

4. Administrador de respaldos	**10.7.1 Gestión de los medios removibles** Todos los procedimientos y niveles de autorización deberían estar documentados con claridad. Información adicional Los medios removibles incluyen cintas, discos, memorias de almacenamiento, unidades de almacenamiento removibles, discos compactos, discos de video digital (DVD) y medios impresos.	1. Elabora un informes a su jefe inmediato, indicando las caracteristicas de cada activo de TI (sevidor, equipo de red) y los servicios, priorizando la necesidad de respaldos. 2. Elabora la programación de la realización de las copias de respaldo, indicando los recursos requeridos. 3 Elabora calendario de rotación de los medios de almacenamiento de los respaldos, según como se indica en la Política para respaldo y restauración de la inforrnacion. 4. Ejecuta la tarea de respaldo de acuerdo a la programación realizada y al calendario de rotación de los medios de almacenamierno. 5. Elabora una bitácora, en la que registra su tarea de generación de copias de respaldos y cualquier novedad acontecida durante la ejecución de la tarea. 6. Verifica los respaldos de la informacion. 7. Valida el período de retencion y rotacion de los respaldos de acuerdo a la pogramacón y calendarios realizados. considerando la Política para respaldo y restauración de la iniorrnación. 8. Coloca la etiqueta a la copla de respaldo. 9. actualiza el inventario de las copias de respaldo. 10.Elabora un informe mensual con indicadores dirigido a su jefe inmediato e informando al Responsable de Seguridad de la información de DTIC acerca de las tareas de administración realizadas, referenciando el cumplimiento con la

		Política para respaldo y restauración de la información.
5. Responsable de Seguridad de la Información de la DTIC	**10.7.3 Procedimientos para el manejo de la información** Se deberían establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.	1. Revisa el informe mensual del Administrador de Respaldos 2. Genera el informe de cumplimento con las recomendaciones respecto a los hitos del EGSI relacionados con la gestión de respaldos de información, dirigido al Oficial de Segundad de la información Institucional, Director de DTIC e informando a su jefe inmediato.
6. Oficial De Seguridad de la Información Institucional	**10.7.4 Seguridad de la documentación del sistema** La documentación del sistema debería estar protegida contra el acceso no autorizado. Guía de implementación Para asegurar la documentación del sistema, se deberían tener en cuenta los siguientes elementos: a) la documentación del sistema se debería almacenar con seguridad; b) la lista de acceso a la documentación del sistema se debería mantener mínima y debería estar autorizada por el responsable de la aplicación;	1. Establece directrices en consenso con Comité de Seguridad para las medidas que se deben tomar y comunica al Responsable de Seguridad de la información de DTIC las decisiones tomadas respecto a sus informes. 2. Reporta sobre el cumplimiento institucional de hitos EGSI a la Secretaría Nacional de Administración Pública (SNAP).

	c) la documentación del sistema en la red pública o que se suministra a través de una red pública, debería tener protección adecuada. Información adicional La documentación del sistema puede contener variada información sensible, como descripciones de procesos de aplicación, procedimientos, estructuras de datos y procesos de autorización.	

Elaboración propia

5.3.3.1.6 Reporte sobre los eventos

13: Reporte sobre los eventos

Políticas de seguridad de la información basadas en la norma ISO 27002	
Institución	Coordinación zonal del INEC - Ambato
Política	Política para el Reporte sobre los eventos
Objetivo	Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.
Responsables	
Cargo	**Responsabilidad**
1. Usuario interno	✓ Reportar eventos, incidentes y requerimientos.
2. Usuario externo	✓ Reportar eventos o incidentes ante un técnico de soporte del DTIC
3. Administrador de procesos TI	✓ Monitorear y analizar el reporte de eventos de los servicios tecnológicos y dar el tratamiento respectivo.
4. Responsable de seguridad de la información del DTIC	✓ Analizar los eventos de seguridad de la información reportados. ✓ Identificar cuáles son los eventos precisos a detectar. ✓ Definir indicadores para medir la gestión de eventos. ✓ Revisar informes mensuales con indicadores acerca de eventos de seguridad de la información. ✓ Reportar al oficial de seguridad de la información y al director del DTIC acerca del cumplimento de los controles de seguridad de la información con respecto a eventos.
5. Oficial de seguridad de la información	✓ Analizar el reporte de eventos de seguridad de la información, verificar las acciones tomadas y coordinar con otras instituciones.

Elaboración propia

I. Introducción

La presente política trata de definir los pasos a seguir para el reporte sobre los eventos de seguridad de la información de los recursos tecnológicos que son administrados por Coordinación zonal del INEC.

II. Alcance

Detectar, recopilar, y reportar todo suceso que tiene importancia para la estructura de toda la información así como las notificaciones creadas por los servicios, los elementos de configuración o las herramientas, control y reporte de las instancias respectivas para su gestión.

III. Disposiciones generales

Es conveniente establecer el reporte formal del evento y los procedimientos de escalada.

Todos los empleados, contratistas y usuarios de tercera parte deberían tener conciencia sobre los procedimientos para el reporte de los diferentes tipos de evento y las debilidades que puedan tener impacto en la seguridad de los activos de la organización.

Se les debería exigir que reporten todos los eventos de seguridad de la información y las debilidades tan pronto sea posible al punto de contacto designado.

IV Acciones

14: Acciones del reporte sobre los eventos

Cargo	Acción Norma 27002 – (Numeral 13.1) Reporte sobre los eventos y las debilidades de la seguridad de la información	Política
1. Usuario interno	Es conveniente establecer el reporte formal del evento y los procedimientos de escalada.	Genera un reporte a soporte técnico.
2. Usuario externo	Todos los empleados, contratistas y usuarios de tercera parte deberían tener conciencia sobre los procedimientos para el reporte de los diferentes tipos de evento y las debilidades que puedan tener impacto en la seguridad de los activos de la organización. Se les debería exigir que reporten todos los eventos de seguridad de la información y las debilidades tan pronto sea posible al punto de contacto designado.	Informa a un técnico de la DTIC, como punto de contacto para el registro respectivo.

3. Administrador de procesos TI	Se debería instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente que establezca la acción que se ha de tomar al recibir el reporte sobre un evento de seguridad de la información. Se debería establecer un punto de contacto para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto se conoce en toda la organización, siempre está disponible y puede suministrar respuesta oportuna y adecuada.	1. Analiza el tipo y forma de los reportes de eventos identificados y registrados por los elementos de configuración. 2. Filtra y reduce los datos duplicados, considerando lo indicado en la política para la gestión de eventos. 3. Realiza la correlación y pone en marcha los mecanismos pertinentes para que se produzca una respuesta, según lo considerado en la política de gestión de eventos. 4. Procede al registro. 5. Elabora informe de los eventos presentados y envía al Responsable de Seguridad de la Información de DTIC.
4. Responsable de seguridad de la información del DTIC	Deberían existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información. La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debería utilizar para	1. Solicita y revisa los reportes mensuales de los indicadores respecto a los eventos acontecidos en los servicios tecnológicos 2. Genera el informe consolidado para el Oficial de Seguridad de la lnformación Institucional e informa al Director de DTIC

	identificar los incidentes recurrentes o de alto impacto.	
5. Oficial de seguridad de la información	La evaluación de los incidentes de seguridad de la información puede indicar la necesidad de mejorar o agregar controles para limitar la frecuencia, el daño y el costo de futuras recurrencias, o de considerarlos en el proceso de revisión de la política de seguridad (véase el numeral 5.1.2).	1. Establece directrices en consenso con el Comité de Seguridad para las medidas que se deben tomar comunica al Responsable de Segundad de la información de DTIC las decisiones tomadas respecto a sus informes.

Elaboración propia

5.3.3.1.7 Acceso a las aplicaciones y a la información

15: Acceso a las aplicaciones y a la información

Políticas de seguridad de la información basadas en la norma ISO 27002	
Institución	Coordinación zonal del INEC - Ambato
Política	Política para el Acceso a las aplicaciones y a la información
Objetivo	Evitar el acceso no autorizado a la información contenida en los sistemas de aplicación.
Responsables	
Cargo	**Responsabilidad**
1. Director del DTIC o Jefe de área	✓ Analizar las solicitudes enviadas por otras unidades de la institución.
2. Jefe de Tic Zonal	✓ Coordina las visitas al data center, asigna los accesos permanentes, temporales para los servicios tecnológicos que administra el DTIC
3. Técnico Delegado de la unidad de infraestructura	✓ Realiza los registros de las personas que ingresan al data center y revisar las actividades que realizan al interior para informar cualquier evento de seguridad.
4. Responsable de Seguridad de la Información del DTIC	✓ Configura los equipos para acceso a internet. ✓ Validar e informar al Director del DTIC y al oficial de seguridad de la información institucional respecto al acceso a los servicios tecnológicos.
5. Oficial de seguridad de la información institucional.	✓ Auditar, asesorar y monitorear el cumplimiento de los controles de seguridad de la información institucional mediante el seguimiento de la gestión del responsable de seguridad de la información del DTIC.

Elaboración propia

I. Introducción

Esta política se presenta para asegurar el control de acceso a la información utilizando los mecanismos que eviten el acceso de personas que no están autorizadas a los diferentes servicios tecnológicos disponibles en la institución.

II. Alcance

La presente política es aplicable a todos los funcionarios de la institución y a aquellos visitantes o proveedores que soliciten acceso a los servicios tecnológicos que administra la Coordinación zonal del INEC.

III. Disposiciones generales

Se deberían usar medios de la seguridad para restringir el acceso a los sistemas de aplicación y dentro de ellos.

El acceso lógico al *software* de aplicación y a la información se debería restringir a usuarios autorizados.

Los sistemas de aplicación deberían:

a) controlar el acceso de usuarios a la información y a las funciones del sistema de aplicación, de acuerdo con una política definida de control de acceso;
b) suministrar protección contra acceso no autorizado por una utilidad, el software del sistema operativo y software malicioso que pueda anular o desviar los controles del sistema o de la aplicación;
c) no poner en peligro otros sistemas con los que se comparten los recursos de información.

IV. Acciones

16: Acciones del acceso a las aplicaciones y a la información

Cargo	Acción Norma 27002 – (Numeral 11.6) Control de acceso a las aplicaciones y a la información	Política
1. Director del DTIC o Jefe de área	El acceso lógico al software de aplicación y a la información se debería restringir a usuarios autorizados. Los sistemas de aplicación deberían: a) controlar el acceso de usuarios a la información y a las funciones del sistema de aplicación, de acuerdo con una política definida de control de acceso; b) suministrar protección contra acceso no autorizado por una utilidad, el software del sistema operativo y software malicioso que pueda anular o desviar los controles del	✓ Analiza la viabilidad del requerimiento, autoriza, responde el correo y asigna al técnico la realización del requerimiento. ✓ En caso de no autorizar el requerimiento, responde al remitente del correo con la respectiva justificación.

	sistema o de la aplicación; c) no poner en peligro otros sistemas con los que se comparten los recursos de información.	
2. Jefe de TIC Zonal	Las restricciones del acceso se deberían basar en los requisitos de las aplicaciones individuales del negocio. La política de control de acceso también debería ser consistente con la política de acceso de la organización (véase el numeral 11.1). Se debería considerar la aplicación de las siguientes directrices con el objeto de dar soporte a los requisitos de restricción del acceso: a) proporcionar menús para controlar el acceso a las funciones del sistema de aplicación; b) controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, eliminar y ejecutar;	✓ Atiende el requerimiento y coordina fecha y hora. ✓ En caso de no autorizar envía correo electrónico negando autorización e indicando el motivo ✓ En caso de autorizar y si es funcionario del INEC envía calendario de fechas disponibles mediante correo. ✓ Designa técnico delegado con acceso permanente que acompañara a los visitantes.

	c) controlar los derechos de acceso de otras aplicaciones;	
3. Técnico Delegado de la unidad de infraestructura	Los sistemas sensibles deberían tener un entorno informático dedicado (aislados).	✓ Registra y programa visita interna o externa en el calendario ✓ Solicita al visitante se registre en el formulario de ingreso. ✓ Acompaña al visitante desde el inicio al fin de las actividades ✓ Solicita al visitante registre la salida en la hoja de registro detallando en el campo Observaciones la fecha y hora de inicio fin de la visita, además de registrar brevemente las actividades que se, realizaron durante la visita.

Elaboración propia

5.3.4 Implementación

Es responsabilidad de la Dirección de la Coordinación Zonal 3 del INEC aplicar las políticas, normas y procedimientos de seguridad de información en base a la norma ISO 27002 para corregir las vulnerabilidades existentes en el proceso actual.

5.3.5 Pruebas

Se realizarán todas las pruebas que sean necesarias, luego de la aplicación de las políticas de seguridad, con el fin de verificar su correcta implementación por parte de las autoridades de la institución, de manera que se verifique si estas políticas están cumpliendo con los objetivos planteados.

5.3.6 Mantenimiento

Se deber realizar el mantenimiento periódico con las respectivas actualizaciones de las políticas, normas y procedimientos con la finalidad de estar al día en cuanto a su estructura, aplicando además los correctivos que sean necesarios para que mantengan su efectividad y se logre minimizar o eliminar los riesgos de la seguridad de la información de la Coordinación Zonal 3 del INEC.

Capítulo 6

Conclusiones y Recomendaciones

6.1 Conclusiones

- ✓ De acuerdo al análisis de la situación actual de la Coordinación Zonal 3 del INEC, se evidenció que existen vulnerabilidades que afectan la seguridad de la información, atribuidas a la falta de aplicación de las políticas que permitan asegurar la información procesada en la institución

- ✓ La implementación de las políticas de seguridad de información es factible, debido a que pueden ser aplicadas en las áreas en las cuales existen riesgos para generar la información

- ✓ Las políticas, normas y procedimientos de seguridad sobre las plataformas tecnológicas y los sistemas de información garantizan la seguridad en la información de la Coordinación Zonal 3 del INEC, por ser las que se adaptan a las necesidades de la institución.

6.2 Recomendaciones

- ✓ Al existir vulnerabilidades o riesgos que pongan en peligro la información es recomendable que permanentemente sea analizada la situación de la Coordinación Zonal 3 del INEC, con la finalidad de tomar los correctivos necesarios que protejan la seguridad de la información.

- ✓ Es recomendable que se apliquen las políticas propuestas en el presente trabajo debido al alcance que éstas tienen y al resultado positivo que se espera de ellas.

- ✓ Debido a que las políticas, normas y procedimientos de seguridad sobre las plataformas tecnológicas y los sistemas de información están basadas en las normas ISO 27002, pueden ser aplicadas en la Coordinación Zonal 3 del INEC, cumpliendo así con los requerimientos del el Acuerdo No. 166 del Registro Oficial del Ecuador, donde se especifica el esquema gubernamental de seguridad de la información.

Apéndices

Apéndice A. Cuestionario de la entrevista No. 1

INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS

COORDINACIÓN ZONAL 3 (INEC)

Entrevista de control seguridad realizada a personeros del departamento de tecnologías de información y comunicación.

1. ¿Existen Políticas de Seguridad de Información aplicadas a la Institución?

2. ¿Considera necesario el desarrollo de Políticas de seguridad de Información?

3. Cómo se respaldan la información

4. Existen amenazas de perdida de información

5. ¿Se ha tenido en cuenta la seguridad informática como criterio en las fases de análisis y diseño de las aplicaciones usadas en sus proyectos?

6. ¿Se ha permitido el acceso a la información sólo a personas debidamente autorizadas, tanto para administrativos cómo para personas externas?

7. ¿Se ha establecido algún control para que los usuarios tanto internos como externos no modifiquen la información de modo no autorizado?

8. ¿Los responsables de la información han podido acceder en todo momento a los datos permitidos para ellos?

9. ¿Se tiene definida alguna política para la realización de copias de seguridad de la información?

10.¿Se tiene definida alguna política de restauración de información en caso de ataques informáticos?

11.¿Quiénes son los responsables de tomar decisiones referentes a seguridad informática?

12.¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?

13.¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la institución?

14.¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?

15.¿Se documentan los cambios efectuados?

16.¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?

17.¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de censores?

18.¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?

19.¿Existen prohibiciones para fumar, consumir alimentos y bebidas?

20. En cuanto a las pruebas del cableado, ¿el departamento de TI, genera sus propios ataques para probar la solidez de la red y encontrar posibles fallas?

21.¿Se cuenta con un inventario trimestral de todos los equipos que integran el centro de cómputo de la Coordinación Zonal 3 INEC?

22.¿Existen lugares de acceso restringido?

Apéndice B. Cuestionario de la entrevista No. 2

INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS

COORDINACIÓN ZONAL 3 (INEC)

Entrevista de control seguridad de equipos, realizada a personeros del departamento de tecnologías de información y comunicación.

Cuestionario No. 2

1. ¿Existen metodologías de respaldo de información?
2. ¿Existe un administrador de sistemas que controle las cuentas de los usuarios?
3. ¿Existe algún estándar para la creación de contraseñas?
4. ¿Se obliga, cada cierto tiempo a cambiar la contraseña?
5. ¿Se tienen software antivirus instalados en los equipos de cómputo?
6. ¿Se tienen instalados anti malware en los equipos de cómputo?
7. ¿Cuenta con licencias de software?
8. ¿Existe un proceso para adquirir nuevas licencias?
9. ¿Se sanciona al integrante del departamento si instala software no permitido?
10. ¿Los usuarios de bajo nivel tienen restringido el acceso a las partes más delicadas de las aplicaciones?

11. ¿El equipo de cómputo cuenta con suficiente espacio en HD en función de los servicios que otorga?

12. ¿El equipo de cómputo cuenta con suficiente memoria RAM en función de los servicios que otorga?

Gracias por su colaboración

APÉNDICE C. Entrevista No. 1

INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS

COORDINACIÓN ZONAL 3 (INEC)

Entrevista de control seguridad realizada a personeros del departamento de tecnologías de información y comunicación.

1. **¿Existen Políticas de Seguridad de Información aplicadas a la Institución?**

   No

2. **¿Considera necesario el desarrollo de Políticas de seguridad de Información?**

   Si

3. **Cómo se respaldan la información**

   Se lo hace en la noche diariamente.

4. **Existen amenazas de perdida de información**

   Si por la falta de seguridades.

5. **¿Se ha tenido en cuenta la seguridad informática como criterio en las fases de análisis y diseño de las aplicaciones usadas en sus proyectos?**

   No debido a la falta de equipo.

6. **¿Se ha permitido el acceso a la información sólo a personas debidamente autorizadas, tanto para administrativos cómo para personas externas?**

   Se controla de acuerdo al nombre usuario asignado a cada usuario de la institución.

7. **¿Se ha establecido algún control para que los usuarios tanto internos como externos no modifiquen la información de modo no autorizado?**

   No

8. **¿Los responsables de la información han podido acceder en todo momento a los datos permitidos para ellos?**

   Sólo el administrador

9. **¿Se tiene definida alguna política para la realización de copias de seguridad de la información?**

   No

10. **¿Se tiene definida alguna política de restauración de información en caso de ataques informáticos?**

    Si se logró respaldar la información en el servidor principal se puede hacer un backup en la zonal de Guayaquil en las bases de datos.

11. **¿Quiénes son los responsables de tomar decisiones referentes a seguridad informática?**

    El director de TI.

12. **¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?**

    No

13. **¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la institución?**

    Si en zonal de Guayaquil

14. **¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?**

    No

15. **¿Se documentan los cambios efectuados?**

    Con oficios de autorización.

16. **¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?**

    No

17. **¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de censores?**

    No

18. **¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?**

    Se cuenta con guardias de seguridad.

19. **¿Existen prohibiciones para fumar, consumir alimentos y bebidas?**

    Si

20. **En cuanto a las pruebas del cableado, ¿el departamento de TI, genera sus propios ataques para probar la solidez de la red y encontrar posibles fallas?**

    No

21. **¿Se cuenta con un inventario trimestral de todos los equipos que integran el centro de cómputo de la Coordinación Zonal 3 INEC?**

No es anual

22. ¿Existen lugares de acceso restringido?

Si donde se encuentra el Rack de comunicaciones.

Gracias por su colaboración

APÉNDICE D. Entrevista No. 2

INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS

COORDINACIÓN ZONAL 3 (INEC)

Entrevista de control seguridad de equipos, realizada a personeros del departamento de tecnologías de información y comunicación.

1. **¿Existen metodologías de respaldo de información?**

   No
2. **¿Existe un administrador de sistemas que controle las cuentas de los usuarios?**

   Si
3. **¿Existe algún estándar para la creación de contraseñas?**

   No
4. **¿Se obliga, cada cierto tiempo a cambiar la contraseña?**

   Cada 45 días.
5. **¿Se tienen software antivirus instalados en los equipos de cómputo?**

   Si McAfee
6. **¿Se tienen instalados anti malware en los equipos de cómputo?**

   Paquete McAfee antivirus y anti malware
7. **¿Cuenta con licencias de software?**

   No en todos los equipos

   Sólo en la adquisición de nuevos equipos se lo hace con licencias
8. **¿Existe un proceso para adquirir nuevas licencias?**

   Cada 2 años de hace renovación de licencias
9. **¿Se sanciona al integrante del departamento si instala software no permitido?**

   No se puede controlar la instalación de software no permitido
10. **¿Los usuarios de bajo nivel tienen restringido el acceso a las partes más delicadas de las aplicaciones?**

    Se pretende instalar una herramienta de monitoreo
11. **¿El equipo de cómputo cuenta con suficiente espacio en HD en función de los servicios que otorga?**

Solo los equipos que han sido adquiridos recientemente.

12. **¿El equipo de cómputo cuenta con suficiente memoria RAM en función de los servicios que otorga?**

    Sólo los indispensables.

Gracias por su colaboración

Referencias

Agé, M. - Sébastien BAUDRU - Nicolas CROCFER - Robert CROCFER - Franck EBEL - Jérôme HENNECART - Sébastien LASSON - David PUCHE - Raphaël RAULT. (2013). "Seguridad informática - Ethical Hacking: Conocer el ataque para una mejor defensa". ACISSI. Auditoría, Consejo, Instalación y Seguridad de Sistemas de Información. Ediciones ENI. 2da Edición. Barcelona, España.

Aguilera, P. (2010). "Seguridad informática. Informática y comunicaciones". Editorial Editex, S. A. Madrid, España.

Amaya, C. (2013). "ISO/IEC 27002: 2013 y los cambios en los dominios de control". Welivesecurity. Disponible en: http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/.

Areitio, J. (2008). "Seguridad de la información. Redes, informática y sistemas de información". LEARNING PARANINFO, S. A. Madrid, España.

Barranco de Areba, J. (2001). "Metodología del análisis estructurado de sistemas". Universidad pontificia Comillas de Madrid. Madrid, España.

Berciano, J. (2010). "La importancia y la necesidad de proteger la información sensible". Redseguridad.com. Disponible en: http://www.redseguridad.com/opinion/articulos/la-importancia-y-la-necesidad-de-proteger-la-informacion-sensible

Borbón, J. (2011) "Buenas prácticas, estándares y normas". REVISTA SEGURIDAD, DEFENSA DIGITAL. REVISTA BIMESTRAL numero-11. Disponible en: http://revista.seguridad.unam.mx/numero-11/buenas-pr%C3%A1cticas- est%C3%A1ndares-y-normas

Carrillo, A. y otros. "Big Data en los entornos de Defensa y Seguridad". Instituto Español de Estudios estratégicos. (IEEE). España. (p. 7).

Corletti, A. (2011). “Seguridad por niveles”. DARFE Learning Consulting, S. L. Madrid, España.

Esponda, Alfredo, Penalva, Gerardo, Palavicini, Jaime, Navarrete. Guillermo. (2001). Hacia una calidad más robusta con ISO 9000: 2000. Panorama Editorial, S. A. de C. V. México D. F., México

Fernández, V. (2006).”Desarrollo de sistemas de información: una metodología basada en el modelado”. Ediciones de la Universidad Politécnica de Catalunya. Barcelona, España.

Franco, D. y Guerrero, C. (2013). “Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC 27002”. LACCEI [En línea]. Disponible en: http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP239.pdf. [Último acceso: 11 10 2014].

FUNIVSCYL. (2012). “Módulo formativo universitario de creación de empresas de base tecnológica”. Fundación Universidades Castilla y León. España.

GOVERNANCE INSTITUTE. (2008). “Alineando CobiT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio del negocio”. Un reporte para gestión del ITGI (IT Governance Institute) y la OGC (Oficina Gubernamental de Comercio)”. EEUU. Disponible en: http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf

Gutiérrez, J., Tena, J. (2003). Protocolos criptográficos y seguridad en redes. Ed Servicio de Publicaciones de la Universidad de Cantabria, 2003. Santander, España.

Heredero, Carmen de P., José Joaquín López-Hermoso Agius, Santiago Martín-Romo Romero, Sonia Medina Salgado, Antonio Montero Navarro, Juan José Nájera Sánchez. (2006). “Dirección y gestión de los sistemas de información en la empresa”. ESIC EDITORIAL. 2da. Edición. Madrid, España.

ISO27000, (2011). “ControlesISO27002-2005”. Disponible en: http://www.iso27000.es/download/ControlesISO27002- 2005.pdf

ISO 27002. (2009). “Código de Práctica para la Gestión de la Seguridad de Información”.

Markus, E. (2008). “Gestión de Riesgo en la Seguridad Informática”. Disponible en : https://protejete.wordpress.com/

Mieres, J. (2009). “Buenas prácticas en seguridad informática”. ESET, LLC. Disponible en: http://www.esetla.com/pdf/prensa/informe/buenas_practicas_seguridad_informatica.pdf

Mifsud, E. (2012). “Políticas de seguridad. ¿Cómo podemos proteger el sistema informático?”. Observatorio tecnológico. Gobierno de España. Madrid, España. Disponible en: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=4

Montes, K. (2014). “Identificación de los Controles de Seguridad Física del Centro de Datos de la Universidad Autónoma de Occidente”. Repositorio Institucional Universidad Autónoma de Occidente. Disponible: http://bdigital.uao.edu.co/bitstream/10614/6604/1/T04621.pdf.

Monsalve, A. (2003). “Teoría de Información y Comunicación Social”. Ediciones ABYA-YALA. Quito, Ecuador.

Romero, C. y Castillo, J. (2011). “Estándar ISO/IEC 27002 para Centro de Cómputo de la Facultad de Ingeniería en Electricidad y Computación (FIEC-ESPOL)”. Tesis. Repositorio de la Escuela Politécnica del Litoral. Guayaquil, Ecuador

Romo, D. y Valarezo, J. (2012). “Análisis e implementación de la Norma ISO 27002 para el Departamento de Sistemas de la Universidad Politécnica Salesiana Sede Guayaquil”. Tesis. Repositorio de la Universidad Politécnica Salesiana sede Guayaquil. Guayaquil, Ecuador.

Sánchez, J., (2003). “Ingeniería de proyectos informáticos: actividades y procedimientos”. Publicaciones de la Universidad Jaume I. Castello de la Plana, España.

Segunda Cohorte del Doctorado en Seguridad Estratégica. (2014). "Seguridad de la Información". Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica. Universidad de San Carlos. Guatemala, Guatemala.

Suárez y Alonso, R. (2007). "Tecnologías de la Información y la Comunicación". Ideaspropias Editorial. Vigo, España.

Téllez, J. (1988). Contratos, riesgos y seguros informáticos. Universidad Autónoma de México. UNAM. Instituto de Investigaciones Jurídicas. México D.F., México.

Resumen Final

Desarrollo de políticas de seguridad de la información basadas en las Normas ISO 27002 para una Coordinación Zonal del INEC

Dorys Natalia Ledezma Espin

113 páginas

Proyecto dirigido por: Mg. José Marcelo Balseca Manzano

Las instituciones que procesan grandes cantidades de información y comunicación, requieren de toda la seguridad posible para el cumplimiento de su gestión institucional y de servicio a la comunidad logrando la eficiencia, e integridad de la información y que ésta no sea modificada, dañada o eliminada por parte de terceras personas que acceden a la misma.

El objetivo principal del presente trabajo consiste en Desarrollar políticas de seguridad de la información basadas en las normas ISO 27002 para una Coordinación Zonal del INEC, de manera que se permita garantizar la adecuada aplicación de las políticas, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información. El presente trabajo se enfocó en analizar los requerimientos necesarios sobre cómo se encuentra la información actual de la institución, para lo cual se realizaron entrevistas personales a personeros de la Coordinación Zonal 3 del INEC y luego se aplicó la Metodología de Cascada, la cual es la que más se adapta al presente trabajo de titulación, aplicado a una Coordinación Zonal 3 del INEC para lograr el objetivo planteado en el presente trabajo de titulación.