UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera de Software

Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información en la Cooperativa de Ahorro y Crédito Imbacoop Ltda., aplicando el estándar ISO/IEC 27001, para fortalecer la disponibilidad de los servicios.

Trabajo de grado previo a la obtención del título de Ingeniero de Software presentado ante la ilustre Universidad Técnica del Norte.

Autor:

Sr. William Andrés De La Torre Yamberla

Director:

MSc. Daisy Elizabeth Imbaquingo Esparza

Ibarra – Ecuador

2024

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1004631865		
APELLIDOS Y NOMBRES:	DE LA TORRE YAMBERLA WILLIAM ANDRES		
DIRECCIÓN:	OTAVALO, ILUMAN		
EMAIL:	wadelatorrey@utn.edu.ec		
TELÉFONO FIJO:	062946047	**TELÉFONO MÓVIL:**	0968870799

DATOS DE LA OBRA					
TÍTULO:	DESARROLLO DE UN PLAN DE SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO IMBACOOP LTDA., APLICANDO EL ESTÁNDAR ISO/IEC 27001, PARA FORTALECER LA DISPONIBILIDAD DE LOS SERVICIOS.				
AUTOR(ES):	WILLIAM ANDRES DE LA TORRE YAMBERLA				
FECHA:	09/02/2024				
PROGRAMA:		**X**	PREGRADO		POSGRADO
TÍTULO POR EL QUE OPTA:	INGENIERO DE SOFTWARE				
DIRECTOR:	MSc. Daisy Imbaquingo				
ASESOR 1:	MSc. Fernando Garrido				
ASESOR 2:	MSc. Pedro Granda				

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 15 días del mes de febrero de 2024

EL AUTOR:

ESTUDIANTE

William Andrés De La Torre Yamberla

C.I: 100463186-5

CERTIFICACIÓN DIRECTOR

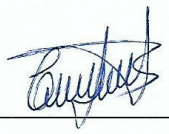
Ibarra 09 de febrero del 2024

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE TITULACIÓN

Por medio del presente yo MSc. Daisy Imbaquingo, certifico que el Sr. William Andrés De La Torre Yamberla portador de la cédula de ciudadanía número 1004631865, ha trabajado en el desarrollo del proyecto de grado **"Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información en la Cooperativa de Ahorro y Crédito Imbacoop Ltda., aplicando el estándar ISO/IEC 27001, para fortalecer la disponibilidad de los servicios"**, previo a la obtención del Título de Ingeniero en Software realizado con interés profesional y responsabilidad que certifico con honor de verdad.

Es todo en cuanto puedo certificar la verdad.

Atentamente.



MSc. Daisy Imbaquingo

DIRECTORA DE TRABAJO DE GRADO

DEDICATORIA

Mi gratitud a Dios, por guiarme con sabiduría en este arduo camino, a mi familia, mis padres María Juana Yamberla y José De La Torre quienes siempre estuvieron en las etapas más difíciles de mi vida, me brindaron su amor, confianza, apoyo y ayuda sin la cual no hubiese sido posible cumplir mi sueño, a mis hermanos quienes siempre estuvieron a mi lado, a todos mis compañeros y amigos con los cuales pude compartir buenos momentos, como no mencionar a los docentes que me brindaron sus conocimientos y experiencias para ser una mejor persona y un buen profesional, y de manera especial a, quien es el principio de esta travesía, la persona más importantes en mi vida y en este proceso. Gracias a todos.

William Andrés De La Torre Yamberla

AGRADECIMIENTO

Agradezco infinitamente a Dios por ser incondicional en mi vida, por nunca soltarme, por llenarme de fortaleza y guiarme con sabiduría en todo este proceso, a mis padres, que con esfuerzo, dedicación y arduo trabajo siempre estuvieron a mi lado apoyándome, a la prestigiosa y distinguida Universidad Técnica del Norte, Facultad en Ciencia Aplicadas FICA, Carrera de Ingeniería en Software quien me dio la oportunidad y me abrió las puertas para cumplir mi sueño. A mis docentes por compartir su tiempo y conocimientos en mi formación personal y profesional, y a todos quienes me han apoyado directa e indirectamente en todo este camino de mi vida estudiantil.

Un agradecimiento especial a mi directora de Tesis al MSc. Daisy Imbaquingo, quien, con su apoyo, concejos y recomendaciones, ayudó a que este trabajo se cumpliera de la mejor manera.

William Andrés De La Torre Yamberla

TABLA DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

El presente documento se encuentra conformado por tres capítulos, en el cual se detalla todo el proceso para llevar a cabo el Trabajo de Grado: "DESARROLLO DE UN PLAN DE SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO IMBACOOP LTDA, APLICANDO EL ESTÁNDAR ISO/IEC 27001 PARA FORTALECER LA DISPONIBILIDAD DE LOS SERVICIOS**.**"

En la parte de introducción se definen los antecedentes, situación actual, prospectiva, planteamiento del problema, objetivo general y específico, alcance, y justificación.

En el capítulo 1, se presenta todo el marco teórico, se describen temas como un antecedente de investigación, detallar como es la clasificación de la información para su manejo seguro y eficiente de la organización, explicar cómo estas normativas específicas que rigen a la seguridad de la información, destacar como la adopción de este estándar ISO/IEC 27001 puede beneficiarse a las organizaciones en términos de seguridad y cumplimiento y la metodología Magerit versión 3.0.

En el capítulo 2, se detalla el levantamiento de información, proceso del levantamiento de información, definición de análisis de riesgos con sus etapas y características correspondientes, requisitos de seguridad, políticas de seguridad etapas y sus fases, además el diseño del plan de seguridad de la información en general con sus enfoques.

En el capítulo 3, se detallan la parte la validación del resultado, el análisis de resultados mediante la encuesta de satisfacción, interpretar los resultados de la encuesta realizada a la institución financiera, análisis de impacto y un apartado entregable de manual de políticas de seguridad de la información para la institución financiera.

Finalmente, se encuentran las conclusiones, recomendaciones, referencias, bibliografías y los anexos.

ABSTRACT

This document is made up of three chapters, in which the entire process to carry out the Degree Project is detailed: “DEVELOPMENT OF AN INFORMATION SECURITY MANAGEMENT SYSTEM PLAN IN THE IMBACOOP LTDA SAVINGS AND CREDIT COOPERATIVE, APPLYING THE ISO/IEC 27001 STANDARD TO STRENGTHEN THE AVAILABILITY OF SERVICES”.

In the introductory part, the problem statement, objective general and specific objectives. It also includes the scope of the study made together with the justification of the realization of this.

In Chapter 1, the entire theoretical framework is presented, topics are described as a research background, detail how information is classified for its safe and efficient management of the organization, explain how these specific regulations that govern information security, highlight how Adopting this ISO/IEC 27001 standard can benefit organizations in terms of security and compliance and the Magerit version 3.0 methodology.

In Chapter 2, the information gathering, information gathering process, definition of risk analysis with its corresponding stages and characteristics, security requirements, security policies, stages and their phases, in addition to the design of the information security plan in general with their approaches.

In Chapter 3, The part details the validation of the result, the analysis of results through the satisfaction survey, interpreting the results of the survey carried out at the financial institution, impact analysis and a deliverable section of the information security policy manual for the institution financial.

Finally, you will find the conclusions, recommendations, bibliographic references and annex.

INTRODUCCIÓN

Tema.

Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información en la Cooperativa de Ahorro y Crédito Imbacoop Ltda., aplicando el estándar ISO/IEC 27001, para fortalecer la disponibilidad de los servicios.

Problema.

Antecedentes.

La Cooperativa de Ahorro y Crédito Imbacoop Ltda., situada en la ciudad de Otavalo, Nace en el año 1998 como una pre cooperativa, en el seno de la Asociación Comunidad Cristiana Católica Liberación (ACLI) en la comunidad La Compañía, del cantón Otavalo de la provincia de Imbabura con apenas 30 socios quienes decidieron organizarse en una institución para impulsar el desarrollo de emprendimientos comunitarios, los mismos que no podían ser realizados por la falta de capital de trabajo, ya que era muy difícil obtener crédito a través de instituciones financieras debido a las limitadas condiciones socioeconómicas de la comunidad.

Con la idea de crear la precooperativa nace el departamento financiero dentro del ACLI que más tarde daría paso a la constitución de la cooperativa, la misma que es legalizada el 12 de agosto del año 2004 mediante ACUERDO MINISTERIAL 3024 e inscrita en registro General de COOPERATIVAS 6694 cuya matriz estará dentro de la Comunidad La Compañía-Otavalo.

Dentro de la Cooperativa, en el departamento de tecnología tiene los siguientes inconvenientes de no tener un plan de seguridad de información, no dispone de políticas de seguridad, tampoco tiene una reglamentación o términos de privacidad para la contratación del personal, no conocen las normativas de seguridad, nadie protege el acceso a la Data-Center, deficiencia en la capacitación del personal administrativa en la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

La ISO 27001, se enfoca en la protección de las vulnerabilidades y riesgos que amenazan la integridad, confidencialidad y disponibilidad de la información, permitiendo gestionar la Seguridad de la información, de este activo tan importante para el área tecnológica de la Cooperativa de Ahorro y Crédito Ltda.

Y tomando en cuenta que existen disposiciones como mención según el autor (ERAZO, 2016) plantea que las disposiciones de la Secretaría Nacional de la Administración Pública (SNAP) se exige a todas las empresas públicas del Ecuador implementar un sistema que gestione la seguridad de la información.

Situación Actual.

En vista de que la cooperativa tuvo un crecimiento considerable sus socios fundadores toman la decisión y asumen el reto de sacar a su institución fuera de su comunidad, debido a que muchos de sus asocios pertenecían a la ciudad de Otavalo; y con apenas 796 socios, abre sus puertas en la ciudad de Otavalo el 24 de noviembre del 2010 para más tarde expandirse a la ciudad de Ibarra reto que se logró el 17 de mayo del 2011 abriendo su sucursal en un sector estratégico con el afán de servir a las comunidades de la ciudad en especial al sector de La Esperanza y sus alrededores.

La información que despliega desde el área de tecnología de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., es muy grande debido a la cantidad de transacciones realizadas al día, Lamentablemente es vulnerable por qué no existe una política de seguridad, hoy la cooperativa cuenta con más de diez mil asociados de las comunidades rurales y urbanas de las sus agencias están en las ciudades de: Otavalo, Cayambe, Antonio Ante, San Pablo, Cotacachi, Ibarra, Baños, Tena y Napo. Por otro lado, los ex empleados hacen el mal uso de información, lo que genera inestabilidad, además no cuenta con una directriz o un perímetro físico asegurado, no existe una red controlada, por lo cual esto puede conllevar ocasionar malas prácticas en procesos de seguridad e incluso puede llegar a una gestión de modificación de datos críticos de la Cooperativa, ocasionando posibles fugas de información.

Prospectiva.

En el presente proyecto de titulación se plantea el desarrollo de un Plan de Gestión de la Seguridad de la Información, donde se va a iniciar con una evaluación de amenazas y vulnerabilidades a la que se encuentra expuesta la información del departamento de Tecnología de la Cooperativa de Ahorro y Crédito Imbacoop Ltda. Mediante el estándar de Seguridad de información ISO/IEC 27001, que permitirá generar una solución a los problemas detectados, minimizando los posibles riesgos con respecto a seguridad.

Planteamiento del Problema.

El control de la información que lleva dentro del área de la tecnología informática de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., se refleja la problemática de la vulnerabilidad, ya que día a día se ve expuesto a diferentes tipos de amenazas, lo que causa riesgo para la información.

Para ello se lleva a cabo un diagrama de causa y efecto, para lo cual se utilizó Matriz de Vester para clasificar los problemas planteados en el proyecto en la Figura 1.

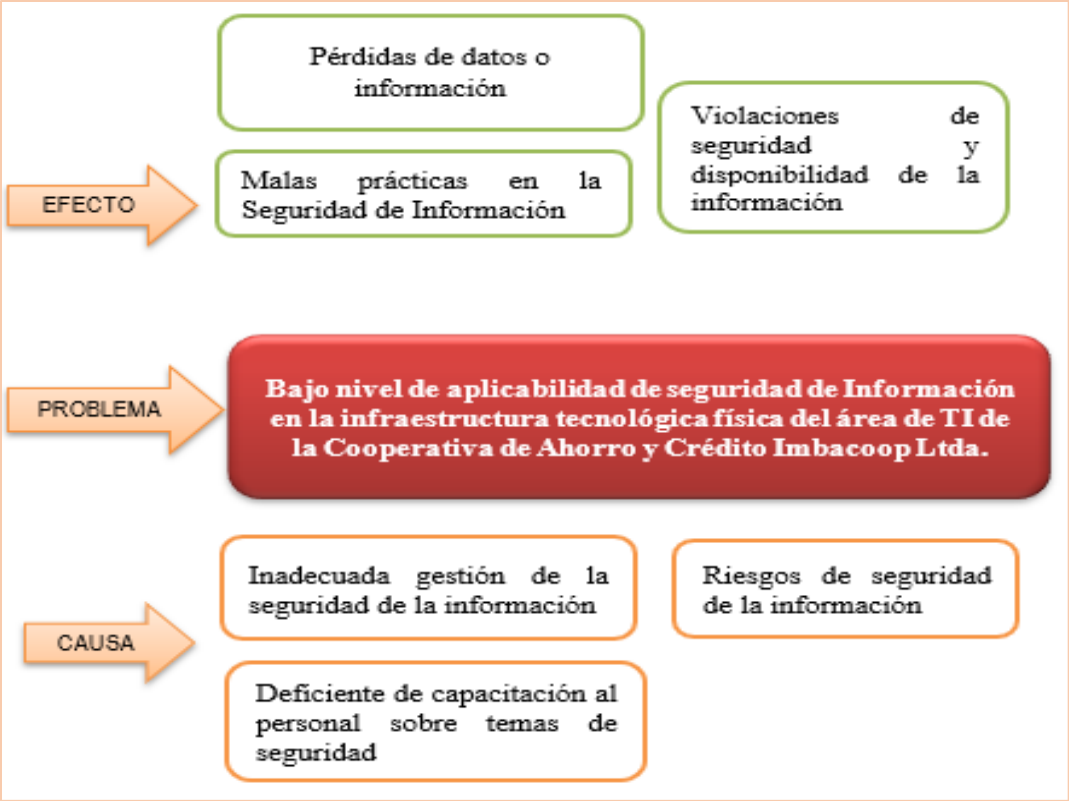


Figura. 1: Diagrama de Vester

Objetivos

Objetivo General

Desarrollar un plan de sistema de gestión de seguridad de la información en la Cooperativa de Ahorro y Crédito Imbacoop Ltda. aplicando el estándar ISO/IEC 27001, para fortalecer la disponibilidad de los servicios.

Objetivos Específicos

- Diagnosticar la situación actual de la seguridad de la información, en la Cooperativa de Ahorro y Crédito Imbacoop Ltda.
- Proponer un plan de seguridad de la información basado en la norma ISO/IEC 27001, para fortalecer la disponibilidad de la información.
- Validar los resultados de la implementación de la información.

Alcance.

Para el En el presente trabajo se realizará un Plan de Gestión de la Seguridad de Información para el área de tecnología de información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., como primer objetivo se efectuará el diagnóstico de la situación actual, con el segundo objetivo se diseñará un plan de seguridad de la información basado en la norma ISO/IEC 27001 la cual brinda una implementación de mejores prácticas, orientación sobre procesos y

controles clave de seguridad de la información, como tercero y último objetivo es validar el modelo de SGSI mediante encuesta de satisfacción y checklist con el fin de aumentar la seguridad de la información dentro de la cooperativa.

Figura. 2: Gráfico de representación del alcance del proyecto

Diagnosticar la situación actual: En la Cooperativa de Ahorro y Crédito Imbacoop Ltda., no cuenta con un sistema de gestión de seguridad de la información, no existe una red controlada, por lo cual esto puede conllevar ocasionar malas prácticas en procesos de seguridad.

Diseñar un sistema de seguridad: Se llevará mediante herramientas tecnológicas para mejorar la seguridad de la información en la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

Validar resultados: Se planificará un ambiente de pruebas, donde se pueda evaluar las vulnerabilidades encontradas, con la finalidad de mostrar la socialización de la propuesta a la gerencia para sugerir mejoras en los procesos ya implementados en la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

Metodología.

Se hará una investigación documental referente a la norma que se ha propuesto con el fin de obtener información necesaria, además se utilizarán técnicas de investigación para justificar la situación actual de la empresa.

A continuación, se analizarán metodologías para evaluación de vulnerabilidades en las TI, considerando tanto los temas organizacionales como los técnicos, examinando detalladamente cómo los usuarios emplean la infraestructura en su entorno.

Implica una práctica fundamental porque genera una visión para la Cooperativa de Ahorro y Crédito Imbacoop Ltda., acerca de las vulnerabilidades, proporcionando una base para futuras mejoras.

Según el autor (Implantaci, 2013) el auditor evaluará el liderazgo entrevistando a uno o más miembros de la gerencia y evaluando su nivel de participación en:

- Evaluación de riesgos y oportunidades.
- Establecimiento y comunicación de políticas.

Para el cumplimiento del objetivo 1, se utilizarán herramientas tecnológicas con el fin de obtener información necesaria.

Para el cumplimiento del objetivo 2, se realizará una planificación de los controles necesarios con el fin de disminuir las vulnerabilidades utilizando la norma ISO/IEC 27001.

Finalmente**,** para el cumplimiento del objetivo 3, se validarán los resultados propuestos mediante encuestas de satisfacción y checklist.

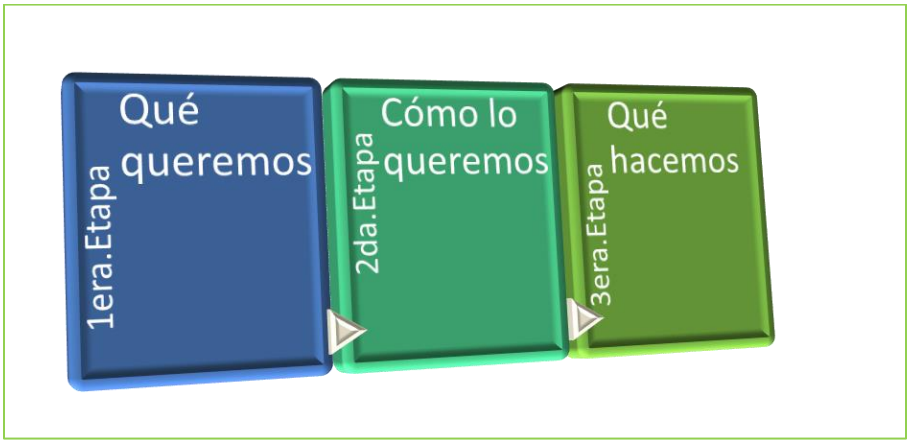


Figura. 3: Gráfico de representación de la metodología del proyecto.

Justificación

La evaluación que se va a realizar se enfoca en dar solución a uno de los Objetivos de Desarrollo Sostenible (ODS), el objetivo N°8 ¨ Trabajo Decente y Crecimiento Económico (ONU, 2015), ya que se prevé reducir los riesgos en cuanto a la seguridad de información, con el fin de mejorar la calidad de trabajo tanto de los trabajadores de la empresa y de los clientes. También para que la empresa pueda disponer de mayor disponibilidad de trabajo para las personas, dando mayor confianza como cooperativa.

El proyecto debe tener una o varios tipos de justificaciones que deben ser especificadas como:

Justificación Tecnológica.

El presente anteproyecto tiene como objetivo resolver el manejo de la información en el área de tecnología de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

Justificación Metodológica.

Se efectuará una investigación científica, proyectiva y mixta que permitirá conocer sobre el manejo de la información, además de elaborar planes con los cuales se alcanzará el objetivo y, por último, validar los datos obtenidos para poder plantear nuevas formas de gestionar la información.

Justificación Social.

Con el presente proyecto se busca minimizar los niveles de vulnerabilidad que existe en la Cooperativa de Ahorro y Crédito Imbacoop Ltda., para lo cual se aplicará un breve diagnóstico con el fin de mejorar la situación en la que se encuentra la empresa.

CAPÍTULO 1

1.1. Antecedentes de la investigación.

En el presente capítulo se efectúa una breve descripción de contenidos de seguridad de la información, con los fundamentos necesarios para el desarrollo de la propuesta. Se analizará la norma ISO/IEC 27001 y la relación con el esquema gubernamental de seguridad de la información.

En la investigación realizada por (Zhou et al., 2020) sobre "Norma de seguridad informática ISO 27001 hacia la mejora de la confidencialidad, disponibilidad e integridad que poseen los sistemas de la Cooperativa de Ahorro y Crédito San Francisco Limitada en el departamento de Sistemas". Plantea que conforme avanzan las tecnologías de la información y la relación que tienen está con el negocio que realizan las organizaciones, están en crecimiento tanto las amenazas y vulnerabilidades. En vista de aquello, es motivo de vital importancia proteger los activos de información que posee una entidad por más simple que esta sea, ya que debe radicar la confidencialidad, disponibilidad e integridad de la información mediante una buena implementación de la gestión de riesgos, logrando identificar aquellos activos más vulnerables.

Uno de los pilares fundamentales de la entidad San Francisco es el departamento de sistemas, ya que es una organización financiera que opera y gestiona información muy importante de los usuarios. Es fundamental garantizar la seguridad y confiabilidad de los datos de cada usuario que se encuentran en la cooperativa y a los que se integren. Esto se logra con el uso de normas que ayudan a manejar y mantener los activos de información.

Para la implementación de un SGSI basado en la norma internacional ISO 27001 en la versión que se mantiene actual desde el 2013, se reúne los recursos necesarios para ser ejecutada, ya que por medio de la mencionada norma se escogerá los controles adecuados acordes a las necesidades de la organización. Se pretende proteger todos los activos que se mantienen en el alcance de la norma, con la finalidad de otorgar confianza a las partes interesadas, ya que el sistema será capaz de ser implantado, supervisado, mantenido y mejorado en el tiempo.

Implementación del primer Sistema de Gestión de Seguridad de la Información en el Ecuador, certificado bajo la norma ISO 27001:2005 elaborado por José Alfonso Aranda Segovia, trabajo realizado en Guayaquil-Ecuador en el año 2009, en cuyas conclusiones dice lo siguiente: La norma ISO 27001 está orientada al tratamiento de la seguridad de la información mediante la gestión del riesgo, tanto para sus activos como para sus procesos; esto garantiza que ante recursos limitados las inversiones sean bien focalizadas, para lograr ello se necesita de la concientización de la compañía, ya que es un pilar fundamental de esta norma, por lo cual las

organizaciones deben ingeniosamente buscar y adoptar mecanismos que permitan que se despierte un interés y compromiso por parte de todos los empleados. Además, al tener implantado un SGSI certificado bajo la norma ISO 27001:2005, no significa contar con seguridad máxima en la información de la organización, sino que esto representa que la empresa cumple con los requerimientos y mejores prácticas establecidas en dicha norma para que su SGSI actual funcione correctamente y además pueda evolucionar hacia la sofisticación manifiesta el autor (Benitez Pineda, n.d.).

Según el autor (NARVÁEZ BARREIROS, 2013), el planteamiento principal y objetivo de este documento es la aplicación de la ISO27001 para la implementación de SGSI en la fiscalía general del Estado, por tanto, es necesario introducir algunos conceptos relacionados con estos términos, así como también la relación entre los distintos componentes que se mencionan. De inicio, se observa una relación directa entre un SGSI y el concepto de información. A fin de poder establecer un lineamiento y contar con un universo de conceptos unificados, se agregarán algunas descripciones o definiciones, varias de ellas ya conocidas, pero a fin de obtener una integridad de conceptos se mencionarán de manera rápida. Siendo el concepto de Información el eje central de donde parte la necesidad de la aplicación de una norma y un sistema de gestión en una institución pública o privada, se define como información a cualquier conjunto de datos que se encuentren organizados, que representan valor a la organización o institución a la que pertenecen, independientemente que estos se encuentren almacenados o transmitidos en forma escrita, gráfica, oral, en correo electrónico, en bases de datos, fax, formato de audio, etc. Ni tampoco de los orígenes que los mencionados datos provengan de fuentes externas o internas, ni de su fecha de elaboración o recepción.

En el proyecto de investigación de (DE LA SOTA SHICSHE & CRISTOBAL MECHAN, 2018) tomó como referencia a una entidad pública peruana “Ministerio de Transporte y Comunicaciones”, la cual después de hacer el análisis de brecha inicial, determinó que no cumplía con la mayoría de los requisitos que exigía la norma. Además, se estableció como el proceso más crítico el proceso tecnológico de emisión de licencias de conducir. Dada la carencia de una administración de seguridad, diseñaron un plan del SGSI, basado en la NTP/ISO. IEC 27001:2008, con el fin de proteger los activos de información en el proceso crítico ya mencionado. Para ello, hicieron uso de la metodología MAGERIT para la evaluación de riesgos y para el desarrollo del proyecto utilizaron la metodología del Ciclo de Deming (Plan - Do - Check - Act). Sin embargo, solo llegaron a cubrir las dos primeras fases, organización (Plan) y planificación (Do). Como resultado, se mejoró el porcentaje de cumplimiento de la norma. Al culminar con las fases restantes, el uso del SGSI traerá como beneficios a futuro: una reducción de riesgos, ahorro

de costos, la gestión de la seguridad de información y la certificación, contribuyendo a obtener un valor agregado en el mercado.

1.1.1. Información.

Comprender Las instituciones financieras manejan grandes volúmenes de información, por ejemplo, en las transacciones, la cual deben tener en cuenta que debe ser más claro, tal manera permita al personal administrativo tomar decisiones correctas.

La información que se maneja en la Cooperativa de Ahorro y Crédito Imbacoop Ltda., está enfocada al crecimiento de clientes/usuarios, personal administrativo, por lo que es sumamente necesario tratar sobre la seguridad de la información.

1.1.2. Definición de clasificación de la información.

La Norma (ISO/IEC 27001:2013) plantea la clasificación de la información con los siguientes criterios:

Los propietarios de los activos son responsables de ello, pero es una buena idea que la alta dirección proporcione pautas basadas en los resultados de la evaluación de riesgos de la organización.

La clasificación de la información según ISO 27001 sigue parámetros específicos. Las organizaciones, generalmente, clasifican la información en términos de confidencialidad; es decir, según a quién se le otorga el acceso a ella en la Tabla 1.

Tabla 1: Clasificación de la información

Clasificación de la información según ISO27001	Caracteristica
Confidencialidad	Acceso restringido a la alta dirección.
Restringido	Directores de área y empleados clave tienen acceso.
Interno	Relativo a la información accesible solo los miembros de la organización, pero de acuerdo con el nivel.
Integridad	Debido a modificaciones no autorizadas en la información.
Disponibilidad	La inaccesibilidad a la información.

1.2. Normativas de seguridad de la información.

1.2.1. Estándares de seguridad de la información.

Uno de los requisitos para implementar un SGSI en una organización es conocer los estándares, su estructura y la relación existente entre cada uno de ellos. Las normas para implementar un SGSI corresponden a la serie ISO/IEC 27000 publicadas por la ISO y la Comisión Electrotécnica Internacional (IEC), compuesta por 17 normas, clasificadas en cuatro categorías:

- La norma que contiene el vocabulario es la siguiente ISO/IEC 27000.

- Las normas de requerimientos que contienen son la norma ISO/IEC 27001 y la norma ISO/IEC 27006.
- Las normas de guía desarrolladas son las siguientes: ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, TR 27008, ISO/IEC 27013, ISO/IEC 27014, TR 27016, ISO/IEC 27032.
- Las normas para sectores específicos son las siguientes normas ISO/IEC 27010, ISO/IEC 27011, TR 27015 y TS 27017.

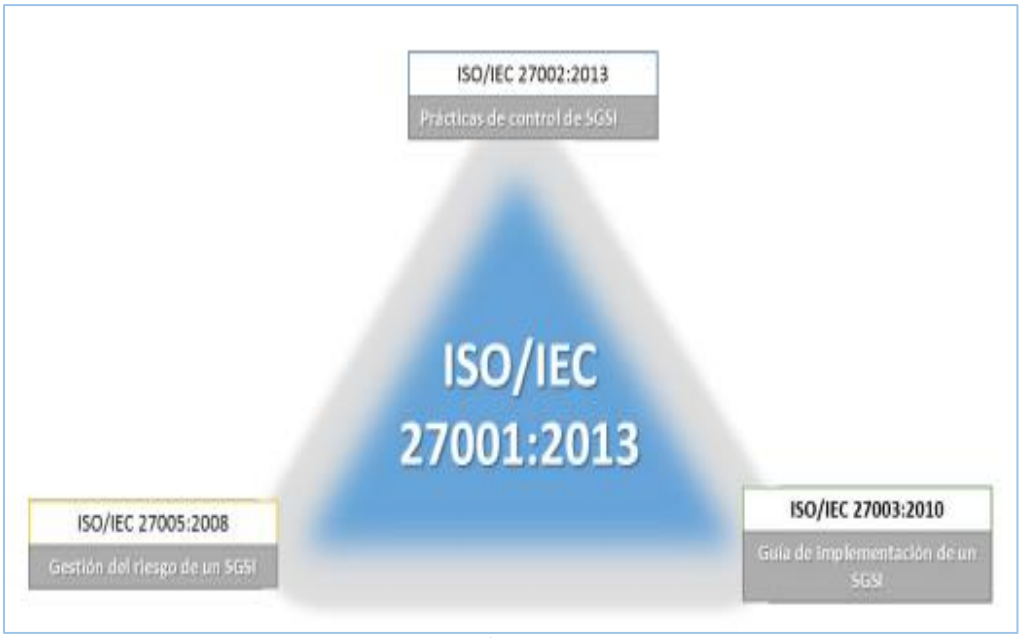


Figura. 4: Estándar de Seguridad
Fuente: Principales normas para implementar un SGSI basado en los estándares de la familia de normas ISO/IEC 27000

A pesar de la cantidad de normas de la serie ISO/IEC 27000, aquellas que sirven de referente para la implementación de un SGSI en una organización se enmarcan en cuatro de ellas, como se puede observar en la Figura 4.

1.2.2. Familia 27000

Según la guía de implantación (NQA, 2017) las normas de la serie 27000 nacen en 1995 con la BS 7799, redactada por el Departamento de Comercio e Industria (DTI) del Reino Unido. Las normas se denominan correctamente "ISO / IEC" porque son desarrolladas y mantenidas conjuntamente por dos organismos internacionales de normas: ISO (la Organización Internacional de Normalización) y la IEC (la Comisión Electrotécnica Internacional). Sin embargo, en el uso diario, la parte "IEC" a menudo se descarta.

Actualmente, hay 45 normas públicas en la serie ISO 27000. La ISO 27001 es la única norma destinada a la certificación. Los otros estándares brindan orientación sobre la implementación de mejores prácticas. Algunos brindan orientación sobre cómo desarrollar el

SGSI para industrias particulares; otros brindan orientación sobre cómo implementar procesos y controles clave de gestión de riesgos de seguridad de la información.

1.2.3. Norma ISO/IEC 27001:2013.

Definición de la norma ISO/IEC 27001:2013.

Según (ISO, 2020) la ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

1.3. ISO 27001.

1.3.1. Estructura de la norma ISO 27001.

En la Tabla 2, se va explicando el tipo y su respectiva característica de la estructura de la norma ISO 27001.

Un SGSI que cumple con la ISO 27001 tiene un conjunto interrelacionado de procesos de mejores prácticas que facilitan y respaldan el diseño, implementación y mantenimiento de los controles. Los procesos que forman parte del SGSI suelen ser una combinación de procesos comerciales centrales existentes (por ejemplo, reclutamiento, inducción, capacitación, compras, diseño de productos, mantenimiento de equipos, prestación de servicios) y aquellos específicos para mantener y mejorar la seguridad de la información (por ejemplo, gestión de cambios, respaldo de información, control de acceso, gestión de incidentes, clasificación de la información) (NQA, 2017).

1.3.2. Que permite la norma ISO 27001

La norma ISO 27001 garantiza que la información proporcionada se mantendrá de forma reservada, íntegra, accesible y acorde con la legalidad, salvaguardándola frente a posibles vulnerabilidades. La implementación de este sistema en la estructura organizativa fomenta la confianza entre clientes, proveedores y empleados, consolidándose como un criterio universal. Además, la puesta en práctica de esta norma facilita la evaluación y gestión de los riesgos identificados, permitiendo la elaboración de un plan preventivo y, en caso de surgir, la mitigación del impacto conexo.

Tabla 2: Estructura de la Norma

Tipo	Característica
Objetivo y campo de aplicación.	La norma comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.
Referencias Normativas	Recomienda la consulta de ciertos documentos indispensables para la aplicación de ISO 27001.
Términos y definiciones	Describe la terminología aplicable a este estándar.
Contexto de la Organización	Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI (Sistema de Gestión de Seguridad de la Información).
Liderazgo	Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello, la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.
Planificación	En esta parte se pone de manifiesto la importancia de la determinación de riesgos, vulnerabilidades y oportunidades a la hora de planificar un Sistema de Gestión de Seguridad de la información, así como de establecer objetivos de Seguridad de la información y el modo de lograrlos.
Soporte	En esta cláusula la norma señala que para el buen funcionamiento del SGSI la organización debe contar con los recursos, competencias, conciencia, comunicación e información documenta pertinente en cada caso.
Operación	Para cumplir con los requisitos de seguridad de información, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos, vulnerabilidades de la seguridad de la información y un tratamiento de ellos.
Evaluación del Desempeño	Dentro de este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección de Seguridad de Gestión de la información para asegurar que funciona según lo planificado.
Mejora	En esta parte encontraremos las obligaciones que tendrá una organización cuando encuentre una conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficiencia del SGSI.

Fuente:(ISO, 2020)

1.3.3. ISO 27001, además de cumplir con sus estándares, también ofrece beneficios a las empresas.

- Obtener un diagnóstico por medio de entrevistas.
- Efectuar un análisis exhaustivo de todos los riesgos que se puedan presentar.
- Crear un plan de acción acorde a las necesidades puntuales de la empresa.
- Diseñar procedimientos.
- Entender los requerimientos de seguridad de la información y la necesidad de establecer una política y objetivos para la seguridad de la información.
- Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- Monitorear y revisar el desempeño y la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI).
- Favorece el mejoramiento continuo con base en la medición del objetivo

1.3.4. Importancia de la norma ISO 27001.

Como se ha mencionado anteriormente, en la actual época de información, los datos corporativos, que constituyen el activo más crucial de las empresas, se enfrentan a riesgos como fraudes, ciberataques, sabotajes, vandalismo, espionaje o uso indebido por parte del personal.

Estas acciones ilegales suelen ser perpetradas por ingenieros, hackers, empleados u organizaciones especializadas en el robo de datos, con la intención de perjudicar la reputación de la compañía. Por esta razón, es imperativo contar con herramientas que prevengan la ocurrencia de tales sucesos.

La implementación de un Sistema de Gestión de Seguridad de la Información en tu empresa no solo te permite cumplir con las obligaciones legales, ya que muchas naciones lo requieren, sino que también te proporciona la metodología necesaria según la norma ISO 27001.

La obtención de la certificación ISO 27001 demuestra el compromiso de una organización con la protección de su información y la de sus clientes, a la vez que les brinda ventajas competitivas y mayor confianza a sus grupos de interés.

1.3.5. Nivel de cumplimiento de la norma ISO 27001:2013.

En la Tabla 3, se apreciarán los niveles de cumplimiento de la norma ISO/IEC 27001:2013.

1.3.6. Gráfico del resumen de la ISO 27001:2013.

En la Figura. 5, se mostrará el resumen del cumplimiento de la normativa ISO/IEC 27001:2013.

Tabla 3: Nivel de Cumplimiento ISO/IEC 27001:2023.

Cláusula.	Descripción del Requisito.	% de Cumplimiento.
4	Contexto de la Organización.	47
5	Liderazgo.	48
6	Planificación.	54
7	Soporte.	53
8	Operación.	50
9	Evaluación del desempeño.	33
10	Mejora.	33

Fuente: (Juan J. Lugo Marín, 2020)

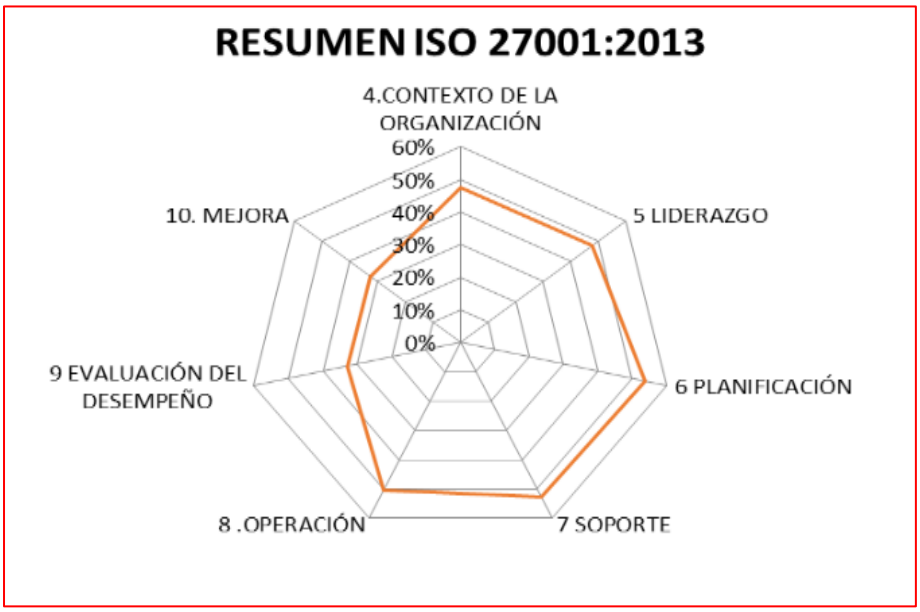


Figura. 5: Resumen de la Norma 27001:2013
Fuente: (Juan J. Lugo Marín, 2020)

1.4. Seguridad de la información.

Dentro de la seguridad de la información, mucho más que un antivirus, cortafuegos o cifrado de datos o información, estos términos son el resultado de operaciones realizadas por segundas personas y son soportadas por la tecnología hoy en día.

1.4.1. Definición.

La definición de la seguridad de la información tributa a una disciplina que se encarga de la implementación técnica de la protección de la información, el despliegue de las tecnologías que establecen de forma que se aseguran las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo, es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y los esquemas normativos, que nos exigen niveles de aseguramiento de procesos y de tecnología para elevar

el nivel de confianza en la creación, utilización, almacenaje, transmisión, recuperación y disposición final de la información mediante la investigación por el autor (Carlos Humberto, 2018).

Information Security es la disciplina que se encarga de proporcionar la evaluación de riesgos y amenazas, trazar el plan de acción y adecuación para minimizar los riesgos, bajo la normativa o las buenas prácticas, con el objetivo de asegurar la confidencialidad, integridad y disponibilidad del manejo de la información de activos.

La seguridad de la información es la disciplina que se encarga de garantizar la:

- Confidencialidad.
- Integridad.
- Disponibilidad de la información.

La seguridad de la información suele estar respaldada por una estrategia de seguridad desarrollada mediante el desarrollo de un plan de seguridad. La gerencia será responsable de registrar todos los esfuerzos de seguridad relacionados con la implementación y verificación por parte del propietario del proceso y procedimientos de planificación para lograr los objetivos especificados en la política de seguridad.

La evaluación será realizada por el equipo responsable de la seguridad informática, los gerentes de procedimientos y seguridad, las responsabilidades de seguridad, el uso de medidas adecuadas para cumplir con la política de seguridad y la evaluación de riesgos de la política.

El cumplimiento de la norma de seguridad de la información ISO 27001 no sólo proporciona los beneficios de reducir riesgos y amenazas, sino que también mejora la planificación y la gestión de seguridad de la empresa. Crea una garantía de continuidad del negocio en una situación imprevista, le da a nuestro partido una imagen respetable y cumple con las regulaciones nacionales.

La seguridad de la información está relacionada con muchas cosas, por lo que no es solo un problema, sino un problema. El papel de la alta dirección y los ejecutivos de la empresa. Organizaciones activas y altos directivos, directores, etc. Si no se une a líderes empresariales como. Es posible que una organización no tenga un historial de seguridad porque se han identificado todos los riesgos. Todo esto se hace bajo el control de la dirección empresarial. Se deben considerar el problema, el proceso y el negocio, así como proteger todos los activos/recursos de las organizaciones, propietarios y beneficiarios que respaldan la seguridad de la información en una función colaborativa.

Además de la seguridad establecida en toda la empresa, se deben tener en cuenta todos los riesgos de la tecnología TIC (organizativos, operativos y físicos). Hoy en día, el riesgo operativo se ha vuelto aún más importante cuando se trata de seguridad de la información. Estos

incluyen la sensibilidad a los riesgos, el comportamiento humano y las decisiones humanas, la resistencia al cambio, la cultura empresarial, la comunicación, etc.

La seguridad de la información no es sólo una cuestión de seguridad informática y de la información; Debería ser el punto central en la protección de los activos y la información importante de organizaciones e individuos. Los riesgos de la información ocurren cuando las amenazas y las vulnerabilidades se combinan. Las amenazas y las vulnerabilidades están estrechamente relacionadas y su coexistencia no producirá consecuencias.

Las amenazas deben usarse de manera negativa y pueden provenir de cualquier lugar afectando el entorno de la organización, ya sea interno o externo. Las vulnerabilidades son debilidades en la tecnología o los procesos de la información y, por lo tanto, se consideran características de los sistemas o procesos de información que las contienen. En pocas palabras, una amenaza es un evento o situación que puede afectar la capacidad de una organización o de un individuo para hacer su trabajo al afectar directamente la forma en que procesan información o datos.

Básicamente, podemos agrupar las amenazas a la información en cuatro grandes categorías que se muestra en la Tabla 4.

1.4.2. Pilares de seguridad de la información.

Para las personas y organizaciones, la información es, ha sido y será el motor para su funcionamiento, uno de sus mayores activos con un valor incalculable para las mismas. La seguridad de la información se enfoca en preservar esencialmente la confidencialidad, integridad y disponibilidad de la información en la Tabla 6; además, puede involucrar otras aristas tales como la autenticidad y no repudio, las cuales se definen por el autor, (Carlos Humberto, 2018).

Tabla 4: Amenazas a la información

No.	Amenazas
1	Factores humanos (accidentales, errores).
2	Fallas en los sistemas de procesamiento de información.
3	Desastres naturales.
4	Actos maliciosos o malintencionados.

Otras amenazas que pueden observar en la Tabla 5.

Tabla 5: Otras Amenazas.

No.	Otras Amenazas
1	Virus informáticos o código malicioso.
2	Uso no autorizado de sistemas informáticos.

3	Robo de información.
4	Fraudes basados en el uso de computadoras.
5	Suplantación de identidad.
6	Denegación de Servicios (DoS).
7	Ataques de fuerza bruta.
8	Alteración de la información.
9	Divulgación de información.
10	Sabotaje, vandalismo.
11	Espionaje.

Tabla 6: Pilares de Seguridad.

Categoría	Descripción
Confidencialidad	La información solo puede ser acedada y utilizada por el personal de la empresa que tiene autorización para hacerlo.
Integridad	Se refiere al momento en que la información no ha sido borrada, copiada o modificada, es decir, cuando se conserva tal como fue creada o enviada desde cualquier medio desde su origen hacia su destino.
Disponibilidad	Se refiere a que la información facilitada en cualquier medio digital o software se encuentre disponible para su procesamiento.
Autenticidad	En este pilar se define información legítima que, al ser interceptada, puede ser copiada de formato original a pesar de que la información sea idéntica.
No repudio.	Es el proceso que garantiza que el emisor no pueda negar lo que hizo. Equivale al término “aceptación” y es una de las características más difíciles de garantizar.

Fuente: (Carlos Humberto, 2018)

Las empresas u organizaciones deben garantizar al menos los tres primeros pilares para asegurar y proteger los datos e información que resguardan, demostrando así un excelente nivel de seguridad de la información. La siguiente gráfica ilustra las interrelaciones de los tres pilares.

La difusión de estrategias de seguridad de la información debe atribuirse a los nuevos avances y nuevas necesidades de servicios, evitando así conceptos erróneos sobre seguridad y aliviando el campo. La tecnología de la información juega un papel importante en un mundo competitivo y cada vez más competitivo.

En este sentido, toda organización debe priorizar la integración de la seguridad de la información en su modelo de negocio, recursos humanos, estándares de capa y tecnología para

asegurar los tres pilares que mencionamos anteriormente. Al ser el eslabón más débil de la cadena, se deben brindar a todos servicios de apoyo y capacitación en el manejo y uso de la información.

Figura. 6: Tres Pilares Fundamentales de la Información
Fuente: (Carlos Humberto, 2018)

La seguridad de los datos es una tarea desafiante. Uno de ellos protegerá los datos personales porque la mayoría de los datos generados en línea provienen de acciones humanas. Por lo tanto, se deben desarrollar estrategias para proteger adecuadamente esta información.

1.4.3. Seguridad informática vs Seguridad de la información.

Antes de abordar un enfoque metodológico para implementar un SGSI es necesario aclarar la diferencia entre seguridad informática y seguridad de la información, la cual radica en el tipo de recursos sobre los que actúa cada una. Mientras que la primera se enfoca en la tecnología propiamente dicha, i.e. en las infraestructuras tecnológicas que sirven para la gestión de la información en una organización, la segunda está relacionada con la información en sí misma, como activo estratégico de la organización según menciona el autor (Valencia-Duque & Orozco-Alzate, 2017).

En este sentido, las TIC son herramientas que permiten optimizar los procesos de gestión de la información en las organizaciones. El concepto de seguridad es el mismo, pero mientras la seguridad informática desarrolla su función sobre todos los elementos técnicos que hacen parte de las TIC, la seguridad de la información actúa sobre la información como activo estratégico para la adecuada toma de decisiones empresariales en las organizaciones modernas manifiesta el autor (Valencia-Duque & Orozco-Alzate, 2017).

Hasta antes que surgieran de forma masiva las TIC, el concepto predominante era el de seguridad de la información; sin embargo, con el advenimiento de las TIC y su nivel de dependencia por parte de las organizaciones y más aún, su nivel de dependencia para un

adecuado tratamiento de la información, se ha pasado de pensar tan solo en la seguridad informática como fin, a pensar en su adecuada implementación como medio para obtener un SGSI que permita garantizar niveles adecuados de protección de la información empresarial como recurso vital para la función decisional, y el diseño de estrategias competitivas que diferencien una organización de otra esto aclara el autor (Valencia-Duque & Orozco-Alzate, 2017).

Desde esta perspectiva, lo que persigue un SGSI es proteger la información como recurso valioso, para lo cual debe proteger de igual forma los diferentes medios a través de los cuales se genera, almacena, procesa, transmite, circula y transforma en un recurso útil para los negocios según menciona el autor (Valencia-Duque & Orozco-Alzate, 2017).

1.4.4. Sistema de Gestión de Seguridad de la Información.

El Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de políticas, procedimientos, controles y procedimientos que utiliza una organización para proteger de manera justa la confidencialidad, integridad y propiedad de su información. El SGSI se basa en la gestión y diseño de la seguridad de la información y los procesos de acuerdo con los objetivos y necesidades de la organización. El objetivo principal del SGSI es desarrollar un sistema de gestión de riesgos para identificar, evaluar y resolver problemas de seguridad de la información que puedan afectar a la organización.

La implementación de SGSI requiere un enfoque que abarque toda la organización y la cooperación de todas las áreas y niveles, desde la alta dirección hasta los empleados. Algunos de los pasos básicos para implementar un SGSI son:

- Establecimiento de políticas y objetivos de seguridad de la información: la organización debe establecer políticas claras y objetivos específicos de seguridad de la información que estén en línea con los objetivos generales de la organización.
- Identificación y evaluación de riesgos: se deben identificar y evaluar los riesgos de seguridad de la información a través de un análisis de riesgos detallado y completo.
- Selección y aplicación de controles: la organización debe seleccionar y aplicar controles de seguridad adecuados para tratar los riesgos de seguridad de la información identificados.
- Monitoreo y revisión: se deben monitorear y revisar regularmente los controles de seguridad para asegurarse de que sean efectivos y estén actualizados para enfrentar nuevos riesgos y amenazas.

- Mejora continua: el SGSI debe estar sujeto a una mejora continua para garantizar que se mantenga alineado con los objetivos y requisitos de seguridad de la organización.

La implementación adecuada de un SGSI puede ayudar a las organizaciones a reducir el riesgo de pérdida de datos, interrupción del negocio y daño a la reputación de la organización. También puede ayudar a cumplir los requisitos legales y reglamentarios para la seguridad de los datos.

ISO 27001 se puede utilizar en cualquier organización, con o sin fines de lucro, privada o pública, pequeña o grande. Escrito por los principales expertos del mundo en el tema, este libro proporciona una manera de implementar la seguridad de la información en su organización. También permite a las empresas obtener la certificación; Esto significa que un organismo de certificación independiente verifica que la organización implementa la seguridad de la información de acuerdo con la norma ISO 27001.

CICLO DE MEJORA CONTINÚA EN LA NORMA ISO/IEC 27001:2013

En la Figura. 7, se aprecia el ciclo de mejora continua de la normativa ISO/IEC 27001:2013 que va a detallar las características de cada una de ellas:

Plan: Consiste en planificar acciones para hacer frente a los riesgos e identificar las oportunidades, para posteriormente evaluarlas y gestionarlas.

Hacer: Indica que la organización debe de disponer los recursos necesarios para establecer, implementar y mantener el SGSI, además de dar a conocer las políticas de seguridad de la información del SGSI.

- Poner en marcha el Plan de gestión de riesgos establecido
- Se implanta el SGSI
- Se establecen los controles de seguridad

Check – Controlar

- Revisar internamente el SGSI.
- Realizar auditorías.
- Se revisan los indicadores y métricas del SGSI.

Actuar

- Llevan a cabo las acciones correctivas.
- Llevan a cabo las acciones preventivas.

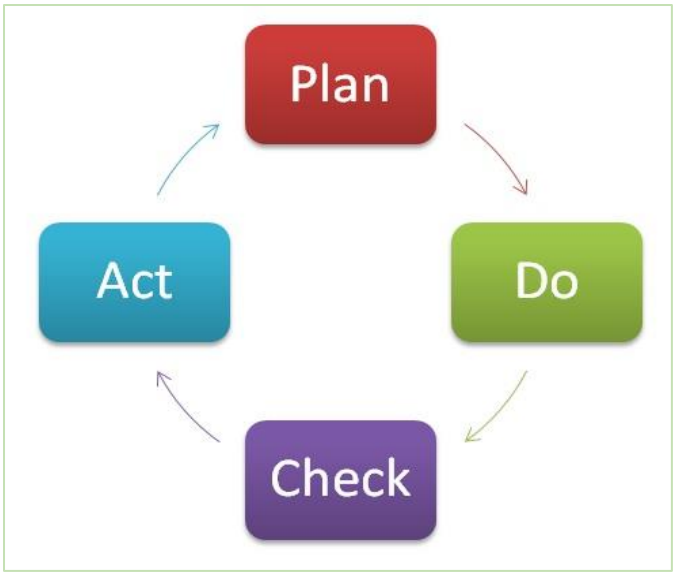


Figura. 7: Ciclo de mejora continua
Fuente: (Jimeno, 2013)

FASES PHVA VS ESTRUCTURA ISO 27001:2013

En la Figura. 8, se muestra como esta las fases PHVA vs Estructura de la normativa 27001:2013, la cual se puede aprecia sus elementos respectivos.

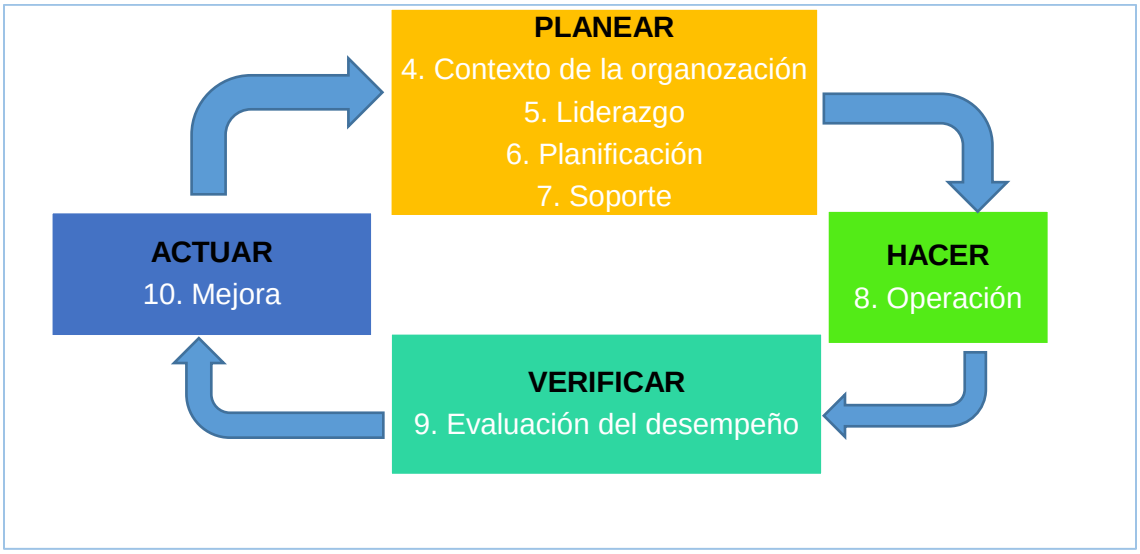


Figura. 8: Ciclo de mejora continua alineado a la norma ISO 27001:2013
Fuente: (Amaya, 2013)

1.5. Protocolos de seguridad de la información.

Existen varios aspectos centrales a entender cuando navegamos en la red. Al buscar información en internet, tanto usuarios como máquinas compartimos datos con distintas páginas de forma intencional o automática. Para proteger dichos intercambios se aplican protocolos que aseguran la seguridad e integridad mediante reglas precisas. Diseñados para evitar el acceso no autorizado a nuestros datos, estos protocolos contemplan:

- **Encriptación**: Este método enmascara la data transmitida entre emisor y receptor, otorgando privacidad durante la transferencia.
- **Lógica ordenada**: Exige que la transmisión siga un orden lógico, explicitando primero los detalles del mensaje, su sentido y propósito, para luego intercambiar la carga útil de forma encubierta.

1.6. Propósito y Utilidad de un Sistema de Gestión de Seguridad de la Información.

En la siguiente Figura.9, se visualizará cómo va surgiendo a detalle para qué sirve un SGSI.

Un Sistema de Gestión de Seguridad de la Información (SGSI) resulta ser altamente provechoso para asegurar el cumplimiento legal y la protección de los datos dentro de una organización. Esto se logra mediante la definición precisa de los procedimientos y controles destinados a salvaguardar la integridad de la información de manera exhaustiva. Además, el SGSI facilita el establecimiento de políticas claras que deben ser conocidas por todos los integrantes de la compañía, brindando transparencia respecto a los posibles riesgos y las estrategias para mitigarlos de la forma más efectiva. Al automatizar muchos de estos procesos, el SGSI permite administrar los permisos de acceso de manera dinámica y trazar el uso de la información con el fin de detectar y corregir cualquier vulnerabilidad de manera temprana.

1.7. Importancia Que incluye un SGSI.

Dentro de un Sistema de Gestión de Seguridad de la Información mediante la norma ISO 27001, indica que debe incluirse los siguientes aspectos importantes que se mostrarán en la Figura. 10.

1.8. Como se implementa un SGSI.

Posteriormente, se presenta cada uno de los pasos que se debe seguir para implementar un Sistema de Gestión de Seguridad de la Información en la Figura. 11.

1.9. Ventajas de implementar un SGSI bajo la norma ISO/IEC 27001.

- Permite, de esa manera, equilibrar los procesos de seguridad, evitando absurdas duplicaciones entre ellos.
- A pesar de que es imposible eliminar totalmente los riesgos, permite crear modelos y metodologías que contribuyan a su reducción y que aumenten la seguridad de las informaciones que se poseen.
- En caso de que se llegue a presentar un riesgo, permite que este no cause pérdidas tan profundas y habrá un plan de acción para actuar de manera eficaz.
- Permite satisfacer los requisitos legales impuestos por las autoridades de control.

- Genera valor agregado dentro de la compañía, pues aún no son muchas las empresas que cuenten con la certificación ISO 27001.
- Gracias a la eficiencia que se emplea, permite bajar los costos.
- Inspira confianza entre todos.

1.10. Metodología Magerit.

1.10.1. Definición.

La metodología Magerit se basa en un enfoque sistemático y estructurado para efectuar la evaluación de riesgos. Proporciona un conjunto de pautas y técnicas para llevar a cabo el proceso de gestión de riesgos de seguridad de la información, que incluye la identificación de activos, la evaluación de amenazas, la determinación de vulnerabilidades, el análisis de impacto y la selección de medidas de seguridad adecuadas en la Figura. 12.

Ayuda a las organizaciones a comprender los riesgos de seguridad asociados a sus sistemas de información y a tomar decisiones informadas sobre las medidas de seguridad que deben implementarse para mitigar esos riesgos.

En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnología de la información según (Magerit versión 2, 2012).

1.10.2. Objetivos

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

1.10.3. Hallazgos de las actividades de análisis y gestión de riesgos.

A continuación, se aprecia los hallazgos de las actividades respectivamente en la Tabla 7 que se puede visualizar.

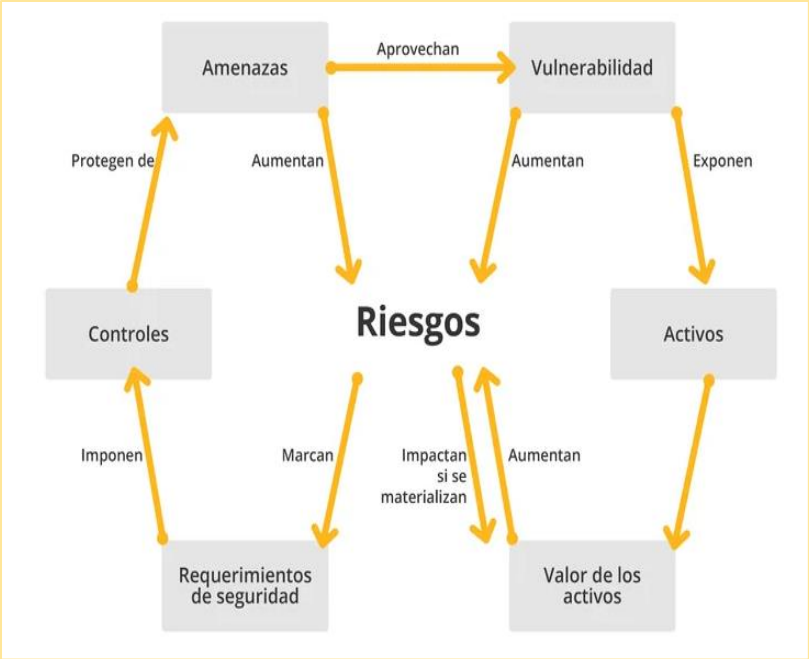


Figura. 9: Propósito y utilidad de un SGSI
Fuente: (ISO27000.ES, s.f.)

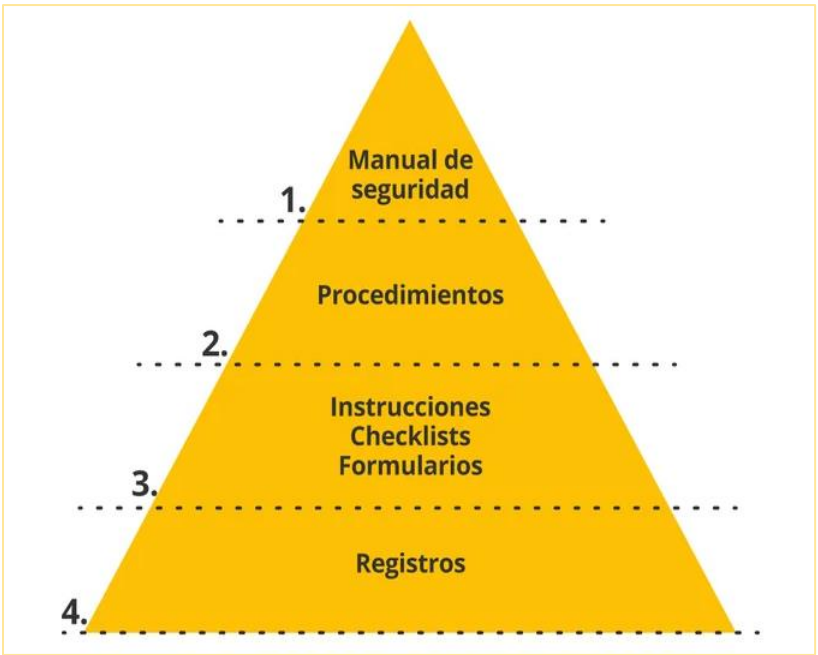


Figura. 10: Cómo incluye un SGSI
Fuente: (ISO27000.ES, s.f.)

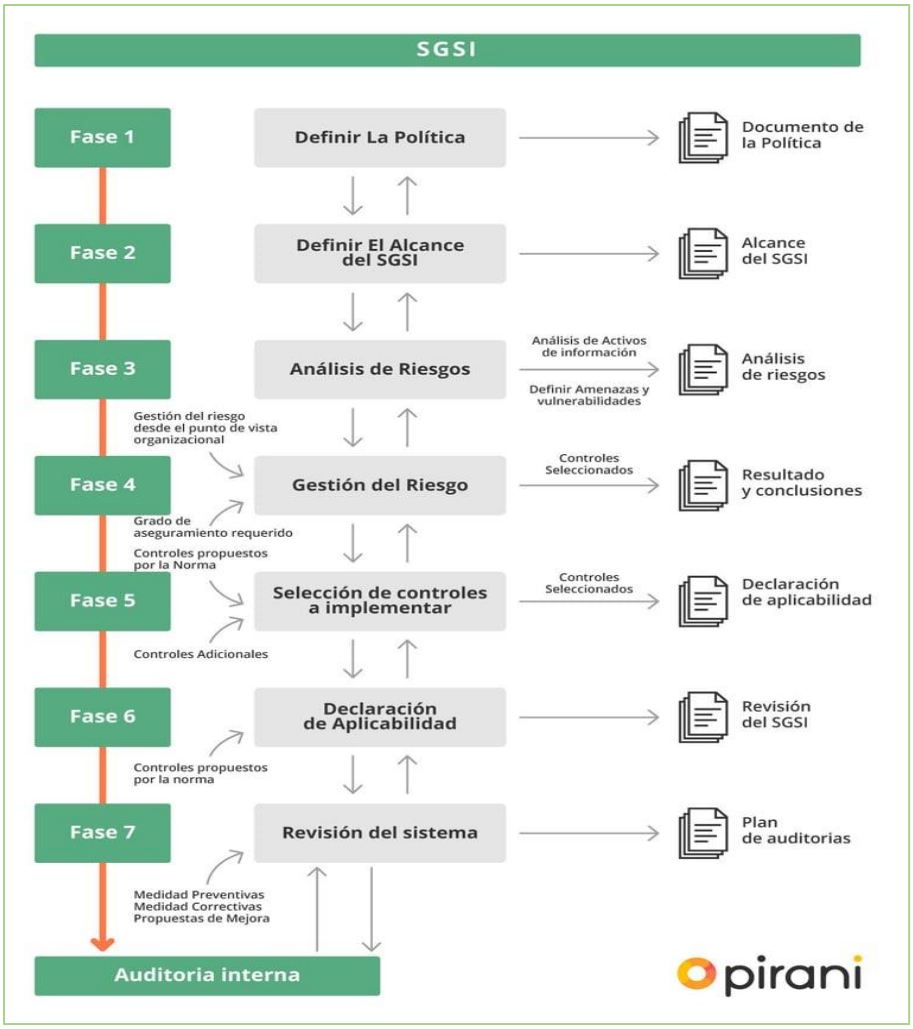


Figura. 11: Implementación de un SGSI
Fuente: (ISO27000.ES, s.f.)

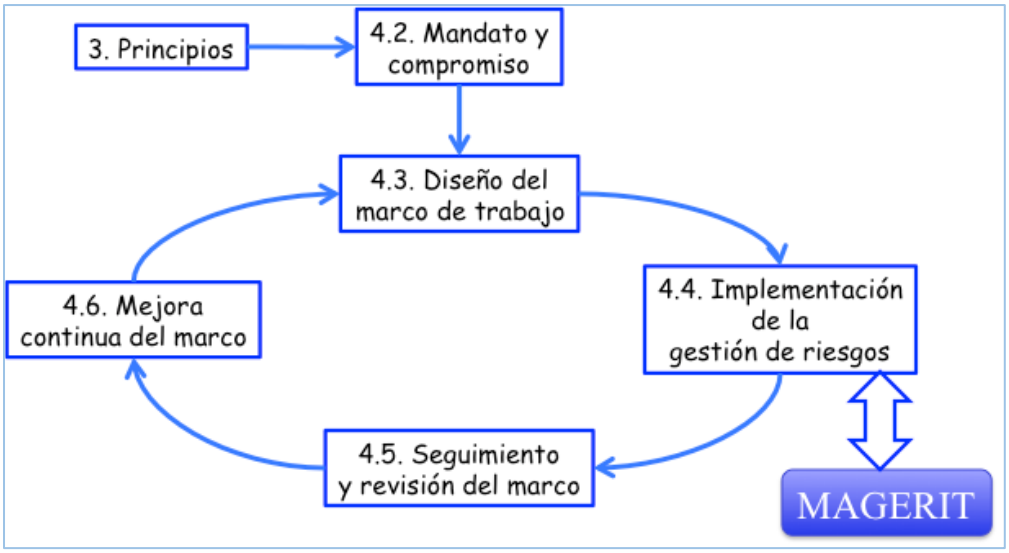


Figura. 12: ISO 31000-Marco de Trabajo de Gestión de Riesgos.
Fuente:(Magerit versión 2, 2012)

Tabla 7: Análisis y Gestión de Riesgos.

Actividades de Análisis	Característica
Modelo de valor.	Caracterización del valor que representan los activos para la Organización, así como de las dependencias entre los diferentes activos.
Mapa de riesgos.	Relación de las amenazas a que están expuestos los activos.
Declaración de aplicabilidad.	Para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.
Evaluación de salvaguardas.	Evaluación de la eficacia de las salvaguardas existentes en relación con el riesgo que afrontan.
Estado de riesgo.	Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.
Informe de insuficiencias.	Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema. Es decir, recoge las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.
Cumplimiento de normativa.	Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normativa correspondiente.
Plan de seguridad.	Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos

Fuente:(Magerit versión 2, 2012)

CAPÍTULO 2

Desarrollo

Durante mucho tiempo las empresas financieras se han preocupado por perfeccionar todos los sistemas informáticos, dejando alado lo más importante que vendría a ser la seguridad de informaciones. Luego de haber investigado y analizado los documentos relacionados con las vulnerabilidades en el entorno de Sistema Financiero de una cooperativa, se ha encontrado diversos conceptos que se va a ir detallando con el fin de dar a conocer el proceso de cómo se ejecutara para llevar la seguridad para el mejoramiento del sistema con las propuestas establecidas.

Según el autor (Erazo, 2016), las disposiciones de la Secretaría Nacional de la Administración Pública (SNAP) se exige a todas las empresas públicas del Ecuador implementar un sistema que gestione la seguridad de la información. Entonces, existen varias metodologías para analizar el riesgo.

La información que despliega desde el área de tecnología de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., se genera una gran cantidad de información que se maneja a diario la cantidad de mil transacciones al día y las claves van cambiando cada 20 días, la información se trabaja mediante VPNs (una red segura) de tal manera las transacciones se hace desde la Cooperativa que se enfoca en un entorno local, el mismo que se encuentra vulnerable por qué no existe una política de seguridad hoy la cooperativa cuenta con más de diez mil asociados de las comunidades rurales y urbanas de las sus agencias están en las ciudades de: Otavalo, Cayambe, Antonio Ante, San Pablo, Cotacachi, Ibarra, Baños, Tena y Napo donde están los datos tanto de administradores internos, clientes, los Ex – Empleados hacen el mal uso de información, la cual generar inestabilidad de información, no cuenta con una directriz o un perímetro físico asegurado, no existe una red controlada por lo cual esto puede conllevar ocasionar malas prácticas en procesos de seguridad e incluso puede llegar a una gestión de modificación de datos críticos de la Cooperativa, ocasionando posibles fugas de información.

En vista de que la cooperativa tuvo un crecimiento considerable sus socios fundadores toman la decisión y asumen el reto de sacar a su institución fuera de su comunidad, debido a que muchos de sus asocios pertenecían a la ciudad de Otavalo; y con apenas 796 socios, abre sus puertas en la ciudad de Otavalo el 24 de noviembre del 2010 para más tarde expandirse a la ciudad de Ibarra reto que se logró el 17 de mayo del 2011 abriendo su sucursal en un sector estratégico con el afán de servir a las comunidades de la ciudad en especial al sector de La Esperanza y sus alrededores.

Por lo cual se utilizará la Norma Estándar ISO/IEC 27001 a cabo para control de vulnerabilidades de una manera adecuadamente y reaccionar a las condiciones y circunstancias que puedan afectar el sistema de control interno.

2.1. Levantamiento de información.

El levantamiento de información puede incluir la recopilación de información a través de entrevistas, encuestas, observación directa, análisis de documentos y registros, entre otros métodos. El objetivo del levantamiento de información es obtener la mayor cantidad de información relevante y precisa posible, para poder identificar patrones, necesidades y requerimientos.

2.1.1. Proceso de levantamiento de información.

El proceso de levantamiento de información se lleva a cabo en las etapas iniciales de un proyecto, y puede ser continuo a lo largo de su desarrollo. Los datos recopilados durante el levantamiento de información pueden ser utilizados para definir los objetivos y requisitos del proyecto, establecer un plan de trabajo, asignar tareas y recursos, y tomar decisiones informadas.

2.1.2. Definición de información.

La información se refiere a los datos digitales que se almacenan, procesan y transmiten a través de sistemas informáticos. Además, se compone de unidades de datos que se organizan y estructuran para ser utilizados en un contexto específico.

La información es el resultado del procesamiento de datos y su presentación en un formato que se pueda entender y utilizar por las personas. La calidad de la información depende de la precisión, relevancia y confiabilidad de los datos y del proceso de transformación y presentación de la información.

2.1.3. Clasificación de información.

La clasificación de información es el proceso de etiquetar la información según su importancia, confidencialidad, integridad y disponibilidad para protegerla de un acceso no autorizado o malintencionado. La clasificación de información ayuda a las organizaciones a identificar y controlar quiénes tienen acceso a los datos y a qué datos tienen acceso.

La clasificación de información se basa en la evaluación de los riesgos asociados con la información y en la definición de los niveles de seguridad requeridos para protegerla adecuadamente. Los niveles de clasificación de información pueden variar según la organización, pero comúnmente incluyen tres niveles: alto, medio y bajo en la Tabla 8.

La clasificación de información es una práctica importante para garantizar la seguridad de los datos de una organización. Al clasificar la información según su nivel de importancia, la

organización puede implementar medidas de seguridad apropiadas para proteger la información adecuadamente y evitar que sea comprometida por acceso no autorizado o malintencionado

Tabla 8: Niveles de clasificación de información

Niveles	Características
Información de alto nivel	Se refiere a la información más crítica de la organización, como datos financieros, secretos comerciales, información personal, entre otros. Esta información debe ser protegida con los más altos niveles de seguridad
Información de nivel medio	Se refiere a información importante para la organización, pero que no es tan crítica como la información de alto nivel. Ejemplos de este tipo de información incluyen planes de negocios, acuerdos de confidencialidad, y documentación de proyectos
Información de bajo nivel	Se refiere a información de uso común que no es crítica para la organización. Ejemplos de este tipo de información incluyen comunicaciones internas, notas de reuniones y correos electrónicos

2.1.4. Activos.

Los activos son elementos o recursos de valor para la organización. Estos activos pueden ser tangibles o intangibles y pueden cubrir diversas áreas, como tecnologías, datos, infraestructura, personal, reputación y otros aspectos relevantes de la organización. Es importante identificar y apreciar los activos organizacionales para comprender su importancia y determinar qué pasos de seguridad deben llevarse a cabo para protegerlos de posibles amenazas y riesgos.

Identificación de activos.

La identificación de activos es un paso fundamental en el proceso de gestión de la seguridad de la información. Este proceso implica identificar y clasificar los activos de una organización para comprender mejor qué activos necesitan protección y cómo deben ser protegidos.

Etiquetado de activos.

La codificación de activos se considera del siguiente orden en la Tabla 9.

2.2. Activos del departamento de tecnología de la Cooperativa

En la Tabla 10, se apreciará los activos correspondientes del departamento de tecnología:

En la Tabla 13, se visualiza la clasificación de activos mediante la metodología Magerit “Catálogos de elementos”.

Tabla 9: Codificación de activos

Activo	Etiqueta
Información	IN-##
Software	SF-##
Hardware	HD-##
Equipamiento Auxiliar	AUX-##
Servicios	SR-##
Infraestructura	IN-##
Personas	PR-##
Redes de comunicación	RD-##

Tabla 10: Activos de TIC

N0	NOMBRE DEL EQUIPO	MARCA	CARACTERISTICA	CANTIDAD EN EXISTENCIAS
1	Laptop y cargador	HP	Procesador Intel® Core™ i7-1065G7 CPU @ 1.30GHz RAM Instalada 8,00 GB (7,69 GB usable) Arquitectura de 64 bits Sistema Operativo Windows 11 Home version 21H2	1
2	Router Board Microtik 3011	MICROTIK	Router Boart 20211 / color negro / 5 Puertos Cat. 5e / 5 Puertos Cat. 6e	1
3	Rack Jupiter – Puerta de acero y vidrio	BEAUCOUP	JPT-20060100/V-N / Alto 2000mm / Ancho 600mm / Profundidad 1000mm Nº. Ur 42 / Peso Kg 116 / Cap Carga Estática 3330 kg	1
4	Bandejas porta Equipos	BEAUCOUP	BNJ-101 / Nº UR 2 / Alto 89.5 / Ancho 442mm / Profundidad 372mm / Capacidad de carga 25Kg	1

Continua…

5	Multitomas de energías polarizadas Horizontales	BEAUCOUP	TPL-72-8 Longitud 1116mm / Toma de cable / Peso 2.55 kg	1
6	Organizadores horizontales con canaleta ranurada	BEAUCOUP	ORGH-43 / Longitud 483mm / Medidas de canaleta 60x80 / Peso 0.48 kg	1
7	Cable de energía 5000mm		Longitud 5000mm / Pico de 3 entradas / Receptor 3 picos	1
8	Switch 24 puertos Cat. 5E	D-LINK	DES-1016A 10/100 Switch	1
9	Pach Corp	QUEST	5 pies color azul Cat. 5e	9
10	UPS 3KVA 120V	FIRMESA	Computer power VTN-1 kwa 120 V / SN: 83111609100425	1
11	Monitor 15”	BENQ	Pulgadas 15” / Modelo SyncMaster 933 / Color negro	1
12	CPU Pentium Inside / SERVIDOR COPE 3.5	S/M CLON	Procesador Intel Pentium Inside CPU G2020 @ 2.9 GHz / Disco Duro 500GB / RAM 4GB / SO Centos 6.6 X86_64	1
13	SISTEMA INFORMATICO COPE	SONUEM	COPE 3.5	1
14	HPE Smart Buy Proliant DL 160 Gen9 / Servidor Webcoop 2.2	HP	HPE Smart Buy ProLiant DL 160 Gen9 Intel Xeon E5 2609v4 8 Core 1.7 GHz 20MB L3 cache / 8GB DDR4 400MHz RDIMM	1
15	SISTEMA INFORMÁTICO WEBCOOP 2.1	WEBCOOP	WEBCOOP PROFESIONAL	1
16	Unifi Uap-ac-lite	UBNT		3
17	Servidor NAS	Wester Digital	WD My Cloud EX4100	2

Tabla 11: Tipos de Activos según Magerit

Tipo de Activo	Descripción
Datos/información	Los datos son el corazón que permite a una organización prestar sus servicios. Además, los elementos de información tienden la forma singular o a la vez agrupados de alguna forma que representa los conocimientos que se tiene de algo.
Servicios	Esta función contiene la satisfacción de una necesidad de los usuarios/clientes. Dentro de los servicios aparecen como activos de un análisis de riesgos, bien como servicios finales, ya sean servicios de comunicación, servicios de seguridad, etc.
Software	En esta función se refiere a las tareas que son automatizadas para su desempeño de un equipo informático. Tal forma es de gestionar, analizar y transformar datos de la información.
Hardware	Esta función habla de bienes materiales, físicos, destinados a soportar directa o indirecta de servicios que presta la organización.
Redes de comunicación	Como servicios de comunicación contratados a terceros, pero centrándose que son medios de transporte que llevan datos de un sitio a otro.
Soporte de información	Se consideran dispositivos físicos que permite guardar información de forma permanente, durante largos periodos de tiempo.
Equipamiento auxiliar	Sirven de soporte a los sistemas de información, sin estar directo relacionado con datos.
Instalaciones	Lugares donde se encuentran los sistemas de información y comunicaciones.
Personal	Son los personales relacionados con los sistemas de información.

Fuente:(Magerit v.3, 2012)

La identificación de los activos se desarrolló con la respectiva ayuda del jefe de Área del departamento de tecnología de la Cooperativa, basándose en la clasificación con la metodología Magerit en la Tabla 12.

La identificación de los activos se desarrolló con la respectiva ayuda del jefe de Área del departamento de tecnología de la Cooperativa, basándose en la clasificación con la metodología Magerit.

2.3. Valoración de activos.

En Magerit, la valoración de los activos es indispensable para entender el valor relativo de los activos y priorizar en consecuencia los recursos de seguridad. Esta valoración funciona como base para la identificación y gestión de riesgos en el contexto de la seguridad de la información.

Esta también forma parte de la gestión de riesgos y seguridad de la información, pues la valoración de activos proporciona información esencial para la toma de decisiones sobre la puesta en práctica de medidas de seguridad. Y afecta a la asignación de recursos para proteger los activos más importantes de una organización.

Tabla 12: Identificación de los activos del área de tecnología

Tipo de activos	Activo	Código
Datos/Información	Base de datos	D-01
	Documentación interna	D-02
Servicios	Servidor NAS	S-01
	Electricidad	S-02
	Internet	S-03
	Telefonía	S-04
	Mantenimiento	S-05
	Correo	S-06
Software	Desarrollo a media	SW-01
	Antivirus	SW-02
	Firewall	SW-03
	Licencias	SW-04
	Sistema operativo	SW-05
Hardware	Laptop	HW-01
	Monitor	HW-02
	HPE Smart Buy	HW-03
	Impresora	HW-04
	Router Board Microtik 3011	HW-05
	Switch 24 puertos Cat. 5E	HW-06
	Unifi Uap-ac-lite	HW-07
Redes de comunicación	red internet	COM-01
	red LAN	COM-02
	telefonía móvil	COM-03
Soportes de información	Electrónicos (one drive de office)	MEDIA-01
Equipamiento auxiliar	Rack Júpiter	AUX-01
	Bandejas porta Equipos	AUX-02
	Multitomas de energía	AUX-03
	Organizadores horizontales con canaleta ranurada	AUX-04
	Cable de energía	AUX-05
	Cable de red-Patch Cord	AUX-06
	Ups	AUX-07
Instalaciones	Cuarto de atención	L-01
	Cuarto de soporte	L-02
Personal	Personal administrativo de DTI	P-01

Magerit considera la importancia de los activos en distintas dimensiones, estas se aprecian en la Tabla 13.

Tabla 13: Valoración de los activos según Magerit

Dimensión	Definición
Confidencialidad	Aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.
Disponibilidad	Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
Integridad	Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
Autenticidad	Aseguramiento de la identidad u origen
Trazabilidad	Aseguramiento de que en todo momento se podrá determinar quién hizo que y en qué momento.

Fuente: (Magerit v.3, 2012)

Dentro de las dimensiones actúan como una faceta de los activos, de tal manera se visualiza la valoración de las mismas tomando en cuenta la escala de criterios que se mostrará en la Tabla 14.

Tabla 14: Criterios de valoración de activos

	Valor	Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: (Magerit v.3, 2012)

2.4. Analisis de Riesgos.

El análisis de riesgos es un proceso sistemático que se utiliza para identificar, evaluar y mitigar los riesgos asociados con una determinada actividad o situación. En el contexto de la seguridad de la información, el análisis de riesgos se utiliza para identificar y evaluar los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de los datos y sistemas de una organización.

El análisis de riesgos se realiza en varias etapas, que incluyen en la Tabla 15.

El análisis de riesgos es un proceso clave para garantizar la seguridad de la información y prevenir la pérdida, daño o acceso no autorizado a los datos y sistemas de una organización. Al identificar y evaluar los riesgos y seleccionar y aplicar los controles adecuados, una organización puede mejorar su capacidad para prevenir y mitigar los riesgos de seguridad de la información.

Tabla 15: Etapas de análisis de riesgos

Etapas	Características
Identificación de los activos	Identificar los activos críticos de la organización, como datos, sistemas, redes, infraestructuras y recursos
Identificación de las amenazas	Identificar las posibles amenazas que pueden afectar los activos de la organización, como malware, hackers, errores humanos, desastres naturales, entre otros.
Evaluación de las vulnerabilidades	Evaluar las vulnerabilidades de los activos identificados, es decir, las debilidades que pueden ser explotadas por las amenazas
Evaluación de los riesgos	Evaluar los riesgos asociados con las amenazas y las vulnerabilidades identificadas, y clasificarlos por su probabilidad y su impacto potencial
Selección de controles	Seleccionar los controles necesarios para mitigar los riesgos identificados y reducir su probabilidad o impacto potencial
Implementación de los controles	Implementar los controles seleccionados para mitigar los riesgos identificados
Monitoreo y revisión	Monitorear y revisar regularmente los controles implementados y actualizar el análisis de riesgos para garantizar su eficacia continua

2.5. Requisitos de seguridad de la información.

La gestión de la seguridad de información expuesta por (OSRI, 2018), consiste en la identificación de los requisitos de la seguridad de la organización según la valorización de riesgos que se mostrara en la Figura. 13.

Con la importancia y la necesidad de proteger la información hoy en día, es imperativo encontrar formas de lograr esta seguridad que se puede lograr a través de políticas. De esta manera, el control y la orientación se consideran un equilibrio y, en última instancia, culminar con los inconvenientes de seguridad.

El autor (OSRI, 2018) manifiesta que, los requisitos de seguridad se determinan examinando los activos informáticos, el historial de amenazas y las evaluaciones de vulnerabilidad. Por otro lado, los requisitos generales se refieren a las normas jurídicas, el estado y los métodos procesales. Además, las necesidades de procesamiento de la información son aquellas que la empresa determina para soportar sus operaciones.

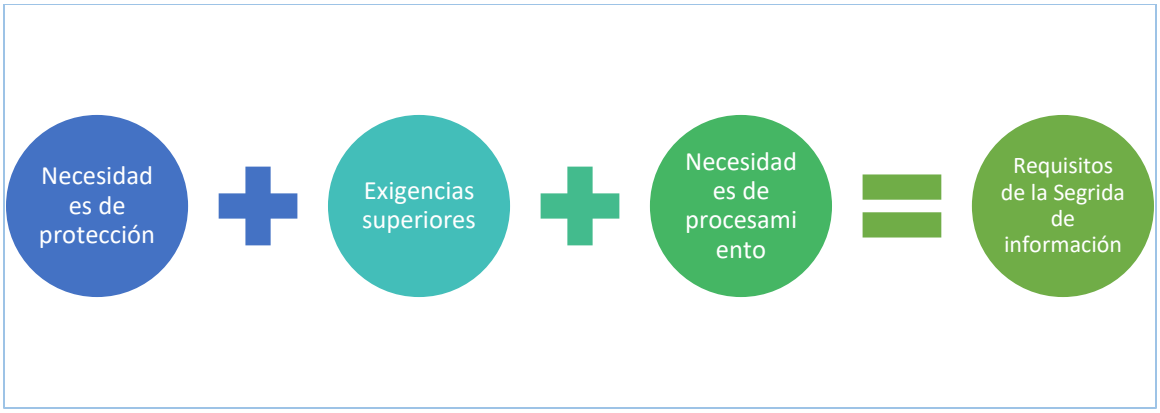


Figura. 13: Requisitos de la Seguridad de información

Además, (27001, 2013) determina la pirámide de evaluación que debe documentar la seguridad de la información, como se visualiza en la Figura. 14.

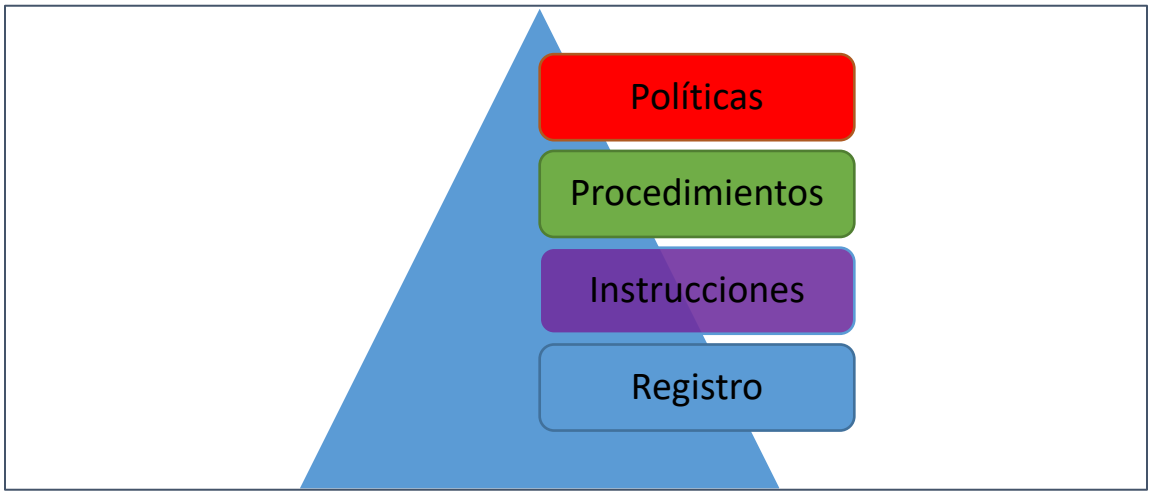


Figura. 14: Pirámide de documentación

2.6. Políticas de seguridad de la información (PSI).

El objetivo fundamental de la definición de las Políticas de Seguridad Informática consiste en proporcionar orientación y apoyo de la dirección para la seguridad informática, de acuerdo con los requisitos de la organización y con las regulaciones y leyes vigentes (OSRI, 2018).

Las políticas de seguridad definen los “QUE”: qué debe ser protegido, qué es más importante, qué es más prioritario, qué está permitido y qué no lo está y qué tratamiento se les darán a los problemas de seguridad. Las políticas de seguridad en sí mismas no dicen “COMO” las cosas son protegidas. Esto es función de las medidas y procedimientos de seguridad.

Para crear una política, en el departamento de tecnologías de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., por la cual se indican las diferentes etapas de cumplimiento que se van conforme a los requerimientos de la institución financiera. En la siguiente Figura. 15, se

aprecia el desglose las 11 etapas, asociando en 4 fases, dentro de cada fase van con las etapas respectivas en cada una de ellas, que se visualizará en la Figura. 15.

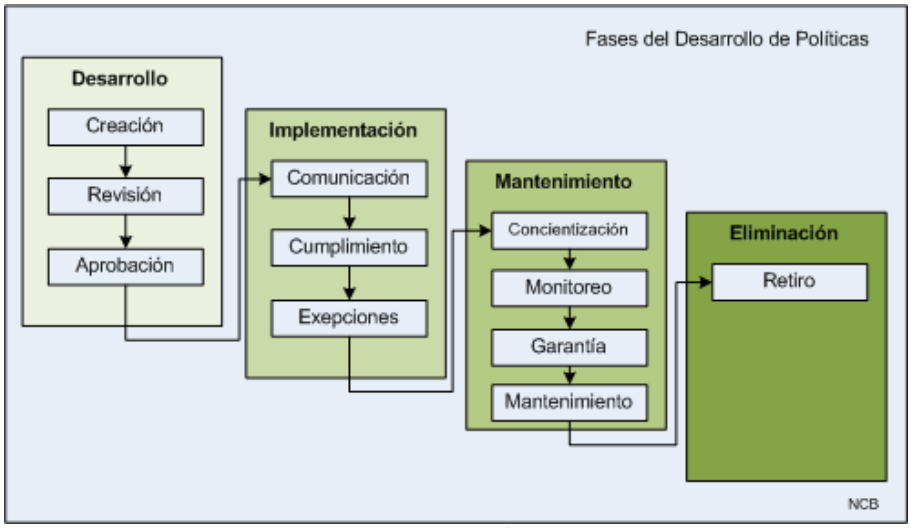


Figura. 15: Etapas de la Política de Seguridad
Fuente: (Seguridad de la Informacion , 2010)

Ciclo de vida de la política de seguridad

El ciclo de vida de una política de seguridad de la información comprende desde la creación hasta el evento de revisión y actualización. Dentro de este ciclo evidencia las etapas por las que debe pasar una política de seguridad de la información a lo largo de su tiempo, tal manera se va a explicar paso a paso lo que contiene un ciclo de vida de una política en la Figura. 16.

Figura. 16: Ciclo de vida de la Política de Seguridad
Fuente: (Mendoza, 2014)

Fase de Desarrollo

En esta fase se desarrolla la política de seguridad de la información, la cual es creada, debe ser revisada, la redacción y aprobada. Durante la creación de la política, se planea, se indaga, se fomenta y coordina con el departamento de la institución financiera. Además, durante

esta fase tiene actividades clave como: necesidad de la política, alcance de la política, roles, responsabilidades establecidas y aplicabilidad de la política.

Siguiendo el orden, pasa a la revisión, donde consiste en emitir la documentación por equipos de supervisores para su evaluación individual, donde se obtiene criterios, recomendaciones para hacer los cambios pertinentes. Finalmente, la aprobación, la cual involucra el compromiso de la institución financiera y da paso posiblemente a la implementación de las políticas de seguridad de la información.

Fase de Implementación

En esta fase, la política introduce la comunicación y cuestión. Esto implica la aplicación práctica de los procedimientos establecidos y controles en la política basándose en el documento que los sustenta y da la continuidad al cumplimiento progresivo. Además, podría que existan excepciones donde no se puedan ejecutarse los debidos procedimientos requeridos, lo cual debe documentar que no conllevara una aplicación temporal.

Fase de Mantenimiento

Los empleados de la institución financiera deben dar la importancia de la política de seguridad de la información, el cumplimiento, monitoreo y las respectivas actualizaciones requeridas. Entender el impulso por garantizar el debido cumplimiento de la política de seguridad de la información, lo cual esto motiva a comunicar al jefe encargado a través de reuniones, capacitaciones a los empleados, correos electrónicos como medio de difusión a todo el personal de la institución financiera. Y siempre asegurarse que la política deber actualizada con la garantía vigente y desarrollo constante.

Fase de Eliminación

En esta última fase de la política se retira cuando llegue al final de la vida útil o a la vez puede darse por ser reemplazado, es decir, a una versión actualizada con respuestas más relevantes en la institución financiera. Durante esta fase debe ser con debida atención, ya que la información requiera archivarse para futuras referencias continuas.

Políticas específicas de seguridad de la información

A continuación, se desarrollan políticas específicas asociadas directamente a los dominios, objetivos de control y controles del Anexo A de la Norma ISO 27001:2013 y relacionadas directamente con la Política General, que especifican la conducta aceptada por la Entidad en el manejo de su información y las acciones que deben ser tomadas para lograr los objetivos de la presente política considera el autor (Purdue, 2017).

Directrices de la Dirección de la seguridad de la información

La dirección debe brindar apoyo y orientación para la seguridad de la información de acuerdo con los requisitos del negocio.

Conjunto de políticas para la seguridad de la información

Definir en conjunto de las políticas de seguridad de la información de acuerdo a las necesidades identificadas en el análisis de riesgos.

Revisión de las políticas para la seguridad de la información

Verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.

Declaración de la política

La política de seguridad de la información de las entidades del sector asegurador tiene como objetivo la protección de los activos de información involucrados en la ejecución de los procesos que desarrolla la Organización en el ejercicio de su actividad, mediante un equipo calificado y comprometido con la seguridad de la información, garantizando la continuidad en las operaciones y procesos que soportan los objetivos del negocio y la mejora continua expresa el autor (Purdue, 2017).

Criterios considerados para desarrollar políticas de seguridad

En esto se establecen los siguientes puntos referentes a considerarse por (OSRI, 2018):

- Tener en cuenta el objeto social de la entidad y sus características. Por ejemplo, la seguridad de una entidad comercial es muy diferente a la de un organismo central o a de una universidad.
- Las políticas de seguridad que se desarrollen deben estar en correspondencia con las políticas, reglas, regulaciones y leyes a las que la entidad está sujeta.

Las políticas deben manejar los asuntos derivados de un problema de seguridad que tiene lugar por causa de un sitio remoto, así como un problema que ocurre en el mismo como resultado de un usuario o computadora local.

Interrogantes en una política de seguridad

Consta de la siguiente manera según el autor, (OSRI, 2018):

- ¿Qué estrategia se adoptará para la gestión de la seguridad informática?
- ¿A quién se le permite utilizar los bienes informáticos?
- ¿Qué se entiende por uso correcto de los recursos?
- ¿Quién está autorizado para garantizar el acceso y aprobar el uso de los
- bienes informáticos?
- ¿Quién debe tener privilegios de administración de los sistemas?

- ¿Cuáles son los derechos y responsabilidades de los usuarios?
- ¿Cuáles son los derechos y responsabilidades de los administradores de
- sistemas frente a los de los usuarios?
- ¿Qué hacer con la información clasificada y limitada?
- ¿Qué hacer ante la ocurrencia de un incidente de seguridad?

2.7. Diseño de un plan de seguridad de la información.

2.7.1. Desarrollo de la PSI.

En el desarrollo de la política de seguridad de la información (PSI) es un elemento clave en la gestión de la seguridad de la información (GSI). La PSI es un documento estratégico que aclara el marco general/marco de trabajo para proteger los activos de información y puesto a garantizar la disponibilidad, confidencialidad e integridad de la información.

Basándonos en el desarrollo de la política de seguridad de la información (PSI) rige a los siguientes aspectos que se van a detallar a continuación:

Compresión de contexto:

- Análisis del entorno.
- Requisitos legales y regulatorios.

Definición de objetivos:

- Objetivos de la PSI.
- Relación con objetivos de negocio.

Participación de las partes interesadas:

- Identificación de partes interesadas.
- Involucramiento y consulta.

Desarrollo de contenidos:

- Declaración de política
- Ámbito de la política.
- Responsabilidades.
- Normas y directrices.
- Protección de activos.

Revisión y aprobación:

- Revisión por expertos.
- Aprobación por alta dirección.

Comunicación y concientización:

- Comunicación interna.

- Programas de concientización.

Implementación y mantenimiento:

- Implementación gradual.
- Actualización periódica.

Evaluación y mejora continua:

- Monitores de indicadores.
- Revisiones y auditorías.
- Mejora continua.

2.7.2. Aprobación y Comunicación.

Dentro de la aprobación y comunicación de Política de Seguridad de la Información (PSI) contiene pasos críticos para contemplar la garantía de que la política sea de manera entendible y adoptable por todos los miembros de la organización.

Además, en la **Aprobación** de la PSI tiene aspectos que se deben considerarse que se van a detallar los siguientes puntos:

- Revisión por expertos: la PSI debe ser revisada por los expertos de seguridad de la información.
- Aprobación de alta dirección: este paso garantiza el compromiso de los involucrados de la organización.
- Firma de aprobación: esta firma indica un compromiso formal con la política de seguridad de la información.

De igual forma, para la **Comunicación** de la PSI se consideran los siguientes puntos:

- Desarrollo de un plan de comunicación: describir detallado el plan como se debe comunicar la PSI.
- Comunicación interna: utilizar canales de comunicación efectivos.
- Sesiones de sensibilización: explicar la importancia de la PSI, riesgos asociados y responsabilidades establecidas.
- Incorporación de la PSI en la Orientación: asegurar que entiendan los principios y expectativas desde el inicio.
- Comunicación externa si es Relevante: comunicar la existencia y principios sobre la PSI puede ser beneficiante.
- Disponibilidad pública: mostrar el compromiso de la empresa con la seguridad de la información.
- Canal de retroalimentación: expresar inquietudes, comentarios sobre la PSI.

- Recordatorios periódicos: recordar los principios y responsabilidades sobre la PSI.
- Inclusión en documentación relevante: políticas internas, documentos relacionados con la PSI.
- Evaluar la efectividad de la comunicación: la PSI sea comprendida y adoptada por todos dentro de la organización.

2.7.3. Implementación y Mantenimiento.

La implementación y mantenimiento de la Política de Seguridad de la Información (PSI) muestran fases críticas para sostener que los principios de seguridad sean esmerados de la manera efectiva y sustentable en la organización.

En una **Implementación** de la PSI contiene varios aspectos que son importantes para la organización, tal manera se detallara a continuación:

- Desarrollo de procedimientos y controles: implementar los principios establecidos en la PSI.
- Planificación de la implementación: establecer cronograma realista y asignar responsabilidades claras y concretas.
- Capacitación y concientización: asegurar que entiendan la PSI, roles y responsabilidades a diario.
- Integración con procesos de negocio: en esta parte garantiza la seguridad de la información que esté incorporada en todas las actividades en la organización.
- Control de cambios: todas las actualizaciones deben ser revisadas y aprobadas antes de ser implementado.
- Monitoreo y auditoría: asegurar la conformidad con la PSI.

Así mismo, en el **Mantenimiento** de la PSI toma varios puntos importantes que se debe seguir:

- Revisión periódica: revisiones regulares en el entorno de seguridad.
- Actualización de procedimientos y controles: actualizar los debidos procedimientos para abordar amenazas dentro de la organización.
- Capacitación continua: mantener a los empleados en capacitación para mejores prácticas.
- Evaluación de riesgos: identificar posibles amenazas y adaptar la PSI conforme sea necesario.
- Comunicación de cambios: comunicar cualquier detalle o cambio realizado.

- Respuesta a incidentes: revisar y adaptar el plan de respuesta a diferentes incidentes.
- Mejora continua: impulsar mejoras continuas de la PSI.
- Cumplimiento normativo: cumplimiento de normativas, estándares y realizar cualquier detalle si es necesario.
- Retroalimentación del personal: recopilar la retroalimentación del personal acerca de la efectividad de la PSI.
- Registro de incidentes y lecciones aprendidas: tener un registro detallado de incidentes y aplicar estas experiencias para tener una mejora y fortalecer la PSI.

CAPÍTULO 3

Validación de Resultados

La validación de los resultados de la propuesta de la investigación que se realizó basándose en la norma ISO/IEC 27001 que se retracta a la seguridad de la información. Se realizó la encuesta utilizando una escala de Likert de 5 niveles de respuesta, que va desde "Excelente" hasta "No tiene conocimientos", por otra parte, cada respuesta tiene una equivalencia de valores que van del 1 al 5, tomándole un valor de 1 a la primera y un valor de 5 a la última, como se puede observar en la Tabla 16.

Tabla 16: Puntuación de escala de Likert

Respuesta	Valor
No tiene conocimientos	1
Muy deficiente	2
Regular	3
Bueno	4
Excelente	5

En la Tabla 17, se detalla las respuestas obtenidas de la encuesta realizada, tal forma se puede mirar los resultados por pregunta.

3.1. Analisis de estudios de los resultados.

3.1.1. Encuesta de Satisfacción.

Con base a la normativa ISO/IEC 27001 se establece una encuesta para la evaluación correspondiente sobre la seguridad de la información, tal razón en este caso para el desarrollo del plan de sistema de gestión de la seguridad de la información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda. Con base a las respuestas obtenidas por parte de los personales de la Cooperativa se determina el nivel de importancia sobre la seguridad de la información que se necesita para la institución financiera.

Se realizó la encuesta utilizando la herramienta Microsoft Forms, con la finalidad de recopilar información relevante a la seguridad de la información, se aprecia en el siguiente enlace: https://forms.office.com/r/XR8J9910UE

En la Tabla 18, se muestran las preguntas que se establecen en la encuesta de satisfacción del anexo 2, cada cuestión establece puntos importantes para verificar el nivel de conocimiento del impacto de la seguridad de la información en la institución financiera.

3.2. Interpretación de resultados

Para la interpretación de los resultados se utilizó la herramienta SPSS para obtener análisis estadísticos esenciales. Valores que se utilizará será a base de la encuesta ejecutada en la Tabla 19.

Análisis descriptivo

Dentro del análisis descriptivo se tiene el N que es el número de preguntas con los valores de la encuesta ejecutado donde se conoce las siguientes variables tales como mínimo, máximo, media y desviación con sus resultados en la Tabla 20.

Tabla 17: Resultados de la encuesta por pregunta

	Respuestas				
Preguntas	**No tiene conocimientos**	**Muy deficiente**	**Regular**	**Bueno**	**Excelente**
Pregunta 1	0	0	3	10	0
Pregunta 2	5	1	7	0	0
Pregunta 3	2	1	9	1	0
Pregunta 4	0	0	8	5	0
Pregunta 5	11	0	2	0	0
Pregunta 6	11	0	1	1	0
Pregunta 7	11	0	0	2	0
Pregunta 8	12	0	0	1	0
Pregunta 9	12	0	0	1	0
Pregunta 10	12	0	0	1	0
Pregunta 11	12	0	0	1	0
Pregunta 12	12	0	0	1	0
Pregunta 13	12	0	0	1	0
Pregunta 14	1	0	1	11	0
Pregunta 15	12	0	0	1	0
Pregunta 16	12	0	0	1	0
Pregunta 17	12	0	0	1	0
Pregunta 18	12	0	0	0	1
Pregunta 19	12	0	0	1	0
Pregunta 20	12	0	0	1	0
Pregunta 21	0	12	1	0	0
Pregunta 22	12	0	0	1	0
Pregunta 23	11	1	0	1	0
Pregunta 24	0	12	0	1	0
Pregunta 25	12	0	0	1	0
Pregunta 26	12	0	0	1	0
Pregunta 27	0	12	0	1	0

Tabla 18: Preguntas de la encuesta realizada

Numeración	Pregunta
Pregunta 1	En una escala del 5 al 1 cuál es su nivel de conocimiento respecto a la seguridad de la información.
Pregunta 2	¿De acuerdo a sus conocimientos en que porcentaje de conocimiento tiene en lo relacionado a la normativa de la seguridad de la información?
Pregunta 3	¿Ha realizado en los últimos años ha realizado capacitaciones en temas de seguridad de la información?
Pregunta 4	¿Cuál es su conocimiento actual sobre la Norma ISO/IEC 27001?
Pregunta 5	¿Qué conocimientos tiene sobre la ley de protección de datos?
Pregunta 6	Se han realizado Auditorias en temas de seguridad de la información, indique el nivel en que se encuentra
Pregunta 7	El medio donde se guardan los archivos de respaldo cuenta con medidas de seguridad (servidores) ¿En qué estado de seguridad se encuentran?
Pregunta 8	Los servicios prestados por proveedores externos cuentan con controles de disponibilidad del sistema ¿qué estado de disponibilidad se encuentran?
Pregunta 9	Los servicios prestados por proveedores externos cuentan con un plan de contingencia en el caso de un fallo ¿Cómo define su accionar en tiempo de respuesta para resolver dichos problemas?
Pregunta 10	Ante el fallo en uno de los servidores de la empresa, dispone de un servidor alterno ¿En qué estado se encuentra el servidor?
Pregunta 11	El sistema de control (registro, bitácoras, cámaras, etc.) para el ingreso a esta área está definida como.
Pregunta 12	El área de servidores de acuerdo a las normativas de seguridad de la información para el diseño y ubicación ¿En qué estado se encuentra?
Pregunta 13	Ante una emergencia, donde se encuentre en riesgo la información y es necesario contar con un plan de contingencia ¿En qué nivel lo define?
Pregunta 14	¿Cómo define el control de correos electrónicos?
Pregunta 15	¿Cómo se define el control de antivirus en los equipos de cómputo de la empresa?
Pregunta 16	La seguridad que tienen los sistemas desarrollados por el personal dentro de la empresa ¿Qué disponibilidad brindan para el manejo de datos?
Pregunta 17	La seguridad que tienen los sistemas contratados por la empresa ¿Qué disponibilidad brindan para el manejo de datos?
Pregunta 18	Cómo definen el acceso y restricción a la red para los usuarios, sea a páginas de navegación como acceso a carpetas compartidas dentro de la red de la Cooperativa Imbacoop Ltda.
Pregunta 19	El software utilizado en la empresa con licenciamiento pagado ¿Qué seguridad posee?
Pregunta 20	El software utilizado en la empresa con licenciamiento libre ¿Qué seguridad posee?
Pregunta 21	¿Cuál es el porcentaje de disponibilidad de los servicios informáticos en la cooperativa de ahorro y crédito bajo las normas ISO 27001?
Pregunta 22	¿Cuáles son los sistemas clave de la cooperativa de ahorro y crédito y cuál es su disponibilidad promedio?
Pregunta 23	¿Qué medidas de seguridad específicas se implementan en la cooperativa para garantizar la disponibilidad de los servicios informáticos?

Continua…

Pregunta 24	¿Cómo se realizan las pruebas de disponibilidad de los servicios informáticos en la cooperativa de ahorro y crédito bajo las normas ISO 27001?
Pregunta 25	¿La cooperativa cuenta con un acuerdo de nivel de servicio (SLA) para medir la disponibilidad de sus servicios informáticos?
Pregunta 26	¿Qué medidas específicas se implementan para garantizar la disponibilidad de los sistemas informáticos en la cooperativa?
Pregunta 27	¿Cuál es el tiempo estimado de recuperación en caso de interrupciones en los servicios informáticos de la cooperativa?

Tabla 19: Valores a base de la encuesta

Valor	Sigla
No tiene conocimientos	(N.T.C)
Muy deficiente	(M.D)
Regular	(R)
Bueno	(B)
Excelente	(E)

Tabla 20: Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desviación
No tiene conocimientos	27	0	12	8,59	5,116
Muy deficiente	27	0	12	1,44	3,816
Regular	27	0	9	1,19	2,573
Bueno	27	0	11	1,74	2,683
Excelente	27	0	1	0,04	0,192
N válido (por lista)	27				

Tabla cruzada

Una tabla de cruce es una herramienta estadística que resume la distribución conjunta de dos o más variables categóricas. También se le conoce como tabla de contingencia o tabla de frecuencias cruzadas. Esta tabla organiza los datos de tal manera que permite visualizar las relaciones entre las variables. Cada celda en la tabla muestra la frecuencia con la que ocurre una combinación específica de categorías de las variables.

De la encuesta ejecutada a base de las preguntas desarrolladas se obtuvo el resumen de procesamiento de casos en la Tabla 21.

Tabla 21: Procesamiento de casos

	Casos Válido N	Porcentaje	Perdido N	Porcentaje	Total N	Porcentaje
No tiene conocimientos * Preguntas	*27	100,0%	0	0,0%	27	100,0%
Muy deficiente * Preguntas	27	100,0%	0	0,0%	27	100,0%
Regular * Preguntas	27	100,0%	0	0,0%	27	100,0%
Bueno * Preguntas	27	100,0%	0	0,0%	27	100,0%
Excelente * Preguntas	27	100,0%	0	0,0%	27	100,0%

Tabla cruzada de la variable No Tiene Conocimientos (N.T.C)

		Preguntas			
		Pregunta 1	Pregunta 10	Pregunta 11	Pregunta 12
No tiene conocimientos	0	1	0	0	0
	1	0	0	0	0
	2	0	0	0	0
	5	0	0	0	0
	11	0	0	0	0
	12	0	1	1	1
Total		1	1	1	1

		Preguntas			
		Pregunta 13	Pregunta 14	Pregunta 15	Pregunta 16
No tiene conocimientos	0	0	0	0	0
	1	0	1	0	0
	2	0	0	0	0
	5	0	0	0	0
	11	0	0	0	0
	12	1	0	1	1
Total		1	1	1	1

		Preguntas			
		Pregunta 17	Pregunta 18	Pregunta 19	Pregunta 2
No tiene conocimientos	0	0	0	0	0
	1	0	0	0	0
	2	0	0	0	0
	5	0	0	0	1
	11	0	0	0	0
	12	1	1	1	0
Total		1	1	1	1

		Preguntas			
		Pregunta 20	Pregunta 21	Pregunta 22	Pregunta 23
No tiene conocimientos	0	0	1	0	0
	1	0	0	0	0
	2	0	0	0	0
	5	0	0	0	0
	11	0	0	0	1
	12	1	0	1	0
Total		1	1	1	1

		Preguntas			
		Pregunta 24	Pregunta 25	Pregunta 26	Pregunta 27
No tiene conocimientos	0	1	0	0	1
	1	0	0	0	0
	2	0	0	0	0
	5	0	0	0	0
	11	0	0	0	0
	12	0	1	1	0
Total		1	1	1	1

		Preguntas				
		Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7
No tiene conocimientos	0	0	1	0	0	0
	1	0	0	0	0	0
	2	1	0	0	0	0
	5	0	0	0	0	0
	11	0	0	1	1	1
	12	0	0	0	0	0
Total		1	1	1	1	1

		Preguntas		
		Pregunta 8	Pregunta 9	Total
No tiene conocimientos	0	0	0	5
	1	0	0	1
	2	0	0	1
	5	0	0	1
	11	0	0	4
	12	1	1	15
Total		1	1	27

Figura. 17: Tabla Cruzada (N.T.C)

Tabla 22: Medidas direccionales (N.T.C)

			Valor	Error estándar asintótico a	T aproximada b	Significación aproximada
Nominal por Nominal	Coeficiente de incertidumbre	Simétrico	0,562	0,054	7,450	1,000c
		No tiene conocimientos dependientes	1,000	0,000	7,450	1,000c
		Preguntas dependientes	0,391	0,052	7,450	1,000c

a. No se presupone la hipótesis nula.

b. Utilización del error estándar asintótico que presupone la hipótesis nula.

c. Probabilidad de chi-cuadrado de razón de verosimilitud.

Tabla cruzada de la variable Muy Deficiente (M.D)

		Preguntas				
		Pregunta 1	Pregunta 10	Pregunta 11	Pregunta 12	Pregunta 13
Muy deficiente	0	1	1	1	1	1
	1	0	0	0	0	0
	12	0	0	0	0	0
Total		1	1	1	1	1

		Preguntas				
		Pregunta 14	Pregunta 15	Pregunta 16	Pregunta 17	Pregunta 18
Muy deficiente	0	1	1	1	1	1
	1	0	0	0	0	0
	12	0	0	0	0	0
Total		1	1	1	1	1

		Preguntas				
		Pregunta 19	Pregunta 2	Pregunta 20	Pregunta 21	Pregunta 22
Muy deficiente	0	1	0	1	0	1
	1	0	1	0	0	0
	12	0	0	0	1	0
Total		1	1	1	1	1

		Preguntas				
		Pregunta 23	Pregunta 24	Pregunta 25	Pregunta 26	Pregunta 27
Muy deficiente	0	0	0	1	1	0
	1	1	0	0	0	0
	12	0	1	0	0	1
Total		1	1	1	1	1

		Preguntas				
		Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7
Muy deficiente	0	0	1	1	1	1
	1	1	0	0	0	0
	12	0	0	0	0	0
Total		1	1	1	1	1

		Preguntas		
		Pregunta 8	Pregunta 9	Total
Muy deficiente	0	1	1	21
	1	0	0	3
	12	0	0	3
Total		1	1	27

Figura. 18: Tabla Cruzada (M.D)

Tabla 23: Medidas direccionales (M.D)

			Valor	Error estándar asintótico a	T aproximada b	Significación aproximada
Nominal por Nominal	Coeficiente de incertidumbre	Simétrico	0,344	0,065	4,392	0,943c
		Muy deficiente dependiente	1,000	0,000	4,392	0,943c
		Preguntas dependientes	0,207	0,047	4,392	0,943c

a. No se presupone la hipótesis nula.

b. Utilización del error estándar asintótico que presupone la hipótesis nula.

c. Probabilidad de chi-cuadrado de razón de verosimilitud.

Tabla cruzada de la variable Regular (R)

		Preguntas				
		Pregunta 1	Pregunta 10	Pregunta 11	Pregunta 12	Pregunta 13
Regular	0	0	1	1	1	1
	1	0	0	0	0	0
	2	0	0	0	0	0
	3	1	0	0	0	0
	7	0	0	0	0	0
	8	0	0	0	0	0
	9	0	0	0	0	0
Total		1	1	1	1	1

		Preguntas				
		Pregunta 14	Pregunta 15	Pregunta 16	Pregunta 17	Pregunta 18
Regular	0	0	1	1	1	1
	1	1	0	0	0	0
	2	0	0	0	0	0
	3	0	0	0	0	0
	7	0	0	0	0	0
	8	0	0	0	0	0
	9	0	0	0	0	0
Total		1	1	1	1	1

		Preguntas				
		Pregunta 19	Pregunta 2	Pregunta 20	Pregunta 21	Pregunta 22
Regular	0	1	0	1	0	1
	1	0	0	0	1	0
	2	0	0	0	0	0
	3	0	0	0	0	0
	7	0	1	0	0	0
	8	0	0	0	0	0
	9	0	0	0	0	0
Total		1	1	1	1	1

		Preguntas				
		Pregunta 23	Pregunta 24	Pregunta 25	Pregunta 26	Pregunta 27
Regular	0	1	1	1	1	1
	1	0	0	0	0	0
	2	0	0	0	0	0
	3	0	0	0	0	0
	7	0	0	0	0	0
	8	0	0	0	0	0
	9	0	0	0	0	0
Total		1	1	1	1	1

		Preguntas					
		Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7	Pregunta 8
Regular	0	0	0	0	0	1	1
	1	0	0	0	1	0	0
	2	0	0	1	0	0	0
	3	0	0	0	0	0	0
	7	0	0	0	0	0	0
	8	0	1	0	0	0	0
	9	1	0	0	0	0	0
Total		1	1	1	1	1	1

		Preguntas	
		Pregunta 9	Total
Regular	0	1	19
	1	0	3
	2	0	1
	3	0	1
	7	0	1
	8	0	1
	9	0	1
Total		1	27

Figura. 19: Tabla Cruzada (R)

Tabla 24: Medidas direccionales (R)

			Valor	Error estándar asintótico a	T aproximada b	Significación aproximada
Nominal por Nominal	Coeficiente de incertidumbre	Simétrico	0,501	0,078	4,802	1,000c
		Regular dependiente	1,000	0,000	4,802	1,000c
		Preguntas dependientes	0,334	0,070	4,802	1,000c

a. No se presupone la hipótesis nula.

b. Utilización del error estándar asintótico que presupone la hipótesis nula.

c. Probabilidad de chi-cuadrado de razón de verosimilitud.

Tabla cruzada de la variable Bueno (B)

		Preguntas				
		Pregunta 1	Pregunta 10	Pregunta 11	Pregunta 12	Pregunta 13
Bueno	0	0	0	0	0	0
	1	0	1	1	1	1
	2	0	0	0	0	0
	5	0	0	0	0	0
	10	1	0	0	0	0
	11	0	0	0	0	0
Total		1	1	1	1	1

		Preguntas				
		Pregunta 14	Pregunta 15	Pregunta 16	Pregunta 17	Pregunta 18
Bueno	0	0	0	0	0	1
	1	0	1	1	1	0
	2	0	0	0	0	0
	5	0	0	0	0	0
	10	0	0	0	0	0
	11	1	0	0	0	0
Total		1	1	1	1	1

		Preguntas				
		Pregunta 19	Pregunta 2	Pregunta 20	Pregunta 21	Pregunta 22
Bueno	0	0	1	0	1	0
	1	1	0	1	0	1
	2	0	0	0	0	0
	5	0	0	0	0	0
	10	0	0	0	0	0
	11	0	0	0	0	0
Total		1	1	1	1	1

		Preguntas				
		Pregunta 23	Pregunta 24	Pregunta 25	Pregunta 26	Pregunta 27
Bueno	0	0	0	0	0	0
	1	1	1	1	1	1
	2	0	0	0	0	0
	5	0	0	0	0	0
	10	0	0	0	0	0
	11	0	0	0	0	0
Total		1	1	1	1	1

		Preguntas					
		Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7	Pregunta 8
Bueno	0	0	0	1	0	0	0
	1	1	0	0	1	0	1
	2	0	0	0	0	1	0
	5	0	1	0	0	0	0
	10	0	0	0	0	0	0
	11	0	0	0	0	0	0
Total		1	1	1	1	1	1

		Preguntas	
		Pregunta 9	Total
Bueno	0	0	4
	1	1	19
	2	0	1
	5	0	1
	10	0	1
	11	0	1
Total		1	27

Figura. 20: Tabla Cruzada (B)

Tabla 25: Medidas direccionales (B)

			Valor	Error estándar asintótico a	T aproximada b	Significación aproximada
Nominal por Nominal	Coeficiente de incertidumbre	Simétrico	0,472	0,075	4,833	1,000c
		Bueno dependiente	1,000	0,000	4,833	1,000c
		Preguntas dependientes	0,309	0,064	4,833	1,000c

a. No se presupone la hipótesis nula.

b. Utilización del error estándar asintótico que presupone la hipótesis nula.

c. Probabilidad de chi-cuadrado de razón de verosimilitud.

Tabla cruzada de la variable Excelente (E)

		Preguntas				
		Pregunta 1	Pregunta 10	Pregunta 11	Pregunta 12	Pregunta 13
Excelente	0	1	1	1	1	1
	1	0	0	0	0	0
Total		1	1	1	1	1

		Preguntas				
		Pregunta 14	Pregunta 15	Pregunta 16	Pregunta 17	Pregunta 18
Excelente	0	1	1	1	1	0
	1	0	0	0	0	1
Total		1	1	1	1	1

		Preguntas				
		Pregunta 19	Pregunta 2	Pregunta 20	Pregunta 21	Pregunta 22
Excelente	0	1	1	1	1	1
	1	0	0	0	0	0
Total		1	1	1	1	1

		Preguntas				
		Pregunta 23	Pregunta 24	Pregunta 25	Pregunta 26	Pregunta 27
Excelente	0	1	1	1	1	1
	1	0	0	0	0	0
Total		1	1	1	1	1

		Preguntas					
		Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7	Pregunta 8
Excelente	0	1	1	1	1	1	1
	1	0	0	0	0	0	0
Total		1	1	1	1	1	1

		Preguntas	
		Pregunta 9	Total
Excelente	0	1	26
	1	0	1
Total		1	27

Figura. 21: Tabla Cruzada (E)

Tabla 26: Medidas direccionales (E)

			Valor	Error estándar asintótico a	T aproximada b	Significación aproximada
Nominal por Nominal	Coeficiente de incertidumbre	Simétrico	0,092	0,065	1,338	0,999c
		Excelente dependiente	1,000	0,000	1,338	0,999c
		Preguntas dependientes	0,048	0,036	1,338	0,999c

a. No se presupone la hipótesis nula.

b. Utilización del error estándar asintótico que presupone la hipótesis nula.

c. Probabilidad de chi-cuadrado de razón de verosimilitud.

Correlación de Pearson

El coeficiente de correlación de Pearson es una herramienta estadística que nos permite evaluar tanto la intensidad como la dirección de la relación lineal entre dos variables cuantitativas. Esta medida, también conocida como correlación producto-momento, fue creada por Karl Pearson y se utiliza ampliamente en el campo de las estadísticas para medir el grado de relación lineal entre dos conjuntos de datos.

Como se calcula el coeficiente de Pearson

$$rxy \frac{\sum z\, xzy}{N}$$

Donde:

“x” es igual a la variable número uno, “y” pertenece a la variable número dos, “zx” es la desviación estándar de la variable uno, “zy” es la desviación estándar de la variable dos y “N” es número de datos.

En la encuesta ejecutada se obtuvo los resultados de los estadísticos descriptivos por Pearson en la Tabla 27.

Tabla 27: Estadístico de la encuesta

	Media	**Desviación**	**N**
No tiene conocimientos	8,59	5,116	27
Muy deficiente	1,44	3,816	27
Regular	1,19	2,573	27
Bueno	1,74	2,683	27
Excelente	,04	,192	27

De igual forma con los resultados de la encuesta ejecutado se realizó Correlaciones de Pearson en la Tabla 28.

El coeficiente de correlación de Pearson se utiliza para medir la relación entre dos variables y determinar su asociación mutua. Aquí hay algunos puntos importantes a considerar:

Correlación menor a cero: Si el coeficiente es menor a cero, indica una correlación negativa, lo que significa que las variables están inversamente relacionadas. Cuando una variable tiene un valor alto, la otra variable tiene un valor bajo. Cuanto más cercano esté el coeficiente a -1, más evidente será la relación inversa extrema.

Correlación mayor a cero: Si el coeficiente es igual a +1, indica una correlación positiva perfecta. En este caso, las variables están directamente relacionadas. Cuando una variable tiene un valor alto, la otra también lo tiene; lo mismo ocurre cuando ambos valores son bajos. Si el coeficiente está cerca de +1, indica una alta covariación entre las variables.

Correlación igual a cero: Cuando el coeficiente es igual a cero, significa que no se puede determinar ninguna relación de covariación entre las variables. Sin embargo, esto no descarta la posibilidad de que exista una relación no lineal entre ellas.

Pruebas de Chi-Cuadrado

La prueba de chi-cuadrado, también llamada prueba de bondad de ajuste se emplea para determinar si existe una diferencia significativa entre las distribuciones observadas y esperadas de un conjunto de datos categóricos. La hipótesis nula sostiene que no hay una diferencia

significativa, mientras que la hipótesis alternativa sugiere que sí existe una diferencia considerable**.**

En la Tabla 29 que se va a visualizar los resultados sobre las pruebas de Chi-Cuadrado se tomaron de las variables de la encuesta son: (No tiene Conocimiento, Muy Deficiente, Regular, Bueno y Excelente)

De la anterior Tabla 29, en conjunto se hace las estadísticas de prueba en Tabla 30 en base a la encuesta ejecutada se obtuvo los resultados por Chi-Cuadrado.

Tabla 28: Resultado por Chi-Cuadrado con las variables de la encuesta

No Tiene Conocimientos

	N observado	N esperada	Residuo
0	5	4,5	,5
1	1	4,5	-3,5
2	1	4,5	-3,5
5	1	4,5	-3,5
11	4	4,5	-,5
12	15	4,5	10,5
Total	27		

Muy Deficiente

	N observado	N esperada	Residuo
0	21	9,0	12,0
1	3	9,0	-6,0
12	3	9,0	-6,0
Total	27		

Regular

	N observado	N esperada	Residuo
0	19	3,9	15,1
1	3	3,9	-,9
2	1	3,9	-2,9
3	1	3,9	-2,9
7	1	3,9	-2,9
8	1	3,9	-2,9
9	1	3,9	-2,9
Total	27		

Bueno

	N observado	N esperada	Residuo
0	4	4,5	-,5
1	19	4,5	14,5
2	1	4,5	-3,5
5	1	4,5	-3,5
10	1	4,5	-3,5
11	1	4,5	-3,5
Total	27		

Excelente

	N observado	N esperada	Residuo
0	26	13,5	12,5
1	1	13,5	-12,5
Total	27		

Tabla 29: Correlaciones de la encuesta

		No tiene conocimientos	Muy deficiente	Regular	Bueno	Excelente
No tiene conocimientos	Correlación de Pearson	1	-,625**	-,549**	-,501**	,133
	Sig. (bilateral)		,000	,003	,008	,508
	Suma de cuadrados y productos vectoriales	680,519	-317,111	-187,963	-178,852	3,407
	Covarianza	26,174	-12,197	-7,229	-6,879	,131
	N	27	27	27	27	27
Muy deficiente	Correlación de Pearson	-,625**	1	-,071	-,157	-,076
	Sig. (bilateral)	,000		,723	,433	,708
	Suma de cuadrados y productos vectoriales	-317,111	378,667	-18,222	-41,889	-1,444
	Covarianza	-12,197	14,564	-,701	-1,611	-,056
	N	27	27	27	27	27
Regular	Correlación de Pearson	-,549**	-,071	1	,197	-,092
	Sig. (bilateral)	,003	,723		,326	,648
	Suma de cuadrados y productos vectoriales	-187,963	-18,222	172,074	35,296	-1,185
	Covarianza	-7,229	-,701	6,618	1,358	-,046
	N	27	27	27	27	27
Bueno	Correlación de Pearson	-,501**	-,157	,197	1	-,130
	Sig. (bilateral)	,008	,433	,326		,519
	Suma de cuadrados y productos vectoriales	-178,852	-41,889	35,296	187,185	-1,741
	Covarianza	-6,879	-1,611	1,358	7,199	-,067
	N	27	27	27	27	27
Excelente	Correlación de Pearson	,133	-,076	-,092	-,130	1
	Sig. (bilateral)	,508	,708	,648	,519	
	Suma de cuadrados y productos vectoriales	3,407	-1,444	-1,185	-1,741	,963
	Covarianza	,131	-,056	-,046	-,067	,037
	N	27	27	27	27	27

**. La correlación es significativa en el nivel 0,01 (bilateral).

3.3. Análisis de impacto.

El enfoque de la norma ISO/IEC 27001 se orienta hacia la gestión de la seguridad de la información e introduce la evaluación de impacto como parte integral de su enfoque de gestión de riesgos. Para entender realmente las posibles consecuencias y ramificaciones de los riesgos identificados en cada una de las áreas de seguridad de la información, es obligado hacer una evaluación de impacto.

Tabla 30: Estadístico por Chi-Cuadrado

	No tiene conocimientos	Muy deficiente	Regular	Bueno	Excelente
Chi-cuadrado	32,778 a	24,000b	70,222c	57,667 a	23,148d
gl	5	2	6	5	1
Sig. asintótica	0,000	0,000	0,000	0,000	0,000

a. 6 casillas (100,0%) han esperado frecuencias menores que 5. La frecuencia mínima de casilla esperada es 4,5.
b. 0 casillas (0,0%) han esperado frecuencias menores que 5. La frecuencia mínima de casilla esperada es 9,0.
c. 7 casillas (100,0%) han esperado frecuencias menores que 5. La frecuencia mínima de casilla esperada es 3,9.
d. 0 casillas (0,0%) han esperado frecuencias menores que 5. La frecuencia mínima de casilla esperada es 13,5.

3.3.1. Impacto Ambiental.

Aspectos positivos

Ahorro de Papel: La implantación de sistemas electrónicos y la gestión de la información digital pueden contribuir a reducir el uso de papel, y de este modo tener un impacto positivo en el medio ambiente.

Menor Consumo Energético: Procesos mejorados y eficiencia en la información pueden que representen un menor consumo de energía, con lo cual habría sostenibilidad.

Aspectos negativos

Uso de Tecnología: El establecimiento de sistemas tecnológicos puede producir desechos electrónicos. Al final de su vida útil es muy importante una gestión adecuada para la eliminación de equipos y dispositivos electrónicos.

3.3.2. Impacto Económico.

Aspectos positivos

Mejora de la Eficiencia: La ISO/IEC 27001 puede mejorar la eficiencia de la gestión de la información, reduciendo errores y tiempos muertos, lo que tendría un impacto beneficioso en la productividad y, en consecuencia, en la economía de la empresa.

Confianza del Cliente: Tener la certificación ISO/IEC 27001 puede aumentar la confianza de los clientes, con lo que, de ser así, los ingresos son un factor positivo.

Aspectos negativos

Costos Iniciales: La implementación inicial de la norma puede requerir inversiones significativas en tecnología, formación y consultaría, teniendo un impacto económico inicial negativo.

3.3.3. Impacto Tecnológico

Aspectos positivos

Seguridad Tecnológica Mejorada: La norma ISO/IEC 27001 se dedica a asegurar la seguridad de la información, y esto puede llevar a mejoras de seguridad tecnológica global.

Uso de Mejores Prácticas Tecnológicas: Puede ser el caso de que la norma se aplique y empuje a la gente a usar tecnologías de la información y comunicación que sean mejores.

Aspectos negativos

Necesidad de una Actualización Tecnológica: La implantación de la norma puede requerir que se hagan este tipo de cambios para cumplir ciertos requisitos. Y esto a su vez es razón para más costos.

CONCLUSIONES.

En entidades financieras, donde la confidencialidad, integridad y disponibilidad de la información son críticas, la aplicación de la norma ISO 27001 es fundamental, tal razón revisando la situación actual de la institución financiera es necesario contemplar con políticas de seguridad de la información, con la finalidad de mitigar las vulnerabilidades existentes. Proporcionando un marco robusto para gestionar riesgos, identificar activos, implementación de controles, mejora continua y garantizar la seguridad de la información financiera sensible.

La implementación de ISO 27001 en entidades financieras facilita el cumplimiento con regulaciones y normativas específicas del sector, como PCI DSS (Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago), garantizando así la seguridad de las transacciones y la protección de la información del cliente. Además, la norma ofrece un marco flexible que se puede adaptar a las necesidades específicas de la organización.

Mediante la encuesta de satisfacción basándonos en la ISO 27001 permite a las entidades financieras adaptarse y protegerse contra amenazas específicas del sector, como ataques cibernéticos dirigidos a datos financieros, fraudes electrónicos y otros riesgos que podrían tener impactos significativos en la confianza del cliente y la estabilidad financiera. La concienciación y la formación del personal son aspectos cruciales para construir una cultura en la que la seguridad de la información sea una responsabilidad compartida.

RECOMENDACIONES.

Dada la rápida evolución de las amenazas cibernéticas, se recomienda que las entidades financieras efectúen evaluaciones de riesgos de manera continua. Esto asegura la identificación temprana de nuevas amenazas y la implementación de controles adecuados en respuesta a cambios en el panorama de seguridad. Para el éxito de la implementación de la ISO 27001, se recomienda un fuerte compromiso de la alta dirección. Esto implica asignar recursos adecuados, establecer políticas claras y proporcionar el liderazgo necesario para fomentar una cultura de seguridad en toda la organización.

La protección de la información del cliente es de máxima importancia. Se recomienda un enfoque centrado en el cliente al implementar medidas de seguridad, incluyendo la encriptación robusta de datos, la autenticación segura y la educación continua del cliente sobre las mejores prácticas de seguridad. Esto facilita la aceptación y cumplimiento por parte de los empleados, ya que los controles están alineados con los objetivos organizativos más amplios.

A pesar de las medidas preventivas, la posibilidad de incidentes de seguridad siempre existe. Se recomienda que las entidades financieras desarrollen planes de respuesta a incidentes sólidos y practiquen simulacros periódicos para asegurar una respuesta rápida y efectiva en caso de violaciones de seguridad.

BIBLIOGRAFÍA.

Amaya, C. G. (9 de Octubre de 2013). *welivesecurity*. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

ERAZO, A. M. (20 de 12 de 2016). *http://repositorio.utn.edu.ec.* Obtenido de http://repositorio.utn.edu.ec: http://repositorio.utn.edu.ec/bitstream/123456789/9001/1/05%20FECYT%20213%20TRABAJO%20DE%20GRADO.pdf

Implantaci, D. E. (2013). *Guía De Implantación Para La Seguridad De La Información.* Obtenido de Guía De Implantación Para La Seguridad De La Información.

ISO27000.ES. (s.f.). Obtenido de ISO27000.ES: www.ISO27000.es

Jimeno, J. (23 de Agosto de 2013). *PDCA HOME*. Obtenido de PDCA HOME: https://www.pdcahome.com/5202/ciclo-pdca/

Juan J. Lugo Marín, H. E. (12 de Junio de 2020). *QUALITAS*. Obtenido de QUALITAS: https://revistas.unibe.edu.ec/index.php/qualitas/article/download/42/177?inline=1)

Mendoza, M. A. (18 de Agosto de 2014). *welivesecurity*. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2014/08/18/ciclo-de-vida-de-las-politicas-de-seguridad/

ONU. (2015). *Objetivos de desarrollo sostenible.* Obtenido de Objetivos de desarrollo sostenible: https://grupoenvera.org/sin-categoria/agenda-2030-asi-contribuye-envera-once-los-objetivos-desarrollo-sostenible/?gclid=CjwKCAiA24SPBhB0EiwAjBgkhtNtvtg2YPkwhb6j3ElonKmPCLvdPhRHKH63ZMOfVl8fFSZyAY_WbxoCTscQAvD_BwE#anchor

Seguridad de la Informacion . (1 de Diciembre de 2010). Obtenido de Seguridad de la Informacion: https://necastro.blogspot.com/2010/12/politicas-de-seguridad-de-la.html

Unidas, N. (2016). *Objetivo 9: Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación.* Obtenido de https://www.un.org/sustainabledevelopment/es/infrastructure/

27001, I. (2013). *Guía De Implantación Para La Seguridad De La Información*.

Benitez Pineda, D. G. (n.d.). *Revision bibliográfica de la norma ISO 27001 y sus componentes*.

Carlos Humberto, P. (2018). *Seguridad informática y seguridad de la información en el mundo , como factor de enseñanza en Colombia*. 7.

DE LA SOTA SHICSHE, K. C., & CRISTOBAL MECHAN, Y. J. (2018). Implementación De Controles Y Cumplimiento De Requisitos De La Iso/Iec 27001:2013 Para La Seguridad De

Información En Una Pyme Consultora. *Universidad San Martin de Porres*.

ISO. (2020). Software ISO - Sistemas de Gestión de Riesgos y Seguridad. *ISOTools Excelence*, 1–15.

Magerit v.3. (2012). Magerit Libro II - Catálogo de Elementos. *Ministerio de Hacienda y Administraciones Publicas*, *2006*, 1–75.

Magerit versión 2. (2012). *Metodología de Análisis y GEstión de Riesgos de los Sistemas de Información de las AdminisTraciones Públicas*. *2006*.

NARVÁEZ BARREIROS, I. R. (2013). *Aplicación De La Norma Iso 27001 Para La Implementación De Un Sgsi En La Fiscalía General Del Estado*.

NQA. (2017). Iso 27001:2013 Guía De Implantación Para La Seguridad De La Información. *Nqa*, *1*, 1–30.

OSRI. (2018). Metodología para la gestión de la seguridad informática. *Oficina de Seguridad Para Las Redes Informaticas*, 1–68.

Purdue, P. (2017). *安全宪 -2017 年季刊 - 第一期 — 0 —*. 0–7.

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Las normas de reciente publicación de ISO incorporan dos elementos comunes. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *22*, 73–88. https://doi.org/10.17013/risti.22.73

Zhou, Yang, & Wang. (2020). No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析 Title. *File:///C:/Users/VERA/Downloads/ASKEP_AGREGAT_ANAK_and_REMAJA_PRINT.Docx*, *21*(1), 1–9.

ANEXOS

ANEXO 1: Entrevista al jefe del Área de Tecnología de la Cooperativa.

UNIVERSIDAD TÉCNICA DEL NORTE

UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC Resolución No 001-073 CEAACES – 2013 – 13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Trabajo de Titulación

Entrevista sobre la situación actual del jefe de Tecnología de la Cooperativa Imbacoop Ltda.

La presente entrevista tiene como finalidad recolectar información necesaria acerca de la situación actual del Área de Tecnología de la Cooperativa.

Para esta entrevista se tomó en consideración al jefe – director del Área de Tecnología de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., Ingeniero Jeison Ramos. La transcripción de la entrevista es la siguiente.

Fecha de la reunión:

Entrevista dirigida por:

Hora inicio:

Hora fin:

Tema:

Dirigida a:

INFORMACION GENERAL

1. Presentación del o de los entrevistadores
2. Definición del tema y objetivos de la evaluación tecnica
3. Solicitar permisos para grabar la entrevista
4. Aclarar términos de confidencialidad de la entrevista

1. **¿La alta dirección ha evaluado la importancia de implementar un Sistema de Gestión de Seguridad de la Información (SGSI)?**

2. **¿Existen políticas formales de seguridad de la información en la cooperativa?**

3. **¿Hay un responsable designado para supervisar la seguridad de la información?**

4. **¿Han considerado la clasificación de activos según su nivel de criticidad?**

5. **¿Cómo se gestiona la seguridad física en el departamento de tecnología de la cooperativa?**

6. **¿El personal recibe capacitación específica en seguridad de la información**

7. **¿La cooperativa tiene planes de contingencia para hacer frente a posibles fugas de información?**

8. **¿Con qué frecuencia se revisa y actualiza la política de seguridad de la información?**

9. **¿El personal de tecnología está capacitado para resolver rápidamente cualquier problema que pueda afectar la disponibilidad de los servicios tecnológicos ofrecidos por la cooperativa?**

10. **¿Cómo se administra el software y los equipos informáticos para el personal de la Cooperativa Imbacoop Ltda.?**

11. **¿Todos los programas utilizados en la cooperativa cuentan con licencia legal?**

12. **¿La cooperativa dispone de herramientas para realizar copias de seguridad de la información de cada empleado?**

13. **¿Cómo se controla el acceso a los servidores de archivos de la cooperativa?**

14. **¿Cuál es el procedimiento que sigue un usuario final al presentar una solicitud al departamento de TI?**

15. **¿Cómo se gestiona la red interna de la cooperativa?**

16. **¿La cooperativa cuenta con medidas para garantizar la disponibilidad ininterrumpida de los servicios tecnológicos para sus miembros?**

17. **¿Existe un plan de contingencia específico para asegurar la disponibilidad de los sistemas en caso de interrupciones inesperadas?**

18. **¿Se realizan pruebas periódicas de los sistemas para evaluar su capacidad de mantener la disponibilidad durante situaciones de alto tráfico o ataques cibernéticos?**

19. **¿La cooperativa tiene acuerdos de nivel de servicio (SLA) establecidos con proveedores de servicios para garantizar la disponibilidad de las aplicaciones y plataformas utilizadas?**

20. **¿Se implementan sistemas de redundancia y balanceo de carga para asegurar la disponibilidad incluso en situaciones de fallos técnicos?**

21. **¿Se tiene políticas o medidas para proteger la disponibilidad de la información que maneja dentro del departamento?**

22. **¿Cómo es la administración de software y equipos informáticos para el personal de la Cooperativa Imbacoop Ltda.?**

23. **¿Todo el software utilizado en la Cooperativa posee licencia?**

24. **¿La Cooperativa cuenta con herramientas para realizar respaldo de información de cada empleado?**

25. **¿Cómo se maneja el acceso a la información de los servidores de archivos de la Cooperativa?**

26. **¿Cuál es el procedimiento de un usuario final para realizar un requerimiento con el departamento de TI?**

27. **¿Cómo es administrada la red interna de la Cooperativa?**

28. **¿Cuentan con plan de auditorías de información?**
29. **¿Tienen establecido un Sistema de Gestión de Seguridad (SGSI) debidamente socializado y reglamentado?**
30. **¿Los controles efectuados fueron efectivos conforme los requisitos y necesidades establecidos de Seguridad de la Información?**
31. **¿Evalúan y aprueban la conveniencia, adecuación, eficacia y planes de mejora del SGSI?**
32. **¿Cuentan con un manual en Gestión de Procesos y Mejoramiento Continuo de la Información y Seguridad Informática?**

ANEXO 2: Cuestionario inicial de validación.

UNIVERSIDAD TÉCNICA DEL NORTE

UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC Resolución No 001-073 CEAACES – 2013 – 13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Cuestionario Inicial

El presente cuestionario tiene como finalidad recolectar información sobre distintos puntos relevantes al Desarrollo de un plan de Sistema de Gestión de Seguridad de la Información para el Área de Tecnología e Informático de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

Según las preguntas planteadas a continuación, seleccione la opción que usted considere apropiada en base a sus conocimientos, de acuerdo a la siguiente escala:

Excelente (5), Bueno (4), Regular (3), Muy Deficiente (2), No Tiene Conocimientos (1)

Conocimiento de Seguridad de la Información

Objetivo: Determinar el nivel de conocimiento que dispone el personal con respecto a las normas de seguridad de la información.

1. **En una estala del 5 al 1 cuál es su nivel de conocimiento respecto a la seguridad de la información**

   5) Excelente
   4) Bueno
   3) Regular
   2) Muy Deficiente
   1) No Tiene Conocimientos

2. **¿De acuerdo a sus conocimientos en que porcentaje de conocimiento tiene en lo relacionado a la normativa de la seguridad de la información?**

   5) Excelente
   4) Bueno
   3) Regular
   2) Muy Deficiente
   1) No Tiene Conocimientos

3. **¿Ha realizado en los últimos años ha realizado capacitaciones en temas de seguridad de la información?**

   5) Excelente
   4) Bueno
   3) Regular

2) Muy Deficiente
1) No Tiene Conocimientos

Conocimiento de la normatividad

Objetivo: Establecer el nivel de conocimiento sobre la Norma ISO/IEC 27001 y ley de protección de datos.

4. **¿Cuál es su conocimiento actual sobre la Norma ISO/IEC 27001?**

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

5. **¿Qué conocimientos tiene sobre la ley de protección de datos?**

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

6. **Se han realizado Auditorias en temas de seguridad de la información, indique el nivel en que se encuentra**

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

Técnicas para la protección de datos y seguridad de la información

Objetivo: Conocer el estado actual sobre la seguridad de la información, a través de los servicios que brinda el personal interno y externo para la empresa.

7. **El medio donde se guardan los archivos de respaldo cuenta con medidas de seguridad (servidores) ¿En qué estado de seguridad se encuentran?**

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

8. **Los servicios prestados por proveedores externos cuentan con controles de disponibilidad del sistema ¿qué estado de disponibilidad se encuentran?**

5) Excelente

4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

9. **Los servicios prestados por proveedores externos cuentan con un plan de contingencia en el caso de un fallo ¿Cómo define su accionar en tiempo de respuesta para resolver dichos problemas?**

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

10. **Ante el fallo en uno de los servidores de la empresa, dispone de un servidor alterno ¿En qué estado se encuentra el servidor?**

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

Acceso al área de servidores o Data Center

Objetivo: Conocer el nivel de seguridad física de acceso al área de servidores que disponga la empresa.

11. **El sistema de control (registro, bitácoras, cámaras, etc.) para el ingreso a esta área está definida como.**

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

12. **El área de servidores de acuerdo a las normativas de seguridad de la información para el diseño y ubicación ¿En qué estado se encuentra?**

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

13. **Ante una emergencia, donde se encuentre en riesgo la información y es necesario contar con un plan de contingencia ¿En qué nivel lo define?**

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

Protección de datos, seguridad de la información y disponibilidad de la información

Objetivo: Definir el nivel de control que disponga el departamento de TI para los servicios que utiliza el personal de la empresa.

14. ¿Cómo define el control de correos electrónicos?

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

15. ¿Cómo se define el control de antivirus en los equipos de cómputo de la empresa?

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

16. La seguridad que tienen los sistemas desarrollados por el personal dentro de la empresa ¿Qué disponibilidad brindan para el manejo de datos?

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

17. La seguridad que tienen los sistemas contratados por la empresa ¿Qué disponibilidad brindan para el manejo de datos?

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

18. Cómo definen el acceso y restricción a la red para los usuarios, sea a páginas de navegación como acceso a carpetas compartidas dentro de la red de la Cooperativa Imbacoop Ltda.

5) Excelente

4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

19. El software utilizado en la empresa con licenciamiento pagado ¿Qué seguridad posee?

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

20. El software utilizado en la empresa con licenciamiento libre ¿Qué seguridad posee?

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

21. ¿Cuál es el porcentaje de disponibilidad de los servicios informáticos en la cooperativa de ahorro y crédito bajo las normas ISO 27001?

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

22. ¿Cuáles son los sistemas clave de la cooperativa de ahorro y crédito y cuál es su disponibilidad promedio?

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

23. ¿Qué medidas de seguridad específicas se implementan en la cooperativa para garantizar la disponibilidad de los servicios informáticos?

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

24. ¿Cómo se realizan las pruebas de disponibilidad de los servicios informáticos en la cooperativa de ahorro y crédito bajo las normas ISO 27001?

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

25. ¿La cooperativa cuenta con un acuerdo de nivel de servicio (SLA) para medir la disponibilidad de sus servicios informáticos?

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

26. ¿Qué medidas específicas se implementan para garantizar la disponibilidad de los sistemas informáticos en la cooperativa?

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

27. ¿Cuál es el tiempo estimado de recuperación en caso de interrupciones en los servicios informáticos de la cooperativa?

5) Excelente
4) Bueno
3) Regular
2) Muy Deficiente
1) No Tiene Conocimientos

ANEXO 3: ISO 27001:2013

UNIVERSIDAD TÉCNICA DEL NORTE

UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC Resolución No 001-073 CEAACES – 2013 – 13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

NORMA ISO/IEC 27001: 2013

nqa.

ISO 27001:2013

GUÍA DE IMPLANTACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

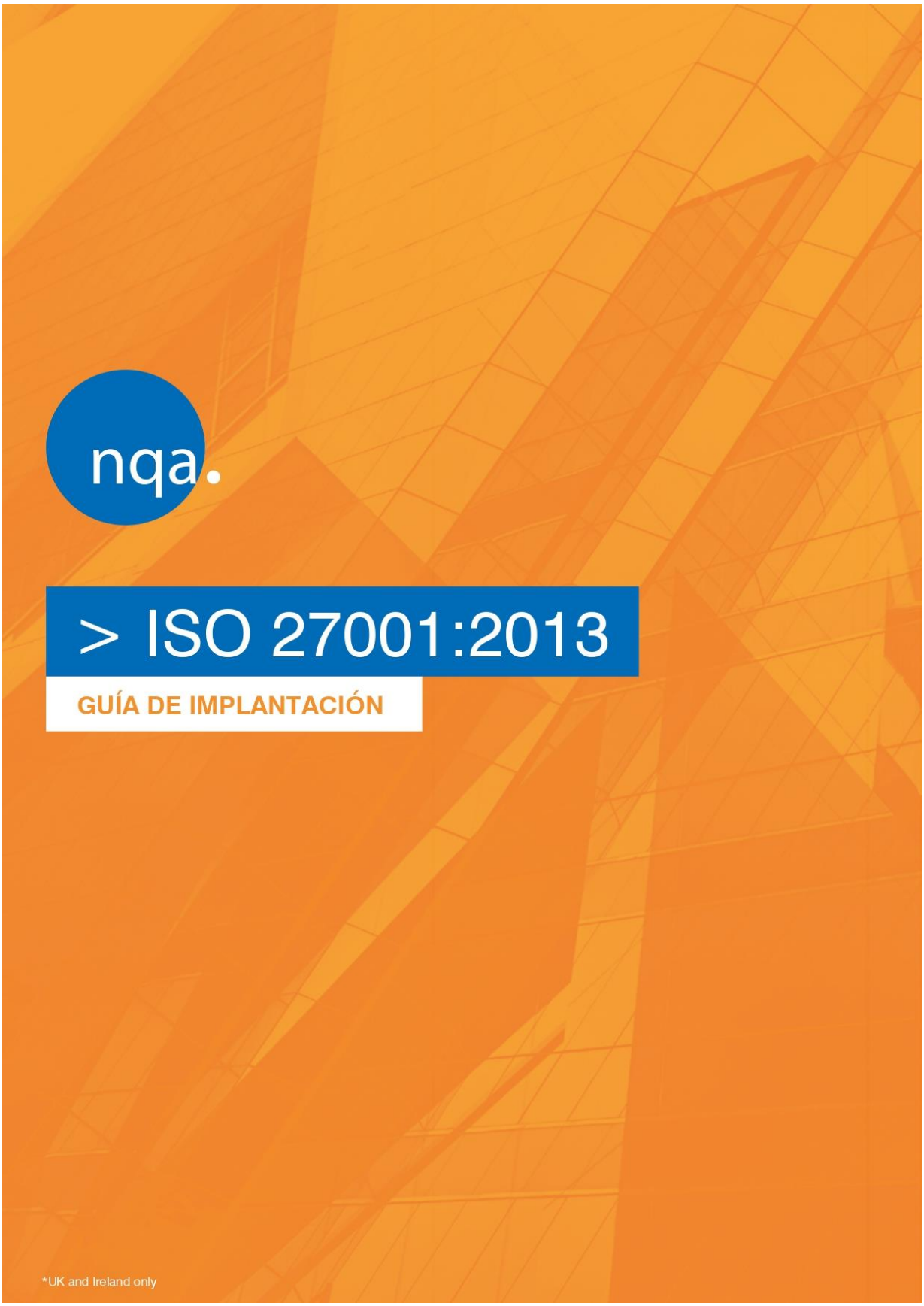
43,000 CERTIFICATES GLOBALLY

100%* ALL INCLUSIVE —FEES—

1000+ EMPLOYEES WORLDWIDE

AVERAGE CUSTOMER PARTNERSHIP 10 YEARS

OPERATING COUNTRIES OVER 90


nqa.
> ISO 27001:2013
GUÍA DE IMPLANTACIÓN
*UK and Ireland only

Contenido

INTRODUCCIÓN A LA NORMA

La mayoría de negocios dispone o tiene acceso a información sensible. El hecho de no proteger adecuadamente dicha información puede tener consecuencias operativas, financieras y legales graves, que pueden incluso llevar a la quiebra del negocio.

El reto que la mayoría de negocios afronta es el de proporcionar una adecuada protección. Particularmente, cómo asegurar que han identificado los riesgos a los que están expuestos y cómo gestionarlos de forma proporcionada, sostenible y efectiva.

La ISO 27001 es la norma internacional para los sistemas de gestión de la seguridad de la información (SGSI). Proporciona un marco robusto para proteger la información que se puede adaptar a organizaciones de todo tipo y tamaño. Las organizaciones más expuestas a los riesgos relacionados con la seguridad de la información eligen cada vez más implementar un SGSI que cumpla con la norma ISO 27001.

La familia 27000

Las normas de la serie 27000 nacen en 1995 con la BS 7799, redactada por el Departamento de Comercio e Industria (DTI) del Reino Unido. Las normas se denominan correctamente "ISO / IEC" porque son desarrolladas y mantenidas conjuntamente por dos organismos internacionales de normas: ISO (la Organización Internacional de Normalización) y la IEC (la Comisión Electrotécnica Internacional). Sin embargo, en el uso diario, la parte "IEC" a menudo se descarta.

Actualmente hay 45 normas publicados en la serie ISO 27000. La ISO 27001 es la única norma destinada a la certificación. Los otros estándares brindan orientación sobre la implementación de mejores prácticas. Algunos brindan orientación sobre cómo desarrollar el SGSI para industrias particulares; otros brindan orientación sobre cómo implementar procesos y controles clave de gestión de riesgos de seguridad de la información.

Revisiones y actualizaciones

Las normas ISO están sujetas a una revisión cada 5 años para evaluar la necesidad de actualizaciones.

La actualización más reciente de la norma ISO 27001 en 2013 produjo un cambio significativo con la adopción de la estructura del "Anexo SL". Si bien se realizaron algunos cambios menores en la redacción en 2017 para aclarar el requisito de mantener un inventario de activos de información, la ISO 27001: 2013 sigue siendo la norma actual para que las organizaciones puedan obtener la certificación.

Si está interesado en implantar un SGSI, estas 3 normas le resultarán de ayuda. Son las siguientes:

- **ISO 27000 Tecnologías de la información – Resumen y vocabulario.**
- **ISO 27002 Tecnologías de la información– Técnicas de seguridad** – Código para prácticas en materia de controles de seguridad de la información. Es la norma más referenciada y está ligada al diseño e implantación de los 114 controles especificados en el Anexo A de la ISO 27001.
- **ISO 27005 Tecnologías de la información– Técnicas de seguridad** – Gestión de la seguridad de la información.

BENEFICIOS DE LA **IMPLANTACIÓN**

La seguridad de la información está ganando notoriedad en las organizaciones y la adopción de la ISO 27001 es cada vez más común. La mayoría de las organizaciones reconoce que las brechas de seguridad ocurren, solo es cuestión de tiempo verse afectado por este hecho.

Implementar un SGSI y lograr la certificación ISO 27001 es una tarea importante para la mayoría de las organizaciones. Sin embargo, si se hace de manera efectiva, existen beneficios significativos para aquellas organizaciones que dependen de la protección de información valiosa o sensible. Estos beneficios generalmente se dividen en tres áreas:

COMERCIAL

Tener el respaldo independiente de un SGSI por parte de un tercero puede proporcionar a la organización una ventaja competitiva y permitirle "ponerse al día" con sus competidores. Los clientes que están expuestos a riesgos importantes de seguridad de la información están haciendo cada vez más que la certificación ISO 27001 sea un requisito en la presentación de ofertas. Si su cliente está certificado en ISO 27001, elegirá trabajar solo con proveedores cuyos controles de seguridad de la información sean fiables y tengan la capacidad de cumplir con los requisitos contractuales.

Para las organizaciones que desean trabajar con este tipo de cliente, contar con un SGSI acorde a la ISO 27001 es un requisito clave para mantener y aumentar los ingresos comerciales.

OPERACIONAL

El enfoque de la ISO 27001 fomenta el desarrollo de una cultura interna que esté alerta a los riesgos de seguridad de la información y tenga un enfoque coherente para enfrentarlos. Esta coherencia de enfoque conduce a controles que son más robustos en el manejo de amenazas. El costo de implementarlos y mantenerlos también se minimiza, y en caso de que fallen, las consecuencias se minimizarán y se mitigarán de manera más efectiva.

TRANQUILIDAD

Muchas organizaciones tienen información que es crítica para sus operaciones, vital para mantener su ventaja competitiva o que es parte inherente de su valor financiero.

Contar con un SGSI sólido y efectivo permite a a la gerencia administrar los riesgos y dorir tranquilamente, sabiendo que no están expuestos a un riesgo de multa, interrupción del negocio o un impacto significativo en su reputación.

La economía se basa en el conocimiento, y casi todas las organizaciones dependen de la seguridad de la información. La implementación de un SGSI proporciona dicha seguridad.

La ISO 27001 es un marco reconocido internacionalmente para una mejor práctica del SGSI y su cumplimiento se puede verificar de forma independiente para mejorar la imagen de una organización y dar confianza a sus clientes.

PRINCIPIOS Y TERMINOLOGÍA

El propósito central de un SGSI es proporcionar protección a la información sensible o de valor. La información sensible incluye información sobre los empleados, clientes y proveedores. La información de valor incluye propiedad intelectual, datos financieros, registros legales datos comerciales y datos operativos.

Los tipos de riesgos que la información sensible y de valor sufren pueden agruparse en 3 categorías:

Confidencialidad

Cuando una o más personas ganan acceso no autorizado a la información.

Integridad

Cuando el contenido de la información se cambia de manera que ya no es precisa o completa.

Disponibilidad

Cuando se pierde o daña el acceso a la información.

Estos tipos de riesgo de seguridad de la información se conocen comúnmente como "CID".

Los riesgos en la seguridad de la información generalmente surgen debido a la presencia de amenazas para los activos que procesan, almacenan, mantienen, protegen o controlan el acceso a la información, lo que da lugar a incidentes.

Los activos en este contexto suelen ser personas, equipos, sistemas o infraestructura.

La información es el conjunto de datos que una organización desea proteger, como registros de empleados, de clientes, datos financieros, de diseño, de prueba, etc.

Los incidentes son eventos no deseados que resultan en una pérdida de confidencialidad (violación de datos), integridad (corrupción de datos) o disponibilidad (fallo del sistema).

Las amenazas son las que causan ncidentes y pueden ser maliciosas (por ejemplo, un robo), accidentales (por ejemplo, un error tipográfico) o un acto de divino (por ejemplo, una inundación).

Las vulnerabilidades, como las ventanas abiertas de la oficina, los errores del código fuente o la ubicación junto a los ríos, aumentan la probabilidad de que la amenaza provoque un incidente no deseado y costoso.

En seguridad de la información, el riesgo se gestiona mediante el diseño, implementación y mantenimiento de controles como ventanas bloqueadas, pruebas de software o la ubicación de equipos vulnerables por encima de la planta baja.

Un SGSI que cumple con la ISO 27001 tiene un conjunto interrelacionado de procesos de mejores prácticas que facilitan y respaldan el diseño, implementación y mantenimiento de los controles. Los procesos que forman parte del SGSI suelen ser una combinación de procesos comerciales centrales existentes (por ejemplo, reclutamiento, inducción, capacitación, compras, diseño de productos, mantenimiento de equipos, prestación de servicios) y aquellos específicos para mantener y mejorar la seguridad de la información (por ejemplo, gestión de cambios, respaldo de información, control de acceso, gestión de incidentes, clasificación de la información).

CICLO PHVA

La ISO 27001 se basa en el ciclo PHVA, también conocido como ciclo de Deming. El ciclo PHVA puede aplicarse no solo al sistema de gestión. sino también a cada elemento individual para proporcionar un enfoque en la mejora continua.

A modo de resumen:

Planificar:

Establecer objetivos, recursos, requisitos del cliente y accionistas, política organizativa e identificar riesgos y oportunidades.

Hacer:

Implantar lo planificado.

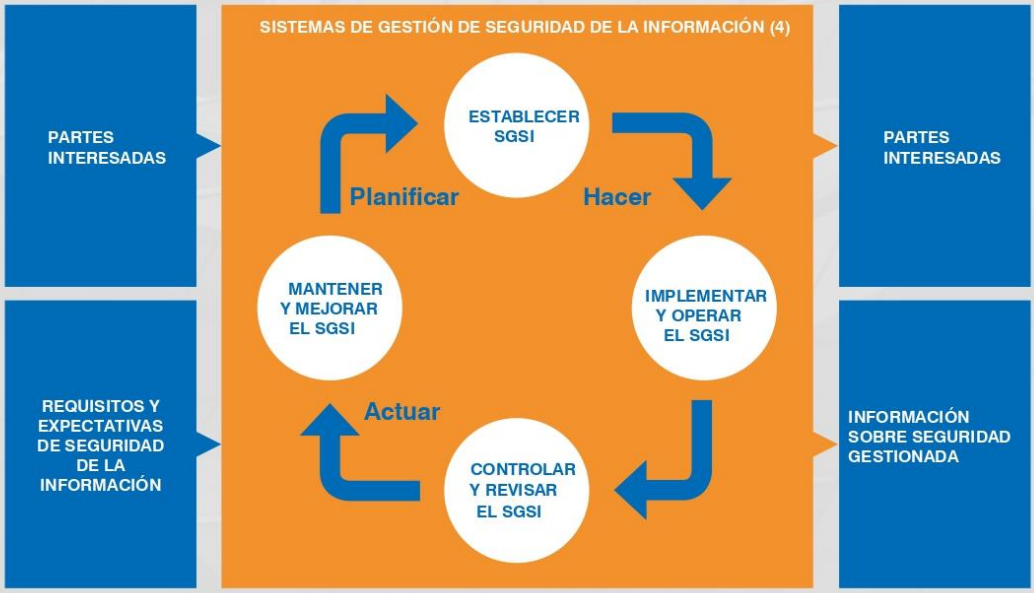
Verificar:

Controlar y medir los procesos para establecer el rendimiento de la política, objetivos, requisitos y actividades planificadas e informar de los resultados.

Actuar:

Tomar acciones para mejorar el rendimiento, en la medida de lo necesario.

Modelo PHVA para ISO 27001



PHVA es un ejemplo de un sistema cerrado en círculo. Esto asegura el aprendizaje de las fases de hacer y verificar y su uso en las fases de planificación y actuación. En teoría hablamos de un proceso cíclico.

MENTALIDAD/ AUDITORÍA BASADA EN RIESGOS

Las auditorías son un proceso de acercamiento sistemático y basado en evidencias para evaluar su SGSI. Se llevan a cabo de forma interna y externa para verificar la efectividad de un SGSI. Las auditorías son un ejemplo brillante de como la mentalidad basada en riesgos se adopta en el sistema de gestión.

Auditorías de 1ª parte: – Auditorías internas

Las auditorías internas son una gran oportunidad para comprender su organización. Proporcionan tiempo para enfocarse en un proceso o departamento en particular para evaluar verdaderamente su desempeño. Su propósito es garantizar el cumplimiento de las políticas, procedimientos y procesos según su organización, y confirmar el cumplimiento de los requisitos de la norma ISO 27001.

Planificación de la auditoría

Diseñar un calendario de auditoría puede parecer complicado. Dependiendo de la escala y complejidad de sus operaciones, puede programar auditorías internas mensuales o anuales. Hay más detalles sobre esto en la sección 9: evaluación del desempeño.

Mentalidad basada en riesgos

La mejor manera de considerar la frecuencia de las auditorías es observar el riesgo del proceso o área a auditar. Cualquier proceso de alto riesgo, ya sea porque tiene un alto potencial de fallo o porque las consecuencias serían graves en caso de fallo, deberá auditarse con mayor frecuencia que un proceso de riesgo bajo.

Cómo evaluar el riesgo depende totalmente de usted. La ISO 27001 no dicta ningún método particular de evaluación de riesgos o gestión de riesgos.

2ª parte: Auditorías externas

Las auditorías de 2ª parte suelen ser realizadas por clientes o proveedores externos. También pueden ser realizadas por reguladores o cualquier otra parte externa que tenga un interés formal en la organización.

Es posible que tenga poco control sobre el tiempo y la frecuencia de estas auditorías, sin embargo, el establecimiento de su propio SGSI le asegurará que está preparado.

3ª parte: Auditorías de certificación

Las auditorías de 3ª parte son llevadas a cabo por organismos externos de certificación acreditados como NQA. El organismo de certificación evaluará la conformidad con la norma ISO 27001:2013. Esto implica la visita de un auditor del organismo de certificación a la organización para evaluar el sistema relevante y sus procesos. Mantener la certificación también implica reevaluaciones periódicas.

La certificación demuestra a los clientes que está comprometido con la calidad.

LA CERTIFICACIÓN GARANTIZA:

- Una evaluación regular para controlar y mejorar procesos de forma continua.
- Credibilidad del sistema para conseguir objetivos deseados.
- Reducir riesgos e incertidumbre y aumentar las oportunidades de negocio.
- Consistencia de los resultados diseñados para cumplir con las expectativas de las partes interesadas.

MENTALIDAD/ AUDITORÍA BASADA EN PROCESOS

Un proceso es la transformación de una entrada en una salida, que tienen lugar como consecuencia una serie de pasos o actividades que tienen unos objetivos planificados. Frecuentemente, la salida de un proceso se convierte en la entrada de otro proceso posterior. Muy pocos procesos actúan de forma aislada.

Proceso: conjunto de actividades relacionadas o que interactúan que utilizan entradas para proporcionar resultados esperados.

ISO 27001:2013 Fundamentales y vocabulario

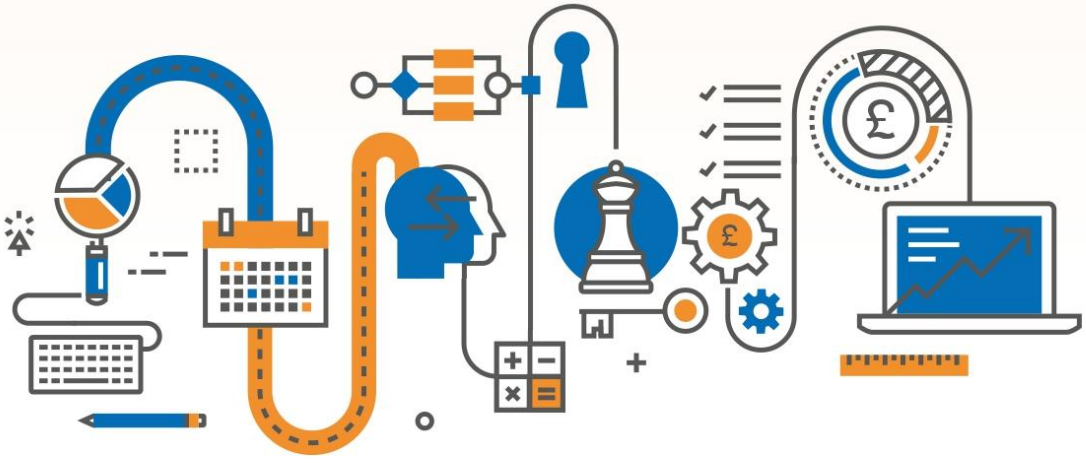
Incluso una auditoría tiene un enfoque de proceso. Comienza con la identificación del alcance y los criterios, establece un curso de acción claro para lograr el resultado y tiene un resultado definido (el informe de auditoría). El uso del enfoque basado en procesos garantiza que se asignen el tiempo y las habilidades necesarias para la auditoría. Esto hace de la auditoría una evaluación efectiva del rendimiento del SGSI.

"Los resultados consistentes y predecibles se logran de manera más efectiva y eficiente cuando las actividades se entienden y gestionan como procesos interrelacionados que funcionan como un sistema coherente".

ISO 27001:2013 Fundamentales y vocabulario.

Comprender cómo los se interrelacionan los procesos y cómo producen resultados puede ayudarlo a identificar oportunidades de mejora y, por lo tanto, a optimizar el rendimiento general. También es aplicable cuando los procesos, o partes de los procesos, se subcontratan. Comprender cómo afecta o podría afectar esto al resultado y comunicarlo claramente al socio comercial (que proporciona el producto o servicio subcontratado) garantiza la claridad y responsabilidad en el proceso.

El paso final del proceso es revisar el resultado de la auditoría y garantizar que la información obtenida se utilice correctamente. La revisión por la dirección supone la oportunidad de reflexionar sobre el desempeño del QMS y de tomar decisiones sobre cómo y dónde mejorar. Dicho proceso se trata con más detalle en la Sección 9: Evaluación del desempeño.



ANEXO SL

Uno de los mayores cambios introducidos en la revisión de la ISO 27001 del 2013 es la adopción de la estructura del Anexo SL. El Anexo SL (antes conocido como Guía 83 ISO) es utilizado por los autores de las normas ISO para proporcionar una estructura común para las normas de sistemas de gestión.

La ISO 27001 (seguridad de la información) adoptó esta estructura durante su revisión de 2013. La ISO 14001 (medioambiente) adoptó esta estructura durante su revisión de 2015. La recientemente publicada ISO 45001 (seguridad y salud laboral) también sigue esta misma estructura común.

Antes de la adopción del Anexo SL, existían diferencias entre las estructuras de las cláusulas, los requisitos y los términos y definiciones utilizados en las varias normas de sistema de gestión. Esto dificultaba la integración, la implementación y gestión de múltiples normas. Medioambiente, calidad, seguridad y salud laboral y seguridad de la información se encuentran entre las normas más comunes.

Estructura de alto nivel

El Anexo SL consiste en 10 cláusulas:

1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del desempeño
10. Mejora

Los términos comunes y las definiciones básicas no se pueden cambiar. Los requisitos no pueden eliminarse ni modificarse, sin embargo, se pueden agregar requisitos y recomendaciones específicos de la disciplina.

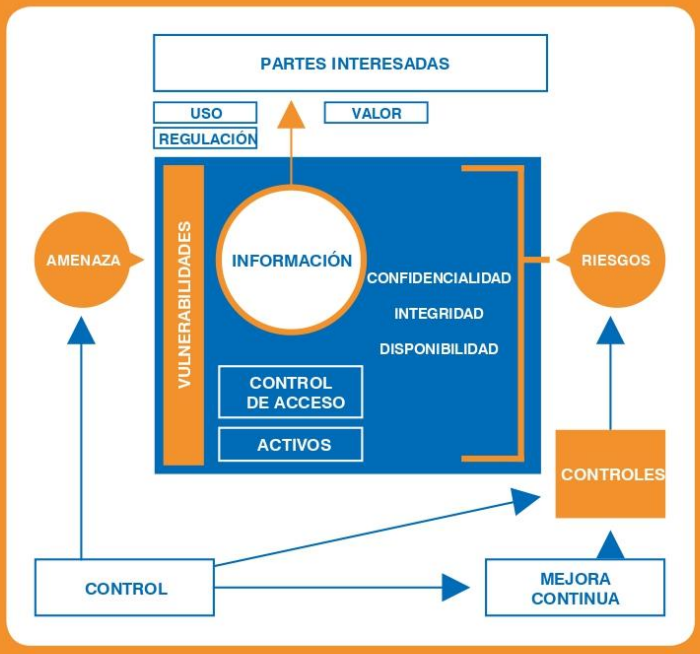
Todos los sistemas de gestión requieren una consideración del contexto de la organización; un conjunto de objetivos relevantes para la disciplina, y alineados con la dirección estratégica de la organización; una política documentada para apoyar el sistema de gestión y sus objetivos; auditorías internas y revisión por la dirección. Cuando existen múltiples sistemas de gestión, muchos de estos elementos se pueden combinar para abordar más de una norma.

LAS 10 CLÁUSULAS DE LA ISO 27001:2013

La ISO 27001:2013 se compone de 10 secciones conocidas como cláusulas.

Al igual que con la mayoría de normas de sistemas de gestión ISO, los requisitos de la ISO 27001 que deben cumplirse se especifican en las cláusulas 4.0 - 10.0. A diferencia de la mayoría de las demás normas ISO, una organización debe cumplir con todos los requisitos de las cláusulas 4.0-10.0 no se pueden declarar una o más cláusulas como no aplicables.

La ISO 27001, además de las cláusulas 4.0-10.0, tiene un conjunto adicional de requisitos detallados en una sección llamada Anexo A, a la que se hace referencia en la Cláusula 6.0. El Anexo A contiene 114 controles de seguridad de la información a modo de buenas prácticas. Cada uno de estos 114 controles debe ser considerado. Para cumplir con la ISO 27001, la organización debe implementar estos controles, o se debe dar una justificación aceptable para no implementar un control en particular. Esta guía proporcionan una explicación del propósito de cada cláusula, resaltando el tipo de evidencia que un auditor esperaría ver para confirmar el cumplimiento.



CLÁUSULA 1: ALCANCE

La sección de alcance de la ISO 27001 establece:

- El propósito de la norma.
- Los tipos de organizaciones para las que se ha diseñado.
- Las cláusulas y los requisitos que una organización debe cumplir para que la organización sea considerada como conforme con la norma.

La ISO 27001 está diseñada para ser aplicable a cualquier tipo de organización. Independientemente del tamaño, la complejidad, el sector industrial, el propósito o la madurez, su organización puede implementar y mantener un SGSI que cumpla con la ISO 27001.

CLÁUSULA 2: REFERENCIAS NORMATIVAS

En las normas ISO, la sección de referencias normativas enumeran otras normas que contengan información relevante para determinar el cumplimiento de una organización con la norma. En la ISO 27001 solo nos encontramos con un documento en cuestión, la ISO 27000 Tecnologías de la información - Resumen y vocabulario.

Algunos de los términos utilizados o requisitos detallados en la ISO 27001 se explican en la ISO 27000. La ISO 27000 es muy útil para la comprensión de los requisitos y su cumplimiento.

CONSEJO: Los auditores externos esperarán que hay considerado la información de la ISO 27000 en el desarrollo e implantación de su SGSI.

CLÁUSULA 3: TÉRMINOS Y DEFINICIONES

No hay términos y definiciones en la ISO 27001. Sin embargo, se hacen referencias a la versión más reciente de la ISO 27000 Sistemas de gestión de seguridad de la información - Resumen y vocabulario. La versión más reciente de dicho documento contiene 81 términos y definiciones utilizados en la ISO 27001.

Además de los términos anteriormente explicados en los "principios y terminología", otros términos muy utilizados son:

'Control de accesos'

– Procesos que garantizan que solo las personas que necesitan acceso a ciertosd activos disponen de dicho acceso yla necesidad se determina acorde a los requisitos del negocio y la seguridad.

'Efectividad'

– Medida en que las actividades planeadas (procesos, procedimientos...) se ejecutan de forma planeada o específica y se consiguen los resultados o salidas esperados.

'Riesgo'

– Combinación de probabilidad de ocurrencia de un evento de seguridad de la información y su resultante consecuencia.

'Evaluación de riesgos'

–Proceso de identificación de riesgos, analizando el nivel de riesgo de cada riesgo en particular y evaluando acciones adicionales necesarias para reducir los riesgos a niveles aceptables.

'Tratamiento de riesgos

– Procesos o acciones que reducen los riesgos indetificados a un nivel tolerable o aceptable.

'Gerencia'

– Grupo de individuos que toman las decisiones dentro de una empresa. Pueden ser responsables de establecer la dirección estratégica y determinar y conseguir los objetivos de los accionistas.

Al redactar la documentación de su SGSI, no tiene que usar estos términos exactos. Sin embargo, definir los términos utilizados puede esclarecer su significado e intención. Puede ser útil proporcionar un glosario junto a la documentación de su sistema.

CLÁUSULA 4: CONTEXTO DE LA ORGANIZACIÓN

El objetivo de su SGSI es proteger los activos de información de su empresa, de manera que la empresa pueda alcanzar sus objetivos.

La forma y las áreas específicas de prioridad dependerán del contexto en el que opere su organización. Se incluyen dos niveles:

- **Interno**: Aspectos sobre los que la organización tiene control.
- **Externo**: Aspectos sobre los que la organización no tiene control directo.

Un análisis cuidadoso del entorno en el que opera su organización es fundamental para identificar los riesgos inherentes a la seguridad de sus activos de información. El análisis es la base que le permitirá evaluar qué procesos necesita considerar agregar o fortalecer para construir un SGSI efectivo.

Contexto interno

A continuación se muestran ejemplos de las áreas que pueden considerarse al evaluar los problemas internos que pueden influir en los riesgos del SGSI:

- **Madurez:** ¿Es usted una nueva empresa con un lienzo en blanco para trabajar, o una institución con procesos y controles de seguridad bien establecidos?
- **Cultura organizativa:** ¿Es su organización flexible o rígida respecto a cómo, cuándo y dónde trabaja la gente? ¿Podría su cultura resistir la implementación de los controles de Seguridad de la Información?
- **Gestión:** ¿Existen canales y procesos de comunicación claros desde los tomadores de decisiones hasta el resto de la organización?
- **Recursos:** ¿Está trabajando con un equipo de seguridad de la información o solo uan persona se encarga de todo?
- **Madurez de los recursos:** ¿Están los recursos disponibles (empleados/contratistas) bien informados, totalmente capacitados, son de confianza y son consistentes, o el personal no tiene experiencia y cambia constantemente?
- **Formato de los activos de información:** ¿Sus activos de información se almacenan principalmente en formato impreso o se almacenan electrónicamente en un servidor en o en sistemas remotos basados en la nube?
- **Sensibilidad/valor de los activos de información:** ¿Su organización tiene que administrar activos de información altamente valiosos o especialmente sensibles?
- **Consistencia:** ¿Cuenta con procesos uniformes en toda la organización o una multitud de prácticas operativas diferentes con poca coherencia?
- **Sistemas:** ¿Su organización tiene muchos sistemas heredados que se ejecutan en versiones de software que ya no son compatibles con el fabricante, o mantiene la tecnología más actualizada?
- **Complejidad del sistema:** ¿opera un sistema principal que hace todo el trabajo o múltiples sistemas departamentales con transferencia de información?
- **Espacio físico:** ¿Tiene una oficina segura y exclusiva o opera en un espacio compartido con otras organizaciones?

Contexto externo

Los siguientes son ejemplos de las áreas que se pueden considerar al evaluar los problemas externos que pueden influir en los riesgos del SGSI:

- **Competencia:** ¿opera en un mercado innovador y cambiante, que requiere muchas actualizaciones del sistema para mantenerse competitivo, o en un mercado maduro y estable con poca innovación?
- **Dueño:** ¿Necesita aprobación para actualizar la seguridad física?
- **Organismos reguladores:** ¿Existe un requisito en su sector para realizar cambios estatutarios, o hay poca supervisión en su sector de mercado?
- **Económico/político:** ¿Afectan las fluctuaciones monetarias y políticas a su organización?
- **Consideraciones ambientales:** ¿Está su sede en una lzona inundable con los servidores ubicados en un sótano? ¿Existen factores que hacen que su sede sea objetivo de ataque terrorista o junto a un posible objetivo?
- **Frecuencia de ataques a la información:** ¿Su organización opera en un sector que regularmente atrae el interés de los hackers?
- **Accionistas:** ¿Están preocupados por la vulnerabilidad frente a las violaciones de datos? ¿Cuán preocupados están por el costo de los esfuerzos de la organización para mejorar la seguridad de su información?

Partes interesadas

Una parte interesada es cualquier persona que sea, pueda ser o se considere afectada por una acción u omisión de su organización. Sus partes interesadas serán claras a través del proceso de llevar a cabo un análisis exhaustivo de los problemas internos y externos. Probablemente incluirán accionistas, propietarios, reguladores, clientes, empleados y competidores y pueden extenderse al público en general y al medio ambiente, dependiendo de la naturaleza de su negocio. No tiene que tratar de comprender o satisfacer todos sus caprichos, pero sí tiene que determinar cuáles de sus necesidades y expectativas son relevantes para su SGSI.

Alcance del sistema de gestión

Para cumplir con al ISO 27001, debe documentar el alcance de su SGSI. Los alcances suelen describir:

- Los límites del sitio físico o sitios incluidos (o no incluidos);
- Los límites de las redes físicas y lógicas incluidas (o no incluidas);
- Los grupos de empleados internos y externos incluidos (o no incluidos);
- tLos procesos, actividades o servicios internos y externos incluidos (o no incluidos); y
- Interfaces clave en los límites del alcance.

Si desea priorizar los recursos mediante la creación de un SGSI que no cubra toda su organización, seleccione un alcance que se limite a la gestión de los intereses clave de las partes interesadas. Esto se puede hacer incluyendo solo sitios, activos, procesos y unidades de negocio o departamentos específicos. Algunos ejemplos de alcance son:

- **Todas las operaciones realizadas por el departamento de TI.**
- **Soporte y gestión de correo electrónico.**
- **Todos los equipos, sistemas, datos e infraestructura en el centro de datos de la organización.**

CONSEJO: Documente o mantenga un archivo de toda la información recopilada en su análisis del contexto de su organización y las partes interesadas, tales como:

- Conversaciones con un representante de la gerencia de la empresa.
- Actas de reuniones o planes de negocios.
- Un documento específico que identifica problemas internos/ externos y partes interesadas y sus necesidades y expectativas. Por ejemplo, un análisis FODA, estudio PESTLE o evaluación de riesgo empresarial de alto nivel.

CLÁUSULA 5: LIDERAZGO

La importancia del liderazgo

El liderazgo significa una participación activa en la dirección del SGSI, promover su implementación y garantizar la disponibilidad de recursos apropiados. Esto incluye:

- Asegurar que los objetivos del SGSI sean claros y estén alineados con la estrategia general.
- Claridad sobre las responsabilidades.
- Que el pensamiento basado en el riesgo está en el corazón de toda toma de decisiones; y
- Hay una comunicación clara de esta información a todas las personas dentro del alcance del SGSI.

La ISO 27001 otorga gran importancia a la participación activa de la gerencia en el SGSI, basándose en el supuesto de que es crucial para garantizar la implementación y el mantenimiento efectivo de un SGSI efectivo.

Política de seguridad

Una responsabilidad vital del liderazgo es establecer y documentar una Política de Seguridad de la Información que esté alineada con los objetivos clave de la organización. Debe incluir objetivos o un marco para establecerlos. Para demostrar que está alineado con el contexto de su organización y los requisitos de las partes interesadas clave, se recomienda que haga referencia o contenga un resumen de los principales problemas y requisitos que debe administrar. También debe incluir un compromiso para:

- Cumplir requisitos aplicables relacionados con la seguridad de la información, tales como requisitos legales, expectativas del cliente y compromisos contractuales; y
- La mejora continua de su SGSI.

La política de seguridad de la información puede referirse o incluir subpolíticas que cubran los controles clave del SGSI de la organización. Los ejemplos incluyen: la selección de proveedores críticos para la seguridad de la información, el reclutamiento y la capacitación de los empleados, el escritorio y monitor limpios, los controles criptográficos, los controles de acceso, etc. Para demostrar la importancia de la Política de Seguridad de la Información, es aconsejable que esté autorizado por la gerencia.

CONSEJO: Para aegurar que la política de la seguridad de la información está bien comunicada y disponible para las partes interesadas, le recomendamos:

- Incluirlo en paquetes de inducción y presentaciones para nuevos empleados y contratistas;
- Publicar la declaración clave en tableros de anuncios internos, intranets y el sitio web de su organización;
- Hacer que su cumplimiento y /o soporte sea un requisito contractual para los empleados, contratistas y proveedores críticos de seguridad de la información.

Roles y responsabilidades

Para que las actividades de seguridad de la información formen parte de las actividades cotidianas para el personal de la organización, las responsabilidades que tienen deben definirse y comunicarse claramente. Aunque no hay ningún requisito en la norma respecto al nombramiento de un representante de Seguridad de la Información, puede ser útil para algunas organizaciones designar a uno para dirigir un equipo de seguridad de la información que coordine la capacitación, el control de los controles y la presentación de informes sobre el desempeño del SGSI a la gerencia. Este individuo puede ser el responsable de la protección de datos o servicios de TI. Sin embargo, para llevar a cabo su función de manera efectiva, lo ideal sería que fuese miembro de la gerencia y con conocimiento de la gestión de seguridad de la información.

Evidenciar el liderazgo al auditor

La gerencia será el grupo de personas que establezca la dirección estratégica y apruebe la asignación de recursos para la organización dentro del alcance del SGSI. Dependiendo de cómo esté estructurada su organización, estas personas pueden o no ser el equipo de administración. Generalmente, el auditor evaluará el liderazgo entrevistando a uno o más miembros de la gerencia y evaluando su nivel de participación en:

- Evaluación de riesgos y oportunidades;
- Establecimiento y comunicación de políticas;
- Establecimiento y comunicación de objetivos;
- Revisión y comunicación del desempeño del sistema;
- Asignación de recursos y responsabilidades apropiadas.

CONSEJO: antes de su auditoría externa, identifique que individuo de la gerencia se reunirá con el auditor externo y prepárelos para la entrevista con un repaso de las posibles preguntas que se les harán.

CLÁUSULA 6: PLANIFICACIÓN

La ISO 27001 es una herramienta de gestión de riesgos que guía a una organización en la identificación de riesgos de seguridad de la información. Como tal, el propósito subyacente de un SGSI es:

- **Identificar los riesgos estratégicamente importantes, obvios y ocultos pero peligrosos;**
- **Asegurarse de que las actividades y los procesos operativos diarios de una organización estén diseñados, dirigidos y tengan recursos para gestionar inherentemente esos riesgos; y**
- **Responder y se adaptarse automáticamente a los cambios para hacer frente a los nuevos riesgos y reducir continuamente la exposición a los mismos.**

Tener un plan de acción detallado que esté alineado, actualizado y respaldado por revisiones y controles regulares es crucial y proporciona evidencia para el auditor de una planificación del sistema claramente definida.

Evaluación de riesgos

La evaluación de riesgos es el núcleo de cualquier SGSI eficaz. Incluso la organización con más recursos no puede descartar la posibilidad de sufrir un incidente de seguridad de la información. La evaluación de riesgos es esencial para:

- Aumentar la probabilidad de identificar riesgos potenciales mediante la participación de personal que utiliza écnicas de evaluación sistemática;
- Asignar recursos para abordar las áreas de mayor prioridad;
- Tomar decisiones estratégicas sobre cómo gestionar los riesgos de seguridad de la información significativos y lograr así sus objetivos.

La mayoría de los marcos de evaluación de riesgos consisten en una tabla que contiene los resultados de los elementos 1-4 con una tabla complementaria que cubre el punto 5.
El auditor externo esperará ver un registro de su evaluación de riesgos, un responsble asignado para cada riesgo identificado y los criterios que ha utilizado.

CONSEJO: el Anexo A (8.1.1) contiene requisitos sobre listas de activos de información, activos asociados con la información (edificios, archivadores, ordenadores...) e instalaciones de procesamiento de información. Si completa su evaluación de riesgos evaluando sistemáticamente los riesgos planteados para cada elemento de esta lista, entonces habrá cumplido dos requisitos dentro del mismo ejercicio. Además, si asigna un responsable, también habrá cumplido con otro requisito del Anexo A (8.1.2).

ISO 27005: la gestión de riesgos de seguridad de la información ofrece orientación en el desarrollo de una técnica de evaluación de riesgos. Cualquiera que sea la técnica que desarrolle, debe incluir los siguientes elementos clave:

1. Proporcionar aviso para la identificación sistemática de riesgos (revisión de activos, grupos de activos, procesos, tipos de información), verificando la presencia de amenazas y vulnerabilidades comunes y registrando los controles que actualmente tiene implementados para administrarlos.
2. Proporcionar un marco para evaluar la probabilidad de que el riesgo ocurra de manera persistente (una vez al mes, una vez al año).
3. Proporcione un marco para evaluar las consecuencias de cada riesgo que ocurra de manera consistente (por ejemplo, pérdidas de capital monetario).
4. Proporcione un marco para calificar o categorizar cada riesgo identificado (por ejemplo, alto/medio/bajo), teniendo en cuenta su evaluación de probabilidad y las consecuencias.
5. Establezca criterios documentados que especifiquen, para cada categoría de riesgo, qué tipo de acción debe tomarse y el nivel o prioridad que se le asigna.

Tratamiento de riesgos

Para cada riesgo identificado en su evaluación de riesgos, deberá aplicar criterios para determinar si:

- **Acepta el riesgo.**
- **Trata el riesgo (tratamiento de riesgos).**

Las opciones para el tratamiento de riesgos incluyen una de las siguientes opciones;

- **Evasión**: dejar de realizar la actividad o procesar la información que está expuesta al riesgo.
- **Eliminación**: Eliminar la fuente del riesgo.
- **Cambio de probabilidad**: implementar un control que reduzca los incidentes de seguridad de la información.
- **Cambio en las consecuencias**: Implemente un control que disminuya el impacto si ocurre un incidente.
- **Transferencia del riesgo**: Externalizar la actividad a un tercero que tenga mayor capacidad para gestionar el riesgo.
- **Aceptar el riesgo**: Si no hay un tratamiento de riesgo práctico disponible para la organización, o si se considera que el costo del tratamiento de riesgo es mayor que el costo del impacto, puede tomar la decisión de aceptar el riesgo. Esto debe ser aprobado por la gerencia.

El auditor externo esperará ver un plan de tratamiento de riesgos (por ejemplo, una lista de acciones) que detalle las acciones de tratamiento de riesgos que ha implementado o planea implementar. El plan debe ser lo suficientemente detallado para permitir que se verifique el estado de implementación de cada acción. También será necesario que exista evidencia de que este plan ha sido aprobado por los responsables de los mismos y por la gerencia.

Anexo A y declaración de aplicabilidad

Todas las opciones de tratamiento de riesgos (a excepción de la aceptación) implican la implementación de controles. El anexo A de la ISO 27001 contiene una lista de 114 controles de seguridad de la información de buenas prácticas. Deberá considerar cada uno de estos controles al formular su plan de tratamiento de riesgos. La descripción de la mayoría de los controles es bastante vaga, por lo que se recomienda que revise la ISO 27002, que contiene más información sobre su implementación.

Como evidencia de que usted ha completado esta evaluación, un auditor externo esperará que usted presente un documento llamado declaración de aplicabilidad. Para cada uno de los 114 controles debe registrar:

- Si es aplicable a sus actividades, procesos y riesgos de seguridad de la información.
- Si lo has implementado o no.
- Si lo ha considerado no aplicable, su justificación para hacerlo.

Para la mayoría de las organizaciones, los 114 controles serán aplicables, y es probable que ya hayan implementado algunos de ellos.

Consejo: La declaración de aplicabilidad no necesita un documento demasiado complejo. Basta con una simple tabla con datos sobre el control, aplicabilidad, implementación y justificación. También es aconsejable registrar cierta información sobre cómo se ha aplicado el control (por ejemplo, hacer referencia a un procedimiento o política) para ayudarlo a responder más fácilmente cualquier pregunta del auditor externo.

Objetivos de seguridad de la información y planificación

En los niveles relevantes, necesitará tener objetivos documentados y relacionados con la seguridad de la información. Estos pueden estar en un nivel superior y aplicarse a toda la organización o solo a nivel departamental.

Cada objetivo establecido debe ser:

- Medible.
- Estar alineado con la política del SGSI.
- Considerar los requisitos a nivel de seguridad de la información.
- Considerar los resultados de la evaluación de riesgos y del proceso de tratamiento de riesgos.

Los objetivos relevantes para la seguridad de la información incluyen:

- No exceder la frecuencia definida para ciertos tipos de incidentes de seguridad de la información.
- Conseguir un nivel medible de cumplimiento con los controles de seguridad de la información.
- Proporcionar una disponibilidad definida para los servicios de la información.
- No exceder un número medible de errores de datos.
- Mejoras en los recursos disponibles a través de selección, formación o adquisición.
- Implementación de nuevos controles.
- Conseguir cumplimiento las normas relativas a la seguridad de la información.

Cada objetivo debe comunicarse a las personas relevantes. Los objetivos deben actualizarse cuando sea necesario para estra actualizados y evaluar el desempeño en función de ellos.

Para cada uno de los objetivos, necesita indicar cómo va a lograrlos. Esto incluye determinar:

- Qué necesidades deben conseguirse.
- Qué recursos se asignan.
- Quién tiene la responsabilidad sobre el objetivo.

- Si hay una fecha objetivo para completar el objetivo o es continuo.
- El método para evaluar el desempeño frente al objetivo (es decir, cuál es su medida).

CONSEJO: las formas efectivas de comunicar los objetivos de seguridad de la información incluyen cubrirlos en la formación, establecerlos como objetivos de los empleados o incluirlos en las evaluaciones de los empleados, establecerlos en acuerdos de nivel de servicio con proveedores o evaluar el desempeño con respecto a ellos en las revisiones de desempeño del proveedor.

CLÁUSULA 7: SOPORTE

La cláusula 7 se refiere a los recursos. Esto se aplica a las personas, infraestructura, medioambiente, recursos físicos, materiales, herramientas, etc. También existe un enfoque renovado en el conocimiento como un recurso importante dentro de su organización. Cuando planifique sus objetivos de calidad, una consideración importante será la capacidad actual y la capacidad de sus recursos, así como aquellos recursos de proveedores/socios externos.

Para implementar y mantener un SGSI efectivo, necesita contar con recursos de apoyo. Estos recursos deberán ser:

- **Capaces**: Si son equipos o infraestructura.
- **Competentes**: Si se trata de personal.
- Disponibles en la revisión por la dirección.

Competencia

La implementación de controles efectivos de seguridad de la información depende del conocimiento y las habilidades de sus empleados, proveedores y contratistas. Para asegurar una base adecuada de conocimientos y habilidades, debe:

- Definir qué conocimientos y habilidades se requieren;
- Determinar quién necesita del conocimiento y habilidades;
- Establezca cómo evaluar que las personas adecuadas tengan los conocimientos y habilidades adecuados.

Su auditor esperará que tenga documentos que detallen sus requisitos de conocimientos y habilidades. Cuando crea que se cumplen los requisitos, será necesario respaldarlo con registros como certificados de capacitación, registros de asistencia al curso o evaluaciones de competencia interna.

CONSEJO: la mayoría de las organizaciones que ya utilizan herramientas como matrices de capacitación/habilidades, evaluaciones o evaluaciones de proveedores pueden satisfacer el requisito de registros de competencia al expandir las áreas cubiertas para incluir la seguridad de la información.

Concienciación

Además de garantizar la competencia del personal clave en relación con la seguridad de la información, los empleados, proveedores y contratistas deberán conocer los elementos del SGSI. Esto es fundamental para establecer una cultura de soporte dentro de la organización.

Todos los empleados, proveedores y contratistas deben tener en cuenta lo siguiente:

- La existencia de un SGSI y su razón de ser.
- Que tiene una política de seguridad de la información y cuáles son sus elementos relevantes.
- Cómo pueden contribuir a que su organización proteja la información y lo que deben hacer para ayudar a la organización a lograr sus objetivos de seguridad de la información.
- Qué políticas, procedimientos y controles son relevantes para ellos y cuáles son las consecuencias de no cumplirlos.

CONSEJO: la comunicación de esta información normalmente se puede realizar a través de los procesos y documentos existentes, como formación, contratos de trabajo, charlas, acuerdos con proveedores, informes o actualizaciones de los empleados.

Comunicación

Para permitir que los procesos en su SGSI funcionen de manera efectiva, deberá asegurarse de tener actividades de comunicación bien planificadas y gestionadas. La ISO 27001 los detalla de manera concisa al exigirle que determine:

- Lo que necesita ser comunicado;
- Cuándo necesita ser comunicado;
- A quién necesita ser comunicado;
- Quién es responsable de la comunicación;
- Cuáles son los procesos de comunicación.

CONSEJO: si sus requisitos de comunicación están bien definidos en sus procesos, políticas y procedimientos, entonces no necesita hacer nada más para satisfacer este requisito. Si no lo están, debería considerar documentar sus actividades clave de comunicación en forma de una tabla o procedimiento que incluya los títulos detallados anteriormente. Recuerde que el contenido de estos documentos también debe ser comunicado.

Información documentada

Para ser de utilidad, la información documentada para implementar y mantener su SGSI debe:

- Ser precisa.
- Ser comprensible para las personas que lo usan regularmente u ocasionalmente.
- Apoyarlo para cumplir los requisitos legales, administrar los riesgos y alcanzar sus objetivos.

Para que su información documentada siempre satisfaga estos requisitos, necesitará contar con procesos para garantizar que:

- La información documentada se revisa cuando lo requieren las personas apropiadas antes de que se divulgue a la circulación general.
- El acceso a la información documentada se controla para que no pueda ser cambiado, corrompido, eliminado o accedido por individuos sin permiso.
- La información se elimina de forma segura o se devuelve a su propietario cuando existe el requisito de hacerlo.
- Puede realizar un seguimiento de los cambios en la información para garantizar que el proceso esté bajo control.

La fuente de su información documentada puede ser interna o externa, por lo que sus procesos de control deben administrar la información documentada de ambas fuentes.

CONSEJO: las organizaciones que tienen un buen control de documentos se caracterizan por tener:

- Una sola persona o un pequeño equipo responsable de garantizar que los documentos nuevos / modificados se revisen antes de su emisión, se almacenen en la ubicación correcta, se retiren de la circulación cuando se reemplacen y se mantenga un registro de cambios.
- Un sistema de gestión de documentos electrónicos que contiene controles y flujos de trabajo automáticos.
- Robusto respaldo de datos electrónicos y procesos de archivado/almacenamiento de archivos impresos.
- Fuerte conocimiento de los empleados sobre el control de documentos, el mantenimiento de registros y los requisitos de acceso/retención de información.

CLÁUSULA 8: OPERACIÓN

Tras la planificación y evaluación de riesgos, estamos listos para pasar a la etapa de "hacer". La cláusula 8 trata de tener un control adecuado sobre la creación y entrega del producto o servicio.

Gestionar sus riesgos de seguridad de la información y alcanzar sus objetivos requiere la formalización de sus actividades en un conjunto de procesos claros y coherentes.

Es probable que muchos de estos procesos ya existan y simplemente necesiten modificaciones para incluir elementos relevantes para la seguridad de la información. Otros procesos pueden ser ad-hoc (por ejemplo, aprobaciones de proveedores), o no existir aún (por ejemplo, auditoría interna).

Para implementar procesos efectivos, las siguientes prácticas son cruciales:

1. Los procesos se crean adaptando o formalizando las actividades de negocio en costumbres dentro de la organización.
2. Identificación sistemática de los riesgos de seguridad de la información relevantes para cada proceso.
3. Definición clara y comunicación de las actividades requeridas para gestionar los riesgos de seguridad de la información asociados cuando ocurre un evento (por ejemplo, un nuevo empleado que se une a la empresa).
4. Asignación clara de las responsabilidades para llevar a cabo actividades relacionadas.
5. Asignación de recursos para garantizar que las actividades puedan llevarse a cabo cuando sea necesario
6. Evaluación rutinaria de la consistencia con la que se sigue cada proceso y su efectividad en la gestión de riesgos de seguridad de la información.

CONSEJO: designe a un individuo como responsable de garantizar que se realicen los pasos 2 a 6 para cada proceso. A menudo se hace referencia a este individuo como el propietario o responsable del proceso.

Evaluación de riesgos de la seguridad de la información

Los métodos de evaluación de riesgos descritos en la cláusula 6 deben aplicarse a todos los procesos, activos, información y actividades dentro del alcance del SGSI.

Dado que los riesgos no son estáticos, los resultados de estas evaluaciones deben revisarse frecuentemente, al menos una vez al año, o con mayor frecuencia si la evaluación identifica la presencia de uno o más riesgos significativos. Los riesgos también deben revisarse siempre que:

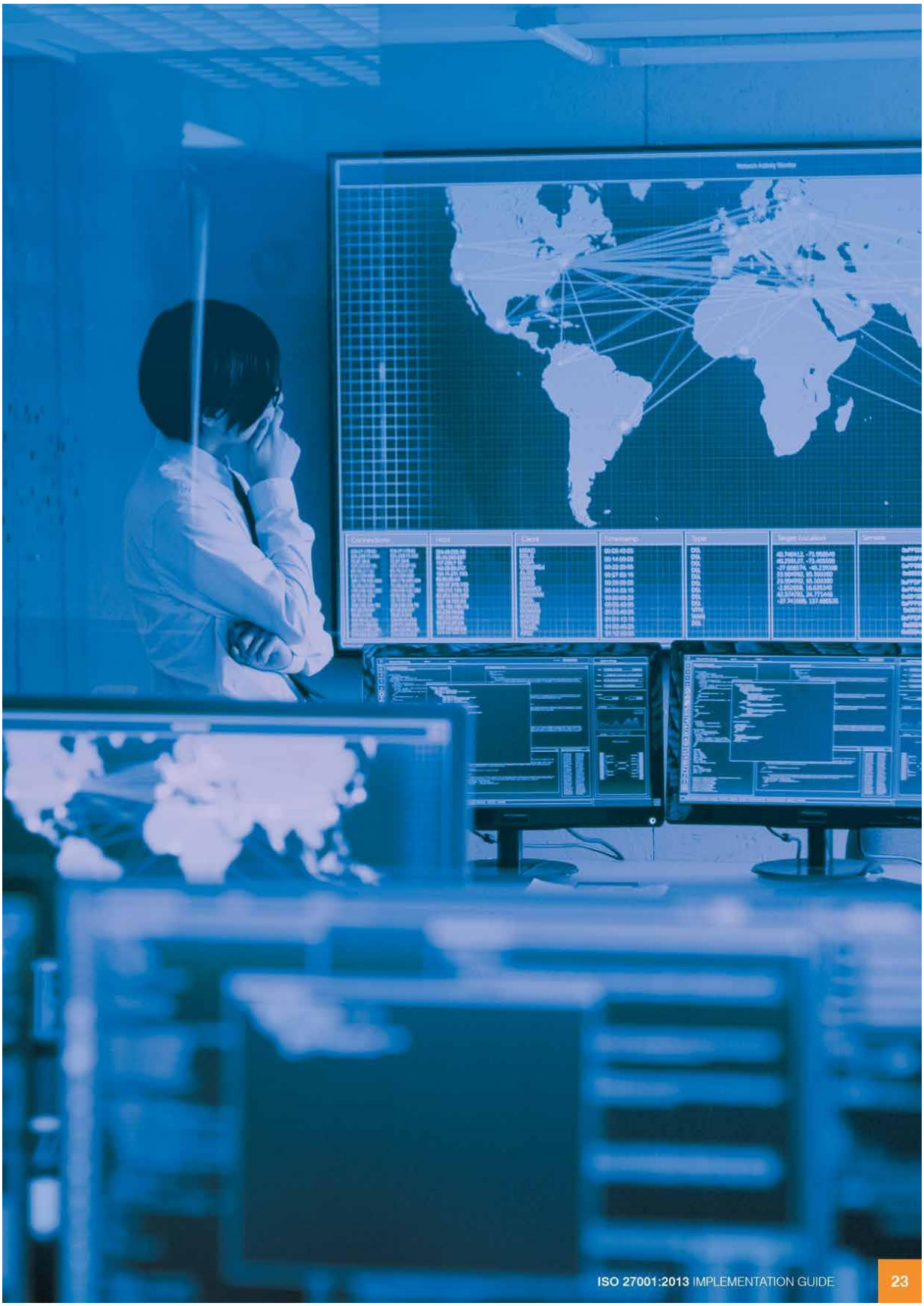
- Se complete un tratamiento de riesgos (ver más abajo);
- Haya cambios en los activos, la información o los procesos de la organización;
- Se identifiquen nuevos riesgos;
- Los datos indiquen que la probabilidad y consecuencia de cualquier riesgo identificado haya cambiado.

CONSEJO: para garantizar que su proceso de evaluación de riesgos cubra los tipos de eventos que requerirían una revisión, también debe tener en cuenta los controles del Anexo A para la gestión de vulnerabilidades técnicas (A.12.6), seguridad en los procesos de desarrollo y soporte (A.14.2) y gestión de entrega de servicios de proveedores (A.15.2).

Tratamiento de riesgos de seguridad de la información

El plan de tratamiento de riesgos que desarrolle no puede permanecer simplemente como una declaración de intenciones, debe implementarlo. Cuando se necesitan cambios para tener en cuenta la nueva información sobre los riesgos y los cambios en los criterios de evaluación de riesgos, el plan debe actualizarse y volver a autorizarse.

También se debe evaluar el impacto del plan y registrar los resultados de esta evaluación. Esto puede hacerse como parte de su proceso de revisión por la dirección o auditoría interna o mediante el uso de evaluaciones técnicas como pruebas de penetración de red, auditorías de proveedores o auditorías de terceros no anunciadas.



CLÁUSULA 9: EVALUACIÓN DEL DESEMPEÑO

Existen 3 formas para evaluar el rendimiento del SGSI:

- Seguimiento de la efectividad de los controles de SGSI.
- Auditorías internas.
- Durante la revisión por la dirección.

Seguimiento, medición, análisis y evaluación

Su organización necesitará decidir qué debe controlar para asegurar que el proceso del SGSI y los controles de seguridad de la información estén funcionando según lo previsto. No es práctico controlar a cada momento, si intenta hacerlo, es probable que el volumen de datos sea tan grande que sea prácticamente imposible usarlo de manera efectiva. Por lo tanto, en la práctica, deberá tomar una decisión informada sobre qué monitorear. Las siguientes consideraciones serán importantes:

- ¿Qué procesos y actividades están sujetos a las amenazas más frecuentes y significativas?
- ¿Qué procesos y actividades tienen las vulnerabilidades más significativas?
- ¿Qué es práctico para controlar y generar información significativa y oportuna?
- Cada proceso de control que implemente, para que sea efectivo, debe definir claramente:
- Cómo se lleva a cabo el control(por ejemplo, esto se define en un procedimiento);
- Cuándo se lleva a cabo;
- Quién es responsable de llevarlo a cabo;
- Cómo se informan los resultados, cuándo, a quién y qué hacen con ellos;
- Si los resultados del control identifican un desempeño inaceptable, ¿cuál es el proceso o procedimiento para afrontar esta situación?

Para demostrarle a un auditor que tiene implementado el procesamiento de monitoreo adecuado, deberá conservar registros de los resultados de monitoreo, análisis, revisiones de evaluación y cualquier actividad relacionada.

Auditorías internas

El propósito de las auditorías internas es evaluar sus deficiencias en los procesos del SGSI e identificar oportunidades de mejora. También proporcionan una verificación de la realidad para la gerencia sobre el desempeño del SGSI. Las auditorías internas pueden ayudar a evitar sorpresas en sus auditorías externas.

Las auditorías internas deben comprobar:

- La consitencia del seguimiento de los procesos, procedimientos y controles;
- El éxito de los procesos, procedimientos y controles para conseguir los resultados esperados;
- Si su SGSI cumple con la norma ISO 27001 y los requisitos de las partes interesadas.

Para asegurar que las auditorías se llevan a cabo a un alto nivel y de forma que aporten valor a la empresa, deben ser llevadas acabo por personas que:

- Sean respetadas.
- Sean competentes.
- Comprendan los requisitos de la ISO 27001.
- Pueden interpretar rápidamente su documentación y tiene experiencia en técnicas de auditoría.

Se les debe asignar el tiempo suficiente para realizar la auditoría y asegurar la cooperación de los empleados relevantes. Debe mantener un plan de auditorías internas. El auditor externo verificará dicho plan para garantizar que todos los procesos del SGSI se auditen durante un ciclo de tres años y que incluya:

- Evidencias de bajo rendimiento (es decir, a través de auditorías previas, o monitoreando resultados o incidentes de seguridad de la información);
- La gestión de riesgos de seguridad de la información.
- Los procesos que se auditan con mayor frecuencia.

El auditor externo también esperará que cualquier acción identificada en la auditoría sea registrada, revisada por los empleados apropiados y tenga acciones implementadas de manera oportuna para rectificar cualquier problema significativo. Al momento del cierre, denen considerar cualquier oportunidad de mejora identificada que requiera una inversión significativa de recursos.

Revisión por la dirección

La revisión por la dirección es un elemento esencial del SGSI. Es el punto formal en el que la gerencia revisa la efectividad del SGSI y asegura su alineación con la dirección estratégica de la organización. Las revisiones por la dirección deben realizarse a intervalos planificados y el programa de revisión general debe cubrir como mínimo una lista de áreas básicas especificadas en la cláusula 9.3 de la norma.

No es esencial que realice una sola reunión de revisión por la dirección que abarque la agenda completa. Si actualmente dispone de una serie de reuniones que cubren las áreas básicas requeridas, no hay necesidad de duplicarlas.

Deberá conservar información documentada de dichas revisiones por la dirección. Normalmente, actas de reuniones o tal vez grabaciones de llamadas si realiza llamadas teleconferencias. No es necesario extenderse mucho, pero deben contener un registro de las decisiones tomadas y las acciones acordadas, incluyendo responsabilidades y plazos.

CONSEJO: si decide modificar el calendario de las revisiones por la dirección y estas reuniones cubren varias áreas, puede considerar resumir las áreas cubiertas en forma de tablas o procedimientos para esclarecer los aspectos cubiertos en cada reunión.

CLÁUSULA 10: MEJORA

El objetivo de la implementación del SGSI debe ser reducir la probabilidad de que ocurran eventos de seguridad de la información, así como su impacto. Ningún SGSI es perfecto, sin embargo, dichos sistemas de gestión mejoran con el tiempo y aumentarán la resistencia frente a los ataques de seguridad de la información.

No conformidad y acción correctiva

La mejora se consigue aprendiendo de los incidentes de seguridad, los problemas identificados en las auditorías, los problemas de rendimiento, las quejas de las partes interesadas y las ideas generadas durante las revisiones por la dirección.

Para cada oportunidad identificada, deberá mantener registros de:

- Lo que ocurrió.
- Si el evento tuvo consecuencias indeseables, qué acciones se tomaron para controlarlo y mitigarlo.
- La causa raíz del evento (si se determina).
- La acción tomada para eliminar la causa raíz (si es necesario).
- La evaluación de la efectividad de cualquier acción tomada.

Análisis de causa-raíz

Para identificar acciones correctivas efectivas, es recomendable completar un análisis de causa raíz del problema. Si no llega al fondo de por qué o cómo sucedió, es probable que cualquier solución que implemente no sea completamente efectiva. El enfoque de los "5 por qué" es una buena herramienta de análisis de causa raíz: comience con el problema y luego pregunte "por qué" hasta llegar a la causa raíz. Por lo general, con 5 pregunta es suficiente, pero los problemas complejos pueden requerir más preguntas.

Por ejemplo:

Declaración del problema:
La organización estba infectada por el virus Wannacry.

¿Por qué?
Alguien hizo click en un enlace de un e-mail y descargó el virus que infectó su PC.

¿Por qué?
No recibieron ninguna formación sobre enlances en e-mails sospechosos.

¿Por qué?
La esponsable de formación está de baja por maternidad y la organización no ha cubierto su baja.

¿Por qué?
El proceso de baja por maternidad no está cubierto en el procedimiento de gestión de cambios, por ello no se realizó una evaluación para identificar riesgos de seguridad de la información.

CONSEJO: es posible que no tenga suficientes recursos para realizar el análisis de causa raíz en cada evento. Para priorizar esfuerzos, primero debe considerar completar una evaluación de riesgo simple y luego realizar un análisis de causa raíz solo para aquellos riesgos de valor medio o alto.

SACAR EL MÁXIMO DE SU SISTEMA DE GESTIÓN

Consejos para la correcta implementación de un SGSI:

1. Pregúntese ¿Por qué?. Asegúrese de que las razones de implantación del SGSI son claras y están alineadas con su dirección estratégica. De lo contrario corre el riesgo de no obtener la aceptación de la gerencia.

2. Considere ¿Para qué?. Implementar y mantener un SGSI requiere un compromiso, así que asegúrese de que su alcance sea lo suficientemente amplio como para cubrir la información crítica que necesita protección, pero no tan amplio como para carecer de recursos para implementarlo y mantenerlo.

3. Involucre a todas las partes interesadas en los momentos apropiados. Alta dirección para el contexto, requisitos, políticas y establecimiento de objetivos; gerentes y empleados con conocimiento para la evaluación de riesgos, diseño de procesos y procedimientos.

4. Comunique durante el proceso a las partes interesadas. Hágales saber lo que está haciendo, por qué lo está haciendo, cómo planea hacerlo y cuál será su participación. Proporcione actualizaciones del progreso.

5. Obtenga ayuda externa. No falle por falta de habilidades o conocimiento. La gestión de los riesgos de seguridad de la información a menudo requiere conocimientos especializados. Asegúrese de verificar las credenciales de un tercero antes de contratarlo.

6. Mantenga procesos y documentación simples. Puede desarrollarlos más adelante si fuese necesario.

7. Diseñe e implemente reglas que pueda seguir en la práctica. No cometa el error de documentar una regla demasiado elaborada que nadie pueda seguir. Es mejor aceptar un riesgo y seguir buscando formas de gestionarlo.

8. Recuerda a los proveedores. Algunos lo ayudarán a mejorar su SGSI, otros aumentarán su riesgo. Debe asegurarse de que los proveedores de alto riesgo tengan controles establecidos tan buenos como los suyos. Si no los tienen, busque alternativas.

9. Forme al personal. Es probable que la seguridad de la información sea un concepto nuevo para sus empleados. Las personas pueden necesitar cambiar sus hábitos y es improbable que una sola sesión informativa de sensibilización sea suficiente.

10. Recuerde asignar recursos suficientes para probar rutinariamente sus controles. Las amenazas a las que se enfrenta su organización cambiarán constantemente y debe probar la respuesta a dichas amenazas.

PASOS TRAS LA IMPLANTACIÓN

1 FORMACIÓN DE CONCIENCIACIÓN

- Su organización debe crear conciencia sobre los diversos estándares cubiertos por el sistema de gestión.
- Debe celebrar reuniones de capacitación separadas para los diferentes niveles de la gerencia, lo que ayudará a crear un ambiente motivador, listo para la implantación.

2 POLÍTICA Y OBJETIVOS

- YSu organización debe desarrollar una política de calidad/integrada y objetivos relevantes para ayudar a cumplir los requisitos.
- Al trabajar con la gerencia, su empresa debe realizar talleres con todos los niveles de personal de gestión para delinear los objetivos integrados.

3 ANÁLISIS DE DEFICIENCIAS INTERNO

- Su organización debe identificar y comparar el nivel de cumplimiento de los sistemas con los requisitos de las normas de su nuevo sistema.
- Todo el personal relevante debe comprender las operaciones de la organización y desarrollar un mapa de procesos para las actividades del negocio.

4 DOCUMENTACIÓN/PROCESO DE DISEÑO

- La organización debe crear documentación de los procesos según los requisitos de las normas relevantes.
- Debe redactar e implantar un manual, procedimientos funcionales, instrucciones de trabajo, procedimientos del sistema y proporcionar los términos asociados.

5 DOCUMENTACIÓN/PROCESO DE IMPLANTACIÓN

- Los procesos/documentos desarrollados en el paso 4 deben implementarse en toda la organización y abarcar todos los departamentos y actividades.
- La organización debe realizar un taller sobre la implementación según corresponda para los requisitos de la norma ISO.

6 AUDITORÍA INTERNA

- Un sistema de auditoría interna robusto es esencial. Recomendamos la formación de auditor interno y NQA puede proporcionar dicha formación para las normas que esté implantando.
- IEs importante implementar acciones correctivas para las mejoras, en cada uno de los documentos auditados, a fin de cerrar las deficiencias y garantizar la eficacia del sistema de gestión.

7 ORGANIZAR LA REVISIÓN POR LA DIRECCIÓN DEL SISTEMA

- La gerencia de debe revisar varios aspectos comerciales de la organización, que son relevantes para las normas a implantar.
- Revise la política, los objetivos, los resultados de la auditoría interna y del desempeño del proceso, los resultados de las quejas, el cumplimiento legal, la evaluación de riesgos y desarrolle un plan de acción y un acta de revisión.

8 ANÁLISIS DE DEFICIENCIAS DE SISTEMAS IMPLANTADOS

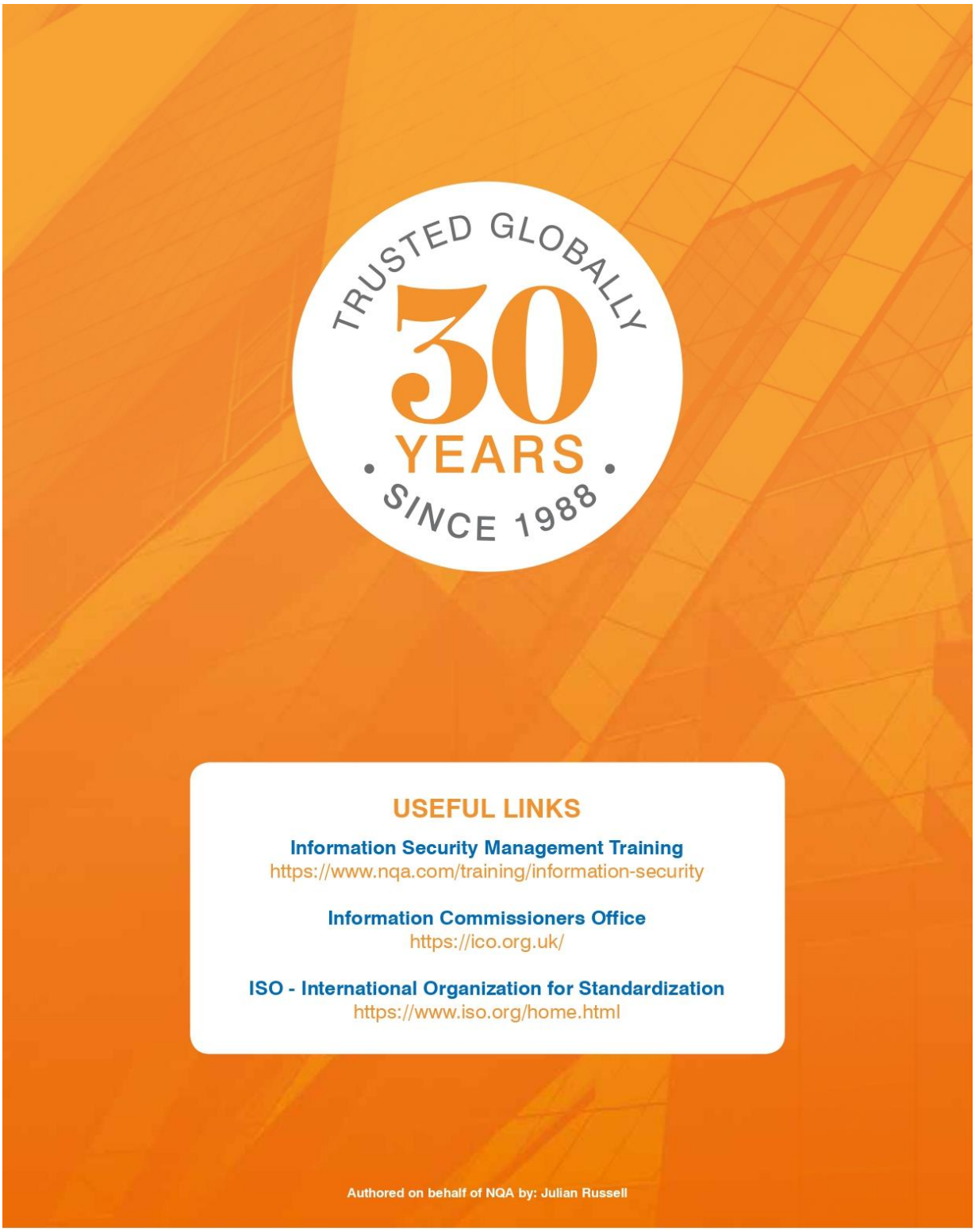
- Debe realizar un análisis de deficiencias para evaluar la efectividad y el cumplimiento de la implantación del sistema en la organización.
- Este análisis de deficiencias preparará a su organización para la auditoría de certificación final.

9 ACCIONES CORRECTIVAS

- La organización estará lista para la auditoría de certificación final, siempre que el análisis de deficiencias y todas las no conformidades (NC) hayan recibido acciones correctivas.
- Verifique que todas las NC significativas estén cerradas y que la organización esté lista para la auditoría de certificación final.

10 AUDITORÍA DE CERTIFICACIÓN FINAL

- Una vez completada la auditoría de forma satisfactoria, su organización recibirá el certificado.
- ¡Enhorabuena!



nqa. www.nqa.com

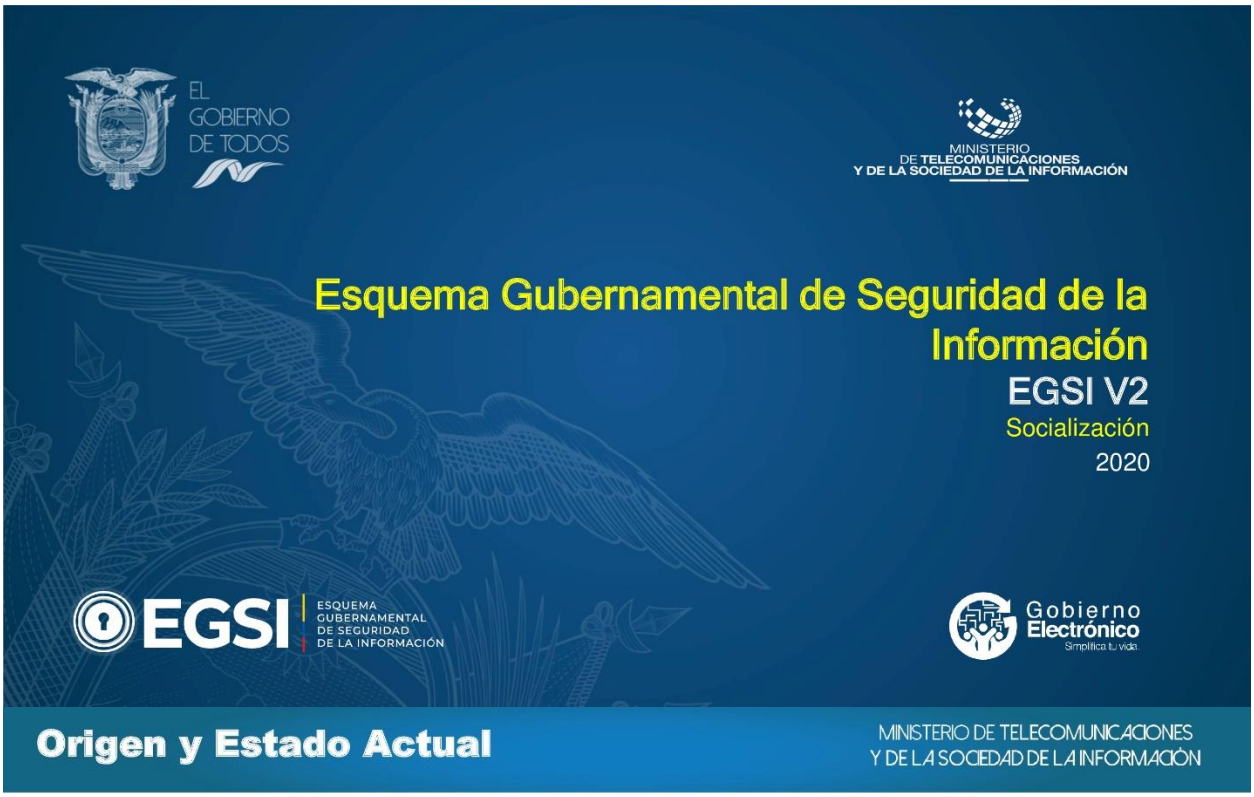
ANEXO 4: Socialización – EGSI-V2.0-Acuerdo Ministerial-025-2019

UNIVERSIDAD TÉCNICA DEL NORTE

UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC Resolución No 001-073 CEAACES – 2013 – 13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

SOCIALIZACION – EGSI-V2.0-ACUERDO MINISTERIAL-025-2019



EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

Comisión SI & TICS

Análisis de la situación respecto de la gestión de la Seguridad de la Información en las entidades APCID

Acuerdo Ministerial 166

Desarrollo del EGSI - basado en la Norma Técnica Ecuatoriana INEN ISO/IEC 27002

Resultados de Implementación

El 86% de instituciones implementaron el EGSI; sin el Estudio de Gestión de Riesgos.

Construcción EGSI Versión 2.0

Proporcionar un instrumento que permita orientar adecuada y ordenadamente en la implementación de un SGSI en las Instituciones Públicas.

Evolución del modelo ISO 27001 - 2005/2013

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

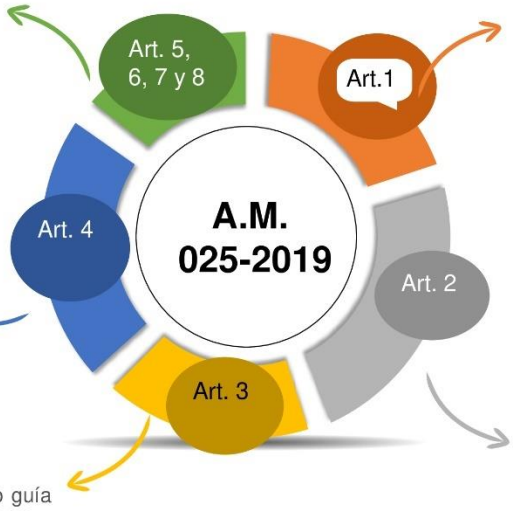
ISO/IEC 27001:2005	ISO/IEC 27001:2013	
NUMERO DE CONTROLES		
133	114	94 Se Mantienen 39 Eliminados 20 Nuevos
DOMINIOS DE SEGURIDAD		
11	14	3 DOMINIOS NUEVOS
REQUISITOS DE GESTION		
102	130	18 REQ-GEST NUEVOS

EGSI V2
NUMERO DE CONTROLES
115
DOMINIOS DE SEGURIDAD
14
REQUISITOS DE GESTION
130

Artículos del A. M. 025-2019

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

- Máxima Autoridad:
  Designación del CSI
- Responsabilidades del CSI
- El Comité de S.I.:
  Designación del OSI
- Respondabilidades del OSI



Expedir el EGSI, que es de Implementación obligatoria en las Instituciones de la APCID.

Plazo EGSI: 12 meses para la implementación
- **5 meses**: Evaluación y Plan para el Tratamiento de Riesgos
- **7 meses**: Implementación de controles.

Las instituciones realizarán la **Evaluación** y el diseño del Plan para el **Tratamiento** de los **Riesgos**.

Recomendar utilicen como guía las **NTE INEN-ISO/IEC 27000**

Disposiciones del A. M. 025-2019

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

Generales

PRIMERA: Designación del Subsecretario de Estado Gobierno Electrónico
SEGUNDA: Una vez finalizado se evaluará el cumplimiento, basado en los criterios que se establezcan.
TERCERA: El MINTEL deberá elaborar hasta el 31 de enero de cada año un Plan de Evaluación.

CUARTA: En caso de no ser posible la implementación de controles establecidos en el EGSI, deberá ser justificado técnicamente y comunicado, para su análisis y aprobación.
QUINTA: Los OSI actuarán como contrapartes del MINTEL, quienes reportarán a través de GPR
SEXTA: Cada año a finales de enero las instituciones de la APCID remitirán un "Informe de cumplimiento de la Gestión de Riesgos".
SÉPTIMA: Es responsabilidad de la máxima autoridad gestionar la implementación de esta normativa asignando los recursos necesarios.

Transitorias

PRIMERA: La designación del OSI debe ser comunicada dentro del plazo de 30 días.

SEGUNDA: Para el seguimiento y control el MINTEL en 60 días creará indicadores de gestión e implementación del EGSI, en el sistema GPR.

TERCERA: el MINTEL en 60 días emitirá el formato para el "Informe de cumplimiento de la Gestión ..."

CUARTA: el MINTEL en un plazo de 90 días, emitirá los lineamientos para el seguimiento y control...

Derogatorias

Deróguese el Acuerdo Ministerial No. 166 y 1606.

Objetivo EGSI Versión 2.0

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

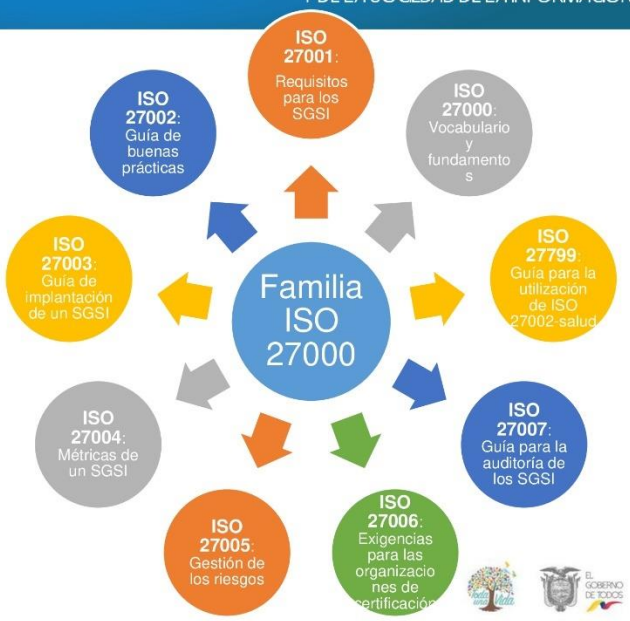
EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

Preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos de seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados

Enfoque de un SGSI

MINISTERIO DE TELECOMUNICACIONES
Y DE LA SOCIEDAD DE LA INFORMACIÓN

EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN



Enfoque de un SGSI

MINISTERIO DE TELECOMUNICACIONES
Y DE LA SOCIEDAD DE LA INFORMACIÓN

EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

Estructura ISO 27001:2013

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

ISO 27001:2013 & EL CICLO PDCA
(Estructura General)

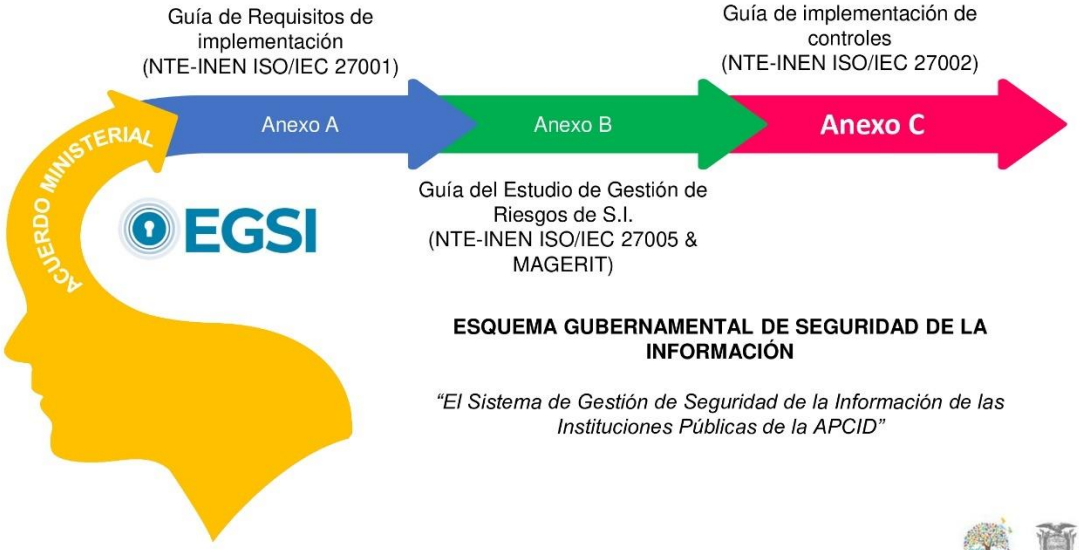
PLAN/PLANEAR				DO/HACER	CHECK/VERIFICAR	ACT/ACTUAR
4. Contexto de la Organización	5. Liderazgo	6. Planificación	7. Soporte	8. Operación	9. Evaluación del desempeño	10. Mejora
Entendiendo la organización y su contexto	Liderazgo y Compromiso	Acciones para abordar riesgos y oportunidades	Recursos	Control y Planificación Operacional	Monitoreo, medición, análisis y evaluación.	Acciones correctivas y no conformidades
Expectativa de las partes interesadas	Política		Competencias			
Alcance del SGSI		Objetivos de S.I. y planes para alcanzarlos.	Concienciación	Evaluación de riesgos de seguridad de la Información	Auditoría interna	Mejora continua
SGSI	Organización, roles, responsabilidades y autoridades		Comunicación		Revisión de gestión	
				Tratamiento de riesgos de seguridad de la Información		
			Información Documentada			

Estructura ISO 27002:2013

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

Estructura del Anexo – EGSI Versión 2.0

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN



ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

"El Sistema de Gestión de Seguridad de la Información de las Instituciones Públicas de la APCID"

Gestión de Riesgo

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

¿Y LA GESTIÓN DEL RIESGO?

Se puede definir como "el proceso de toma de decisiones en un ambiente de incertidumbre sobre una acción que puede suceder y sobre las consecuencias que existirán si esta acción ocurre"

La Gestión de Riesgo implica:

- ❑ Determinar **qué** se necesita proteger.
- ❑ **De qué** hay que protegerlo.
- ❑ **Cómo** hacerlo.

Estándares y Metodologías de Gestión de riesgos.

- ISO 31000
- ISO 27005
- AS 4360 (AUSTRALIANA)
- MAGERIT
- NIST

Fuente: ISEC Ecuador, http://www.isec-global.com/isec/home_ec.html

Definiciones

MINISTERIO DE TELECOMUNICACIONES
Y DE LA SOCIEDAD DE LA INFORMACIÓN

AMENAZA

evento, suceso o una acción que anticipa la intención de dañar

VULNERABILIDAD

Ausencia o Deficiencia de un control. Debilidad o grado de exposición de un sujeto, objeto o sistema.

PROBABILIDAD

Potencial de ocurrencia de un hecho que pueda manifestarse en un lugar específico, con una duración e intensidad determinadas.

IMPACTO

resultado de un suceso que afecta a los objetivos

Fuente: ISEC Ecuador, http://www.isec-global.com/isec/home_ec.html

Qué es Riesgo?

MINISTERIO DE TELECOMUNICACIONES
Y DE LA SOCIEDAD DE LA INFORMACIÓN

Riesgo para la seguridad de la información

El potencial de que una **amenaza** dada explote las **vulnerabilidades** de un activo o grupo de activos de información, causando **daño** a la organización.

Se mide en términos de una combinación de la probabilidad de un evento y sus consecuencias.

PROBABILIDAD X IMPACTO = RIESGO

Guía para Gestión de Riesgo

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

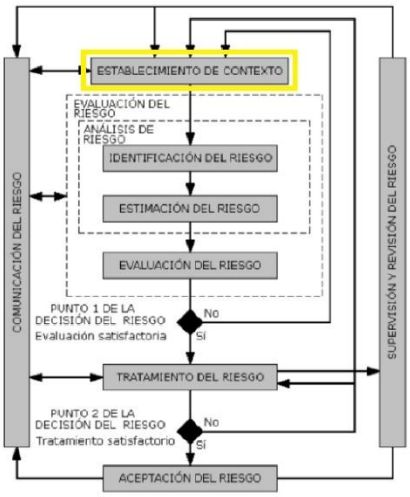
Actividades para la gestión del riesgo de la seguridad de la información:

PROCESO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN	
ACTIVIDADES	**PASO**
Establecimiento del contexto	*1. Consideraciones Generales - Levantamiento de información inicial* *2. Establecer criterios básicos para la Gestión del Riesgo* *3. Definir alcance y límites de la Gestión del Riesgo* *4. Establecer una organización para la operación del SGRSI*
Valoración del Riesgo	*5. Identificar Activos de Información* *6. Identificar las amenazas y las vulnerabilidades* *7. Identificar los controles existentes* *8. Identificar consecuencias* *9. Valorar las consecuencias* *10. Valorar los incidentes* *11. Determinar el nivel de estimación del riesgo* *12. Evaluar el riesgo*
Tratamiento del Riesgo	*13. Seleccionar controles*
Aceptación del Riesgo	*14. Aceptar el riesgo*
Comunicación del Riesgo	*15. Comunicar el riesgo*
Monitoreo y Revisión del Riesgo	*16. Monitorear y revisar los riesgos*

Proceso Gestión de Riesgo de la S.I.

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

Establecer el Contexto



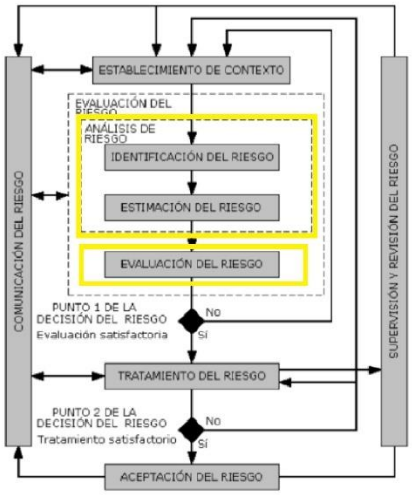
Implica **establecer los criterios básicos** necesarios para la gestión de riesgos y de la seguridad de información, **definir e alcance y los límites** y establecer una organización adecuada que opere la gestión de riesgos en S.I.

Análisis del riesgo

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

La valoración del riesgo consta:

- Análisis del riesgo
  - Identificación del riesgo
  - Estimación del riesgo
- Evaluación del riesgo



Análisis del riesgo

Identificar el riesgo

- ❑ Identificación de los activos
- ❑ Identificación de las amenazas
- ❑ Identificación de vulnerabilidades
- ❑ Identificación de la existencia de controles.

Valoración del Riesgo

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

Identificación de activos de información

Tipos de activos:

PRIMARIOS

- ❑ Información (Electrónica, Impresa)
- ❑ Actividades y Procesos del Negocio

SOPORTE

- ❑ Software (Aplicaciones de herramientas, software)
- ❑ Hardware (Servidores, Networking. otros equipos)
- ❑ Servicios (computación, comunicaciones)
- ❑ Personas (Habilidades, experiencia, calificación)
- ❑ Intangibles (Reputación , marca, imagen)
- ❑ Ubicación
- ❑ Estructura de la organización

Fuente: ISEC Ecuador, http://www.isec-global.com/isec/home_ec.html

Ejemplo: Identificación de Activos

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

Ejemplo de identificación de activos:

IDENTIFICACION DE LOS ACTIVOS DE INFORMACION						
Nro. Activo	Proceso Macro	Subproceso	Tipo de Activo	Nombre de Activo	Descripción del activo	Ubicación
A1	Apoyo de Tecnologías de la Información y Comunicaciones	Infraestructura	Hardware	Controladora Wireless, puntos de acceso	puntos de acceso inalámbrico en toda la institución	Data Center
A2			Hardware	Firewall Fortigate	Control de acceso y permisos de seguridad perimetral para la red institucional	Data Center
A3		Redes y comunicaciones	Redes	Switch Core Cisco 4700	Procesamiento de trafico de red para distribución en la red interna e Internet	Data Center
A4			Redes	Switchs de Acceso Cisco 2960	Procesamiento de trafico de red de acceso en cada piso del edificio	Data Center
A5		Aplicaciones informáticas	Software	Antivirus Institucional	Software de seguridad end point	Data Center
A6			Software	Servicio de correo Exchange	Información de buzones de correo electrónico institucional	Data Center
A7		Instalaciones	Localidad	Datacenter	Centro de Datos Institucional	Edificio Matriz
A8		Talento Humano	Personal	Personal de soporte	Funcionarios de Soporte Técnico Nivel 1 - Institucional	Edificio Matriz
A9			Personal	Personal de desarrollo de sistemas	Personal técnico que desarrolla aplicaciones o automatiza procesos	Edificio Matriz

Identificación de Activos

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

Valoración de activos

CONFIDENCIALIDAD	Criterio
Alto (3)	La divulgación no autorizada de la información tiene un efecto crítico para la institución Ej. Divulgación de información confidencial o sensible.
Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la institución Ej. Divulgación de información de uso interno
Bajo (1)	La divulgación de la información no tiene ningún efecto para la institución Ej. Divulgación de información pública.

DISPONIBILIDAD	Criterio
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución
Bajo (1)	interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución

INTEGRIDAD	Criterio
Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución
Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución
Bajo (1)	La destrucción o modificación de la información tiene un efecto leve para la institución

Identificación de Activos

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

VA: Ejemplo

$$VA = \frac{C + I + D}{3}$$

VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Nro. Activo	Nombre de Activo	Tipo de soporte	Ubicación	Valoración de Impacto (pérdida) C: Confidencialidad I: Integridad D: Disponibilidad			
				C	I	D	VA
A1	Controladora Wireless, puntos de acceso	Físico y Lógico	Centro de Datos	1	1	2	1,33
A2	Red de datos	Físico	Edificio Institucional	1	1	3	1,67
A3	Firewall Fortigate	Físico y Lógico	Centro de Datos	2	2	2	2,00
A4	Biométricos	Físico y Lógico	Sala de recepción Institucional	1	1	1	1,00
A5	Cámaras de seguridad	Físico y Digital	Edificio Institucional	1	1	1	1,00
A6	Switch Core Cisco 4700	Físico y Lógico	Centro de Datos	1	1	3	1,67
A7	Switchs de Acceso Cisco 2960	Físico y Lógico	Centro de Datos	1	1	1	1,00
A8	Enlaces de internet	Físico y Lógico	Centro de Datos	1	1	1	1,00
A9	Antivirus Institucional	Lógico	Centro de Datos	1	1	2	1,33
A10	Sistema Talento Humano SIRHA	Lógico	Centro de Datos	1	1	1	1,00

Análisis del riesgo

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

Identificación de amenazas

Tienen el potencial de causar daños, las amenazas pueden afectar a más de un activo. En tales casos pueden causar diferentes impactos dependiendo los activos que se vean afectados.

ANÁLISIS DE RIESGOS

Subprocesos	Nro. Activo	Nombre Activo	Amenaza
Infraestructura	A1	Controladora Wireless, puntos de acceso	Intrusos en la red
			Indisponibilidad de servicios
	A2	Red de datos	Indisponibilidad de servicios
	A3	Firewall Fortigate	Acceso no deseado a activos críticos
			Indisponibilidad de servicios
	A4	Biométricos	Desarrollo de nuevas funcionalidades para la gestión de TH
	A5	Cámaras de seguridad	Acceso de personas no deseables y/o pérdidas de activos.
			Acceso de personas no deseables y/o pérdidas de activos.

Identificación de vulnerabilidades

Se debe identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o a la institución.

ANÁLISIS DE RIESGOS				
Subprocesos	**Nro. Activo**	**Nombre Activo**	**Amenaza**	**Vulnerabilidad**
Infraestructura	A1	Controladora Wireless, puntos de acceso	Intrusos en la red	Actualización de firmware equipo antiguo
			Indisponibilidad de servicios	No existe equipo de redundancia
	A2	Red de datos	Indisponibilidad de servicios	Red de datos mixta (cat. 5e, 6a)
	A3	Firewall Fortigate	Acceso no deseado a activos críticos	imposibilidad de actualizar firmware por falta de recursos del equipo
			Indisponibilidad de servicios	Inexistencia de equipo de redundancia
	A4	Biométricos	Desarrollo de nuevas funcionalidades para la gestión de TH	Incompatibilidad del software base con plataforma de desarrollo actual (php)
	A5	Cámaras de seguridad	Acceso de personas no deseables y/o pérdidas de activos.	Existencia de áreas sin vigilancia
			Acceso de personas no deseables y/o pérdidas de activos.	Vigencia Tecnología, equipos continuamente dañados

Análisis del riesgo

MINISTERIO DE TELECOMUNICACIONES
Y DE LA SOCIEDAD DE LA INFORMACIÓN

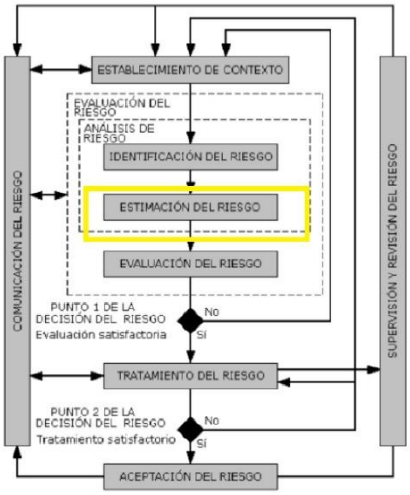
Identificación de existencia de de controles

Anáslis de Riesgos					Evaluación de Riesgos				
					Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo
Subprocesos	Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad		
Infraestructura	A4	Controladora Wireless, puntos de acceso	Indisponibilidad de servicios	Red de datos mixta (cat. 5e, 6a)	1,67			Mantenimiento local	1,67
Infraestructura	A5	Red de datos	Acceso no deseado a activos críticos	imposibilidad de actualizar firware por falta de recursos del equipo	2,00			Soporte contratado	8,00
			Indisponibilidad de servicios	Inexistencia de equipo de redundancia	2,00			Soporte contratado	8,00
Infraestructura	A6	Firewall Fortigate	Desarrollo de nuevas funcionalidades para la gestión de TH	Incompatibilidad del software base con plataforma de desarrollo actual (php)	1,00			Mantenimiento local	1,00
Infraestructura	A7	Biometricos	No cumplimiento de actividades del usuario con daño en su equipo	Ausencia de equipos de reemplazo temporal	1,33			Mantenimiento local	2,67
			Disminución de la gestión del proceso	Hardware con recursos limitados	1,33			Mantenimiento local	2,67
Infraestructura	A9	Cámaras de Seguridad	Acceso de personas no deseables y/o pérdidas de activos.	Existencia de áreas sin vigilancia	1,00			Mantenimiento local	2,00
			Acceso de personas no deseables y/o pérdidas de activos.	Vigencia Tecnología, equipos continuamente dañados	1,00			Mantenimiento local	1,00

Estimación del riesgo

"Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo"

El análisis de riesgo cualitativo usa una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales (por ejemplo, baja, media y alta) y la probabilidad de esas consecuencias.



Criterios de probabilidad de ocurrencia de amenazas:

Nivel de amenazas	Criterio por probabilidad	Criterio por condición de ocurrencia	Criterio por atractivo	Ejemplo
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%)	Bajo circunstancias normales	El atacante se beneficia en gran medida por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Código malicioso
Medio (2)	La ocurrencia es probable (probabilidad =50%)	Por errores descuidos	El atacante se beneficia de alguna manera por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Falla de hardware
Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y <50%)	en rara ocasión	El atacante no se beneficia del ataque	desastres naturales

Criterio de la Evaluación de Riesgos

$$Nivel\ de\ riesgo = VA(CID) * Nivel\ de\ amenaza * Nivel\ de\ vulnerabilidad$$

Nivel de Riesgo	
1 - 3	El riesgo es BAJO
4 - 8	El riesgo es MEDIO
9 - 27	El riesgo es ALTO

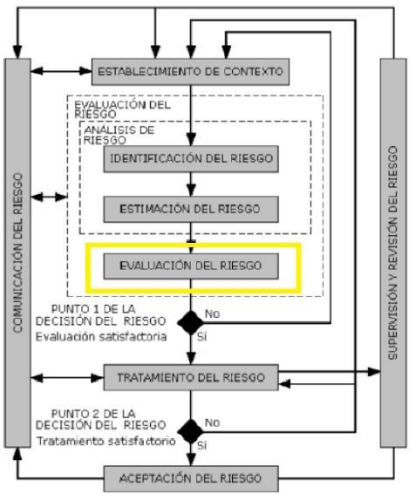
Criterio de probabilidad de ocurrencia de vulnerabilidades

Nivel de vulnerabilidad	Criterio	Ejemplo
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza	No se utilizan contraseñas para que los usuarios ingresen a los sistemas
Medio (2)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable	Existen normas para la utilización de contraseñas, pero no se implementa
Bajo (1)	La medida de seguridad es adecuada	Existen normas para la utilización de contraseñas y es aplicada

Evaluación del Riesgo

MINISTERIO DE TELECOMUNICACIONES
Y DE LA SOCIEDAD DE LA INFORMACIÓN

Consiste en comparar los riesgos estimados con los criterios de evaluación y de aceptación de riesgos definidos en el establecimiento del contexto.



Evaluación del riesgo

MINISTERIO DE TELECOMUNICACIONES
Y DE LA SOCIEDAD DE LA INFORMACIÓN

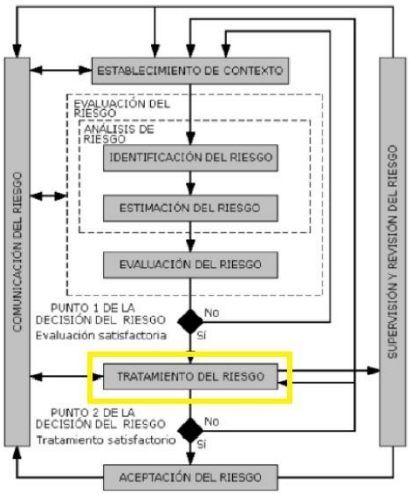
Nivel del riesgo

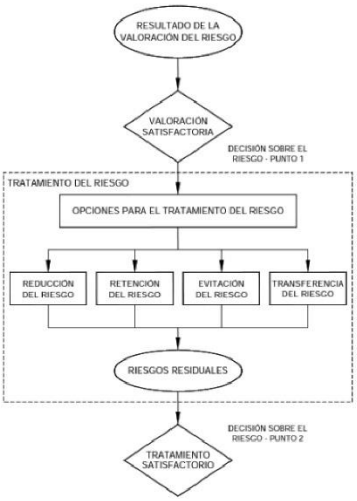
				Evaluación de Riesgos					
				Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad			
A1	Controladora Wireless, puntos de acceso	Intrusos en la red	Actualización de firware equipo antiguo	1,33	1	1	Soporte contratado	1,33	BAJO
		Indisponibilidad de servicios	No existe equipo de redundancia	1,33	1	1	Soporte contratado	1,33	BAJO
A2	Red de datos	Indisponibilidad de servicios	Red de datos mixta (cat. 5e, 6a)	1,67	1	1	Mantenimiento local	1,67	BAJO
A3	Firewall Fortigate	Acceso no deseado a activos críticos	imposibilidad de actualizar firware por falta de recursos del equipo	2,00	2	2	Soporte contratado	8,00	MEDIO
		Indisponibilidad de servicios	Inexistencia de equipo de redundancia	2,00	2	2	Soporte contratado	8,00	MEDIO
A4	Biometricos	Desarrollo de nuevas funcionalidades para la gestión de TH	Incompatibilidad del software base con plataforma de desarrollo actual (php)	1,00	1	1	Mantenimiento local	1,00	BAJO
A5	Cámaras de seguridad	Acceso de personas no deseables y/o pérdidas de activos.	Existencia de áreas sin vigilancia	1,00	1	2	Mantenimiento local	2,00	BAJO
		Acceso de personas no deseables y/o pérdidas de activos.	Vigencia Tecnología, equipos continuamente dañados	1,00	1	1	Mantenimiento local	1,00	BAJO

Tratamiento del Riesgo de la S.I.

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

Existen cuatro opciones disponibles para el tratamiento del riesgo:

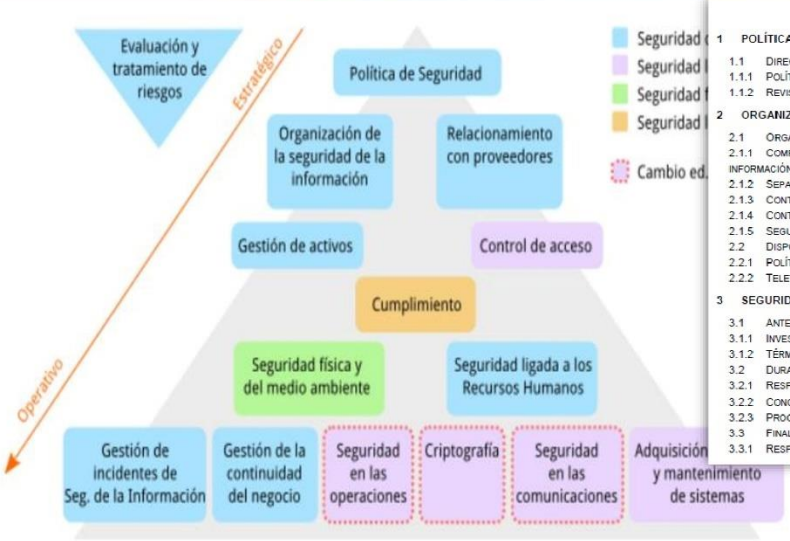




- Reducción
- Retención
- Evitación
- Transferencia

Estructura ISO 27002:2013

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN



CONTENIDO

Tratamiento del Riesgo de la S.I.

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

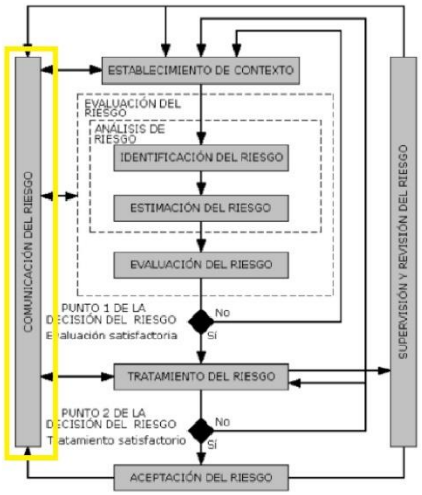
Ejemplo de tratamiento del riesgo.

Evaluación de Riesgos					Tratamiento de Riesgos								
Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	Riesgo residual
CID	Nivel de amenaza	Nivel de vulnerabilidad											
1,67	2	2	Soporte contratado	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	11.2.2 - EGSI	1	1	1,67	BAJO	ACEPTABLE
1,67	2	2	Plan aplicado de pruebas y backup	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	11.1.3 - EGSI	1	1	1,67	BAJO	ACEPTABLE
1,67	2	2	Plan aplicado de pruebas y backup	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	11.2.1 - EGSI	1	1	1,67	BAJO	ACEPTABLE
1,67	1	2	Soporte contratado	3,33	BAJO	ACEPTAR	CONTROL PREVENTIVO	11.1.2 - EGSI	1	1	1,67	BAJO	ACEPTABLE
1,67	2	2	Soporte contratado	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	11.1.2 - EGSI	1	1	1,67	BAJO	ACEPTABLE
1,67	1	2	Soporte contratado	3,33	BAJO	ACEPTAR	CONTROL PREVENTIVO	11.2.1 - EGSI	1	1	1,67	BAJO	ACEPTABLE

Comunicación de los Riesgo de la S.I.

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

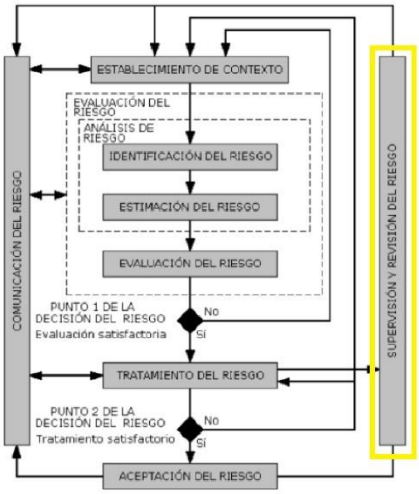
Garantiza que los responsables de la implementación de la gestión del riesgo y aquellos con intereses establecidos comprendan las bases sobre las cuales toman las decisiones y por qué se requieren acciones particulares.



Monitoreo y revisión del riesgo de la S.I.

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

Las amenazas, las vulnerabilidades, la probabilidad o las consecuencias pueden cambiar abruptamente sin ninguna indicación. Por ende, es necesario el monitoreo constante para detectar estos cambios.



Beneficios esperados – EGSI versión 2.0

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

- Reducción del riesgo de pérdida, robo o integridad de la información sensible institucional.
- Revisión continua de los riesgos y los controles de seguridad de la información implementados en las Instituciones de la APCID.
- Proyectos de adquisición alineadas a la matriz de riesgos, que permitirán la reducción de los costos en compra sistemática de productos y tecnologías.
- Garantizar la continuidad del servicio tras un incidente de seguridad de seguridad de la información de impacto alto.


Hoja de ruta - implementación EGSI versión 2.0
MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN
Primera Etapa
PROGRAMA: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN INSTITUCIONES APCID (GPR – MINTEL)
PROYECTO: IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN – EGSI – Versión 2.0 (GPR – INSTITUCIONES DE LA APCID)
INICIO Primera Etapa Enero 2020
PERFIL DEL PROYECTO
ALCANCE EGSI
POLÍTICA DE SEGURIDAD
METODOLOGIA DE EVALUACIÓN DE RIESGOS
PLAN DE COMUNICACIÓN
PROCESO DE ANALISIS Y EVALUACIÓN DE LOS RIESGOS
FIN Primera Etapa Diciembre 2020
1
2
3
4
5
6
Publicación del Acuerdo Ministerial en el Registro Oficial
INFORME DE LA EVALUACIÓN DE RIESGOS
Hitos de control GPR
Fichas de Cumplimiento


Hoja de ruta - implementación EGSI versión 2.0
MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN
Segunda Etapa
PROGRAMA: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN INSTITUCIONES APCID (GPR – MINTEL)
PROYECTO: IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN – EGSI – Versión 2.0 (GPR – INSTITUCIONES DE LA APCID)
INICIO Segunda Etapa Diciembre 2021
Declaración de Aplicabilidad (SoA)
Plan de Tratamiento de los riesgos
9 - 123
PROCESO DE IMPLEMENTACIÓN DE (115) CONTROLES
Plan de Auditoría Interna
Informe Revisión Dirección
Informe Medidas Correctivas
FIN Segunda Etapa Julio 2021
6
7
8
124
125
126
127
INFORME DE LA EVALUACIÓN DE RIESGOS
INFORME DE CIERRE DEL PROYECTO
Hitos de control GPR
Fichas de Cumplimiento

Puntos de contacto oficial:

MINISTERIO DE TELECOMUNICACIONES
Y DE LA SOCIEDAD DE LA INFORMACIÓN

EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

ASISTENCIA TÉCNICA

soporte@gobiernoelectronico.gob.ec

EL GOBIERNO DE TODOS

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

Gracias

Presentado por:
SUBSECRETARÍA DE GOBIERNO ELECTRÓNICO Y REGISTRO CIVIL

EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

Gobierno Electrónico
Simplifica tu vida

ANEXO 5: Certificado del entregable a la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERIA EN SOFTWARE

ACTA DE ENTREGA DEL INFORME DEL DESARROLLO DEL PLAN DE SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CON LA ISO 27001: 2013, DE LA COOPERATIVA DE AHORRO Y CRÉDITO IMBACOOP LTDA.

En la ciudad de Ibarra a los 31 días del mes de enero del año 2024, se entrega al jefe del Departamento de Tecnología del Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., al ing. Jeison Ramos los siguientes documentos:

- Informe de políticas de seguridad de la información

Considerando que las partes manifiestan su total conformidad, se ratifica y aceptan todo su contenido, entendiendo su alcance y significado.

Recibe conforme:

Ing. Jeison Ramos

Jefe de DTI

Entrega conforme:

William De La Torre

Estudiante

CERTIFICADO DE ENTREGA Y RECEPCION

Ingeniero Jeison Ramos, jefe del Departamento de Tecnología de la Información de la Cooperativa Ahorro y Crédito Imbacoop Ltda., apetición verbal del interesado.

CERTIFICA:

Que el señor William Andrés De La Torre Yamberla con número de cédula 1004631865, se realizó la entrega del CONTENIDO y FORMATO del trabajo de titulación denominado: Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información en la Cooperativa de Ahorro y Crédito Imbacoop Ltda., aplicando el estándar ISO/IEC 27001, para fortalecer la disponibilidad de los servicios.

Es todo cuanto puedo certificar en honor a la verdad, pudiendo el interesado hacer uso del presente como lo estime conveniente.

Otavalo, 31 de enero del 2024

Atentamente

.....

Ing. Jeison Ramos
JEFE DE TECNOLOGIAS
COAC IMBACOOP LTDA


IMBACOOP