

**FACULTAD DE CIENCIAS EMPRESARIALES Y ADMINISTRACIÓN**

**DEPARTAMENTO DE INGENIERÍA INDUSTRIAL**

**METODOLOGÍA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN  
COMO CONTRIBUCIÓN A LA CONTINUIDAD DEL NEGOCIO. APLICACIÓN EN  
LA OFICINA TERRITORIAL DE NORMALIZACIÓN DE HOLGUÍN**

**TESIS PRESENTADA EN OPCIÓN AL TÍTULO ACADÉMICO DE  
MÁSTER EN INGENIERÍA INDUSTRIAL  
MENCIÓN CALIDAD**

**Autora: Ing. Yailín Rojas Pupo**

**Tutor: MSc. Pedro F Tamayo García**

**HOLGUÍN, 2021**

## **Resumen**

La presente investigación tiene como objetivo desarrollar una metodología para la gestión de la seguridad de la información que contribuya a la continuidad del negocio, aplicando técnicas de seguridad alineadas con el estándar NC ISO/IEC 27001:2016. Se basa en una orientación a riesgos para garantizar la confidencialidad, integridad y disponibilidad de la información, así como en el análisis de los procesos claves de la organización para determinar planes y estrategias que garanticen la continuidad de la seguridad de la información.

La metodología consta de cuatro etapas y doce pasos, brindando solución al problema científico identificado. Durante su desarrollo se emplearon diferentes métodos teóricos de la investigación científica como: histórico-lógico, análisis y síntesis, inducción-deducción; además de métodos empíricos para caracterizar el problema y estadísticos para el análisis y procesamiento de los datos.

Se presentan los resultados de la aplicación de la metodología en la Oficina Territorial de Normalización de Holguín, la misma permitió la consolidación de una política de seguridad de la información, elevar la cultura de todo el personal referente a la seguridad de la información y determinar el nivel de madurez del sistema de gestión de seguridad de la información.

Se desarrolla una herramienta informática. Con su aplicación se conocen los tipos de activos de información por procesos, se optimiza la identificación de las amenazas asociadas, evaluando los niveles inaceptables del riesgo de cada una de ellas, para así seleccionar e implementar medidas para modificarlos y sean tratadas a tiempo o anticipadamente.

## **Abstract**

The objective of this research is to develop a methodology for information security management that contributes to business continuity, applying security techniques aligned with the NC ISO / IEC 27001: 2016 standard. It is based on a risk orientation to guarantee the confidentiality, integrity and availability of the information, as well as on the analysis of the key processes of the organization to determine plans and strategies that guarantee the continuity of the information security.

The methodology consists of four stages and twelve steps, providing a solution to the identified scientific problem. During its development, different theoretical methods of scientific research were used, such as: historical-logical, analysis and synthesis, induction-deduction; in addition to empirical methods to characterize the problem and statistics for data analysis and processing.

The results of the application of the methodology in the Territorial Office of Standardization of Holguín are presented, it allowed the consolidation of an information security policy, raising the culture of all personnel regarding information security and determining the maturity level of the information security management system.

A computer tool is developed. With its application, the types of information assets are known by processes, the identification of the associated threats is optimized, evaluating the unacceptable levels of risk of each one of them, in order to select and implement measures to modify them and be treated on time or in advance.

## Índice

<b>Introducción</b> .....	1
<b>Capítulo I Marco teórico práctico referencial</b> .....	6
<b>1.1 Seguridad de la Información.</b> .....	7
1.1.1 Principios básicos de la SI .....	9
1.1.2 Relación de la SI, la calidad y la continuidad del negocio .....	12
<b>1.2 La gestión de la SI y su continuidad</b> .....	14
1.2.1 Surgimiento, evolución y relación de los SGSI y SGCN .....	16
1.2.2 Gestión de riesgos de SI .....	17
1.2.3 La continuidad de la SI .....	19
<b>1.3 Metodologías, procedimientos y guías relacionadas con la gestión de la SI</b> .....	21
<b>1.4 Informatización del proceso de análisis de los riesgos de la SI y su plan de continuidad</b> .....	24
<b>1.5 Marco legal y normativo en SI en Cuba</b> .....	26
1.5.1 Estado actual en la OTNH de la gestión de la SI .....	28
<b>Conclusiones del capítulo</b> .....	31
<b>Capítulo 2: Metodología para la gestión de la SI como contribución a la continuidad del negocio</b> .....	32
<b>Etapa 1: Planificación del proyecto</b> .....	32
Paso 1 Compromiso de la alta dirección .....	33
Paso 2 Conformación del comité de SI.....	34
Paso 3 Concienciación y formación .....	35
Paso 4 Determinar el alcance del SGSI .....	36
<b>Etapa 2: Diagnóstico</b> .....	37
Paso 5 La organización y su contexto .....	37
Paso 6 Análisis de brechas.....	38
<b>Etapa 3: Desarrollo</b> .....	39
Paso 7: Gestión de activos .....	39
Paso 8: Análisis y evaluación de riesgos.....	41
Paso 9: Continuidad de la SI .....	46
<b>Fase 4: Verificación y mejora</b> .....	48
Paso 10. Monitoreo .....	48
Paso 11: Auditorías internas.....	49
Paso 12: Acciones de mejora.....	52

<b>Conclusiones del capítulo</b> .....	53
<b>Capítulo 3: Aplicación de la metodología para la gestión de la SI como contribución a la continuidad del negocio</b> .....	54
<b>Etapas 1: Planificación del proyecto</b> .....	54
Paso 1 Compromiso de la alta dirección .....	54
Paso 2 Conformación del comité de SI .....	55
Paso 3 Concienciación y formación .....	56
Paso 4 Determinar el alcance del SGSI .....	57
<b>Etapas 2 Diagnóstico</b> .....	59
Paso 5 La organización y su contexto .....	59
Paso 6 Análisis de brechas .....	64
Documentos obligatorios y registros requeridos por NC ISO/IEC 27001:2016 .....	66
<b>Etapas 3 Desarrollo</b> .....	67
Paso 7 Gestión de activos .....	67
Paso 8 Análisis y evaluación de riesgos .....	68
<b>Conclusiones del capítulo</b> .....	69
<b>Conclusiones generales</b> .....	70
<b>Recomendaciones</b> .....	71
<b>Referencias bibliográficas</b> .....	72
<b>Anexos</b> .....	76

## Introducción

Las actuales sociedades avanzadas son denominadas frecuentemente sociedades de la información, pues el volumen de datos que es procesado, almacenado y transmitido es inconmensurablemente mayor que en cualquier época pretérita. Además, no sólo el volumen sino la importancia de esta información para el desarrollo económico y social, no tiene parangón con la que tuvo en cualquier otra época. De hecho, en la actualidad, las empresas consideran que la información es un bien más de sus activos y en muchos casos prevalece sobre los restantes, por lo que la protección de esta es un objetivo prioritario para la operación del negocio. La información está cada vez más disponible en ambientes interconectados lo que genera un riesgo a posibles vulnerabilidades y amenazas por lo que se hace indispensable contar con mejores prácticas de seguridad de la información (SI) para minimizar los daños y asegurar la continuidad del negocio (Berrío López, 2016).

El avance de las Tecnologías de la Información y las Comunicaciones (TIC) durante los inicios del presente siglo, ha creado una dependencia tal para el desarrollo de las actividades de cualquier organización (empresa, organismo estatal, organización social) que el no poder contar con estas tecnologías en un momento determinado provoca un verdadero desastre, el cual, en función de su magnitud puede acarrear incluso la desaparición de la propia organización. Debido a la existencia de este riesgo se ha convertido en un aspecto estratégico vital de la política de las organizaciones, garantizar la SI, abordando un proceso donde se adopten los controles y procedimientos más efectivos y coherentes con la estrategia de negocio (Solarte Solarte, Enriquez Rosero, & Benavides Ruano, 2015) al cual se debe dar prioridad basado en estándares, modelos y normas que, a través de una serie de mejores prácticas, proporcione una adecuada gestión que les permita asegurar, tanto interna como externamente, que se está realizando una gestión eficaz de la información.

Con el surgimiento de la teoría de la organización, se acentuó la importancia de la información. Una organización es un sistema conformado por personas, recursos materiales e información (Aja Quiroga, 2002), por esta razón, deben considerarse a las organizaciones como sistemas de información.

Toda organización intercambia información con el entorno, por lo cual un objetivo fundamental es minimizar las pérdidas, modificaciones y divulgaciones no autorizadas de esta. Una estrategia global para darle cumplimiento a estos objetivos es la implementación de un sistema de gestión de la calidad (SGC) por la norma ISO 9001, enfocado a dirigir y controlar la organización en relación a la calidad. Sin embargo, a raíz del desarrollo de los sistemas de información y las TIC las organizaciones están obligadas a implementar controles adicionales

para conocer y medir los nuevos requisitos orientados a garantizar la SI. Es por esto que surge la necesidad de implantar un sistema de gestión de la seguridad de la información (SGSI) que forme parte y esté integrado con los procesos y con la estrategia de gestión global de la organización. El estándar ISO/IEC 27001 emplea la estructura de alto nivel, lo que facilita la integración entre los distintos sistemas de gestión que tienen en común el cumplimiento de requisitos. La gestión de la calidad se entiende como una resultante integradora de la gestión de la información con la calidad requerida, bajo el cumplimiento de los principios de confidencialidad, disponibilidad e integridad, para la supervivencia y mejora de la organización. Dentro de las estrategias más utilizadas internacionalmente para el logro de la competitividad y una mejor imagen de la organización se encuentran los enfoques de gestión de SI, entre los que se encuentra el enfoque normalizado según la ISO/IEC 27001. Los principios básicos de esta norma internacional han sido recibidos y asimilados por la esfera económica, y crece cada día más el número de organizaciones que adoptan programas de este tipo. Según la encuesta ISO Survey realizada por la Organización Internacional de Normalización (ISO) hasta septiembre de 2020 había un total de 36362 certificados presentes en 133 países, encontrándose en el tercer sistema de gestión más certificado después de ISO 9001 e ISO 14001.

El estándar ISO/IEC 27001:2016 mantiene una relación de confluencia en ciertos puntos con la norma ISO 22301:2019 “Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio – Requisitos”, que establece el código de un conjunto de buenas prácticas para la Gestión de Continuidad del Negocio (Business Continuity Management, BCM por sus siglas en inglés), pero sobre todo de complementación, logrando altos niveles de garantía en relación a la correcta evaluación, prevención, tratamiento y solución de riesgos relacionadas con las tecnologías de la información.

Con esta investigación se sostiene que ambos modelos de gestión brindan las herramientas necesarias para gestionar la SI y garantizar su continuidad en caso de presentarse hechos disruptivos que pongan en riesgo el correcto funcionamiento de la organización. Se consigue mediante la implantación de un conjunto adecuado de controles, que incluye políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware (NC ISO/IEC 27002,2016) considerando el entorno, contexto, activos de las TIC, información y factores externos e internos. Estos controles deberían establecer, implementar, revisar y mejorar cuando sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y de continuidad de la organización, con el fin de lograr una visión completa y coordinada de los riesgos de SI, reducir su impacto y garantizar su reanudación en caso de que se materialicen fallos importantes en los sistemas de información.

Cuba está inmersa en llevar la informatización a todos los niveles de la sociedad para contribuir a un mejor desarrollo económico del país. Para el período 2016-2021 se incluye en los Lineamientos de la Política Económica y Social del Partido y la Revolución, específicamente el 108 y otros de manera complementaria definen las áreas y sectores donde se debe avanzar estratégicamente en el proceso de informatización de la sociedad. El Plan Nacional de Desarrollo Económico y Social hasta 2030 también plantea la necesidad de fortalecer nuestra infraestructura tecnológica y por ende elevar la soberanía tecnológica en el desarrollo de la informática y las telecomunicaciones.

No solo el país está enfocado en el desarrollo de las TIC, sino que moviliza los recursos necesarios para lograr el empleo seguro y eficiente de las mismas en función de las necesidades que requiere el desarrollo. Esto de manera general constituye una ventaja para la implementación de un SGSI, destacando que reduce el riesgo de que se produzcan pérdidas de información en las organizaciones.

Si bien el país declara la importancia de la información y la necesidad de incentivar las medidas de control sobre esta, la SI es asumida de manera desarticulada, siendo tratada desde una perspectiva del control de la seguridad informática y la ciberseguridad en las empresas, observada como un simple tema de cumplimiento legal o un simple problema técnico. Tampoco es tratada como un suplemento para la continuidad de negocio, por lo que no disminuye el impacto y el caos ante cualquier incidente y que la organización esté preparada para tomar acciones pertinentes ante estos eventos.

La Oficina Territorial de Normalización de Holguín (OTNH) no está ajena a estos avances y por lo tanto está expuesta a un número cada vez más elevado de amenazas que aprovechando las vulnerabilidades existentes pueden someter a sus activos de información a diversas formas de fraude, espionaje, sabotajes o vandalismo. Se contemplan los virus informáticos o los riesgos de sufrir incidentes de seguridad, causados voluntaria o involuntariamente dentro de la propia organización o aquellos que puedan ser provocados accidentalmente por catástrofes naturales o fallos técnicos.

Estas particularidades crean la necesidad de desarrollar un mecanismo para salvaguardar los activos de información, pues se evidencia en los resultados de auditorías internas, revisiones por la dirección, supervisiones y otras actividades de seguimiento y medición a los procesos diferentes deficiencias en la gestión de la SI relacionados mayormente con: cultura y compromiso del personal, gestión de activos, gestión de riesgos, insuficientes políticas y procedimientos de SI, ausencia de herramientas informáticas para el monitoreo y control de la SI, falta de controles de SI para la gestión de eventos disruptivos o planes de continuidad para reanudar operaciones claves, ausencia de roles y responsabilidades de SI.



El estándar NC ISO/IEC 27001 establece los requisitos a cumplir para gestionar de forma segura la información pero no la técnica a emplear, de ahí la importancia de establecer una metodología que permita orientar cómo se debe abordar este tipo de procesos, con el respaldo de las normas internacionales promulgadas para la implementación de los controles dentro del SGSI, que proteja los activos de manera rentable a partir de un análisis de riesgos que determine qué activos se tratan de proteger, de qué se quieren proteger y por qué. Lo hasta aquí explicado constituye la situación problemática de la presente investigación, por lo que se definió el siguiente **problema científico**: ¿Cómo favorecer a la gestión de la seguridad de la información en la Oficina Territorial de Normalización de Holguín que contribuya a la continuidad del negocio?

Como **objeto de investigación** se definió: la seguridad de la información.

El **objetivo general** es: Desarrollar una metodología para la gestión de la seguridad de la información en la Oficina Territorial de Normalización de Holguín que contribuya a la continuidad del negocio.

Como **objetivos específicos** se definieron los siguientes:

- Determinar los principales enfoques, teorías y técnicas mediante el análisis y revisión documental que actualmente se utilizan para la evaluación, control y reducción de riesgos de la SI.
- Diseñar una metodología para la gestión de la SI en la Oficina Territorial de Normalización de Holguín como contribución a la continuidad del negocio.
- Aplicar la metodología para la gestión de la SI en la Oficina Territorial de Normalización de Holguín.

**Campo de acción:** La gestión de la SI en la Oficina Territorial de Normalización de Holguín.

En correspondencia con el problema científico, el objetivo general y el campo de acción se establece como **idea a defender** la siguiente: El desarrollo de una metodología para la gestión de la SI en la Oficina Territorial de Normalización de Holguín contribuirá a la continuidad del negocio.

En el proceso de la investigación se utilizaron métodos teóricos, empíricos y estadísticos:

Teóricos:

Históricos - lógico: se utiliza para realizar análisis lógicos de la situación problemática, para su comportamiento histórico evolutivo y para la construcción del marco teórico y práctico de la investigación.

Analítico - sintético: para analizar y sintetizar la información que se necesita a partir de la revisión de bibliografías, para el tratamiento y resumen de la información y la elaboración de conclusiones.

Inducción – deducción: al realizar generalizaciones con respecto a las posiciones teóricas y al elaborar y aplicar la metodología para la gestión de la SI, para arribar a conclusiones particulares a partir de la misma.

Empíricos:

La observación directa para caracterización del problema.

Entrevistas a trabajadores para constatar el nivel de conocimiento para evaluar la situación actual en cuanto a la gestión de la SI en la OTNH.

Revisión documental en literatura especializada, además en registros, manuales y procedimientos establecidos para los procesos de la OTNH.

Métodos estadísticos: El análisis de centralidad, análisis de frecuencia por variables, análisis de conglomerados jerárquico por variables. Para el procesamiento de los datos se utilizaron los softwares SPSS V. 19.0; UCINET, QDA MINER LITE y hojas de cálculo EXCEL.

Para su presentación, esta investigación se estructura de la forma siguiente: un capítulo I, que contiene el marco teórico práctico referencial que sustenta la investigación; en el capítulo II, se describirá el instrumental metodológico desarrollado y un capítulo III, donde se presentan los resultados de su aplicación parcial en la OTNH, así como conclusiones y recomendaciones derivadas de la investigación; la bibliografía consultada y finalmente, un grupo de anexos de necesaria inclusión, como complemento de la investigación realizada.

## Capítulo I Marco teórico práctico referencial

Este capítulo está estructurado en cinco epígrafes que permiten realizar la fundamentación teórica de la investigación como resultado de consultas de bibliografías especializadas. Se realizó un análisis de los conceptos fundamentales asociados a la SI y su evolución a raíz de los avances tecnológicos, se analizan los distintos enfoques investigativos de la SI para luego desarrollar una valoración general de las metodologías, procedimientos y guías aplicados en el mundo y en Cuba. También se realiza una caracterización del estado actual del SGSI en la entidad objeto de estudio.

El hilo conductor seguido para desarrollar el marco teórico y práctico referencial se muestra en la figura 1:

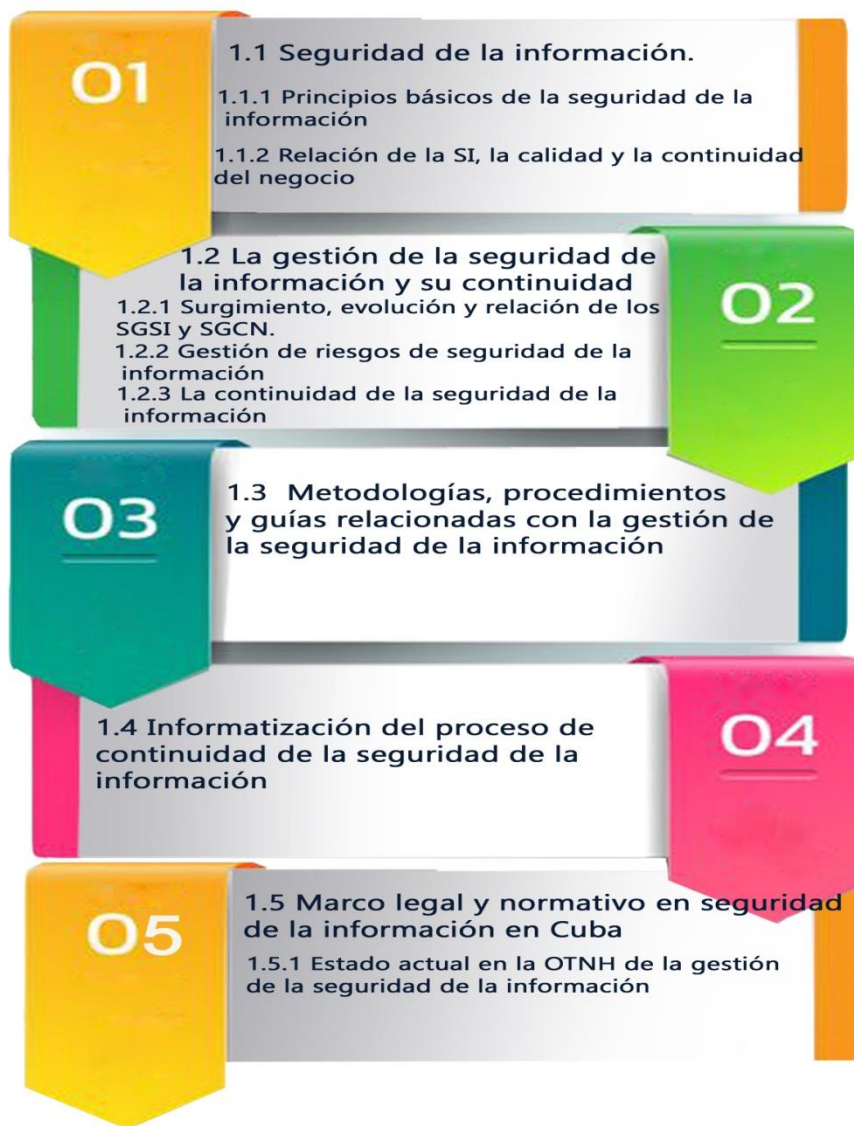


Figura 1. Hilo conductor del marco teórico práctico de la investigación

### 1.1 Seguridad de la Información.

Cuando se aborda el término "SI", debe analizarse primeramente qué significado tiene la información de forma independiente. Según la Asociación Española de Normalización y Certificación (AENOR, 2010) la información es uno de los principales activos de las organizaciones, es el conjunto de datos organizados en poder de una entidad que poseen valor para la misma, independientemente de la forma en que se archive o transmita, de su origen o de la fecha de creación.

(Murillo Varón, Bonilla Pineda, & Buitrago Estrada, 2012) consideran que dependiendo del valor que posea la información para la organización, puede clasificarse como:

**Crítica:** Es indispensable para la operación de la empresa.

**Valiosa:** Es un activo muy importante para la empresa.

**Sensible:** Solo debe ser conocida por las personas autorizadas.

La NC ISO/IEC 27000 conceptualiza a la SI como la preservación de la confidencialidad, integridad y disponibilidad de la información y se basa en la gestión de riesgos y su control sistemático.

Las organizaciones han de establecer estrategias y controles adecuados que garanticen una gestión segura de los procesos del negocio, por lo que (Gaona Vásquez, 2013) sustenta en su investigación que la SI es la implantación de un conjunto adecuado de controles, políticas, procedimientos, estructuras organizativas y funciones de software.

Garantizar la seguridad total es inalcanzable, pero mediante un proceso de mejora continua se puede conseguir un nivel de seguridad altamente satisfactorio, que reduzca al mínimo los riesgos a los que se está expuesto y el impacto que ocasionarían si efectivamente se produjeran (Andrés & Gómez, 2009), por lo que este investigador plantea que la SI es la preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

Por su parte (Isaca, 2012) defiende una idea más contemporánea planteando que a pesar de que la SI es un tema que le compete a cualquier organización independientemente de su enfoque de negocios o área de productividad, es más común que los SGSI sean implementados por organizaciones que están relacionadas con las tecnologías de la información.

La SI es muy extensa, no es sólo una cuestión técnica sino que supone una responsabilidad de la alta dirección, por lo que (Figuroa-Suárez, Rodríguez-Andrade, Bone-Obando, & Saltos-Gómez, 2018) consideran que la SI debe estar básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas.

Para (Guamán, Vivar, Rivera, & Calderón, 2019) la SI es el conjunto de medidas preventivas y reactivas que las organizaciones deben generar y aplicar políticas, normas, procedimientos, evaluar el riesgo, planes de contingencia, entre otras medidas, con el objetivo de mantener y asegurar la confidencialidad, integridad y disponibilidad de la información, mediante un proceso de gestión de riesgo que garantice la reducción o eliminación de estos.

Una importante reflexión lo constituye la pronunciada por (Murillo Varón et al., 2012) que plantea que la SI es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

(Chilán-Santana & Pionce-Pico, 2017) consideran a la información como uno de los principales recursos de las organizaciones, que debe protegerse de todas las amenazas que pueden poner en peligro a la empresa, por lo que los investigadores sustentan que la SI, tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, disrupción o destrucción no autorizada.

Aunque se cuente con un presupuesto ilimitado la información nunca estará fuera de los peligros asociados al desarrollo de las TIC. El objetivo a perseguir es garantizar que los riesgos de la SI sean conocidos, asumidos, gestionados y minimizados (Maldonado & Cano, 2014).

Las organizaciones poseen información que debe ser protegida frente a riesgos y amenazas para asegurar su correcto funcionamiento es por lo que (Delgado, 2014) sostiene en su investigación que la SI es el conjunto de medidas preventivas y reactivas de las organizaciones que permiten resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad.

(Murillo Varón et al., 2012) refiere que la SI involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto clave el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo. O sea, que ayuden a proteger tanto la información como los sistemas que la almacenan y administran. La SI incumbe a gobiernos, entidades militares, instituciones financieras, hospitales y empresas privadas con información confidencial sobre sus empleados, clientes, productos, servicios, investigación y su situación financiera.

Las definiciones de SI aportadas por los investigadores varían de acuerdo a los campos de la ciencia que los estudian. El análisis de la literatura consultada muestra que las definiciones no han sido conceptuadas de forma íntegra, sino fragmentada, de acuerdo al enfoque y valoración de cada disciplina, incrementando la complejidad en la que es entendido por las personas. La autora se auxilia de la herramienta QDA Miner Lite para realizar un análisis cualitativo de

frecuencia por variables graficando la presencia de los siguientes términos en los conceptos estudiados (figura 2).

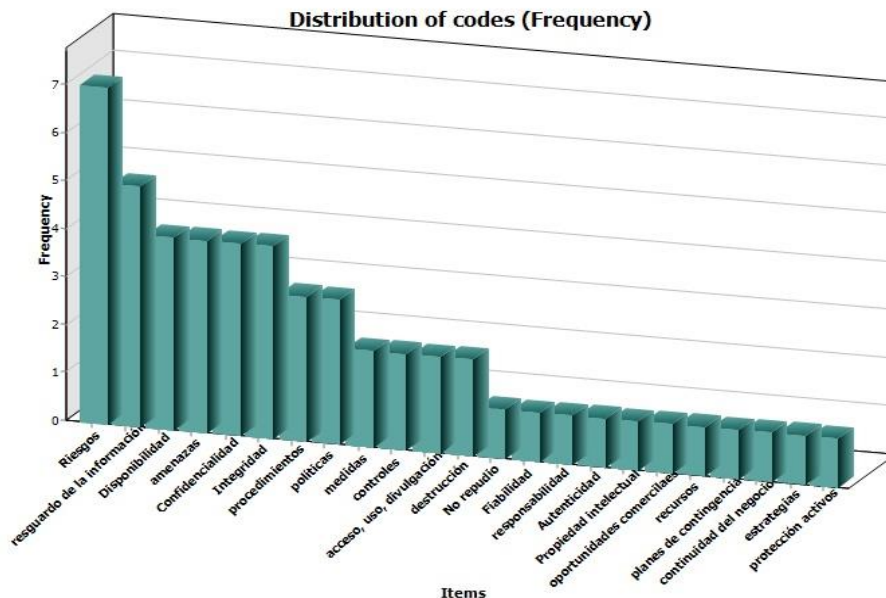


Figura 2. Análisis cualitativo de frecuencia por variables

El análisis de los diferentes conceptos de SI permitió apreciar una concordancia entre los autores en cuanto a la utilización de los términos riesgos y resguardo de la información como las de mayor incidencia para definir la SI y como una variable aislada continuidad del negocio, tratada de forma superficial por pocos autores.

A través de este análisis la autora asume el concepto planteado por la autora Carol Estefanie Murillo Varón abarcando el mayor índice de frecuencia de las variables abordadas en los diferentes términos analizados, también por abordar en su definición la continuidad del negocio, aunque en el análisis realizado refleja el menor índice de frecuencia es objetivo que persigue esta investigación.

### 1.1.1 Principios básicos de la SI

La confidencialidad, integridad y disponibilidad (conocidos como la tríada CIA, del inglés: “Confidentiality, Integrity, Availability”) han sido siempre considerados como los principios básicos de la SI (Tejena-Macías, 2018).

La gestión de la SI persigue el establecimiento y mantención de controles, políticas y programas que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, así lo considera dentro de sus requisitos la norma cubana NC ISO/IEC 27001 en su versión del 2016.

Cuando alguno de estos principios es violado, la información no está segura. La seguridad no es un hito, sino un proceso continuo que debe ser gestionado conociendo siempre las

vulnerabilidades y amenazas que existen sobre cualquier información, teniendo siempre en cuenta las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener para la organización, para adoptar oportunamente las medidas de seguridad necesarias.

Autores como (Fernández & Álvarez, 2012) considera como principios de SI la confidencialidad, la integridad y la disponibilidad de la información, pero él amplía este concepto planteando, que además puede abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

### **Confidencialidad**

La confidencialidad es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. Asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización (Andrés & Gómez, 2009).

Otros autores como (Areitio Bertolín, 2008) plantea en su investigación que la confidencialidad busca prevenir el acceso no autorizado, ya sea en forma intencional o no intencional a la información. La norma NC ISO/ISO 27001 considera a la confidencialidad como la garantía de que la información no sea accesible para personas no autorizadas.

La pérdida de la confidencialidad de la información puede adoptar muchas formas, ejemplo cuando la información se pone a disposición y se revela a individuos, entidades o procesos no autorizados, así lo considera (Sánchez Torres, 2014).

### **Integridad**

La integridad es mantener con exactitud la información tal y como fue generada libre de modificaciones, sin ser alterada por personas o procesos no autorizados. La violación de integridad se presenta cuando un empleado, programa o proceso modifica o borra datos importantes que son parte de la información.

(Andrés & Gómez, 2009) en su aporte de una Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información, consideran que la información es íntegra cuando es exacta y completa.

Autores como (Areitio Bertolín, 2008) tienen un concepto más amplio de la integridad al plantear que no solo busca asegurar las no modificaciones por personas no autorizadas a los datos o procesos, sino que tampoco se realicen modificaciones no autorizadas por personal autorizado y que estos sean consistentes tanto interna como externamente.

La NC ISO/IEC 27001:2016 refiere que la integridad protege la información y los sistemas para que no sean modificados por personas no autorizadas.

### **Disponibilidad**

En los sistemas informáticos los controles de seguridad utilizados para proteger los canales de comunicación que se utilizan para acceder a la información deben estar funcionando

correctamente. La información debe estar disponible en todo momento, evitando interrupciones de los servicios debido a cortes de energía, fallos de hardware o de software, previniendo ataques de denegación de servicios, etc.

La disponibilidad según (Sánchez Torres, 2014) es el acceso y utilización de la información y los sistemas de tratamiento de la misma, por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

La NC ISO/IEC 27000 categoriza a la disponibilidad como la propiedad de ser accesible y estar listo para su uso a demanda de una entidad autorizada.

### **Autenticidad**

El garantizar que la fuente de información es quien dice ser, o quien accede o modifica los datos es quien tiene que hacerlo, puede suponer que la información pierda totalmente su valor, no sea fiable su calidad y por tanto se haya perdido el activo de información.

Según la Real Academia Española (RAE) es la certificación con que se testifica la identidad y verdad de algo.

Según la NC ISO/IEC 27000 la autenticidad es la propiedad consistente en que una entidad es lo que dice ser.

Autores como (Solarte Solarte et al., 2015) la categorizan como el saber exactamente quien hace o ha hecho cada cosa.

### **Trazabilidad**

Disponer de un control completo de las acciones y usos que se le da a un determinado activo, de quien las realiza y en qué momento, puede ser necesario para garantizar su calidad.

Según (Solarte Solarte et al., 2015) la trazabilidad es saber a quién se le presta el servicio.

La trazabilidad es entendida por los autores (Moltoni & Moltoni, 2015) como un conjunto de acciones, medidas y procedimientos técnicos con el fin de identificar y registrar.

### **Fiabilidad**

La RAE la categoriza como la probabilidad de buen funcionamiento de algo.

La NC ISO/IEC 27000 la define como la propiedad relativa a la consistencia en el comportamiento y en los resultados deseados.

Autores como (Prieto & Delgado, 2010) la conceptualizan como la consistencia o estabilidad de las medidas cuando el proceso se repite.

### **No repudio**

La NC ISO/IEC 27000 lo define como la capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron.



El análisis de las diferentes literaturas relacionadas con los principios de la SI demuestra que los conceptos no son considerados de forma íntegra, sin embargo, se aprecia un alto nivel de concordancia en cuanto a los términos confidencialidad, integridad y disponibilidad. También los autores analizados tienen presentes propiedades como la trazabilidad, la autenticidad y el no repudio. La autora se auxilia de la herramienta QDA Miner Lite para realizar un análisis cualitativo de frecuencia por variables graficando la presencia de los siguientes términos en los conceptos estudiados (figura 3).

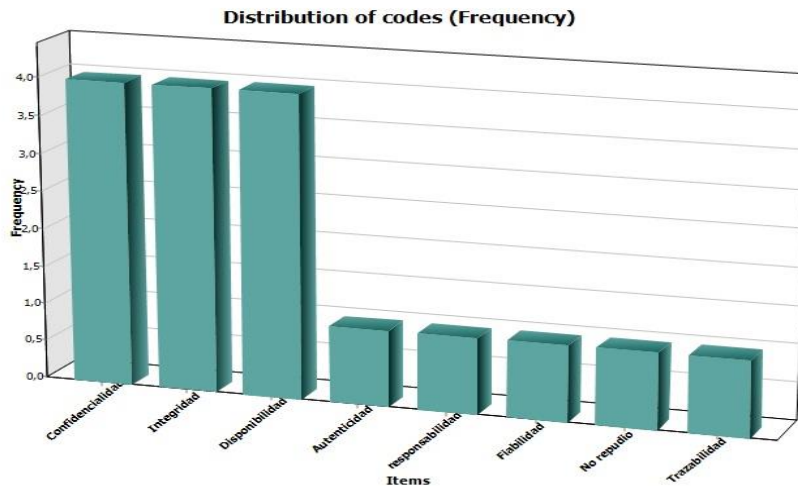


Figura 3. Análisis cualitativo de frecuencia por variables

Después del análisis realizado la autora adopta lo referenciado en la NC ISO/IEC 27001 que plantea que para que la información se considere segura tiene que preservar la confidencialidad, integridad y disponibilidad de la información. Estos principios contribuyen a la exitosa implementación de un SGSI y coinciden con lo exigido en el requisito para la información documentada de un SGC.

### 1.1.2 Relación de la SI, la calidad y la continuidad del negocio

Las organizaciones dependen de sus clientes y por lo tanto deberían comprender sus necesidades, satisfacer sus requisitos y exceder sus expectativas. Los principios de calidad de Deming, Ishikawa, Juran y Crosby se usan para mejorar la calidad de los productos; también en la actualidad se emplean estos principios en la gestión de la información (Olivera Argota, 2019). El estándar NC ISO/IEC 27001 es la norma internacionalmente reconocida para la gestión de la SI. Este modelo se centra en salvaguardar la información crítica de la organización, ya sea de origen externo o generada por la propia organización. La información es considerada un bien más y su valor varía según el tipo de documentación con la que opera y controla los procesos, además de ofrecer soporte para recoger la información enfocada a la documentación de los sistemas implementados. La documentación también es un requisito abordado por el estándar

NC ISO 9001. Se define de forma más genérica, especificando como información documentada la que se tiene que controlar y mantener, así como el medio en que se encuentra contenida (IsoToolsExcelence, 2016).

La implementación del SGSI soportará toda la información documentada según la estructura de gestión global implementado por la organización, para asegurar su buen desempeño. Esta es necesaria para demostrar la eficacia, proporcionando referencias de los estándares definidos y evidencias del cumplimiento o no de los requisitos. La información documentada se conservará como evidencia de la conformidad y se tiene que proteger frente a posibles modificaciones no intencionadas (NC/ISO-9001, 2015).

La SI es responsabilidad de la organización, al ser el apoyo de las industrias en el control de calidad de sus procesos, productos y servicios, planteando como objetivo asegurar resultados confiables a los clientes y partes interesadas (Murillo Varón et al., 2012). Estos controles deben garantizar que la información documentada requerida por el sistema esté disponible para su uso y sea protegida adecuadamente contra la pérdida de confidencialidad e integridad, principios que garantiza la implementación del estándar NC ISO/IEC 27001. Esta idea también es defendida por el autor (Maravilhas, 2015), en su investigación declara que para ser considerada de calidad, la información debe presentar criterios como la integridad, accesibilidad, exactitud, precisión, objetividad, consistencia, relevancia, puntualidad y transparencia.

Los enfoques normalizados para planear y operar los diferentes sistemas de gestión, aún respondiendo a distintas dimensiones, permite que puedan alinearse e integrarse gracias a la estructura de alto nivel que emplean. Ambos estándares promueven la estrategia de procesos. Persiguen garantizar un adecuado nivel de SI a través de la identificación, la valoración y el tratamiento de los riesgos a los que están sujetos los productos/servicios prestados a la propia clientela y enfocado a aumentar su satisfacción. Es por lo que (Canchari Pastor, 2014) plantea que la calidad de la información y análisis que respalda las decisiones de las empresas, se enfatiza en la necesidad de aplicar sistemas que les permitan identificar, medir, controlar y monitorear sus riesgos de una manera eficiente.

Ambos modelos contemplan la continuidad de negocio como un elemento clave dentro su gestión. Según (Castro Marquina, 2013) crear un SGSI es vital para preservar la continuidad del negocio. (IsoTools Excelence, 2016) acuña a la continuidad de negocio como el término para referirse a las estrategias y planificación mediante las cuales las organizaciones se preparan para dar respuesta a eventos catastróficos tales como incendios, inundaciones, ataques cibernéticos, accidentes o errores humanos.

La implementación de los requisitos del estándar ISO 22301 sería una estrategia para asegurar la continuidad de los procesos, actividades y servicios a los cuales la organización se

compromete ante los clientes. Esta estrategia estará enfocada en minimizar el tiempo de interrupción tras la materialización de eventos disruptivos, ya sean naturales o no, accidentales o provocados, relacionados con los activos de información, cuyas consecuencias puedan poner en serio riesgo la continuidad de la SI.

La norma ISO 22301 es una norma internacional susceptible de aplicarse a todo tipo de organizaciones, que quieran diseñar y ejecutar un plan de continuidad de su negocio. Describe los procesos y procedimientos a funcionar para garantizar que las funciones críticas puedan continuar durante y después de un desastre. Es fundamental para las organizaciones donde la habilidad de continuar trabajando es de suma importancia para el negocio, clientes y partes interesadas.

Es objetivo de esta investigación profundizar dentro de este enfoque, ya que la NC ISO/IEC 27001 solicita dentro de sus requisitos la implementación de la continuidad de la SI. Resumiendo, esta sección insta que se planifiquen, se implementen y se desplieguen todos los temas relacionados a la continuidad del negocio dentro del alcance del SGSI, enfocándose no solo en la implementación, sino en la verificación, revisión y pruebas periódicas, para poder determinar si son adecuados o no. La disponibilidad de las instalaciones de procesamiento de información, las exigencias de disponibilidad, puede aconsejar el mantenimiento de sistemas redundantes, que permitan reaccionar en tiempo real a la caída de sistemas o activos de información estratégicos para la organización.

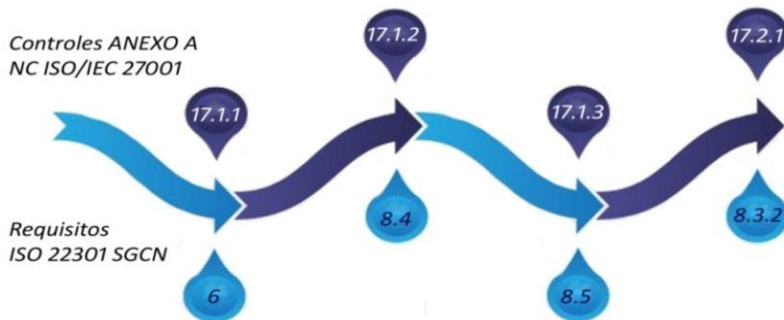


Figura 4: Puntos en común NC ISO/IEC 27001 e ISO 22301, fuente: elaboración propia

## 1.2 La gestión de la SI y su continuidad

Un SGSI es para una organización el diseño, implantación, mantenimiento y mejora de un conjunto de procesos que permiten gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información y minimizar los riesgos de SI.

(Maldonado & Cano, 2014) refieren que este término es utilizado principalmente por la ISO/IEC 27001 constituyendo su base central, aunque no es la única normativa que lo utiliza.

Los SGSI son el camino más efectivo de minimizar los riesgos vinculados con la información, al asegurar en su gestión el tratamiento de los activos y el análisis y evaluación de riesgos, donde se empleen los controles más efectivos vinculados con la estrategia de negocio de la organización.

Como todo proceso de gestión, un SGSI debe seguir siendo eficaz durante un largo tiempo, adecuándose a los cambios internos que pueda sufrir la organización como los de su entorno.

A raíz del establecimiento de regulaciones para el manejo, respaldo y uso de la información, creadas por los considerados rectores de las organizaciones bancarias como el Financial Services Authority (FSA) en Reino Unido y el Securities Exchange Commission (SEC) en Estados Unidos, se propulsa la continuidad del negocio (González Villalobos, 2015).

Según (Drewitt, 2013) la gestión de la continuidad del negocio es la disciplina que prepara a una organización para lo inesperado. Es un proceso de gestión que ofrece un marco de trabajo para darle resiliencia a la operación ante riesgos de interrupción, de tal manera que se garantice la continuidad en los servicios críticos.

Rodrigo Ferrer plantea en su aporte de una Metodología para la Gestión de la Continuidad del Negocio", publicado en 2015 que "La gestión de la continuidad de negocio (GCN) busca sostener en niveles previamente definidos y aceptados, los productos y servicios críticos del negocio a través de la estructuración de procedimientos, tecnología e información, los cuales son desarrollados, compilados y mantenidos en preparación para su uso durante y después de una interrupción o desastre, con el fin de proteger los intereses de las partes interesadas, la reputación, las finanzas, los activos críticos y otros aspectos generadores de valor".

Un SGCN bajo la óptica de la norma ISO 22301 ayuda a las organizaciones a prepararse para las emergencias, a gestionar las crisis y mejorar su capacidad de recuperación operacional, asegurar la cadena de suministro y proteger su reputación ante una crisis (IsoTools Excellence, 2016).

Según (ISO, 2012) referenciado por el autor (González Villalobos, 2015) los SGCN son sistemas holísticos que se encargan de administrar, establecer, implementar, monitorear y mantener la continuidad del negocio.

(Castro-Marquina, 2013) en su diseño de un sistema de un SGCN bajo los principios de este mismo estándar plantea que tiene como fin contrarrestar interrupciones en las actividades empresariales y en los procesos críticos de negocio derivados de fallos importantes en los sistemas de información y garantizar su reanudación. Esta norma indica que crear un SGSI es vital para preservar la continuidad del negocio.

### **1.2.1 Surgimiento, evolución y relación de los SGSI y SGCN**

Las computadoras facilitan el procesamiento de datos y por ende el desarrollo de muchos procesos de negocios. Sin embargo los riesgos a los que está expuesta la información en medio del tránsito hacia la digitalización, la falta de fiabilidad de estos equipos, la forma en la que se maneja, el formato en que se almacena (datos, video, voz) en medios tradicionales o magnéticos, revelaron la pronta necesidad de mitigar cualquier evento adverso para la organización (Drewitt, 2013). Debido a esta necesidad constante de acceso a la tecnología, para expertos como Tony Drewitt, sería la base para la continuidad del negocio, ya que la base para hacer negocios involucraba el uso de ordenadores, la criticidad de los mismos y el crecimiento exponencial de los datos (González Villalobos, 2015).

La NC ISO/IEC 27001 se encarga de toda la SI, incluyendo los controles establecidos en su anexo A y su código de práctica NC ISO/IEC 27002. Debe regularse bajo estos controles y está enfocada en la aplicación de un sistema de gestión de SI, lo cual permite que haya confidencialidad, integridad y acceso a la información.

La actual norma NC ISO/IEC 27001 y su código de práctica NC ISO/IEC 27002 datan de 2016 cuando fueron adoptadas por Cuba como normas cubanas con las siglas NC, ambas provienen de su versiones en inglés publicadas en 2013 por la Organización Internacional de Normalización y por la Comisión Electrónica Internacional (IEC por sus siglas en inglés), pero descienden de una larga estirpe de normas, algunas ya ISO y otras eran publicadas por el British Standard Institution (BSI por sus siglas en inglés).

En 1995 el BSI publica la norma BS 7799-1, con objeto de proporcionar a cualquier organización un conjunto de buenas prácticas para la gestión de la SI, lo que se recoge actualmente en el estándar ISO/IEC 27002. Posteriormente se realizó la segunda parte de la norma en 1998, en la que establecieron los requisitos, para realizar un sistema de Gestión de la SI la que hoy se conoce como ISO/IEC 27001. En el año 1999 se realiza una revisión conjunta de ambos estándares británicos dando origen a la norma internacional ISO 17799 sustituyendo a la BS 7799-1. Posteriormente en el año 2005 ambas se adoptan como normas ISO/IEC de la familia 27000.

En todos estos modelos normalizados llegando hasta sus versiones del año 2005 se solicitaba dentro de sus objetivos de control que las organizaciones implanten continuidad del negocio, lo cierto es que estos requisitos podían ser un poco confusos y quedaba poco claro como implantar un sistema de continuidad del negocio, estas carencias venían suplidas por otras normas, en aquel entonces las BS 25999-1/2 publicadas en noviembre del 2007 por el BSI para tratar la gestión del plan de continuidad del negocio(Granda, Espinosa, & Vásquez, 2017), que provenían del Publicly Available Specification 56 (PAS 56) publicado por el BSI en la década del

90 (Drewitt, 2013), fundamentalmente enfocado a la disponibilidad de la información, que sirvieron en gran medida de base para un nuevo estándar internacional de continuidad de negocio, la ISO 22301 de 2012.

Actualmente la versión vigente es del año 2019 titulada “Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio – Requisitos”. Por lo tanto, cuando se realiza la revisión y actualización de ambos estándares de SI ya no tenía sentido venir a solicitar lo mismo que ya se pedía en otra norma, por lo que su versión de 2013 introdujo cambios relevantes. En resumen, el punto de control A 17 del estándar NC ISO/IEC 27001 solicita la planificación, implementación, verificación, revisión, pruebas periódicas y mejora, para garantizar la continuidad de la SI, que viene apoyada para su implantación de las técnicas de seguridad recogidas en el modelo NC ISO/IEC 27002.

Tanto la SI como la continuidad del negocio tienen como base para el cumplimiento de sus objetivos un eficaz proceso de gestión de riesgos. Los riesgos de la SI pueden afectar la confidencialidad, integridad y disponibilidad de un activo de información, es por lo que se deben aplicar los controles establecidos, orientados a mitigar los riesgos encontrados, de manera que se encuentren por debajo del nivel asumido por la organización. La continuidad del negocio por su capacidad de resiliencia tiene características previsoras, cuenta con respuestas oportunas ante eventos disruptivos que puedan dañar los procesos críticos de la organización, lo que conlleva a la pronta recuperación de los procesos claves ante los posibles impactos en caso de manifestarse.

### **1.2.2 Gestión de riesgos de SI**

Como es de conocimiento general, toda organización se encuentra expuesta a riesgos; debido a que no existe un entorno 100% seguro, ya que la exposición de riesgos es constante. Por tal motivo toda organización deberá estar alerta a cualquier cambio o situación extraña y que considera que podría afectar negativamente a un activo, a un dominio o a toda su organización (Gaona Vásquez, 2013).

(Castro & Bayona, 2011) refieren en su investigación que la materialización de riesgos puede implicar impactos grandes sobre el negocio, asociado a altos costos por recuperación e indisponibilidad de los servicios o productos que ofrece la organización.

Parte importante y relevante de la continuidad de la SI es la gestión de riesgos y su adecuado tratamiento evita que sean activados los planes de continuidad. Es fundamental que sean efectivos, se tengan claros los riesgos asociados y el efecto sobre los activos de información de la organización.

La apreciación de los riesgos de SI y el proceso de tratamiento recogido en la NC ISO/IEC 27001 se alinean con los principios y directrices genéricas definidos en la NC ISO 31000:2018.

Según NC ISO 31000, el riesgo es el efecto de la incertidumbre sobre la consecución de los objetivos.

La NC ISO/IEC 27001 considera al riesgo como la probabilidad de que las amenazas aprovechen vulnerabilidades que afecten a los activos de información y causen daño a la organización.

El estándar IEEE 1228-1994 define el riesgo como una métrica que combina la probabilidad de que un peligro cause un accidente y la severidad del mismo.

Un riesgo de un proyecto o activo, es un evento o condición incierta que, si se produce tendrá un efecto positivo o negativo sobre al menos un objetivo del proyecto o activo, como tiempo, costo, alcance o calidad.

El análisis y gestión de riesgos son procedimientos formales para encontrar los riesgos que existen en un sistema de información y mediante un estudio responsable, recomienda medidas apropiadas que deberían acogerse para controlarlos, además se podrá saber el estado real de seguridad en una empresa (Gaona Vásquez, 2013).

Según (ISOTools Excellence, 2014) se debe analizar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información, evaluando de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades e impactos en los activos.

(Tejena-Macías, 2018) plantea la existencia de varias metodologías y estándares de análisis de riesgos como: OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS y NIST SP 800-30 e ISO 31000, las cuales se orientan hacia el mismo objetivo, pero tienen características propias que las hacen atractivas para las empresas en todos los sectores, brindar estrategias y consejos para desarrollar un mayor grado de madurez en la SI. Sin embargo, la implementación de alguno de ellos, requiere consideraciones adicionales. En el anexo 1 se muestra una tabla comparativa con las ventajas y desventajas que presentan las antes mencionadas.

El estándar (NC ISO/IEC 27001, 2016) establece la figura de dueño del riesgo, asociándose cada amenaza potencial o real a un responsable, que es la persona que se asegura que se lleven a cabo las distintas actividades.

En la SI se lleva a cabo la clasificación de las alternativas para manejar los posibles riesgos que un activo de información puede tener dentro de los procesos de organización. Esta clasificación se denomina tratamiento de riesgos, la cual conlleva una estructura bien definida, con un control adecuado y su manejo; habiéndolos identificado, priorizados y analizados a través de acciones factibles y efectivas. Una organización puede afrontar el riesgo básicamente de cuatro formas diferentes: eliminarlo, reducirlo, trasladarlo o asumirlo (Valencia & Alzate, 2017).

**Asumir el riesgo:** Se acepta la pérdida probable y se elabora un plan para su manejo.

**Reducir el riesgo:** Implica tomar medidas de prevención para disminuir el riesgo como medidas de protección para disminuir el impacto.

**Transferir el riesgo:** Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones.

**Evitar el riesgo:** Se toman medidas para evitar su presencia.

La selección de un marco de referencia que permita la gestión de los riesgos de SI de la organización es uno de los objetivos que se pretende alcanzar en esta investigación. Después de evaluar los factores internos y externos en que se manifiesta el objeto de estudio, las ventajas y desventajas de alguna de las metodologías existentes, se propone la norma NC ISO 31000:2018, adaptada a los modelos nacionales y armonizada con el estándar NC ISO/IEC 27001 que en la cláusula 6 sugiere la utilización de este estándar y para homogeneizar los resultados, específicamente para la clasificación de los activos y determinar las amenazas asociadas se propone MAGERIT, como una metodología que expone terminologías y criterios que permiten comparar e integrar el análisis realizado (Magerit, 2012), ya que estos se encuentran entre los principales elementos para el análisis de riesgo.

### **1.2.3 La continuidad de la SI**

Hoy en día toda organización depende, aunque sea en un porcentaje mínimo de alguna TIC, aunque existen muchos soportes documentales diferentes, como la información en papel o los soportes analógicos, lo cierto es que la mayor parte del procesamiento de los datos, almacenamiento y transmisión de la información por una organización se sustenta de forma digital. Por estas razones el autor (Drewitt, 2013) plantea en su investigación que la falta de fiabilidad de estos equipos y el riesgo potencial de perder información, revelaron la pronta necesidad de mitigar cualquier evento adverso para la organización.

Tomando como referencia que las organizaciones dependen de su información y la consideran un bien más de sus activos y en muchos casos prevalece sobre los restantes, los autores (Murillo Varón et al., 2012) en su contribución de una metodología para la implementación del SGSI plantean que la protección de esta es un objetivo prioritario para la operación del negocio. Las tecnologías son un detonante clave para la aparición de riesgos a los que están asociados amenazas y vulnerabilidades por lo que se deben desarrollar estrategias para prever ataques que perjudiquen la confidencialidad, integridad y disponibilidad de la información.

Ante estos posibles impactos se eleva aún más la necesidad de tener un plan de continuidad de la SI, que permita disponer de la infraestructura para recuperar las copias de seguridad en situaciones de desastre. Esto no sólo permitirá proteger la información crítica ante una posible destrucción total, sino que también hará posible el análisis de los procesos, para volver a la normalidad en caso de desastre parcial o total de los procesos claves de la organización.



(Bautista, 2014) en su investigación refiere que un plan de continuidad del negocio es proporcionar procedimientos para mantener en funcionamiento los servicios críticos de la organización a causa de una interrupción de los mismos mientras se realiza la recuperación, en caso de un desastre natural o causado por humanos.

El primer paso para estar preparados ante incidentes disruptivos siempre será identificar todos aquellos sucesos naturales o no, relacionados con los activos de información, cuyas consecuencias puedan poner en serio riesgo la continuidad de la SI de los procesos claves de la organización. Dado que el impacto en la relación con los clientes, o sus costos económicos, podrían hacer que la organización llegase a cerrar.

(Lizbeth Morales, 2010) defiende en su investigación que la gestión de la continuidad de la información tiene como objetivo garantizar la pronta recuperación de los procesos críticos relacionados con las tecnologías de la información tras un desastre, y evitar en la medida de lo posible las perniciosas consecuencias de un desastre o causa de fuerza mayor.

(Granda et al., 2017) plantea la necesidad de conocer las diferencias y el alcance entre el plan de continuidad de negocio (BCP) y el plan de recuperación de desastre (DRP), un BCP es una estrategia de mitigación, y facilita la recuperación rápida de las operaciones de negocio críticas e incluye a todas las partes o funciones de la organización; el DRP en cambio, es un plan de recuperación que da respuesta de emergencia del área de TIC, referente a los componentes de hardware y software, enfocado en las interrupciones que requieren reubicación en centros alternativos, por lo que obvia interrupciones menores que no necesitan de este tipo de tratamientos, DRP es un subconjunto del BCP.

El BCP proporciona a la organización el plan de negocios estratégico a largo plazo para la continuación después de una interrupción, mientras que un DRP es más táctico y proporciona un plan de corto plazo para hacer frente a las interrupciones específicas orientadas a TI (Zhang & McMurray, 2013).

Un BCP es un plan de mitigación que utiliza el análisis de impacto del negocio, el cual determina procesos críticos que deben ser tomados en cuenta y la rapidez con que éstos deben recuperarse a fin de estar dentro del Tiempo Máximo Tolerable de Interrupción (Maximum Tolerable Down time, MTD por sus siglas en inglés), si este límite es sobrepasado, la empresa podría desaparecer del mercado (Boehmer, 2009; Faertes, 2015; Zambon, Bolzoni, Etalle, & Salvato, 2007).

Un factor del BIA, es el Tiempo Objetivo de Recuperación (Recovery Time Objective, RTO por sus siglas en inglés) indica el tiempo disponible para recuperar sistemas/recursos de información que han sufrido una alteración.

Otro factor es el Punto de Recuperación Objetivo (Recovery Point Objective, RPO por sus siglas

en inglés), se refiere a la dimensión de pérdida de datos en términos de un periodo de tiempo que puede ser permitido por un proceso.

Además de MTD, RTO y RPO otro factor resultante del BIA es el Tiempo de Recuperación del Trabajo (Work Recovery Time, WRT por sus siglas en inglés) es el tiempo disponible para recuperar datos perdidos (ISO 22301, 2019).

La continuidad de la SI es un requisito incluido dentro de un SGSI, enfocado en garantizar la continuidad de los procesos luego de haber sufrido el impacto de un evento disruptivo. Para lograr este nivel de operatividad se debe trazar una estrategia o procedimiento que sea parte del sistema global adoptado por la organización o encaminado solamente al alcance de la gestión de la SI.

### **1.3 Metodologías, procedimientos y guías relacionadas con la gestión de la SI**

Son muchas las metodologías, procedimientos y guías que permiten gestionar la SI enfocadas a obtener mejores resultados, algunos son puntuales y aplicables en ciertos tipos de organizaciones y otros son más genéricos, pero todos inciden de una forma u otra en que la información es un recurso de vital importancia para la organización y es imprescindible contar con mejores prácticas de SI, para minimizar los daños causados por los riesgos a los que están asociados amenazas y vulnerabilidades.

Varios autores como es el caso de Espinosa, Martínez & Amador, (2014), Nieves (2017), NC ISO 27001 (2016), Quirós Agustín L. (2010), Villena Aguilar (2014), Berrío López(2016), Cordero Torres(2015), Estupiñan, Pulido, & Jaime(2013), Gaona Vásquez (2013), (Miranda Cairo, Valdés Puga, Pérez Mallea, Portelles Cobas, & Sánchez Zequeira, 2016), (Murillo Varón, Bonilla Pineda, & Buitrago Estrada, 2012), Cuervo(2017), Gallegos & Murillo(2017) abordan elementos comunes para garantizar la SI y proponen en las metodologías para su implantación etapas que abarcan, entre otras, recogida y preparación de la información, identificación, clasificación y valoración de los activos de información y la gestión de riesgos de SI como la principal fuente para el control y contribución a la mejora de la organización.

Se analizan diez variables que son tratadas por los autores, resultado del estudio y revisión de sus investigaciones, teniendo en cuenta sus aportes y limitaciones, y otras partiendo de los principales aspectos presentes en la NC ISO/IEC 27001: 2016. Este análisis es posible realizarlo mediante la elaboración de una matriz binaria donde se analizó la relación o no entre variables de los enfoques analizados de diferentes autores (Anexo 2). Posteriormente se convirtió en una matriz unitaria mediante el software SPSS Statistics versión 19.0, tomando como medida Jaccard para crear la matriz de similitudes por autores y variables.

Luego se introdujo dicha matriz en el programa UCINET 6 para el procesamiento de los datos, resultando un 51.18% de densidad de la red. El módulo NetDraw creó la siguiente red (Figura 5)



(Castro & Bayona, 2011) presenta una metodología para gestionar riesgos tecnológicos cuya base son los estándares ISO 31000 e ISO/IEC 27005. Además, incluye recomendaciones y buenas prácticas de otros estándares y guías internacionales para manejo de riesgos, seguridad y gestión de servicios.

(Cordero Torres, 2015) realiza un estudio comparativo entre las metodologías MAGERIT y CRAMM utilizadas para el análisis y gestión de riesgos de la SI, en base a los mecanismos de identificación de activos, identificación de vulnerabilidades, funciones de probabilidad y variables de medición y cálculo de riesgos. Contiene elementos afines a esta investigación, pero quedan muchos objetivos de la NC ISO/IEC 27001 sin tratar, objetivo que sigue esta investigación.

(Espinosa, Martínez, & Amador, 2014) presentan la aplicación de la metodología OCTAVE-s para el análisis y gestión del riesgo en la SI, siguiendo las directrices de la norma ISO/IEC 27005. Se centra en las deficiencias de su campo de acción, razón que debilita su implementación en otras organizaciones.

(Solarte Solarte et al., 2015) permiten conducir proyectos de diagnóstico para la implementación e implantación de un SGSI, alineado con el estándar ISO/IEC 27001 y el sistema de control propuesto en la norma ISO/IEC 27002. Se presentan los resultados de una experiencia aplicando las fases de auditoría y la metodología de análisis y evaluación de riesgos. Se centra en los riesgos que inciden en la información digital. No se presentan acciones para mitigar los riesgos, siendo esta una de los principales objetivos a perseguir en la investigación.

(Tejena-Macías, 2018) se enfoca en exponer algunas opciones y permitir generar argumentos sólidos para identificar cuál es la metodología de análisis de riesgos que proporciona una mejor oportunidad de toma de decisiones dentro de una organización frente a la custodia de la información, para garantizar la seguridad y la continuidad del negocio. Se centra en demostrar las ventajas y desventajas de las diferentes metodologías y no se describe el proceso de gestión de riesgos, y la continuidad de la SI es tratada de forma superficial, sin llegar al desarrollo del plan de negocio como respuesta ante situaciones de desastres, que conlleven a la pérdida de información.

(Cuervo Álvarez, 2017) describe la implementación de un plan director de seguridad en una organización, que constituye la ruta a seguir para gestionar la información, aborda la gestión de activos, análisis de amenazas, impacto, riesgo y otros elementos afines a esta investigación, aunque no desarrolla en su plan la planificación, implementación, verificación y prueba de la continuidad de la SI, objetivo que persigue esta investigación.

El análisis de los procedimientos y métodos seleccionados permitió determinar las carencias existentes, identificando como una brecha la ausencia de herramientas y técnicas para llevar a

cabo una adecuada gestión de riesgos de SI, que se ajuste a esta investigación. También se identifica la ausencia de guías para la planificación, implementación, verificación y prueba de la continuidad de la SI, parte relevante de la gestión de la SI. Este proceso identifica todas las actividades que son críticas para el correcto funcionamiento del negocio en una organización, y sobre la base de ellos, traza estrategias y formula planes que dan respuesta a la reacción oportuna antes, durante y después de la materialización de un evento disruptivo.

Lo anteriormente expuesto permite diseñar una metodología que permita gestionar de forma abarcadora la SI como contribución a la continuidad del negocio, adaptada al marco legal reglamentario de Cuba, estableciendo el orden lógico para cada paso emitiendo objetivos, acciones a ejecutar, responsables de la ejecución de las tareas y recomendaciones.

#### **1.4 Informatización del proceso de análisis de los riesgos de la SI y su plan de continuidad**

En Cuba, la SI es un tema relativamente joven. Antes del año 2000, las tecnologías de la información eran tan escasas que solo se miraba la SI como la necesidad de proteger la información clasificada de una entidad. El volumen de datos procesado a través de las tecnologías era muy poco y en muchas ocasiones de baja importancia.

En la actualidad muchos de los procesos que tienen lugar en las entidades se lleva a cabo mediante las TIC, el volumen de información procesado es mucho mayor y la importancia de la información que se maneja es elevada y en muchos casos superior a los restantes activos de la organización. El tema SI ha ido tomando importancia en los últimos años como consecuencia del desarrollo tecnológico creciente y del proceso de informatización de la sociedad que tiene lugar en el país.

Actualmente, la mayoría de las empresas productoras de software del país tienen en cuenta el tema únicamente para desarrollar sus aplicaciones y no para desarrollar aplicaciones que tengan conexión directa con éste tema. Por tales motivos las aplicaciones informáticas de producción nacional dirigidas a fortalecer o controlar la SI son escasas o prácticamente nulas.

Existe en nuestro país desarrollado por la Oficina de Seguridad para la Redes Informáticas (OSRI) la aplicación informática DIÓGENES, por sus características la aproximación más cercana en relación con el tema de esta investigación. La misma está diseñada para su utilización en los organismos y entidades, enfocada a establecer una mayor seguridad y confianza durante el empleo de las TIC. DIÓGENES es una aplicación que permite la verificación del estado de conformidad en lo establecido oficialmente en la base legal en su momento vigente Resolución 127:2007 del Ministro de la Informática y las Comunicaciones, actualmente sustituida por la Resolución 128:2019.

Esta aplicación tiene como objetivo determinar el nivel de riesgo a que está sometida una

entidad y su posible impacto en correspondencia con la forma en que se gestiona la seguridad de las tecnologías de la información, caracterizado por la creciente interconectividad de disímiles equipos. Los resultados se obtienen a partir del completamiento del “*Cuestionario de Autoevaluación de la Seguridad Informática*”, el cual posee un máximo de 40 preguntas que abarcan los aspectos relativos al personal, los procesos, las tecnologías y a la relevancia que tienen las tecnologías de la información en cada entidad.

Para cada uno de las preguntas a responder se ofrecen entre cuatro o cinco opciones para seleccionar solo una. A cada respuesta se le otorga un valor de puntos. Del procesamiento de los valores obtenidos y considerando la relevancia de las tecnologías en la entidad se determina el nivel de riesgo general para la entidad y el riesgo parcial en lo relativo al personal, los procesos y las tecnologías, expresado en por cientos. De acuerdo a las respuestas que incidieron en el nivel de riesgo obtenido se brindan recomendaciones que pueden ser utilizadas para elevar la seguridad.

La aplicación DIOGENES no realiza un proceso de gestión de riesgos, está enfocada solamente a la parte informática de la organización, el proceso de gestión de incidentes solamente los identifica si existen en la entidad y se les asigna un valor de 0 hasta 2 según su criticidad y de cada deficiencia marcada propone una solución con el fin de contribuir a solucionar el problema detectado. Esta herramienta no cumple con lo establecido en la NC ISO/IEC 27001:2016 cláusula N.6 de análisis de riesgo, proceso alineado con la NC ISO 31000. Este estándar establece como punto de partida la identificación, clasificación y valoración de los activos de información, según la criticidad que tenga para la organización suponer una pérdida de confidencialidad, integridad y disponibilidad para cada uno de ellos. Según inventario de activos de información la detección de amenazas y vulnerabilidades es clave para el proceso de evaluación del riesgo. La aplicación de los criterios de aceptación del riesgo tiene en cuenta dos variables, la probabilidad de ocurrencia y el impacto que tendría que el riesgo se plasmara, para luego aplicar los controles como medidas de seguridad, orientados a mitigar los riesgos encontrados, de manera que se encuentren por debajo del nivel asumido por la organización.

La aplicación DIOGENES no está enfocada al proceso de gestión de continuidad de la SI. No identifica proactivamente los efectos que pueden tener las interrupciones, ya que no identifica los procesos que son cruciales para la existencia de la organización y por tanto no establece las respuestas necesarias en caso de que un incidente de gran alcance se produzca.

Es por lo que se propone para el perfeccionamiento de esta metodología el desarrollo de una herramienta informática, que mediante el análisis de los procesos se identifiquen, clasifiquen y se valoren los activos de información. Siguiendo a este proceso se conozcan las amenazas asociadas, para evaluar los niveles de riesgo de cada una de ellas, aplicar los criterios de

aceptación definidos por la organización y emplear los controles correspondientes para mitigarlos. Se determinan los procesos relevantes de la organización mediante un análisis continuo. En base a estos resultados, conjuntamente con el análisis de riesgos, se definen planes y estrategias, identificando las mejores alternativas de recuperación de estos servicios críticos y así garantizar la continuidad de la SI.

### **1.5 Marco legal y normativo en SI en Cuba**

Nuestro país, a pesar de todas las limitaciones que posee, también ha dado grandes pasos de avance en el mundo de las TIC. El programa de informatización de la sociedad tan mencionado a todas las instancias es un esfuerzo bien encaminado a fomentar el desarrollo tecnológico de nuestra sociedad, dirigido de forma directa por el Ministerio de Comunicaciones (MINCOM) ejemplo:

- Creación de los Joven Club (1987), con el objetivo de contribuir a la socialización e informatización de la sociedad cubana.
- Creación de la Oficina Nacional para la Informatización (2002-2013)
- Despliegue del cable submarino de fibra óptica ALBA-1(2007-2012)
- Despliegue de la Televisión Digital Terrestre (2012- hasta la actualidad)
- Apertura de áreas públicas de conexión WiFi (2015- hasta la actualidad)
- Inicia el Servicio Nauta Hogar (2016- hasta la actualidad)
- Inicio del servicio de datos móviles 3G/4G (2018- hasta la actualidad)
- Gobierno y Comercio Electrónico (2018- hasta la actualidad)
- Legalización de las Redes Privadas de Datos a personas naturales (2019- hasta la actualidad)

Es por esta razón que actualmente el estado moviliza los recursos necesarios para lograr el empleo seguro y eficiente de las TIC en función de las necesidades que requiere el desarrollo del país en la aprobación de leyes y decretos enfocados a garantizar una parte de estos. Además, a través de la Oficina Nacional de Normalización como la organización gubernamental cubana encargada de dar representación al país ante las instituciones y organizaciones en el ámbito internacional se realiza el proceso de generación de normas cubanas (NC) y adopción de estándares internacionales emitidas por organismos internacionales como la ISO, organización internacional a la que Cuba pertenece desde el año 1962.

Dentro de las principales bases legales a las que se encuentra sujeta la organización, y las que pueden afectar la gestión de la seguridad de información se encuentran:

- Los lineamientos de la política económica y social del Partido y la Revolución para el período 2016-2021. Expresamente en el Lineamiento 108, y además de manera complementaria, los lineamientos 68, 69, 112, 119, 186, 209, 243 y 271, definen las

áreas y sectores donde se debe avanzar estratégicamente en el proceso de informatización de la sociedad.

- El plan nacional de desarrollo económico y social hasta 2030; enfatiza en los objetivos específicos: 8 y 11 la necesidad de fortalecer nuestra infraestructura tecnológica y por ende elevar el desarrollo de la informática y las telecomunicaciones.
- Decreto ley 221 de 2001(Consejo de Estado de la República de Cuba) establece las normas y principios que rigen la actividad archivística en el territorio nacional.
- Decreto Ley 265 de 2009 (Consejo de Estado de la República de Cuba) “Del Sistema Nacional de Archivos de la República de Cuba”, establece las disposiciones generales para la protección del Patrimonio Documental de la Nación, así como las normas y principios que rigen la gestión documental en el territorio nacional.
- Decreto ley 370 (Consejo de Estado de la República de Cuba, 2018). Sobre la Informatización de la Sociedad en Cuba
- El Decreto 360 del Consejo de Ministros aprobado el 5 de junio de 2019 “Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional”. El objetivo general de este Decreto es establecer los niveles de seguridad en correspondencia con los riesgos asociados a la evolución de las TIC y las posibilidades reales de enfrentar estos últimos. Y tiene como objetivos específicos proteger el ciberespacio nacional y preservar la soberanía sobre su utilización.
- La Resolución 128 aprobada el 24 de junio de 2019 del MINCOM “Reglamento de Seguridad de las Tecnologías de la Información y la Comunicación”. Esta Resolución tiene por objeto complementar las disposiciones del Decreto 360 y establecer las funciones de los sujetos que intervienen en esta, así como garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país. Derogó a la Resolución 127/2007 y la 192/2014 del MINCOM.
- La Resolución 129 aprobada el 24 de junio de 2019 del MINCOM “Metodología para la gestión de la seguridad informática” del MINCOM. Tiene por objeto determinar las acciones a realizar en una entidad durante el diseño, la implementación y posterior operación de un sistema de gestión de la seguridad informática y constituye un complemento del Decreto 360 y de la Resolución 128/2019 en cuanto a la obligación de diseñar, implantar y mantener actualizado un sistema de seguridad informática, a partir de los bienes a proteger y de los riesgos a que están sometidos.
- Resolución 41/2009. Del Ministerio de Ciencia Tecnología y Medio Ambiente (CITMA) “Política de archivos y conservación de documentación/ Sistema Nacional de Archivos.



- Resolución N. 60/2011 de la Contraloría General de la República (CGRC) "Normas del sistema de control interno".
- Guía de Ciberseguridad: documento emitido por el MINCOM, que ofrece una herramienta de autodiagnóstico, que permite realizar una evaluación de su nivel de ciberseguridad a través de un breve y simple cuestionario luego de lo cual se le presentan una serie de recomendaciones personalizadas.

La aproximación más cercana para el desarrollo de un sistema de SI está declarado por la Resolución 129 y constituye un complemento a lo exigido en el "Decreto de Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional" y el "Reglamento de Seguridad para las Tecnologías de la Información y la Comunicación" en cuanto a la obligación de diseñar, implantar y mantener actualizado un sistema de seguridad informática, además de establecer las funciones y garantizar un respaldo legal para lograr el empleo seguro y eficiente de las TIC en función de las necesidades que requiere el desarrollo del país.

Esta metodología tiene por objeto determinar las acciones a realizar en una entidad durante el diseño, la implementación y posterior operación de un sistema de seguridad informática a partir de los bienes a proteger y de los riesgos a que están sometidos, pero aunque se apoya en la norma NC ISO/IEC 27001 se enfoca en el empleo y salvaguarda de los activos de información en formato digital y los sistemas informáticos que los procesan y almacenan, obviando la información física y los peligros a la que está sometida. La seguridad informática es un proceso que se encuentra inmerso en la SI, siendo esta última más abarcadora, no solo preserva los activos de información sin importar su forma o estado contra cualquier forma de amenaza, sino que proporciona medidas con respecto a las personas que la manipulan.

Si bien el país declara la importancia de la información y la necesidad de incentivar las medidas de control sobre esta, la SI es asumida de manera desarticulada, siendo tratada desde una perspectiva del control de la seguridad informática en las empresas, observada como un simple tema de cumplimiento legal o un simple problema técnico.

### **1.5.1 Estado actual en la OTNH de la gestión de la SI**

La Oficina Territorial de Normalización de Holguín es una organización gubernamental, adscripta al Ministerio de Ciencias, Tecnología y Medio Ambiente, es el organismo cubano encargado de dar representación ante las instituciones y organizaciones en el ámbito regional, en relación a las actividades de normalización, metrología y calidad, asumiendo las responsabilidades, obligaciones y compromisos que de ello se deriven, así como programar, organizar y controlar, la participación de la economía en el territorio. La OTNH ha implantado un

sistema integrado de gestión (SIG) en correspondencia con su objeto social, demostrar su competencia para el desarrollo de las actividades vinculadas a la calibración y la evaluación de la conformidad obligatoria (inspección estatal) mediante procesos de acreditación según las versiones vigentes de las normas cubanas NC ISO/IEC 17025 y NC ISO/IEC 17020. Para los servicios de capacitación a entidades de la economía e información científico técnica, se trabaja bajo la óptica de un SGC por la norma cubana NC ISO 9001 y el sistema de control interno según la Resolución N. 60/11 de la CGRC. Su establecimiento ha conllevado a la elaboración de un amplio sistema documental existente en diferentes formatos, que incluye políticas, objetivos, manuales, procedimientos, instructivos y otra serie de documentos importantes para el desarrollo de otras actividades. Toda esta información documentada es almacenada, procesada y transmitida por diferentes medios digitales y físicos, que es necesario mantener y conservar adecuadamente con niveles de seguridad adecuados a su importancia.

Al realizar un análisis de las principales problemáticas existentes en la entidad relacionadas a la SI evidenciadas en las auditorías internas, revisiones por la dirección, auditorías de seguridad informática y otras actividades de medición y control se demuestra que mayormente están relacionadas con la carencia de medidas organizativas, técnicas y por desconocimiento y mal uso de los activos de información; las cuales no requieren inversión alguna para su solución. Siendo las más significativas las siguientes:

- 1- La metodología actual para la evaluación de los riesgos identificados en la OTNH, sustenta su análisis en la subjetividad de la experiencia de cada jefe de proceso y miembros del comité de prevención y control, obviando el punto de partida de este proceso, que es la identificación de los activos críticos de información de la entidad a proteger.
- 2- No realizan una valoración de los riesgos de la pérdida de información documentada, que para el caso particular de la organización es uno de los riesgos que tiene mayor importancia, porque ante su posible manifestación el impacto es grave.
- 3- Existencia de planes de seguridad informática que no son efectivos para proteger los activos informáticos de la organización por los siguientes motivos:
  - Las políticas de seguridad definidas tienen carácter general y no responden totalmente a la minimización de los riesgos identificados, además quedan sin establecerse otras de importancia para garantizar la seguridad de la información.
  - No se definen de manera específica las medidas de seguridad a implementar para los diferentes servicios que se brindan en la red.
  - En el plan de recuperación ante contingencias no definen la matriz de recursos

necesarios para dar solución ante la ocurrencia de incidentes o violaciones de la seguridad informática, el mismo está enfocado solamente en la información digital.

- 4- Carencia de aterramiento para la protección de equipamientos ante descargas eléctricas.
- 5- Empleo rutinario de dispositivos externos *USB*, principalmente memorias flash, sin contar con un procedimiento efectivo para el control de estos medios y de la información que almacenan.
- 6- Deficiente configuración de las políticas de auditorías locales, que permiten monitorear los principales eventos del sistema operativo (*eventos de seguridad, sistema y aplicación*) que revisten importancia para realizar una investigación ante la posible ocurrencia de un incidente de seguridad.
- 7- Falta de actualización y desatención de los sistemas operativos y softwares empresariales empleados, permitiendo la presencia de vulnerabilidades críticas de seguridad que comprometen los sistemas.
- 8- Existencia de políticas de salva de la información de los usuarios y las configuraciones de los servicios que no garantizan la recuperación de la entidad ante la ocurrencia de un fallo de seguridad por los siguientes motivos:
  - Carecen de informes precisos y completos de las copias de respaldo.
  - No cuentan con copias de respaldo en ubicaciones fuera de las entidades, situación que dificultaría el proceso de recuperación después de producirse desastre o fallo de los medios de almacenamiento.
  - Quedan sin definir concretamente cual es la información vital para el funcionamiento de la entidad.
- 9- No existen implantadas estrategia de continuidad de la SI que garanticen que la organización reanude sus operaciones y servicios en tiempos adecuados en caso de una interrupción.

En la actualidad la entidad de forma general, aún no cuenta con la garantía que brinda una metodología para la gestión de la SI que contribuya a su continuidad, a partir de un adecuado proceso de gestión de riesgos que permita evaluar y analizar los riesgos de SI. La SI es tratada desde un punto de vista totalmente informático, obviando la información física y los peligros a la que está sometida. En la OTNH no existen estrategias implantadas de recuperación si una disrupción se presenta, por lo que no se puede controlar su impacto como consecuencia de la materialización de un determinado riesgo, y así garantizar un futuro confiable para la organización. Después de todo lo expuesto y las insuficiencias encontradas en relación a la gestión de la SI se justifica el desarrollo de una metodología para la gestión de la SI que

contribuya a la continuidad del negocio y su aplicación en la OTNH.

### **Conclusiones del capítulo**

La revisión de las diferentes bibliografías manifiesta que la implementación de un SGSI es un suplemento óptimo para la continuidad del negocio, garantizando que la organización pueda sobrevivir ante un acontecimiento que pueda poner en riesgo su futuro. Como resultado, el nivel de seguridad deberá elevarse, ya que las deficiencias detectadas constituyen un freno para obtener niveles de confianza aceptables, que garanticen la confidencialidad, integridad, disponibilidad y continuidad de la SI.

El análisis de los procedimientos y métodos seleccionados de los diferentes autores permitió determinar que las diferentes investigaciones tienen en común la gestión de riesgo como el punto concéntrico de la gestión de la SI. Se identifican brechas al identificar la ausencia o carencia de herramientas y técnicas utilizadas en el desarrollo de otras etapas que son de vital importancia para llevar a cabo una adecuada gestión de SI. En los diferentes enfoques metodológicos no se aborda la gestión de la continuidad de la SI, es tratado de forma superficial, siendo un proceso importante vinculado a la SI y objetivo que persigue esta investigación.

El análisis del marco teórico práctico sobre el objeto demuestra la necesidad de desarrollar una metodología para la gestión de la SI en la Oficina Territorial de Normalización que contribuya a la continuidad de la organización.

## Capítulo 2: Metodología para la gestión de la SI como contribución a la continuidad del negocio

El objetivo de este capítulo es diseñar una metodología que permita la gestión de la SI y garantice su continuidad, alineada con los principales aspectos de la norma cubana NC ISO IEC 27001. Promueve la adopción de un sistema basado en enfoque de procesos, por lo que se puede decir que, es coherente con el ciclo de gestión PHVA (Planear, Hacer, Verificar, Actuar) de Walter Andrew Shewhart, más popularizado por William Edwards Deming.

En esta metodología se exponen las herramientas y técnicas que pueden ser utilizadas en cada paso a realizar. Está estructurada en 4 etapas y 12 pasos como se puede apreciar en la figura 6.

Con la intención de agilizar y facilitar la compleja tarea que acarrearán los procesos de gestión de activos, análisis y evaluación de riesgos y continuidad de la SI, la autora desarrolla la herramienta informática “Gestión de la Seguridad de la Información”, la cual permite generar informes de cada uno de los pasos implementados.



Figura 6: Metodología para la gestión de la SI como contribución a la continuidad del negocio

### Etapa 1: Planificación del proyecto

En esta etapa la alta dirección de la organización aprueba y se compromete con el proyecto. Ordena las tareas para el cumplimiento de los objetivos, garantizando la previsión de recursos, la dotación de personal calificado, ambiente físicos e inversión que garanticen la SI y su

continuidad.

### **Paso 1 Compromiso de la alta dirección**

**Objetivo:** En este paso la alta dirección debe comprometerse con el proyecto de implementación, establecimiento, mantenimiento, revisión y mejora del SGSI, para llegar a obtener un modelo coherente con la naturaleza del negocio, y alineado con los objetivos de la organización.

#### **Acciones a ejecutar**

Se debe realizar previamente un encuentro con los miembros del consejo de dirección, que propicie al intercambio, se aborden sus preocupaciones y dudas con respecto al proyecto, además se expongan las ventajas de implementar un SGSI y como influiría para el logro de la competitividad y una mejor imagen de la organización.

La alta dirección deberá aprobar el proyecto para la implementación del SGSI para ello debe:

- Definir los recursos, tiempos y áreas involucradas en la ejecución de la tarea, conjuntamente con los responsables.
- Definir la política de SI y sus objetivos, y que estos sean compatibles con la dirección estratégica de la organización.
- Garantizar la integración de los requisitos del SGSI en los procesos de la organización.
- Determinar las necesidades de SI y de continuidad para la gestión de la SI en situaciones adversas.
- Asegurar que los recursos necesarios para el SGSI se encuentren disponibles.
- Asegurar que el SGSI logre los resultados previstos y esté alineado con la estrategia de continuidad de SI de la organización.
- Dirigir y apoyar a las personas, para contribuir a la eficiencia del SGSI.
- Promover la mejora.

**Responsables:** Alta dirección de la organización

#### **Recomendaciones**

En la ejecución de las reuniones con todos los implicados en el SGSI quedarán claro los objetivos que se persiguen con el mismo y los resultados esperados. Definir los recursos pertinentes para el desarrollo del SGSI y la forma de acceder a ellos. Se debe dejar constancia documentada de este proceso. Para lograr la integración de los requisitos del SGSI con los procesos de la organización se debe asegurar la formación del personal, para poder asignar los roles y responsabilidades a cada trabajador; los controles seleccionados como aplicables deben estar incluidos en un conjunto de políticas y procedimientos para la SI, aplicados a todos los

procesos de la organización. Se recomienda para su desarrollo herramientas como la observación directa, revisión bibliográfica, tormenta de ideas y trabajo en grupo.

## **Paso 2 Conformación del comité de SI**

**Objetivo:** Establecer las políticas y procedimientos para el cumplimiento de las funciones encomendadas al Comité de SI, su ámbito de acción, conformación, funcionamiento y funciones como máximo órgano consultivo sobre SI en la organización.

### **Acciones a ejecutar**

Este comité deberá estar conformado por los representantes de los procesos relevantes y que aporten al SGSI, según sus cláusulas y controles. Deberán reunirse en periodos planificados para evaluar la situación institucional en materia de SI y el plan de acción correspondiente para mejorarla continuamente.

Este comité podría estar integrado por:

- Personal administrativo, que en los diferentes procesos responden por los activos de información que se procesan en las tecnologías.
- Personal jurídico, es el responsable de la actualización del marco regulatorio vigente, aportando y apoyando al comité.
- Personal de informática, que domina los aspectos técnicos necesarios para la implementación de los controles de seguridad relacionados con las TIC.
- Alta gerencia, como líder del proyecto.
- RRHH, parte importante del comité, relacionado con las cláusulas de confidencialidad y seguridad antes de contratar al personal relacionado con la SI, una vez contratado y cuando finaliza el vínculo contractual del mismo.
- Profesionales de protección a partir de su responsabilidad en la custodia de los activos de información de la organización.
- Gestores de riesgos, resulta idóneo para motivar el análisis y la discusión grupal, de manera que el equipo de trabajo pueda ampliar su comprensión del riesgo.
- Responsable de SI (RSI), como encargado de realizar las propuestas de SI ante el comité y responsable ante la dirección sobre la ejecución de los cronogramas propuestos.

Entre las principales funciones del comité estarían:

- Informar de la situación institucional en materia de SI.
- Designar al RSI.
- Patrocinar y participar en la implementación, operación, monitoreo, revisión, mantenimiento y mejora del SGSI.

- Tratar los casos que hayan ocurrido en la organización en materia de SI.

**Responsables:** Alta dirección

### **Recomendaciones**

Con el objetivo de aplicar la metodología se deben determinar las necesidades de capacitación del comité de SI y elaborar un plan a corto plazo con los temas identificados. Como parte de la preparación para la realización del diagnóstico este comité debe dominar las principales técnicas y herramientas a utilizar para su correcta ejecución. Se deben realizar reuniones planificadas para evaluar la situación actual en materia de SI y el plan de acción para mejorarla.

### **Paso 3 Concienciación y formación**

**Objetivo:** Lograr un nivel alto de compromiso y actuación de todos los integrantes de la organización como parte fundamental del modelo de SI, orientado a sensibilizar a todas las personas para identificar las amenazas que enfrenta la información y así garantizar su continuidad.

### **Acciones a ejecutar**

- Establecer las condiciones organizativas como: logística y presupuesto a utilizar para el desarrollo de la actividad, determinar los temas a capacitar para un mejor desempeño referente a la SI, selección de instructores internos/externos preparado en materia de SI que garanticen la correcta formación del personal, contar con un cronograma de las acciones de formación/concienciación y los medios a utilizar.
- Estimular al cambio y lograr el compromiso de los implicados, contando con el apoyo y participación activa de la alta dirección, de manera que los empleados confíen y se motiven.
- Constituir los diferentes grupos objetivos y definir una estrategia para las actividades de formación y la comunicación que debe llegar a cada grupo.
- Comunicar a todas las partes interesadas la estrategia de SI y las mejores prácticas y hábitos de comportamiento que son importantes para poder obtener un nivel adecuado de protección de los activos de información.
- Elevar la cultura de SI para nuevas modalidades como el teletrabajo, a raíz de la materialización de eventos catastróficos, que obliguen a la organización a adaptarse a los nuevos cambios.
- Definir los planes de capacitación requeridos para generar las competencias necesarias en el personal, para que lleven a cabo las actividades de SI que sean desplegadas hacia sus procesos, se interiorice su importancia y la necesidad de garantizar su continuidad.



- Fomentar discusiones con los trabajadores sobre SI, para aumentar su cultura en el tema,
- Discutir sobre los riesgos de SI que están asociados a posibles amenazas, para evitar situaciones que puedan poner en peligro los activos de la organización y así evitar incidentes de seguridad.

Se debe dejar evidencia sobre el desarrollo de acciones realizadas.

**Responsables:** Comité de SI y Especialista RRHH

### **Recomendaciones**

Se debe comunicar de la mejor manera a la organización la estrategia y el panorama de riesgos de SI, sus impactos a la organización y principalmente sobre el recurso humano. Los planes de capacitación definidos deben estar alineados con los planes y proyectos de tratamiento de riesgos para que las personas estén preparadas para hacer uso de nuevas tecnologías, procedimientos o tener nuevas actuaciones con respecto a la SI. La cultura en SI debe ser una de las primeras en realizarse y debe ser lo suficientemente exitosa para que todas las demás gestiones se soporten en la buena actuación y compromiso del recurso humano, con respecto a las actividades que hay que desplegar a través de toda la organización. Como técnica fundamental se recomienda la modalidad de capacitación en el puesto de trabajo, para lo cual se responsabilizará a los propietarios de procesos con el desarrollo de la acción de formación con sus colaboradores, asegurando que su personal sea consciente de la pertinencia e importancia de sus actividades y de cómo contribuyen al logro de los objetivos del SGSI.

### **Paso 4 Determinar el alcance del SGSI**

**Objetivo:** Establecer los límites que abarcará el SGSI en la organización, en función de las características del negocio, localización, activos y tecnología disponible.

#### **Acciones a ejecutar**

- Determinar los procesos que por sus funciones y responsabilidades ayudan en primera instancia a dar cumplimiento a la misión institucional y están vinculados a la SI.
- Precisar en qué actividades de la organización se desea implantar el SGSI y en cuáles no es necesario, teniendo en cuenta las cuestiones externas e internas que son pertinentes para cumplir con los objetivos propuestos y que se ajusten a las necesidades de la organización.
- Determinar las partes interesadas relevantes para el SGSI y sus requisitos asociados, que pueden ser legales, regulatorios u obligaciones contractuales.

**Responsables:** Comité SI

## **Recomendaciones**

Definir el alcance no implica abarcar toda la organización, es recomendable empezar por un alcance limitado, en el que se involucren los procesos del negocio que contengan la información más relevante para la organización, es decir los que se han identificado en el mapa como misionales. Es necesario disponer para el desarrollo de este paso del mapa de procesos de la organización

Tener claro las terceras partes y su influencia sobre la SI, es importante en el momento de definir el alcance; los requisitos legales y contractuales relacionados con la SI deben quedar contemplados también dentro del alcance del sistema (Murillo Varón, 2012).

El alcance debe estar como información documentada y disponible para todo el personal. Se recomiendan para su desarrollo herramientas como la observación directa, tormenta de ideas y el trabajo en grupo.

## **Etapa 2: Diagnóstico**

En esta etapa se conoce a la organización para determinar qué los puede afectar a nivel interno y externo. Se realiza un análisis de brechas para conocer el nivel de madurez en temas de SI, analizando el cumplimiento o no de los requisitos de la norma NC/ISO/IEC 27001 y su anexo A. El resultado es el informe de diagnóstico.

## **Paso 5 La organización y su contexto**

**Objetivo:** Determinar las limitaciones existentes para mantener las funciones críticas del negocio en los niveles aceptables que generen las menores pérdidas posibles, recuperarse rápida y eficazmente y minimizar el impacto generado.

### **Acciones a ejecutar**

Las organizaciones tienen un contexto interno que incluye misión, visión, políticas, objetivos, procedimientos, registros, metas, estrategias, roles y responsabilidades, documentos de referencia, entre otros. De igual forma interactúa con su medio externo, en el que deben considerarse aspectos como regulaciones legales aplicables, economía, tecnología, cultura y demás aspectos que se consideren precisos. La importancia de entender estos aspectos es saber que requiere ser protegido y cuáles son las limitaciones existentes para esta protección y garantizar su continuidad ante una interrupción.

**Responsables:** Comité SI

## **Recomendaciones**

Como fuentes de información se recomienda emplear documentación existente en la organización relacionada con la SI, planeación estratégica y planes que brinden información que permitan posicionar a la organización con respecto a su medio, entrevistas con altos mandos, encuestas con el personal, visitas a instalaciones, revisión documental, análisis de

fortalezas, debilidades, oportunidades y amenazas de la organización, observación de procesos y actividades.

### **Paso 6 Análisis de brechas**

**Objetivo:** Analizar la situación actual en temas relacionados a SI de la organización y compararlo con los requisitos establecidos de la NC ISO/IEC 27001. Definir documentos requeridos para la implementación del SGSI.

### **Acciones a ejecutar**

Las brechas existentes en la organización con relación a la SI son actividades que se tienen que realizar para cubrir ese margen de implementación y poder cumplir con lo establecido en la NC ISO/IEC 27001, para este paso se toma como referencia la investigación de (Cuervo Álvarez, 2017), modificado y adaptado según las características de esta investigación.

Se puede desarrollar un modelo de madurez de la capacidad (CMM) con el propósito de ayudar a evaluar el grado de implementación del SGSI y evaluar la totalidad de los 114 controles incluidos en este estándar, mejorar las prácticas de situaciones críticas del negocio, y evolucionar y madurar los procesos. Para el análisis se pueden estimar 5 niveles (Tabla 1).

Tabla 1: Modelo CMM para la madurez, fuente (Cuervo Álvarez, 2017)

CMM	Nivel	Descripción
1	Inexistente	Carencia de un proceso reconocible, la organización no ha reconocido la existencia de un problema a resolver.
2	Iniciado	La organización reconoce la existencia de un problema a resolver, pero no existen métodos aplicar de forma normalizada. No hay comunicación o entrenamiento formal.
3	Definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
4	Gestionado	Se puede monitorear y medir con indicadores numéricos o estadísticos la evolución de los procesos, mejorando continuamente y proveyendo buenas prácticas.
5	Optimizado	Los procesos están optimizados hasta niveles de mejores prácticas, basado en resultados bajo constante mejora. Se dispone de tecnología para automatizar el flujo de trabajo y mejorar la calidad y la efectividad.

Según estos niveles de CMM se realiza un análisis de brechas sobre la base de los requisitos de la norma NC ISO/IEC 27001:2016 y la situación actual dentro de la organización. Se deben listar los requisitos del SGSI de las cláusulas 4 a la 10 y determinar en qué nivel de madurez se encuentra la organización conforme a cada uno de ellos, para esto se propone el modelo de la (tabla 2). También se analizan los objetivos de control del Anexo A, determinar el nivel de cumplimiento de cada uno de ellos, para sobre esa base generar un reporte y determinar las brechas a cubrir. Para su confección se propone la (tabla3). El resultado es el informe de análisis de brechas, del cual se generan estrategias, procedimientos y acciones para llegar al cumplimiento de los objetivos de la organización.

Tabla 2: Nivel de madurez de los requisitos NC ISO/IEC 27001

N.	ID	Cláusula	Nivel de madurez

Tabla 3: Nivel de madurez Anexo A NC ISO/IEC 27001

Controles	Contenido	Nivel de madurez:
<b>Observaciones:</b>		

**Responsable:** Comité de SI

### **Recomendaciones**

Se recomienda para la ejecución de este paso el trabajo en grupo, entrevista con directivos de la organización, jefes de áreas y personal vinculado con la gestión de la información. La utilización de listas de chequeo vinculadas a la documentación requerida del SGSI y análisis documental, muy importante para comprender la magnitud de este.

### **Etapas 3: Desarrollo**

En esta etapa se definen que activos de información requieren protección. Se analizan, evalúan y estiman los riesgos potenciales asociados a los activos de información que impacten en su seguridad y de acuerdo a los recursos actuales como podrían salvaguardarse. Se desarrolla un plan de continuidad de SI para garantizar que las funciones esenciales puedan continuar durante y después de cualquier incidente y que su operación no se vea afectada.

### **Paso 7: Gestión de activos**

**Objetivo:** Identificarlos activos de la organización por procesos, que de una forma u otra mantienen relación con la información, independiente del formato en que se encuentren. Definir sus propietarios, clasificarlos y determinar su criticidad.

### Acciones a ejecutar

El inventario de activos de información se realizará por procesos, por lo que es necesario durante la realización del análisis contar con la participación activa del comité de SI. En el inventario deben estar identificados e incluidos todos los activos que de una forma u otra estén asociados a la información y a los recursos para su tratamiento que intervengan en dicho proceso.

Cada activo según las características que posea y función que desempeña debe ser clasificado y contar con la asignación de una categoría; por cada uno que figure en el inventario debe tener fijado un propietario (figura 7). El proceso de clasificación de activos como se analizó en el capítulo 1 se recomienda la utilización del catálogo de elementos de la metodología MAGERIT. Esta metodología muestra una serie de categorías para clasificar los activos, ya sean para:

Datos personales (DP): Cualquier información concerniente a personas físicas identificadas o identificables.

Información (D): Datos de interés para la administración pública o datos vitales (registros de la organización).

Instalaciones (L): Lugares donde se hospedan los sistemas de información y comunicaciones.

Servicios (S): Función que satisface una necesidad de los usuarios (del servicio). Servicios prestados por el sistema.

Software o aplicaciones informáticas (SW): Tareas que han sido automatizadas para su desempeño por un equipo informático (programas, aplicaciones, herramientas, etc.)

Hardware o equipamiento informático (HW): Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.

Personal (P): Personas relacionadas con los sistemas de información.

Redes de comunicaciones (COM): Instalaciones dedicadas como servicios de comunicaciones contratados a terceros; son medios de transporte que llevan datos de un sitio a otro.

Soportes de información (media): Se consideran dispositivos físicos que permiten almacenar información de forma permanente o durante largos periodos de tiempo.

Equipamiento auxiliar (Aux): Se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

No.	Nombre del activo	Descripción del activo	Dominio del activo	Propietario del activo	Proceso al que pertenece
1					

Figura 7: Identificación, clasificación y propietario de activos

Cada activo debe tener determinado un valor, que son las características o atributos que lo hacen valioso para la organización. MAGERIT para valorar las consecuencias de la

materialización de una amenaza utiliza cinco dimensiones, para esta investigación el autor adopta las propiedades que considera el estándar NC ISO/IEC 27001 como resultado del análisis realizado en el Capítulo 1; por lo que se propone valorar el impacto en base a las propiedades de confidencialidad, integridad y disponibilidad, que contribuyen a la exitosa implementación de un SGSI.

Para establecer la valoración de los activos se ha seleccionado un método semi-cuantitativo, donde se utiliza la escala de likert establecida en cinco niveles, cuanto más impacte la materialización de un hecho mayor será su valoración (tabla 4).

Tabla 4: Valoración de impacto, fuente (Gómez Morales, 2014)

Nivel	Categoría	Descripción
1	Insignificante	Si el hecho llega a presentarse tendría consecuencias mínimas para la organización
2	Menor	Si el hecho llega a presentarse tendría un bajo impacto o efecto para la organización
3	Dañino	Si el hecho llega a presentarse tendría medianas consecuencias o efectos para la organización
4	Severo	Si el hecho llega a presentarse tendría altas consecuencias o efectos para la organización
5	Crítico	Si el hecho llega a presentarse tendría desastrosas consecuencias o efectos para la organización

Según esta valoración se determinan que activos son críticos para la organización y necesitan mayores niveles de protección (figura 8).

No.	Dominio	Activo	Confidencialidad	Disponibilidad	Integridad	Impacto
1						

Figura 8: Valoración de activos, pantalla software “Gestión de la SI”

**Responsables:** Comité de SI

**Recomendaciones**

Herramientas como el trabajo en grupo y la tormenta de ideas facilitan la ejecución de este paso. Para el proceso de gestión de activos se recomienda usar la herramienta informática "Gestión de la SI" desarrollada por la autora (Anexo 4).

**Paso 8: Análisis y evaluación de riesgos**

**Objetivo:** Analizar, evaluar y estimar los riesgos potenciales asociados a los activos de información que impacten en su seguridad, para lograr minimizar las consecuencias que afecten la continuidad de la SI.

### **Acciones a ejecutar**

La gestión de riesgo es una parte importante de la gestión de la SI. Es el proceso que se encarga de identificar y cuantificar la probabilidad de ocurrencia de las amenazas asociadas a los activos de información y el impacto que estas tendrían para la organización en caso de materializarse. Luego establecer los niveles de aceptación del riesgo, es decir, definir en qué nivel se aceptan, en cuál se aplican controles y en cuál se transfieren.

Para realizar un análisis de riesgos es necesaria una metodología que se ajuste a las necesidades de la organización, debe ser comprobable en el tiempo y demuestre evolución en la implementación de controles a la hora de reducirlos. Se deben identificar los dueños de los riesgos, ya que necesariamente los dueños de los activos de la organización no son los dueños de los riesgos, por lo que es necesario durante la realización del análisis contar con la participación del comité de SI, ya que este está integrado por los representantes de los procesos de la organización.

En el capítulo 1 se identificó la norma cubana NC ISO 31000 como la metodología más apropiada para la gestión de riesgo de acuerdo a las características de esta investigación y para el proceso de selección de las amenazas se propone el catálogo de posibles amenazas sobre los activos que describe la metodología MAGERIT, para homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios que permiten compararlos e integrarlos. Para su desarrollo se proponen una serie de tareas.

#### Gestión de activos (previamente gestionados en el paso 7)

##### Análisis del riesgo

A partir del inventario de activos asignados con sus respectivos propietarios se analizan bajo que amenazas están expuestas, una breve descripción de cada una de ellas y que vulnerabilidades pueden ser aprovechadas para que se materialicen.

##### Evaluación del riesgo

En esta tarea se deben listar todos los riesgos y calcular su valor. Se determinan dos variables para el cálculo del riesgo, la probabilidad de ocurrencia y el impacto que causaría si el riesgo se materializase, según la fórmula  $\text{Riesgo} = \text{probabilidad de ocurrencia} * \text{valoración del impacto}$ . Para establecer los criterios de evaluación del riesgo se ha seleccionado un método semi-cuantitativo, se utiliza una escala de likert, para definir los valores de la probabilidad y determinar el impacto, establecida en cinco niveles, cuanto más impacte la materialización de un hecho mayor será su valoración. Se define la probabilidad de ocurrencia del riesgo de la siguiente forma (tabla 5):

Tabla 5: Probabilidad de ocurrencia, fuente (Gómez Morales, 2014)

Valor	Frecuencia	Descripción
1	No se ha presentado en los últimos 3 años	Raro: Es improbable que se manifieste el riesgo
2	Al menos una vez en los últimos 3 años	Improbable: El riesgo se manifiesta raras veces
3	Al menos una vez en los últimos 2 años	Posible: El riesgo puede manifestarse en algunas ocasiones
4	Al menos una vez en el último año	Probable: El riesgo se manifiesta casi siempre
5	Más de una vez al año	Casi seguro: El riesgo siempre se manifiesta

Para evaluar el impacto dirigirse a la (tabla 4) del paso 7 de esta metodología, es importante que se tengan en cuenta los principales factores que inciden en materia de SI.

Luego de tener definidas ambas variables para cada uno de los riesgos identificados en el inventario se aplica la fórmula del cálculo del riesgo y se definen los criterios de aceptación de los riesgos según determine la organización. En la figura 9 se muestran las zonas de riesgo.

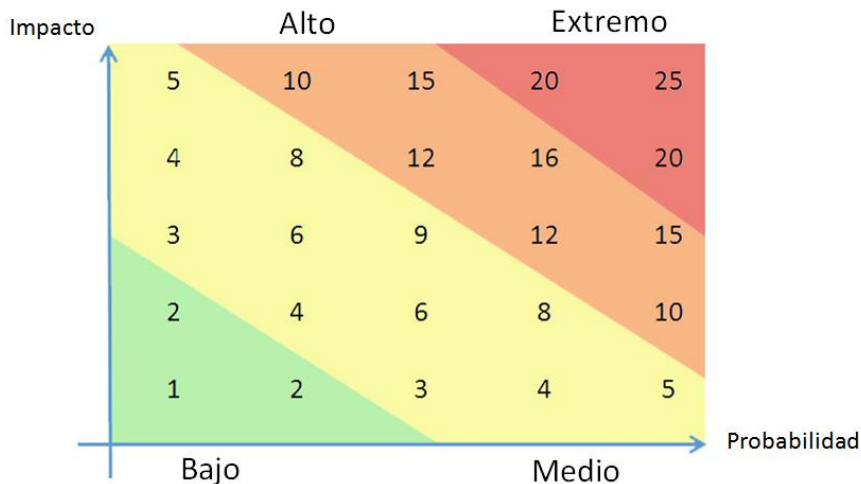


Figura 9: Zonas del riesgo, fuente: elaboración propia

Aplicación de los criterios de aceptación aprobados

El tratamiento del riesgo comprende la selección y la implementación de una o varias opciones para modificarlos. Se determinan 4 niveles de aceptación.

El nivel 1 es la zona de riesgo bajo, se asumen aceptando las pérdidas probables, ya que la organización posee los medios de protección necesarios y pueden ser manejados. El nivel 2 es la zona de riesgo moderada, estos se reducen, adoptando medidas encaminadas a la disminución tanto de la probabilidad de ocurrencia como del impacto. Los niveles 3 y 4 son las zonas de riesgos altos o extremos, estos riesgos se evitan, tomando medidas encaminadas a



prevenirlos, se reducen detectando su materialización o se transfieren minimizando su efecto a través del traspaso de las pérdidas a otras organizaciones.

Al finalizar el cálculo los riesgos se ubican de acuerdo a los rangos definidos por la organización y se clasifican en correspondencia a los criterios de aceptación determinados. Luego se ordenan de mayor a menor y se aborda cada uno de acuerdo a su prioridad. Se recomienda para su confección el modelo (figura 10).

No.	Activo	Amenaza	Impacto de amenaza	Valor del Impacto	Probabilidad de ocurrencia	Valor de la probabilidad	Total	Zona de riesgo
-----	--------	---------	--------------------	-------------------	----------------------------	--------------------------	-------	----------------

Figura 10: Cálculo del riesgo, pantalla del software “Gestión de la SI”

### Selección de controles

Los controles son salvaguardas que se aplican para evitar la materialización de los riesgos o mitigar su impacto. Generalmente en las organizaciones se implantan distintos tipos de controles, destacándose tres categorías. Pueden ser preventivos, anticipando eventos y aplicando medidas enfocadas a que no se materialice el riesgo, tratan de evitarlo o atenuarlo. Los controles detectivos que permiten identificar los eventos en el momento en que se presentan, midiendo la efectividad de la implementación de las medidas preventivas y los controles correctivos que se aseguran de tomar medidas después de ocurrir un evento para evitar nuevamente su materialización.

### Análisis costo-beneficio

El análisis costo-beneficio es una herramienta financiera que permite comparar lo que se pierde por el efecto de materializarse un riesgo, contra lo que cuesta aplicar una acción para evitarlo.

Los costos de los controles seleccionados dependen de la criticidad de los riesgos y de sus requerimientos de inversión para implantarlos. La organización debe definir en qué controles invierte sus recursos. Los costos de transferencia dependen de los controles implantados, ya que estos disminuyen en la misma medida que mejoran los controles de los riesgos.

Se debe realizar un análisis cuantitativo que permita expresar en valores monetarios lo que implicaría para la organización la concreción de los riesgos, que según los niveles de aceptación definidos se les deben de aplicar controles, para evitar su materialización o mitigar su impacto. El análisis costo-beneficio cuantitativo es una herramienta para sustentar la asignación y la distribución de recursos para evaluar la repercusión de las inversiones, para ellos se debe:

- Calcular todos los beneficios financieros a obtener de la inversión a realizar, bajo diferentes situaciones (óptima, base, pésima), para el cálculo de estos beneficios se estiman los costos evitados por la no presentación de los riesgos.

- Calcular todos los costos asociados a la inversión en base a las distintas situaciones, para ello la autora se auxiliará de la ecuación de exposición planteada por (López Díaz, Suárez García, & Vila Alonso, 2020) mediante la ecuación  $PE = F \times V$ , donde PE = Pérdidas Esperadas, expresada en pesos y en forma anual, F = Frecuencia, veces probables en que el riesgo se concrete en el año y V = Pérdidas estimadas para cada caso en que el riesgo se concrete expresado en pesos.
- Se debe utilizar el análisis Costo / Beneficio (C/B) al comparar los costos y beneficios de las diferentes decisiones mediante el cálculo  $(C/B) = \text{Beneficios} / \text{Costos} \geq 1$ , mayor que uno es rentable el proyecto a aplicar y los beneficios superan a los costos.

#### Aplicación de controles

Con el objetivo de que cada riesgo identificado previamente quede cubierto y pueda ser auditable, la norma NC ISO/IEC 27001:2016 establece en su última versión hasta 114 puntos de control, que son un conjunto de acciones, documentos, medidas, procedimientos a adoptar para dar cumplimiento a los objetivos de la organización, que se dividen por las políticas de SI y controles operacionales. Los controles son medidas de seguridad orientadas a mitigar los riesgos encontrados en el análisis de estos de manera que se encuentren por debajo del nivel asumido por la organización.

Cada organización, según sus características, puede añadir más puntos de control si lo considera conveniente, así como personalizarlos para adaptarlos a su propio plan estratégico, pero siempre deben estar alineados a lo que pide la norma. Los controles seleccionados por la organización serán recogidos en un documento llamado declaración de aplicabilidad, donde se comparan los controles seleccionados con los del anexo A de la NC ISO IEC 27001, se justifican las inclusiones y exclusiones de los 114 controles, estén implementados o no.

Formará parte de las herramientas de control de utilidad para el comité de SI y responsables del sistema de control interno de la organización. Para la elaboración de la misma se recomienda la utilización de la tabla declaración de aplicabilidad recogida en el (Anexo 5), en la misma se recogen las siguientes informaciones:

Clausula: Número de la cláusula de la norma al que pertenece el control.

Objetivos: Número del objetivo de la norma al que pertenece el control.

Controles: Número del control de la norma a analizar.

Aplicabilidad S/N: Se determina si el control es aplicable o no en la organización.

Justificación: Las razones para comprender si el control es aplicable o no.

### Asignación del dueño del riesgo

Se definirá por el comité de SI, es la persona encargada de asumir el riesgo e implementar las salvaguardas para mitigar su impacto en la organización.

### Elaboración del plan de tratamiento de riesgos

Es importante tener en cuenta que la elaboración de un plan de tratamiento de riesgos requiere un análisis de costo-beneficio de los controles a implementar y el presupuesto asignado para su elaboración, de allí la importancia de darle prioridad a aquellos escenarios de riesgo que son más críticos para la organización (Valencia-Duque, 2017).

El propósito del plan es documentar como será implementado, que sea consistente con las metas y objetivos de la organización en la planificación del proceso de gestión, incluyendo las razones del tratamiento, los beneficios que se esperan obtener, los responsables de su aprobación e implementación, los recursos que se necesitan, medidas de tratamiento, tiempo y programación de cada una de las actividades.

**Responsable:** Comité de SI y responsables del sistema de control interno

### **Recomendaciones**

Para la realización de este análisis se propone tormenta de ideas, listas de verificación, observación directa, informes anteriores de no conformidades, informe de análisis de brechas. Se recomienda para el proceso de gestión de riesgos el uso de la herramienta informática "Gestión de la SI" desarrollada por la autora (anexo 6), que a su vez se apoya para el desarrollo de este paso en el catálogo de posibles amenazas sobre los activos que propone la metodología MAGERIT.

### **Paso 9: Continuidad de la SI**

**Objetivo:** Garantizar la continuidad de la SI de las funciones críticas de la organización en caso de registrarse un evento disruptivo en sus operaciones.

### **Acciones a realizar**

La gestión de la SI debe estar estructurada por tareas que apoyarán a que tenga una continuidad de forma fácil. Este proceso debe estar planificado y aprobado previamente por la alta dirección conjuntamente con los objetivos del SGSI.

Se comienza por:

- Análisis y evaluación de riesgos como el punto concéntrico de la continuidad de la información, partiendo del alcance del SGSI.
- Análisis de impacto al negocio, para determinar que procesos son críticos para la continuidad de la organización y sobre la base de estos priorizar que procesos se van a restaurar con mayor prontitud.

- Desarrollo de estrategias sobre la base del análisis de impacto al negocio y la evaluación y análisis de los riesgos de SI.
- Desarrollo del plan.

Análisis y evaluación de riesgos (previamente gestionados en el paso 8)

Análisis de Impacto al Negocio (BIA)

El BIA es un paso crítico en el desarrollo de una estrategia de recuperación de desastres, consiste en determinar que procesos son críticos para la organización y van a ser restaurados con mayor premura. Se deben seleccionar aquellos procesos que por sus funciones se relacionen con la misión y el cumplimiento de los objetivos de la organización. Una vez seleccionados los procesos que van a intervenir en el estudio se realiza un análisis en base a qué factores se verían afectados en la organización si se materializase un evento disruptivo. Los factores que pueden afectar a la organización son factores tangibles e intangibles. Dentro de los tangibles tenemos factores financieros/económicos, costos/gastos; los intangibles son factores regulatorios, de imagen, de servicios.

Para evaluar el impacto de estos factores se ha seleccionado un método semi-cuantitativo utilizando la escala de Likert establecida en cinco niveles (insignificante, menor, dañino, severo, crítico), cuanto más impacte la pérdida de un factor mayor será su valoración. Para evaluar el impacto dirigirse a la (tabla 4) del paso 7 de esta metodología, basta con tener un factor valorado como crítico para señalar que el proceso es crítico. Luego se priorizan aquellos que son críticos y se dejan para una segunda instancia los restantes analizados, aunque sean definidos como no críticos, considerando que están dentro del alcance del SGSI.

Para las actividades que se identifiquen como críticas se determina el MTD que es el tiempo máximo tolerable de interrupción que puede soportar la organización, el RTO indica el tiempo en el cual se vuelve a operar en condiciones mínimas aceptables y siempre va a ser menor que el MTD. Otro factor es el RPO, que es el punto desde el cual se debe recuperar la información para no tener pérdidas considerables, es donde se le asigna a cada proceso la prioridad de recuperación teniendo en cuenta el MTD definido. Otro factor resultante del BIA es el WRT, definidos como el tiempo disponible para recuperar datos perdidos (figura 11 y figura 11.1).

			Impacto Factores					
			Tangibles		Intangibles			
N.	Procesos	Activos	Financieros	Costos	Regulatorio	Imagen	Servicios	Criticidad S/N

Figura 11: Análisis de impacto al negocio, pantalla del software “Gestión de la SI”

### Estrategias

En base a los resultados del BIA y del análisis de riesgos, el objetivo que se persigue en esta tarea es definir escenarios disruptivos, para determinar las estrategias a seguir identificando las alternativas de recuperación de los procesos críticos de la organización en concordancia con los tiempos definidos y acordados.

N.	Procesos críticos	MTD	RPO	RTO	Riesgo residual	Posibles escenarios disruptivos

Figura 11.1: Identificación de escenarios disruptivos

La elección de las diferentes alternativas de recuperación depende de las necesidades de la organización: tiempos de recuperación, costos, recursos, entre otros.

### Desarrollo del plan

Una vez que las estrategias han sido definidas, deben identificarse los métodos, plazos, personas, recursos y tareas necesarias para implementarlas, así como también, la puesta en marcha por los encargados de la recuperación de desastres de la organización, que serían las personas encargadas de asumir los riesgos e implementar las estrategias determinadas.

**Responsables:** Alta dirección y Comité de SI

### **Recomendaciones**

Para la realización de este análisis se propone tormenta de ideas, listas de verificación, observación directa, informes anteriores de no conformidades, informe de análisis de brechas. Se recomienda el uso del software desarrollado por la autora, el mismo tiene como base la gestión de activos de información y el análisis y evaluación de los riesgos, desarrollados anteriormente en los pasos 7 y 8.

### **Fase 4: Verificación y mejora**

#### **Paso 10. Monitoreo**

**Objetivo:** Asegurar la SI.

#### **Acciones a realizar:**

- Supervisar la organización, ejecución y revisión del inventario de activos de información y el plan de tratamiento de riesgos.
- Realizar pruebas al plan de continuidad de la SI, garantizando su utilización como instrumento ante eventos disruptivos que afecten los activos de información incluidos en los procesos críticos de la organización.

**Responsables:** Comité de SI

### **Recomendaciones:**

La organización analizará y evaluará los cambios internos y externos del entorno, a fin de actualizar el inventario y el plan de tratamiento de riesgos. Este trabajo puede enriquecerse con las opiniones de los directivos y trabajadores, de forma individual o en asambleas, con la finalidad de hacer las propuestas que se estimen oportunas a partir de las nuevas condiciones, pudiendo contribuir a la eliminación de algún riesgo identificado, o a la determinación de nuevos riesgos.

En el caso de aparecer nuevos riesgos, después de su correspondiente gestión y el análisis de la criticidad de los procesos, se deben de identificar nuevos escenarios disruptivos que afecten la continuidad de la SI y por ende el correcto funcionamiento de la organización. Sobre la base del desarrollo de estos escenarios se deben de determinar las estrategias a seguir, para garantizar en el menor tiempo posible que la organización vuelva a operar en condiciones normales.

### **Paso 11: Auditorías internas**

**Objetivo:** Identificar el estado de protección del SGSI, para prevenir y corregir las posibles vulnerabilidades y amenazas que aprovechan las brechas de seguridad a las que está expuesta la organización.

#### **Acciones a realizar**

El SGSI debe ser auditado regularmente a intervalos determinados. Muchas veces las personas no son conscientes de que están haciendo algo mal y de saberlo no quieren ser descubiertos y esto puede llegar a dañar a la organización. A continuación, se despliega el procedimiento para planificar y llevar a cabo las auditorías internas del SGSI que da solución a la gestión eficaz de auditoría en seguridad.

#### Selección de auditores

El RSI debe seleccionar y proponer para su aprobación al auditor líder y demás miembros del equipo auditor. Debe asegurar que los miembros seleccionados del equipo auditor cuenten con las competencias y hayan participado en las actividades de desarrollo profesional continuo apropiadas para mantener los conocimientos y habilidades necesarias para gestionar el programa de auditoría.

En el caso de que se contrate a un auditor externo para la realización de una auditoría interna, se solicitará los documentos acreditativos que evidencien sus competencias para realizar la actividad.

#### Crear el programa de auditoría interna

Las auditorías internas al SGSI deberán estar integradas al programa anual de auditorías del

SIG de la organización, será elaborado por el RSI en coordinación con el director de la entidad, quién tendrá la responsabilidad de aprobarlo y presentarlo al consejo de dirección al finalizar el año, según formato del (Anexo 7), en el mismo se recogen las siguientes informaciones:

Auditoría: Se pondrá el número de la auditoría y el área que será auditada

Plan: Fecha en que se planifica realizar la auditoría in situ. En las columnas debajo de cada mes se deberán expresar la fecha plan y real de cada auditoría

Elaborado: Deberá ser firmado por el RSI.

Aprobado: Deberá ser firmado por el Director de la organización.

Fecha de aprobación: Fecha en que se aprobó el programa.

#### Establecer la independencia, objetividad e imparcialidad

Las auditorías internas se realizan por personal externo o de la propia organización, que deben contar con la formación necesaria para la realización de esta actividad, siempre prestando especial atención al cumplimiento del principio de independencia. Deben ser personas imparciales, objetivas, éticas y responsables, siempre prestando atención al manejo de la información durante la auditoría.

#### Planificar las actividades de auditorías

El RSI es el encargado de planificar y organizar las auditorías internas al SGSI. Para la planificación de las actividades de auditoría es conveniente que estén claros que procesos son críticos para la organización y si están dentro del alcance definido. Se ha de contar con un procedimiento que contenga las responsabilidades de cada una de las partes involucradas en la auditoría y las obligaciones que han de cumplir para la planificación y los registros que se generan con el desarrollo de la misma.

#### Asignar y administrar los recursos del programa de auditoría

Para ejecutar un programa de auditoría de forma eficaz se tendrá en cuenta la disponibilidad de la información, la cooperación del auditado, los tiempos acordados y recursos apropiados. Si el equipo auditor que desempeñará la tarea es personal interno de la organización este tiene que ser liberado de sus actividades cotidianas para efectuar la tarea con la calidad requerida. Si de lo contrario se realizará con personal externo se debe contar con los recursos necesarios para la contratación del servicio. El RSI es el responsable de informar de estos requerimientos a la alta dirección para su aprobación y posterior cumplimiento.

#### Realizar actividades de auditoría

Las auditorías se iniciarán con una reunión de apertura con la dirección del auditado y personal de las áreas auditadas. La misma será presidida por el auditor líder, donde se hará la presentación de los participantes, se confirmarán los horarios, recursos y arreglos necesarios al plan para su adecuación.

Las auditorías del SGSI son revisiones del sistema y controles. Estas pueden centrarse en la parte técnica, donde se revisa completamente el informe de declaración de aplicabilidad o los requisitos establecidos en la NC ISO/IEC 27001:2016. El informe de declaración de aplicabilidad es en la práctica el documento por el cual el auditor verificará el cumplimiento o no de las inclusiones/exclusiones de los controles documentados.

Se recopilará la información obtenida por diversas fuentes tales como: registros, entrevistas, análisis de datos, indicadores de desempeño, observaciones directas, retroalimentación del cliente, entre otras. El equipo auditor evaluará las evidencias de la auditoría frente a los criterios de auditorías para documentar los hallazgos y clasificarlos en no conformidades y observaciones; registrando los mismos en el (Anexo 8).

El auditor líder preparará el informe de la auditoría en conformidad con lo establecido en el (Anexo 9). Se presentará por el auditor líder al director en un período no mayor de 5 días posterior a la reunión de cierre, quién aprobará el mismo.

#### Finalización de la auditoría

La auditoría finaliza cuando todas las actividades descritas en el plan de la auditoría se hayan realizado y el informe de la auditoría aprobado se haya distribuido.

#### Actividades de seguimiento

El RSI asegura el seguimiento y cierre de las no conformidades derivadas de los resultados de las auditorías internas, mediante visitas, presentación de evidencias o auditorías posteriores, comprobando la implementación y eficacia de las acciones.

Para evaluar la eficacia del programa de la auditoría se tendrá en cuenta entre otros los siguientes indicadores:

- Cumplimiento del programa.
- Cumplimiento de los objetivos específicos de cada auditoría.
- Eficacia de las acciones implementadas para eliminar las no conformidades identificadas en las auditorías anteriores, analizando en profundidad las no conformidades que se repiten.
- Resultado de la evaluación del desempeño de los auditores.
- Acciones desarrolladas para el mantenimiento y mejora de la competencia de los auditores.

**Responsables:** RSI y auditores

#### **Recomendaciones**

Para realizar el proceso de auditoría es de apoyo la norma NC ISO 19011 que establece las directrices para auditar sistemas de gestión. Es necesario contar con los resultados de las



auditorías anteriores internas/externas, resultados de la aplicación de controles periódicos, peticiones, quejas, reclamos, sugerencias, cumplimiento de los requisitos legales y otros requisitos. Suponiendo que la organización a implementar este paso tenga implementado un SIG o SGC y cuenten con un procedimiento de auditoría, solo deben de hacer uso de las cualidades distintivas de las actividades descritas. Para el caso objeto de estudio de esta investigación se recomienda en las tareas de establecimiento de independencia, objetividad e imparcialidad del equipo auditor, conjuntamente con la planificación de las actividades de auditorías y finalización de la misma, deben estar alineados con las actividades descritas en el procedimiento de auditoría interna del SIG de la organización.

### **Paso 12: Acciones de mejora**

**Objetivo:** Seguimiento del SGSI e implementar acciones que permitan asegurar el perfeccionamiento continuo del sistema.

#### **Acciones a realizar**

La organización tiene el deber de mejorar continuamente la eficacia de su SGSI. El principal elemento del proceso de mejora de un SGSI son las no conformidades, derivadas tras la realización de auditorías, ya sean de carácter interno/externo, revisiones por la dirección y otras actividades de medición y control. Dichas no conformidades se tienen que contabilizar, analizar las causas que las motivan y adoptar las acciones necesarias para evitar su recurrencia o repetición.

Se deben aplicar nuevos controles, si se detectan cambios en las actividades, en el contexto y los objetivos de la organización, en base a la experiencia y la detección de situaciones que excedan los niveles de aceptación de los riesgos asumibles por la entidad o que se compruebe que los controles establecidos no son eficaces ante situaciones adversas y no garanticen la continuidad de la SI. Siempre teniendo en cuenta que ante modificaciones es necesario un análisis costo/beneficio para luego aplicar nuevamente los controles, tareas incluidas en el paso 8 de esta metodología.

Los jefes de los diferentes procesos pueden detectar oportunidades de mejora, que deberían documentar y ser entregados al RSI, luego serán presentados por este al comité de SI para su aprobación o no. El RSI debe determinar los plazos donde se llevarán a cabo las acciones de mejora del SGSI, y es la persona con más responsabilidad en el desarrollo de esta tarea.

Es necesario la elaboración de un plan, en el que estarán incluidas las oportunidades de mejora aprobados por el comité de SI, siempre con el objetivo de que tributen a la mejora continua del SGSI y de los procesos. El comité de SI debe realizar reuniones siempre que la situación lo amerite, con el fin de discutir y seguir las acciones de mejora, por lo que el mantenimiento de este plan será de forma continua y sistemática. Una vez culminadas las acciones de mejora

plasmadas en el plan, se aplica nuevamente el diagnóstico, utilizando la lista de chequeo consolidada de los requisitos de la NC ISO/IEC 27001 y su anexo A, sustentado en el código de práctica NC ISO/IEC 27002. Este nuevo estudio permite comparar los resultados del análisis de brechas obtenido antes de la implementación de las acciones de mejora y después de haber llevado a cabo las mismas.

**Responsables:** RSI y Comité de SI

### **Recomendaciones**

El plan debe contener otros datos que puedan ser de interés (ej. información sobre la descripción de la mejora, responsables de ejecución, acciones de seguimiento). Debe permitir el control y seguimiento de las diferentes acciones a desarrollar.

### **Conclusiones del capítulo**

Se logra diseñar una metodología para la gestión de la SI como contribución a la continuidad del negocio. La misma logra una eficaz gestión de la SI, a partir de la integración de modelos, normas, herramientas y buenas prácticas en la implementación de un SGSI, que se alinea con el estándar NC ISO/IEC 27001:2016 y coherente con el ciclo de mejora continua.

La metodología elaborada sigue un enfoque de procesos, en el que se sustenta el desarrollo de la herramienta informática para la gestión de activos de información, el análisis y evaluación de riesgos y la continuidad de la seguridad de la información. Las características de la metodología permiten que sea aplicable a organizaciones de cualquier sector empresarial.

### **Capítulo 3: Aplicación de la metodología para la gestión de la SI como contribución a la continuidad del negocio**

En el capítulo se recoge el resultado de la aplicación parcial de la metodología propuesta aplicada en la OTNH. La presente es una investigación que aún está en pleno desarrollo y dado el factor tiempo solo se ha podido llegar hasta el proceso de análisis y evaluación de riesgo. En la etapa desarrollo se hace uso de la herramienta informática desarrollada por la autora, con el objetivo de realizar una eficaz gestión de activos, resultado base para el proceso de análisis y evaluación de riesgos y continuidad de la SI.

#### **Etapas 1: Planificación del proyecto**

##### **Paso 1 Compromiso de la alta dirección**

El primer paso en esta etapa fue la búsqueda de referencias bibliográficas que permitió la actualización de la información en relación a la SI. Para ello se consultaron artículos de bases de datos Redalyc, Google Scholar, Dialnet, ScienceDirect y Scielo, así como metodologías, guías y procedimientos afines al objeto de investigación.

Luego se procedió a realizar encuentros y reuniones preliminares con los directivos de la organización, donde se presentaron los resultados obtenidos de la investigación y los principales conceptos para mejor entendimiento de la actividad. Se resaltaron las ventajas de implementar un SGSI, encaminado a mejorar el desempeño de la organización a través de una adecuada gestión de los riesgos relacionados con la información. De forma general se realizaron 6 encuentros con el consejo de dirección donde se cumplieron las siguientes actividades:

- Se efectuó un intercambio entre los miembros del consejo, donde se propició un debate abordando sus preocupaciones y aclarando sus dudas.
- Se especificaron los escenarios de aplicación de la gestión de la SI, principalmente relacionados con los activos de información vinculados a los procesos y subprocesos donde los riesgos pueden impactar negativamente con mayor intensidad.
- Se definió la política de SI adecuada al propósito de la organización, en la que se incluyen los objetivos de SI y su vinculación con el SIG (anexo 10).
- Se definieron los tiempos, las áreas involucradas, los recursos necesarios para la implementación del SGSI y la forma de acceder a ellos.
- Se definieron los recursos que garantizarán la continuidad de la SI en caso de un evento disruptivo.

- Se formuló el compromiso de SI y se manifestó a través de la firma del acta la voluntad del consejo de dirección en el cumplimiento de sus funciones y responsabilidades sobre la SI.

Por tanto, se logró el compromiso y la disposición de los actores, principalmente de la alta dirección con respecto a la puesta en práctica de la metodología, brindando las facilidades para su ejecución.

## **Paso 2 Conformación del comité de SI**

Como órgano máximo consultivo sobre la SI en la organización se crea el comité de SI. El mismo se establece en reunión efectuada con consejo de dirección ampliado, contando con la presencia de los jefes de procesos de las áreas relevantes y que aporten al SGSI.

El mismo quedó estructurado por la responsable de seguridad informática, encargada de la ejecución de los cronogramas propuestos y responsable de realizar las propuestas de SI ante el comité. Lo integran también el jefe de grupo de seguridad y protección, a partir de su responsabilidad en la protección de los activos físicos de información, el administrador de red como persona que domina los aspectos técnicos relacionados con las TIC, el asesor jurídico para la actualización del marco legal vigente en temas de SI y las TIC, la especialista de recursos humanos por la importancia que tiene a la hora de contratar al nuevo personal que ocupará cargos relacionados con la SI y la especialista de control interno como parte importante en la gestión de riesgos.

Este comité también contó con la participación del director como líder del proyecto y de los jefes de departamentos de las áreas relevantes, que en los diferentes procesos almacenan y transmiten información que se procesan en las TIC. Luego de su conformación, el comité de SI fue presentado en una reunión al consejo de dirección, el cual aprobó en su totalidad el grupo conformado y designó como representante del SGSI ante la dirección y del comité de SI al responsable de seguridad informática.

Con el objetivo de aplicar la metodología se determinaron las principales técnicas y herramientas útiles para que puedan ejecutar el diagnóstico, además de diferentes prácticas de trabajo en grupo para la solución de problemas. Se determinaron las necesidades de aprendizaje de los integrantes del comité de SI, para ello se elaboró un plan de capacitación a corto plazo (Anexo 11), con los temas identificados en las necesidades de aprendizaje, es responsabilidad del área de recursos humanos garantizar la ejecución del plan. De forma general, se cumplió con el 100% de las actividades de capacitación planificadas para los miembros del comité de SI, en los horarios, fechas y lugares correspondientes.

### **Paso 3 Concienciación y formación**

La concienciación referida a la SI es un pilar fundamental de la gestión de la seguridad y por tanto un cambio en la cultura actual requiere desaprender o modificar las creencias actuales de la totalidad de los empleados de la organización.

Como primera acción se realizó un encuentro en el que participaron el RSI conjuntamente con el consejo de dirección y se definieron los financiamientos requeridos para cubrir al menos los requisitos mínimos de concienciación y formación que garantiza el involucramiento de la totalidad de los trabajadores. Se efectuó un segundo encuentro, donde se incluyeron los aspectos de SI derivados de la política de SI en la estrategia de comunicación institucional y en el plan de divulgación, incluyendo las responsabilidades, qué se comunica, a quién y cuándo; se responsabilizó de esta tarea a la jefa del departamento de gestión.

En un tercer encuentro realizado por el RSI y el consejo de dirección se definieron las competencias básicas que son necesarias para llevar a cabo las diferentes actividades en materia de SI y que a su vez son desplegadas hacia sus procesos, por lo que se concretó un plan de formación (anexo 12).

Para el desarrollo de este plan se conformaron 5 grupos objetivos, que por sus funciones tienen más sensibilización con la información y continúan hacia abajo en la jerarquía. Se comenzó con el consejo de dirección y los puestos de responsabilidad, ya que los altos cargos son los que convencen al resto de los trabajadores y conocen las necesidades reales de la SI. Un segundo grupo para el personal de informática y comunicación, los primeros encargados de la implementación y control de las salvaguardas de los medios informáticos, que asesoran y están prestos a aclarar cualquier duda que se presente por parte de los usuarios de las computadoras y comunicación, como parte importante para esquematizar la estrategia de SI que se da a conocer por los diferentes medios, tanto para el personal interno como externo. Un tercer grupo con los especialistas de los procesos que de una forma u otra son los que generan, procesan, transmiten y reciben la información. Un cuarto grupo conformado por el personal técnico y un quinto grupo con el personal de servicios, que, aunque no opere directamente con la información deben conocer los aspectos básicos y estar involucrados en el proyecto.

En ese mismo encuentro se define que al iniciar un trabajador su vínculo laboral, en conciliación con el área recursos humanos, éste recibe instrucciones respecto al uso de las tecnologías informáticas, incluyendo el conocimiento del código de ética para el uso de los servicios que existen en la entidad y sus responsabilidades con el SGSI.

Las personas (internas o externas) que realizan trabajos bajo el control de la OTNH deberán tener en cuenta la política de SI. La misma fue socializada por los medios de comunicación existentes en la OTNH, a través de la Intranet, página web institucional, redes sociales,

carteles, salvapantallas en los ordenadores de trabajo, alertas generadas por ordenador, mensajes de correo electrónico, chats. En el caso del personal externo, se establecieron los mecanismos para implantar y medir el control, de acuerdo al contrato existente y a la legislación vigente.

Se realizaron charlas en los matutinos donde se expusieron las principales conceptualizaciones para un mejor desarrollo y entendimiento, encaminadas a asegurar que las personas tomen conciencia de la importancia de su implicación en los procesos y actividades del SGSI. Se abordaron las mejores prácticas y hábitos de comportamiento que son importantes para evitar que se materialicen riesgos y así poder garantizar niveles de protección adecuados.

#### **Paso 4 Determinar el alcance del SGSI**

El comité de SI como primera tarea establece los límites para la implementación del SGSI, con el objetivo de definir qué se quiere proteger y detectar y contrarrestar las acciones que pongan en peligro la confidencialidad, disponibilidad e integridad de la información.

La sede principal de la OTNH, sita en Carretera al Valle de Mayabe No. 161, entre 12 y 12 A, Reparto Villanueva, es una construcción civil de dos plantas, con un área de 6 600 m<sup>2</sup>. Su estructura organizativa comprende los departamentos de Mediciones Electro-fisicoquímicos, Mediciones Mecánicas, Normalización e inspección y supervisión, así como departamentos de Recursos Humanos, Economía y Gestión, como áreas de regulación y control; todos con sus funciones, responsabilidades y autoridad definidas según el Reglamento Orgánico, las fichas de cargos y en los propios documentos generales y específicos del SIG. A ella se subordinan dos unidades territoriales ubicadas en las provincias de Granma y Las Tunas.

La organización gestiona sus actividades y recursos por procesos por lo que se seleccionaron en primera instancia aquellos que por sus funciones y responsabilidades ayudan a dar cumplimiento a la misión institucional y están vinculados a la SI.

El SGSI aplica a todos los procesos, servicios y actividades que presta la OTNH, que tienen vinculación con los activos de información, por lo que se propone un nuevo mapa de procesos (anexo 13) en el que se incluya la gestión de la SI. Los activos protegidos son ubicaciones físicas, información impresa, información digital, registros, política de SI y las complementarias de temas específicos, procedimientos, software, hardware, redes de comunicaciones, medios auxiliares.

La OTNH al prestar sus servicios confía en proveedores externos como DESOFT CITMATEL, SERTOC, que mediante acuerdos contractuales proporcionan habilidades y componentes de la infraestructura para brindar soluciones a servicios que acceden, almacenan, comunican, tratan y procesan la información de la OTNH.

La OTNH también está obligada a compartir información con Delegación del CITMA, Gobierno Provincial, Oficina Nacional de Normalización, CONAS, OSRI, DESOFT y otras instituciones externas debido a asuntos legales, regulatorios, requisitos legales o comerciales.

La OTNH garantiza la protección de la información que se encuentra en sus instalaciones y el derecho de propiedad del cliente, que abarca equipos de medición, instalaciones e informes de resultados de servicios prestados, al garantizar procesos de adquisición sólidos, amparados por procedimientos, acuerdos contractuales y otros para compartir información.

Emplea una fuerza laboral de 109 trabajadores vinculados directamente a los procesos, actividades y operaciones fundamentales; que son los encargados de recopilar, procesar, almacenar y transmitir la información, con el objetivo de cumplir las funciones, objetivos y metas de la organización. La tabla 6 muestra el levantamiento de activos de información identificado por áreas:

Tabla 6: Levantamiento de activos de información

<b>Tipo</b>	<b>Ubicación</b>
HW, SW, Media, P, D, L, Aux, DP	Dirección
HW, SW, Media, P, D, L, Aux, DP	Asesor Jurídico
HW, SW, Media, P, D, L, Aux	Seguridad y Protección
HW, SW, Media, P, D, L, Aux, DP	Recursos Humanos
HW, SW, Media, P, D, L, Aux	Gestión
HW, SW, Media, P, D, L, Aux, DP	Ventas
HW, SW, Media, P, D, L, Aux, DP	Recepción y Entrega
HW, SW, Media, P, D, L, Aux, COM, S, DP	Informática
HW, SW, Media, P, D, L, Aux	Economía
HW, SW, Media, P, D, L, Aux	Servicios Internos
HW, SW, Media, P, D, L, Aux	Aseguramiento metrológico
HW, SW, Media, P, D, L, Aux	Normalización
HW, SW, Media, P, D, L, Aux, DP	Inspección y supervisión
HW, SW, Media, P, D, L, Aux	Vicedirección
HW, SW, Media, P, D, L, Aux	Masa
HW, SW, Media, P, D, L, Aux	Volumen
HW, SW, Media, P, D, L, Aux	Dimensional
HW, SW, Media, P, D, L, Aux	Electricidad
HW, SW, Media, P, D, L, Aux	Temperatura
HW, SW, Media, P, D, L, Aux	Presión
HW, SW, Media, P, D, L, Aux	Físico Químico

Datos personales (DP), Información (D), Instalaciones (L), Servicios (S), Software o aplicaciones informáticas (SW), Hardware o equipamiento informático (HW), Personal (P), Redes de comunicaciones (COM), Soportes de información (Media), Equipamiento auxiliar (Aux)

Quedan fuera del alcance del SGSI en una primera etapa las unidades territoriales de las provincias de Las Tunas y Granma. Una vez consolidado el SGSI en la OTN de Holguín se irá ampliando paulatinamente el alcance a las unidades territoriales.

## **Etapa 2 Diagnóstico**

### **Paso 5 La organización y su contexto**

Para el desarrollo de este paso se hace uso de la documentación existente en la organización relacionada con la SI, planeación estratégica y planes que brindan información que permiten posicionar a la organización con respecto a su medio. Se realizaron entrevistas con altos mandos, análisis de las fortalezas, debilidades, oportunidades y amenazas de la organización, observación de procesos y actividades.

Se analizaron los documentos legales de constitución de la organización y su objeto social, se revisaron los componentes fundamentales de la planeación estratégica, tales como misión, visión, políticas y objetivos, entre otros. A criterio de la autora son apropiados, retadores, contribuyen al mejoramiento de la organización y tributan al crecimiento de la economía nacional y la elevación de la calidad de vida de la población.

Desde el año 2015 comenzó el proceso de informatización de todas las actividades del centro. Estos servicios soportados en las TIC son vitales para el funcionamiento y estabilidad del correcto funcionamiento de los procesos de la OTNH, que están enfocados en el mejoramiento de su estructura, su desarrollo organizacional y mejores servicios enfocados al cliente. Por tal motivo se propone la introducción de la gestión de la SI como proceso estratégico, ya que soporta la infraestructura tecnológica que acarrea los procesos del negocio y garantiza la seguridad de los activos de información.

El software NORMET, administra, recolecta, recupera, procesa, almacena y distribuye información relevante de todos los procesos fundamentales de la OTNH, incluyendo informaciones confidenciales generadas de los servicios de inspección estatal. El proceso de planificación está informatizado con las facilidades que brinda la herramienta Agenda Express, este proceso llega a todas las áreas del centro. Se cuenta con la implementación de la herramienta OCS Inventory para el proceso de informática, recopila la información correspondiente al hardware y software de los equipos que hay conectados en la red, y para el proceso de capacitación externa se cuenta con la implementación de una plataforma virtual, herramienta que brinda las posibilidades de realizar enseñanza en línea, contribuyendo a la formación y superación de las entidades de la economía. También en la entidad están informatizados los procesos de recursos humanos con la aplicación FASTOS y economía, conjuntamente con el área de facturación con la aplicación RODAS, gestionándose a través de



ellas toda la información que se genera de estos procesos, que por sus características son de carácter sensible. La gestión de la información se explota mediante la utilización de una intranet, que contiene toda la información documental del SIG, además está vinculada con el software RODAS para la gestión de las incidencias de cada trabajador.

La entidad cuenta con 48 PC, existen además de ellas 6 servidores con sus diferentes funciones. Los sistemas operativos instalados son Windows XP, 7, 8, y 10. El cableado de la red está soportado por cable UTP y protegido con canaletas. Las estaciones de trabajo se agrupan por áreas a partir de un conmutador. Los servidores soportan distintos servicios que brindan a los usuarios de la organización

El intercambio de mensajería se realiza a través de los protocolos POP3 e IMAP para la recepción y SMTP para el envío. La autenticación del servicio se hace mediante protocolo seguro SSL y https. El servicio de conectividad se recibe a través de ETECSA por medio de una línea arrendada de 4 Mb/s.

En la organización los usuarios se benefician de los servicios de internet, correo nacional e internacional, internet en residencias mediante acceso conmutados, acceso a internet a través de la incorporación de una red wifi dentro de las instalaciones, por lo que se hace necesario crear los mecanismos para el correcto uso de la misma, para ello se deben aplicar políticas de seguridad específicas. Todos servicios que se brindan son autorizados por el director de la OTNH. Los encargados de controlarlos y garantizar el correcto funcionamiento son el administrador de la red y el responsable de seguridad informática.

El personal de informática es el encargado de impartir capacitación en computación al personal interno, en coordinación con el área de capacitación. También asesora y aclara cualquier duda que se presente por parte de los usuarios de las computadoras. Cuando un trabajador ingresa a la entidad se le da capacitación de la legislación vigente referente a la seguridad informática y el procedimiento que rige la seguridad informática. El personal que opera los medios, aun cuando no es experto en informática, posee los conocimientos y preparación necesaria para su empleo, en su mayor parte posee instrucción media o superior según el cargo que ocupa.

Se cuenta con una estructura documental vinculada con la actividad informática. Los procedimientos y registros se encuentran internos en el manual del SIG. No obstante, el procedimiento para la actividad informática está desactualizado ya que fue desarrollado sobre la base de la resolución N.127:2007 del MINCOM existiendo una actualización con la resolución N.128:2019 del mismo ministerio.

Todos los usuarios tienen asignado sus credenciales para acceder a las computadoras, cumpliendo con los requisitos establecidos para las claves de acceso. Por políticas de dominio

implementadas estas claves serán cambiadas cada 2 meses, con una longitud mínima de 8 caracteres, combinando números, letras y caracteres especiales.

Todas las computadoras de la entidad tienen instalado y actualizado el antivirus según las condiciones establecidas en el artículo N. 47 del decreto N.360:2019 del Consejo de Ministros, aunque se evidencia que ante códigos malignos detectados que se han eliminado por el mismo los usuarios no hacen uso del registro de incidencias establecido.

Todo el personal realiza salvallas periódicas para evitar la posible pérdida o destrucción de la información, aunque se evidencia que la mayoría no hace uso del registro establecido para el control de salvallas. El área de informática realiza salvallas mensuales de las bases de datos de los programas de software utilizados para el procesamiento de los datos, de las trazas del correo e Internet, de las trazas de los sistemas operativos de los servidores y de los ficheros de configuración de cada servicio de la red. A pesar de realizar copias de respaldo de toda la información vital del centro se incumple con lo establecido en el artículo N.63 del decreto 360:2019 del MINCOM, que establece que esta se debe almacenar en otra ubicación, que le permita no afectarse en caso de desastre en la ubicación principal.

A pesar del ancho de banda contratado para un mejor rendimiento de los servicios prestados, no pueden ser aprovechados totalmente por los usuarios porque el equipamiento tecnológico está obsoleto, lo que impide la creación de nuevos servicios mejorados informáticamente.

La organización cuenta con un plan de seguridad informática (PSI) que especifica las responsabilidades de cada uno de los participantes en el proceso informático. El mismo establece que las personas autorizadas a procesar información clasificada, una vez que cumpla su finalidad esta debe ser eliminada mediante el borrado seguro, utilizando para ello una herramienta que realice varias sobrescrituras; este proceso no se realiza según lo establecido. Las hojas de cálculos elaboradas en las diferentes áreas no tienen todas las celdas protegidas con clave. No se tiene en cuenta el análisis de riesgos contemplado en el PSI para la actualización del plan de tratamiento de riesgo de la organización, quedando amenazas sin tratar.

Los documentos específicos de los diferentes procesos son editados por el personal responsabilizado de su elaboración, entregando el original en copia dura al responsable del SIG (RSIG) para su conservación y control en el archivo maestro. Este archivo maestro se encuentra ubicado en el local de trabajo del RSIG, no teniendo implementadas las suficientes medidas de seguridad ante robo o destrucción de la información, ni poseyendo medidas de protección básicas para enfrentar un desastre.

**Se evidencian dificultades en el PSI en relación a:**

- Incluye en la estructura de gestión de la actividad informática y la seguridad informática cargos que no están establecidos en el centro y otros que no tienen vinculación con la actividad informática. Se propone la inclusión de una nueva estructura (Anexo 14).
- No coinciden los modelos definidos en el procedimiento del SIG para la actividad informática con los expuestos en el PSI, por lo que existe duplicidad de modelos (registro de salvas, registro de incidentes, registro de mantenimiento de recursos informáticos) para registrar la misma información.
- Se realiza un análisis de riesgos por una metodología poco entendible, calculando el riesgo de forma general y no calculando un valor para cada amenaza.
- Se calcula el riesgo solo teniendo en cuenta su impacto, obviando la probabilidad de ocurrencia para calcular su valor.
- No se definen ni se aplican criterios de aceptación de los riesgos que pueden ser asumido por la entidad.
- En el plan de recuperación ante contingencias están contempladas amenazas que no parten de análisis de riesgos realizado.
- En el epígrafe relacionado con los resultados del análisis de riesgo se hace referencia solamente a tres amenazas importantes, lo cual no se corresponde con lo obtenido en el análisis de riesgo desarrollado.
- Las políticas definidas tienen carácter general, quedando sin definirse elementos concretos de su implementación encaminados a proteger los servicios que se brindan en la red (correo electrónico, ftp, navegación, entre otros.).
- La clasificación de las áreas o zonas controladas no se realiza de manera adecuada por los siguientes motivos:
  1. No se identifican todas las áreas controladas existentes en la entidad.
  2. Se identifica el local de los servidores como área limitada, lo cual no se corresponde con la clasificación prevista en la base legal vigente.

Se aplicó la guía de ciberseguridad, emitida por el MINCOM arrojando los resultados siguientes:

- Cuentan con registros de incidencias en las diferentes áreas, el cual no es efectivo, quedando sin reflejarse los principales incidentes de seguridad.
- El administrador de la red y el especialista en ciencias informáticas trabajan en el local de los servidores y no existe una barrera de protección física que los separe.
- Se encuentra implementada una política de salva de la información la cual no es efectiva, ya que no cuentan con respaldo de la misma en una ubicación fuera de la

entidad, situación que dificultaría el proceso de recuperación después de producirse un ataque informático, desastre o fallo de los medios de almacenamiento en la ubicación principal.

- No tienen implementada la solución de antivirus reforzada.
- La entidad no cuenta con aterramiento para la protección del equipamiento ante descargas eléctricas.
- No se cuenta con fuentes de respaldo en las computadoras de trabajo.

### **Análisis del escenario de la organización**

Para formular las estrategias con relación a la SI se enumeran las fortalezas, debilidades, oportunidades y amenazas, con la finalidad de analizar las rutas en que la organización tome ventajas de los puntos fuertes para reducir las debilidades y se aprovechen las oportunidades para evitar o minimizar las amenazas.

### **Análisis de los factores internos**

#### **Fortalezas:**

1. Condiciones adecuadas de infraestructura (instalaciones y espacios de trabajo).
2. Disponibilidad de tecnología informática (equipos, red, intranet, correo y acceso a Internet).
3. Procesos normalizados.
4. Disponibilidad de recursos para la formación del personal.
5. Disponibilidad de información actualizada.
6. Alto potencial del personal técnico.
7. Elevado sentido de pertenencia del personal.
8. Flujo informativo a través de encuestas a clientes externos.

#### **Debilidades:**

1. Dificultades para reponer el equipamiento informático y limitaciones con la impresión de documentos.
2. Insuficiente comunicación institucional.
3. Falta de recursos para garantizar niveles adecuados de seguridad para resguardar la información.
4. Inadecuada gestión de riesgos
5. Poca implementación de controles preventivos y detectivos que garantice adecuados niveles de seguridad.
6. Desconocimiento de herramientas de SI

## Análisis de los factores externos

### Oportunidades:

1. Regulación favorable.
2. Competencia débil.
3. Necesidad del servicio.
4. Mejor imagen de los servicios y de la organización a nivel nacional.
5. Mejora de los servicios enfocados al cliente.

### Amenazas:

1. Existencia limitada en el mercado de recursos informáticos necesarios para la prestación de los servicios.
2. Aumento de precio de insumos.
3. Mala situación económica nacional.

## Paso 6 Análisis de brechas

Para el desarrollo de este paso se parte de que los puntos anteriores de esta metodología se han desarrollado según lo previsto. Para una estimación inicial del nivel de madurez del SGSI se han evaluado los requisitos de la norma NC ISO/IEC 27001, arrojando los siguientes resultados (Anexo 15).

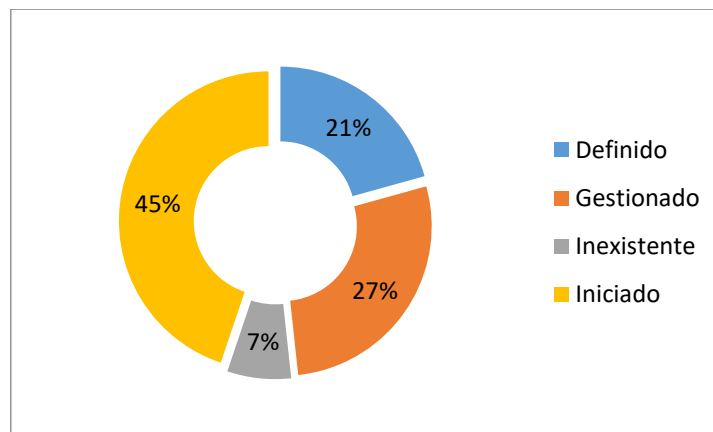


Figura 11: Nivel de madurez cumplimiento de requisitos NC ISO/IEC 27001

La figura 11 muestra los resultados del análisis de brecha para los requisitos de la norma NC ISO/IEC 27001 en porcentaje (%). Los % de cada uno de los requisitos son vinculados al nivel de madurez, asociado al cumplimiento o no de cada uno de ellos.

El resultado final del análisis de brecha vinculado a la organización se obtiene por el cálculo del promedio de los valores generales de cada requisito evaluado, obteniendo una calificación de 2.6, lo que posiciona a la organización con respecto a la gestión de la SI en un nivel de madurez iniciado. Esto demuestra que se ha trabajado en el desarrollo de registros, controles, procedimientos y buenas prácticas reconociendo la existencia de los problemas que deben ser

resueltos, pero se evidencia que los procesos son tratados de forma individual, no existiendo un método que se aplique de forma normalizada.

Se evidencia el apoyo de la alta dirección con el proyecto de implementación del SGSI, garantizando los recursos necesarios cuando se necesiten y así asegurar los resultados previstos. La política de SI está documentada y comunicada por los distintos medios de comunicación dentro de la OTNH y a otras partes interesadas. La misma proporciona objetivos enfocados a su establecimiento y coherentes con la dirección estratégica, prestando principal atención a las cuestiones internas y externas que pueden influenciar en su cumplimiento y dentro del alcance definido. Los roles, responsabilidades y autoridades para la SI se definen en el reglamento interno y en el código de ética que firma cada trabajador una vez contratado, también fueron definidos y asignados las responsabilidades para la implementación del SGSI mediante la conformación de un comité de SI, que fue comunicado a todos los trabajadores.

A pesar de que existe un proceso documentado para identificar los riesgos a nivel organizacional, se evidencia que quedan fuera de este las amenazas vinculadas a la SI que no son tratadas, el inventario de riesgos no se realiza a partir de un inventario de activos, en el que deberían estar incluidos los activos de información. La gestión del riesgo es reactiva, solamente determinando el impacto una vez que el riesgo se ha manifestado. No están definidos los criterios de aceptación del riesgo, lo que impide efectuar una adecuada evaluación de los mismos, lo que obstaculiza la creación de documentos específicos de SI como la declaración de aplicabilidad y el plan de tratamiento de riesgos.

Están definidos y efectuados los planes de formación y concienciación y los objetivos de SI fueron incluidos en la estrategia de comunicación, incluyendo las responsabilidades, qué se comunica, a quién y cuándo.

Existe un procedimiento para la aprobación, revisión y actualización de los documentos, identificación de los cambios y estado de versión, disponibilidad en los puntos de uso, identificación y disposición de los documentos que forman parte del SIG, pero no tiene incluido el alcance del SGSI. No están definidos que indicadores de eficacia de SI que serán evaluados, a través de qué método, responsable, y quien analizará y evaluará los resultados. A pesar que se cuenta con procedimientos para la realización de auditorías internas, revisión por la dirección, no conformidad y acciones de mejora, no están incluidos aspectos de SI que se derivan de las políticas de SI, procedimientos, objetivos, base normativa del SGSI, documentos de referencia y requisitos legales aplicables.

En la figura 12 se muestran los resultados del análisis de brecha para cada punto de control incluido en el anexo A de la norma NC ISO/IEC 27001 en porcentaje (%). Los % de cada nivel de madurez corresponde al cumplimiento o no de cada uno de los controles. En el (Anexo 16),

se muestran desplegado por objetivos de control las observaciones detectadas de la evaluación realizada.

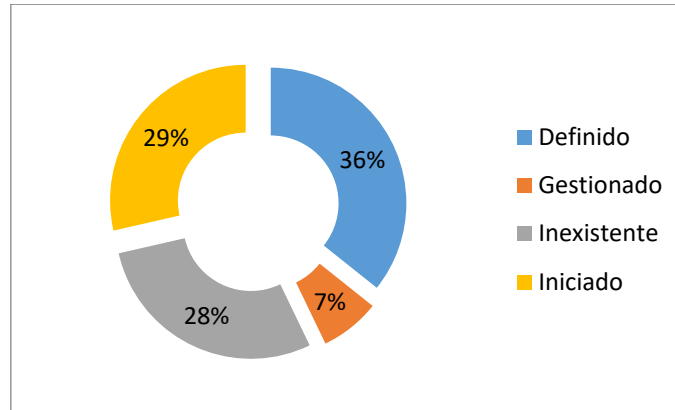


Figura 12: Nivel de madurez objetivos de control Anexo A, NC ISO/IEC 27001:2016

#### Documentos obligatorios y registros requeridos por NC ISO/IEC 27001:2016

- El alcance del sistema de gestión de seguridad de la información (cláusula 4.3)
- Política de seguridad de la información y objetivos (cláusulas 5.2 y 6.2)
- Metodología de evaluación y tratamiento de riesgos (cláusula 6.1.2)
- Declaración de aplicabilidad (cláusula 6.1.3 d)
- Plan de tratamiento de riesgo (cláusula 6.1.3 e y 6.2)
- Informe sobre evaluación de riesgos (cláusula 8.2)
- Definición de roles y responsabilidades de SI (cláusulas A.7.1.2 y A.13.2.4)
- Inventario de activos (cláusula A.8.1.1)
- Uso aceptable de los activos (cláusula A.8.1.3)
- Política de control de acceso (cláusula A.9.1.1)
- Procedimientos de operación para gestión de TI (cláusula A.12.1.1)
- Principios de ingeniería de sistemas seguros (cláusula A.14.2.5)
- Política de seguridad para proveedores (cláusula A.15.1.1)
- Procedimiento para gestión de incidentes (cláusula A.16.1.5)
- Procedimientos de Continuidad de la SI (cláusula A.17.1.2)
- Requerimientos legales, regulatorios y contractuales (cláusula A.18.1.1)

#### Registros obligatorios:

- Registros de formación, habilidades, experiencia y calificaciones (cláusula 7.2)
- Seguimiento y resultados de medición (cláusula 9.1)
- Programa y resultados de auditoría interna (cláusula 9.2)
- Resultados de la Revisión por Dirección (cláusula 9.3)
- Resultados de acciones correctivas (cláusula 10.1)

- Registros de las actividades de usuario, excepciones y eventos de seguridad (cláusulas A.12.4.1 y A.12.4.3)

### Etapa 3 Desarrollo

#### Paso 7 Gestión de activos

En este paso se identifican por procesos los activos de la organización. Con el objetivo de aplicar parcialmente la metodología debido al limitado tiempo de la investigación, no se seleccionaron aquellos activos que eran similares destinados a cumplir funciones análogas, con la finalidad de no repetirlos en el inventario, pues las estimaciones que se realicen para uno, serán similares en los demás.

A cada activo que está incluido en el inventario se le asigna un propietario y se describe de forma resumida su finalidad. La clasificación se realiza de acuerdo a sus características por las categorías definidas (figura 13).

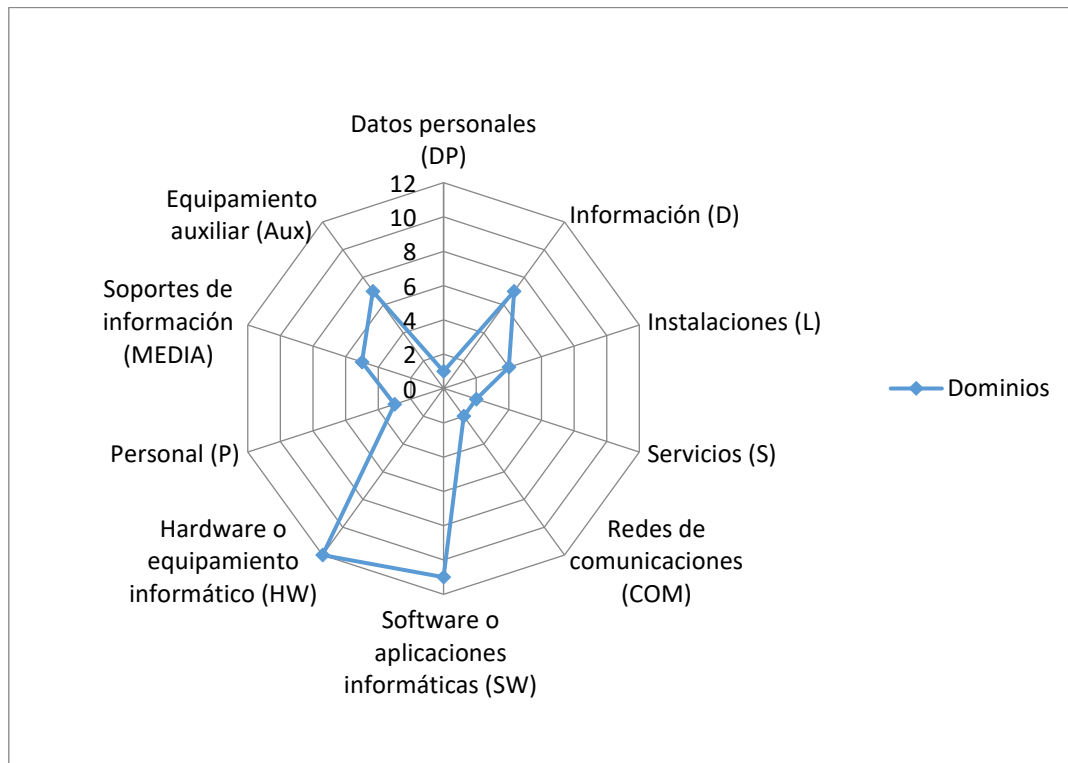


Figura 13: Clasificación de activos

La valoración se realiza a partir de la importancia y el papel que juegan dentro de la organización, teniendo en cuenta las propiedades de confidencialidad, integridad y disponibilidad (figura 14). El resultado se muestra en el (anexo 17).



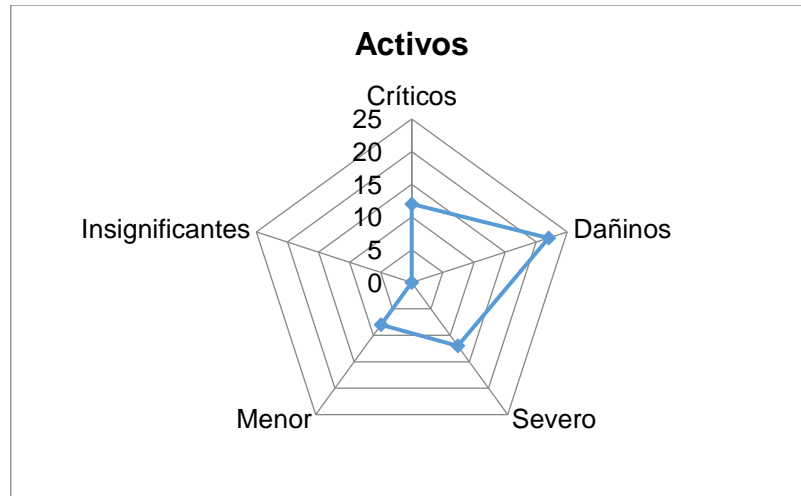


Figura 14: Valoración de activos

El inventario de activos se realizó según la clasificación de la metodología MAGERIT. Se identificaron 54 activos de información distribuidos por los distintos dominios.

### **Paso 8 Análisis y evaluación de riesgos**

En este paso se identificaron 49 amenazas vinculadas a los diferentes activos de información. Se obtuvo el valor del riesgo para cada una de ellas mediante la estimación de la probabilidad de ocurrencia y el impacto, asociado al daño que causaría en un activo su materialización.

Debido a la extensión de los resultados obtenidos, se selecciona una muestra de activos de los distintos dominios identificados y las amenazas que los afectan, con su respectiva evaluación, arrojando los siguientes resultados (anexo 18).

Tras el análisis realizado se identificaron las amenazas a las que está expuesta la organización y los activos que son susceptibles a ellas y sobre la base de los criterios de aceptación definidos, la organización asume los riesgos que están ubicados en una zona de riesgo baja y medio.

Por razones lógicas de disponibilidad de tiempo en esta investigación no serán tratados los activos que tienen asociados amenazas ubicadas en zonas de riesgo alto o extremo. Para estos casos se deben de aplicar tratamientos mediante la selección y la implementación de una o varias opciones para modificarlos, no sin antes haber realizado un análisis sobre lo que cuesta aplicar un control para prevenir, detectar o corregir los riesgos, contra lo que se pierde por el efecto o impacto de llegar a producirse, al comparar los costos y beneficios de las diferentes decisiones mediante el cálculo  $(C/B)=\text{Beneficios}/\text{Costos} \geq 1$ , precisar las personas a asumirlos y los periodos de implementación de las salvaguardas para mitigar su impacto.

Luego de este paso fundamental, se identifican los procesos que soportan los servicios críticos para el funcionamiento de la organización, que conjuntamente con el proceso de análisis y

evaluación de riesgos facilita el desarrollo de las estrategias, que permiten realizar la protección y recuperación de las actividades críticas del negocio.

### **Conclusiones del capítulo**

La aplicación parcial de la metodología en la OTN de Holguín manifiesta su utilidad práctica como un instrumento metodológico. El resultado muestra que es imprescindible el apoyo y compromiso de la alta dirección para el desarrollo de una gestión de la SI eficaz. Se concretó la política de SI conforme a la dirección estratégica, enfocada en la gestión de la SI y en las necesidades de la organización.

La implementación del SGSI en la OTN de Holguín se encuentra en un nivel de madurez “iniciado”, aunque se evidencia que la organización reconoce los problemas que necesitan ser resueltos o perfeccionados. Como parte del proceso de análisis y gestión de riesgos se identifican, clasifican y valoran los activos de información. Se identifican y cuantifica la probabilidad de ocurrencia de las amenazas asociadas a los activos y el impacto que tendrían para la organización en caso de materializarse, aplicando los criterios de aceptación definidos.

### Conclusiones generales

Como resultado de esta investigación, se arribó a las conclusiones siguientes:

1. El análisis de la bibliografía permitió construir el marco teórico – práctico referencial. Se sintetizaron los principales referentes teórico–metodológicos que sustentan la gestión de la SI.
2. En las metodologías consultadas se identifica como una brecha la ausencia de herramientas y técnicas para llevar a cabo una adecuada gestión de SI, que incluya el proceso de análisis y evaluación de riesgos como punto concéntrico para garantizar la continuidad de la SI.
3. Se propone una metodología que permite la gestión de la SI, que garantiza su confidencialidad, disponibilidad, integridad y continuidad de la SI, la misma cuenta con cuatro etapas fundamentales: la planificación inicial, diagnóstico, desarrollo y verificación y mejora.
4. Durante el desarrollo de la metodología se creó la herramienta informática “Gestión de la SI” que tiene como objetivo agilizar y facilitar la compleja tarea que acarrear los procesos de gestión de activos, análisis y evaluación de riesgos y continuidad de la SI.
5. La aplicación de la metodología en la Oficina Territorial de Normalización de Holguín permitió:
  - La consolidación de una política de SI.
  - Elevar la cultura de todo el personal referente a la SI.
  - Determinar el nivel de madurez de la organización en relación al cumplimiento de los requisitos de la NC ISO/IEC 27001 y sus objetivos de control.
  - Mayor control sobre sus activos, su valor y las amenazas asociadas que pueden afectarlos.
  - Identificar, analizar y evaluar los riesgos, como el medio más efectivo para minimizarlos, garantizando la confidencialidad, integridad y disponibilidad de la información y como el punto concéntrico de la continuidad de la SI.

### **Recomendaciones**

A partir del estudio realizado y sus conclusiones se recomienda:

1. Continuar con el desarrollo e implementación de la herramienta informática creada.
2. Avanzar con la investigación y extender paulatinamente su aplicación a las unidades territoriales de Granma y Las Tunas, así como también generalizar en el sistema ONN.
3. Proseguir con la aplicación de la metodología para la gestión de la seguridad de la información hasta su fase final, de manera que se complete el ciclo de desarrollo donde se aborda la continuidad de la SI y se logre la mejora de los resultados en la organización.
4. Socializar las experiencias y resultados obtenidos de la investigación a través de publicaciones científicas en revistas y eventos científicos nacionales e internacionales, para propiciar el intercambio y su posible aplicación a otros sectores.

## Referencias bibliográficas

1. Aja Quiroga, L. (2002). Gestión de información, gestión del conocimiento y gestión de la calidad en las organizaciones. ACIMED, 10, 7-8.
2. Andrés, A., & Gómez, L. (2009). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes: AENOR.
3. Areitio Bertolín, J. (2008). Seguridad de la información, Redes, informática y sistemas de información.
4. Avellaneda, J. C. (2011). Medición de un SGSI: diseñando el cuadro de mandos.
5. Bautista, M. (2014). Marco de Referencia para la Formulación de un Plan de Continuidad de Negocio para TI, un caso de estudio. Revista Técnica "energía", 10(1), 200-207 pp.
6. Berrío López, J. P. (2016). Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO/IEC 27001. Ingeniería de Sistemas e Informática.
7. Bertolín, J. A. (2008). SI. Redes, informática y sistemas de información: Editorial Paraninfo.
8. Canchari Pastor, S. C. (2014). Análisis y diseño de un sistema de gestión de continuidad de negocio en caso de ocurrencia de sismos para una empresa aseguradora local basado en la ISO/IECD 22301: 2012.
9. Castro-Marquina, L. D. (2013). Diseño de un sistema de gestión de continuidad de negocios (SGCN) bajo la óptica de la norma ISO/IEC 22301.
10. Castro, A. R., & Bayona, Z. O. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. Ingeniería, 16(2), 56-66.
11. Castro Marquina, L. D. (2013). Diseño de un Sistema de Gestión de Continuidad de Negocios (SGCN) para la RENIEC bajo la óptica de la Norma ISO/IEC 22301.
12. Cely, R. (2018). Diseño del sistema de gestión de seguridad de la información (SGSI) con base al modelo de seguridad y privacidad de la información según lineamientos del Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la estrategia GEL. Colombia: Universidad Nacional Abierta y a Distancia (UNAD). Especialización en seguridad informática
13. Cordero Torres, K. G. (2015). Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para análisis y gestión de riesgos de seguridad de la información. Universidad del Azuay.
14. Cuervo Álvarez, S. (2017). Implementación ISO 27001.
15. Chilán-Santana, E. I., & Pionce-Pico, W. F. (2017). Apuntes teóricos introductorios sobre la seguridad de la información. Dominio de las Ciencias, 3(4), 284-295.

16. Delgado, M. F. (2014). Taller de Implementación de la norma ISO 27001. Recuperado el, 20.
17. Drewitt, T. (2013). A Manager's Guide to ISO22301: A practical guide to developing and implementing a business continuity management system: IT Governance Ltd.
18. Espinosa, D., Martínez, J., & Amador, S. (2014). Gestión del riesgo en la seguridad de la información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la Metodología OCTAVE-S. Caso de estudio: proceso de inscripciones y admisiones en la división de admisión registro y control AC. Ingenierías USBMed, 5(2), 33-43.
19. Fernández, L. G., & Álvarez, A. A. (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes: AENOR.
20. Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. Polo del conocimiento, 2(12), 145-155.
21. Gallegos, F. P., & Murillo, M. F. (2015). Metodología de gestión de la información enfocado a las Industrias de Telecomunicaciones en el Ecuador. Ecuador: Escuela Politécnica Nacional. Tesis para optar por el título de máster
22. Gaona Vásquez, K. d. R. (2013). Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito SA en la ciudad de Machala.
23. Gómez Morales, G. (2014). Implementación de un SGSI basado en la norma ISO IEC 27001:2013.
24. González Villalobos, J. A. (2015). Elaboración de un plan de auditoría para evaluación de cumplimiento en sistemas para gestión de la continuidad del negocio basado en la normativa ISO 22301.
25. Granda, E. L., Espinosa, J. N., & Vásquez, C. C. (2017). Modelo de evaluación de gestión de continuidad del negocio basado en la norma ISO 22301: 2012. Espacios, 38(1), 17.
26. Guamán, C. R. S., Vivar, S. A. M., Rivera, D. P. P., & Calderón, F. A. C. (2019). Percepción de Seguridad De La Información en Las Pequeñas Y Medianas Empresas en Santo Domingo. Investigación Operacional, 40(3), 421-428.
27. ISOTools Excelence, I. (2016). ISO 22301: Sistema de Gestión de Continuidad de Negocio.
28. ISOTools Excellence. (2014). ISO-27001-sistema-gestion-seguridad-informacion.
29. ISOToolsExcelence. (2016). ISO 9001 2015: Información documentada.

30. Landázuri, M. C. (2017). Formulación de una propuesta para un modelo de sistema de gestión de seguridad de la información para empresas de la industria bancaria en el sector privado. Tesis para optar por el título de máster
31. Lizbeth Morales, Y. (2010). Propuesta de una metodología para elaborar un programa de continuidad del negocio en México.
32. López Díaz, N., Suárez García, J. C., & Vila Alonso, Z. M. (2020). Análisis costo-beneficio de la gestión de riesgos ambientales en empresa de cigarrillos Ramiro Lavandero Cruz. *Revista Universidad y Sociedad*, 12(5), 343-353.
33. Lozano, M. (2017). Diseño de un plan estratégico de seguridad de información para una compañía del sector asegurador. Colombia: Institución Universitaria Politécnico Gran Colombiano. Tesis de grado
34. Magerit. (2012). versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos.
35. Maldonado, G. B., & Cano, J. A. O. (2014). Metodología de la seguridad de la información como medida de protección en pequeñas empresas. *Cuaderno Activa*, 6, 71-77.
36. Maravilhas, S. (2015). Information quality and value *Encyclopedia of Information Science and Technology*, Third Edition (pp. 3981-3989): IGI Global.
37. Miranda Cairo, M., Valdés Puga, O., Pérez Mallea, I., Portelles Cobas, R., & Sánchez Zequeira, R. (2016). Metodología para la implementación de la Gestión Automatizada de Controles de Seguridad Informática. *Revista Cubana de Ciencias Informáticas*, 10(2), 14-26.
38. Moltoni, L. A., & Moltoni, A. F. (2015). Trazabilidad: el rol de la información en el marco del nuevo paradigma de la calidad: CIAAL.
39. Murillo Varón, C. E., Bonilla Pineda, D. H., & Buitrago Estrada, J. C. (2012). Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información-SGSI, en el sector de laboratorios de análisis microbiológicos, basado en ISO 27001. Universidad Ean.
40. NC-ISO-IEC-27000. (2016). Tecnología de la información-técnicas de seguridad-sistemas de gestión de SI-visión de conjunto y vocabulario. Cuba: Oficina Nacional de Normalización
41. NC-ISO-IEC-27001. (2016). Tecnología de la información-técnicas de seguridad-sistemas de gestión de SI-requisitos. Cuba: Oficina Nacional de Normalización
42. NC-ISO-IEC-27002, O. (2016). Tecnología de información - Técnica de seguridad - Código de prácticas para controles de SI. Cuba: Oficina Nacional de Normalización

43. NC/ISO-9001. (2015). Sistemas de gestión de la calidad — requisitos. Cuba: Oficina Nacional de Normalización
44. NC ISO 31000:2018. (2018). Gestión de Riesgos - Directrices. Cuba: Oficina Nacional de Normalización
45. Nieves, A. C. (2017). Diseño de un sistema de gestión de la SI (SGSI) basados en la norma Iso/iec 27001: 2013.
46. Olivera Argota, Y. (2019). Procedimiento para implementar un sistema de gestión de seguridad de la información como contribución a la calidad de la información de los servicios de consultoría.
47. Paillacho, S. (2015). Modelo de un proceso de la gestión del riesgo de la seguridad de la información en entidades gubernamentales. Ecuador: Escuela Politécnica Nacional.
48. Prieto, G., & Delgado, A. R. (2010). Fiabilidad y validez. Papeles del psicólogo, 31(1), 67-74.
49. QUIRÓS, AGUSTÍN L. (2010). Uso de la norma ISO/IEC 27004 para Auditoría Informatic.
50. Sánchez, L. E., Villafranca, D., Fernández-Medina, E., & Piattini, M. (2009). MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES. Paper presented at the V Congreso Iberoamericano de Seguridad Informática.
51. Sánchez Torres, S. A. (2014). Importancia de implementar el SGSI en una empresa certificada.
52. Santofimio, Y. L., & Manrique, C. T. (2015). Técnicas de evaluación del riesgo para determinar la viabilidad del proyecto en la etapa de formulación. Santiago de Cali, Colombia: Universidad San Buenaventura Cali.
53. Solarte Solarte, F. N., Enriquez Rosero, E. R., & Benavides Ruano, M. d. C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica-ESPOL, 28(5).
54. Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. doi: 10.23857/pc.v3i4.809
55. Valencia, F. J. D., & Alzate, M. O. (2017). Implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. doi: 10.17013/risti.22.73–88



## Anexos

### Anexo 1: Cuadro comparativo de metodologías de gestión de riesgos

Metodologías	Ámbito de aplicación	Ventajas	Desventajas
OCTAVE	Análisis de riesgos para seguridad de sistemas de información: PYMES	Es una metodología auto dirigida, es decir, la organización gestiona y dirige la evaluación de sus riesgosa través de un equipo multidisciplinario. <ul style="list-style-type: none"> <li>- Comprende los procesos de análisis y gestión de riesgos.</li> <li>- Involucra a todo el personal de la entidad.</li> <li>- Se considera de las más completas, ya que involucra como elementos de su modelo de análisis: procesos, activos y dependencias, recursos, vulnerabilidades, amenazas y salvaguardas.</li> </ul>	No toma en cuenta el principio de no repudio de la información como objetivo de seguridad. <ul style="list-style-type: none"> <li>- Usa muchos documentos anexos para llevar a cabo el proceso de análisis de riesgos, lo que la hace tediosa, complicada de entender.</li> <li>- Requiere de profundos conocimientos técnicos.</li> <li>- No explica en forma clara la definición y determinación de los activos de información</li> </ul>
MAGERIT	Análisis y gestión de riesgos de los sistemas de información: Gobierno, Organismos, grandes compañías, PYME, compañías comerciales y no comerciales	<ul style="list-style-type: none"> <li>- Se le considera con un alcance completo, tanto en el análisis como en la gestión de riesgos.</li> <li>- Posee un extenso archivo de inventarios en lo referente a Recursos de Información, Amenazas y tipo de Activos.</li> <li>- Permite un análisis completo cualitativo y cuantitativo</li> <li>- De carácter Público.</li> <li>- No requiere autorización previa para su uso.</li> </ul>	El hecho de tener que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa. <ul style="list-style-type: none"> <li>- No involucra a los procesos, recursos ni vulnerabilidades como elementos del modelo a seguir</li> <li>- No posee un inventario completo en lo referente a políticas</li> </ul>
NC ISO/IEC 27005	Estándar para la gestión de riesgos de seguridad de la información: Aplicable a cualquier organización	<ul style="list-style-type: none"> <li>- Estándar internacional, lo que le faculta mayor aceptación</li> <li>- Posee una cláusula completa orientada a la</li> </ul>	<ul style="list-style-type: none"> <li>- No detalla la forma de valorar las amenazas.</li> <li>- No es certificable - No posee</li> </ul>

	sin importar tipo, tamaño o naturaleza	<p>monitorización y revisión de riesgos.</p> <ul style="list-style-type: none"> <li>- Se le considera con un alcance completo, tanto en el análisis como en la gestión de Riesgos.</li> <li>- Posee la fase de aceptación de riesgos, previa su justificación.</li> <li>- Permite un análisis completo cuantitativo.</li> </ul>	herramientas, técnicas, ni comparativas de ayuda para su implementación.
MEHARI	Gobierno, organismos, empresas medianas y grandes, compañías comerciales, sin fines de lucro (educación, salud, servicios públicos, organizaciones no gubernamentales)	<ul style="list-style-type: none"> <li>- Usa un modelo de análisis de riesgos cualitativo y cuantitativo.</li> <li>- Es un método capaz de evaluar y lograr la disminución de riesgos en función del tipo de organización.</li> <li>- Posee bases de datos de conocimientos con manuales, guías y herramientas que permiten realizar el análisis de riesgos cuando sea necesario.</li> <li>- Complementa y se acopla a las necesidades de la norma ISO 27001, 27002 y 27005 para definir los SGSI y la gestión de riesgos.</li> <li>- Por medio de esta metodología se detectan vulnerabilidades mediante auditorías y se analizan las situaciones de riesgo.</li> <li>- Combina análisis y evaluación de riesgos; particularmente, se especifica un módulo de evaluación rápida y uno de evaluación detallada.</li> </ul>	<ul style="list-style-type: none"> <li>- Sólo toma en cuenta los principios de confidencialidad, integridad y disponibilidad de la información como objetivos de seguridad, dejando a un lado el no repudio.</li> <li>- La recomendación de los controles no la incluye dentro del análisis de riesgos sino en la gestión de los riesgos.</li> <li>- La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos</li> </ul>
NC-ISO 31000:2018 Gestión del riesgo. Directrices.	Gobierno, organismos, empresas grandes y medianas, compañías comerciales sin ánimo de lucro (educación, salud, servicios públicos, organizaciones privadas).	<ul style="list-style-type: none"> <li>- Estructura las actividades para poner en marcha y mejorar continuamente los procesos de gestión de riesgos.</li> <li>- Es parte de la organización y el liderazgo.</li> <li>- Fundamental en la manera en que se gestiona la organización en todos sus niveles.</li> <li>- Contribuye a la mejora de los sistemas de gestión.</li> <li>- Es parte de todas las actividades de una</li> </ul>	

		<p>organización e incluye la interacción con las partes interesadas.</p> <ul style="list-style-type: none"> <li>- Considera el contexto externo e interno de una organización, incluido el comportamiento humano y los factores culturales.</li> <li>- Se puede aplicar a cualquier tipo de riesgo, cualquiera que sea su naturaleza, y tanto si sus consecuencias son positivas o negativas.</li> </ul>	
NC-ISO /IEC 31010:2015 Gestión del riesgo. Técnicas de apreciación del riesgo	Gobierno, organismos, empresas grandes y medianas, compañías comerciales sin ánimo de lucro (educación, salud, servicios públicos, organizaciones privadas).	<ul style="list-style-type: none"> <li>- Se puede aplicar a cualquier tipo de riesgo, cualquiera que sea su naturaleza, y tanto si sus consecuencias son positivas o negativas.</li> </ul>	

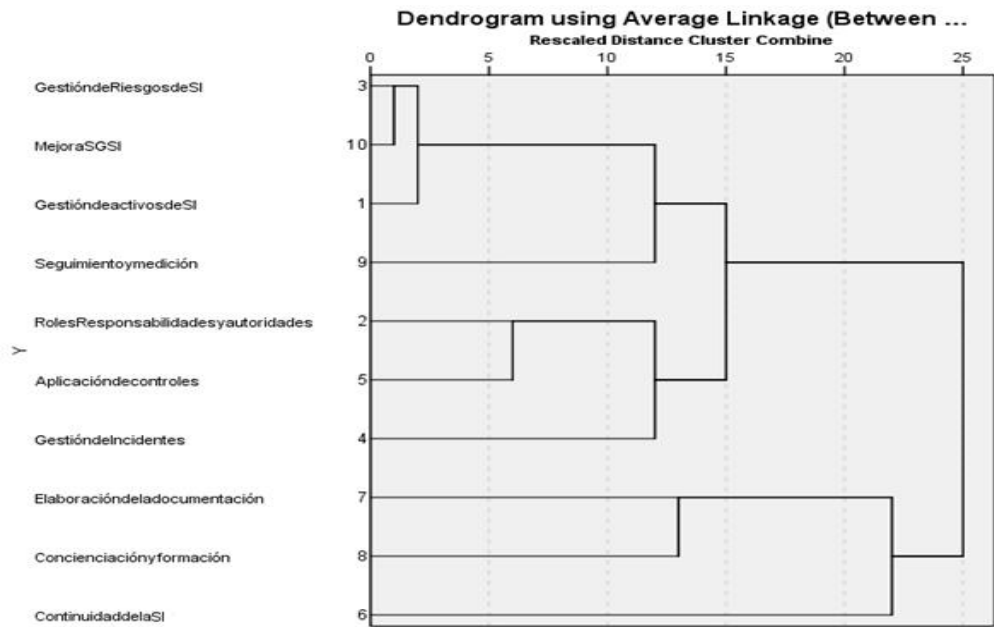
### Anexo 2: Matriz binaria relación de autores y variables

Variables \ Autores	Gestión de activos SI	Roles, Responsabilidades y autoridades	Gestión de riesgos de SI	Gestión de Incidentes	Aplicación de controles	Continuidad de la SI	Elaboración de la documentación	Concienciación y formación	Seguimiento y medición	Mejora SGSI
Alvarez (2004)	1	1	1	1	1	0	1	1	0	1
Avellaneda (2011)	0	0	1	1	1	0	1	1	0	1
Castro & Bayona (2011)	1	1	1	1	1	0	0	1	0	1
Espinosa, Martínez & Amador, (2014)	1	1	1	1	1	0	1	0	1	1
Huidobro (2007)	0	1	1	0	1	0	1	1	0	1
Nieves (2017)	1	1	1	1	1	0	0	0	1	1
NC ISO 27001 (2016)	1	1	1	1	1	1	1	1	1	1

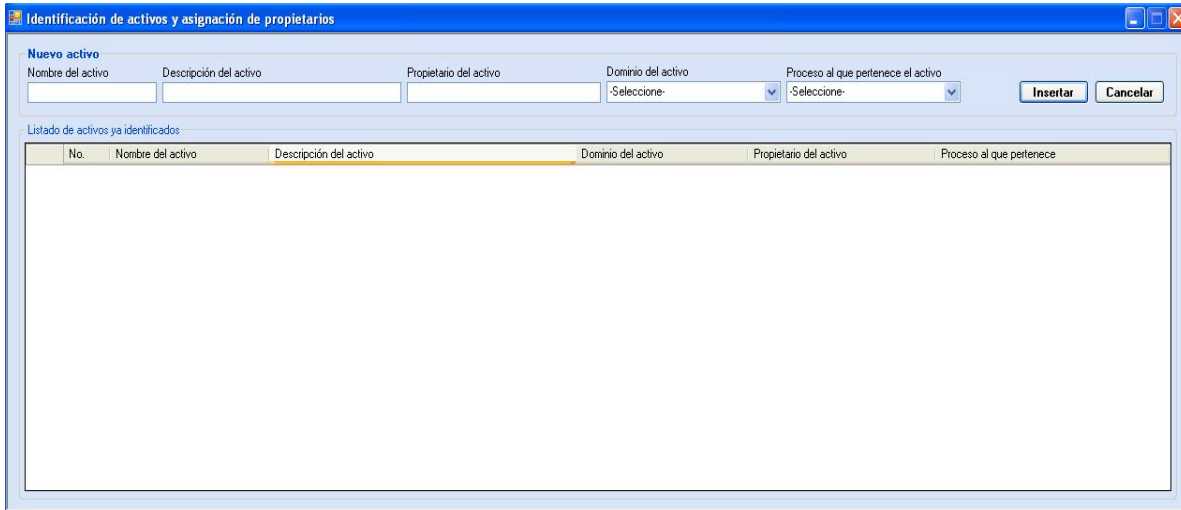
QUIRÓS, AGUSTÍN L. (2010)	1	1	1	1	1	0	1	1	1	1
Solarte, Rosero & del Carmen Benavides (2015)	1	1	1	1	1	0	0	0	0	1
Villena Aguilar (2006)	1	1	1	1	1	0	0	1	1	1
(Berrío López, 2016)	1	0	1	1	1	1	1	1	1	1
(Cordero Torres, 2015)	1	1	1	1	1	0	0	0	1	1
(Tejena-Macías, 2018)	1	1	1	0	1	1	1	1	1	1
(Gaona Vásquez, 2013)	1	1	1	1	1	0	1	1	1	1
(Maldonado & Cano, 2014)	1	1	1	1	0	0	1	1	0	1
(Miranda Cairo, Valdés Puga, Pérez Mallea, Portelles Cobas, & Sánchez Zequeira, 2016)	1	1	1	1	1	0	1	0	1	1
(Murillo Varón et al., 2012)	1	1	1	1	1	0	1	1	1	1
(Sánchez, Villafranca, Fernández- Medina, & Piattini, 2009)	1	1	1	0	0	0	0	1	1	1
Cuervo(2017)	1	1	1	0	1	1	1	0	1	1
Gallegos & Murillo(2017)	1	1	1	1	1	0	0	0	1	1
Landázuri(2017)	1	0	1	0	0	0	0	0	0	1

Lozano(2017)	1	0	1	0	0	1	0	1	1	1
Cely(2018)	0	1	0	1	1	0	0	0	1	1
Paillacho(2015)	1	1	1	0	0	1	1	0	1	1
Santofimio & Manrique(2015)	1	0	1	0	0	0	0	0	1	1
Tibaquira(2015)	1	1	1	0	1	0	0	0	0	1
Delvasto(2016)	1	1	1	1	1	0	0	0	0	1
Torres(2017)	1	0	1	1	0	1	0	0	1	1

**Anexo 3: Análisis de grupos de conglomerados por variables**



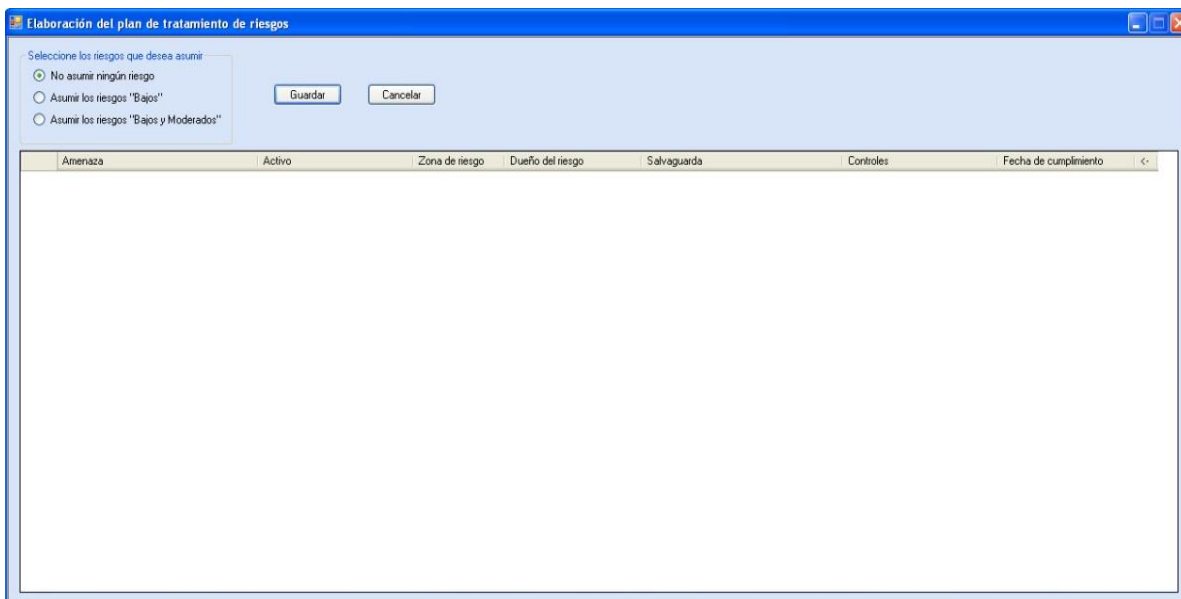
### Anexo 4: Herramienta “Gestión de la SI” Gestión de activos



### Anexo 5: Declaración de aplicabilidad

LOGO DE LA ORGANIZACIÓN			REGISTRO	CÓDIGO:	
Cláusulas	Objetivos	Controles		Aplicable	Justificación
5			<b>POLÍTICAS DE SI</b>		
	5.1		<b>Directrices de gestión de la SI</b>		
		5.1.1	Políticas para la SI		
		5.1.2	Revisión de las políticas para la		

### Anexo 6: Herramienta “Gestión de la SI” Gestión de riesgos



### Anexo 7: Programa de auditorías internas

<b>LOGO DE LA ORGANIZACIÓN</b>		<b>REGISTRO</b>											<b>CÓDIGO:</b>		
													<b>PÁGINA: de</b>		
Programa de auditorías internas													Año _____		
Auditoría		Ene	Feb.	Mar.	Abr.	May	Jun.	Jul.	Ago	Sep.	Oct.	Nov	Dic.	Auditor líder	
	Plan														
	Real														
Elaborado _____							Aprobado _____								
RSI							Director								
Fecha de aprobación:															

### Anexo 8: No conformidades y observaciones de la auditoría

<b>LOGO DE LA ORGANIZACIÓN</b>		<b>REGISTRO</b>			<b>CÓDIGO:</b>	
<b>No conformidades y observaciones de la auditoría</b>						
Auditoría No:				Fecha:		Página: de:
No conformidad:						
Observación:						
Nombre y firma del auditor Líder:						

### Anexo 9: Informe de auditoría interna

<b>LOGO DE LA ORGANIZACIÓN</b>		<b>REGISTRO</b>		<b>CÓDIGO:</b>	
Informe de auditoría interna					
Auditoría N.:			Área o actividad auditada		
Equipo Auditor:					
Objetivos y alcance:					
Fecha:		Desde:		Hasta:	
Criterios de auditoría:					
Declaración del auditor					
Resultados de la auditoría:					
Juicio del equipo auditor:					
Auditor Líder:				Fecha:	
Conformidad del director de la organización:					
Relación de distribución del informe:					
Se prohíbe la reproducción parcial o total de este documento a personal no autorizado.					

## **Anexo 10: Política de SI**

La Oficina Territorial de Normalización de Holguín considera a la información como un bien más de sus activos y asegurarla con niveles de protección adecuados es una prioridad para garantizar la confidencialidad, integridad y disponibilidad para realizar sus procesos y actividades. Establece los mecanismos de protección en los medios de procesamiento, almacenamiento y transmisión de la información y de diferentes tipos de amenazas, tanto internas como externas y proporciona una seguridad razonable al logro de los objetivos institucionales y del negocio, en correspondencia con el contexto en el que opera, con el fin de garantizar la continuidad de la SI.

Esta política constituye un firme propósito de la alta dirección y de todos los trabajadores para:

- La gestión de los riesgos asociados a los activos de información teniendo en cuenta los niveles de aceptación definidos.
- Cumplir con los requisitos para la gestión de la seguridad de la información bajo el estándar de referencia NC ISO/IEC 27001.
- Garantizar la protección de la información confidencial y el derecho de propiedad del cliente, que abarca equipos de medición, instalaciones, informes de los resultados relacionados con los clientes.
- Conservar la integridad de los documentos de la organización.
- Mantener la disponibilidad de los servicios y aplicaciones internas soportadas en las TIC y aquellas dispuestas a los servicios del cliente externo que ayudan al cumplimiento de los requisitos del negocio.
- Aprovisionar a todo el personal de las competencias requeridas, los recursos necesarios, y el interés por el cumplimiento de los requisitos del negocio, los requerimientos legales y reglamentarios vigentes aplicables y las obligaciones de seguridad contractuales.
- Considerar la SI como un proceso de mejora continua, que permita alcanzar cada vez mayores niveles de seguridad.

La alta dirección responde por el aseguramiento de la SI de la organización, así como los mecanismos para respaldar la difusión y actualización de esta política como de las demás complementarias, según la declaración de aplicabilidad adoptada. Cada trabajador es responsable de mantener la SI dentro de las acciones que realiza. El personal externo que acceda a la organización debe cumplir con las medidas de seguridad establecidas y deben ser exigidas por el personal interno.

Aprobado: Director OTNH \_\_\_\_\_



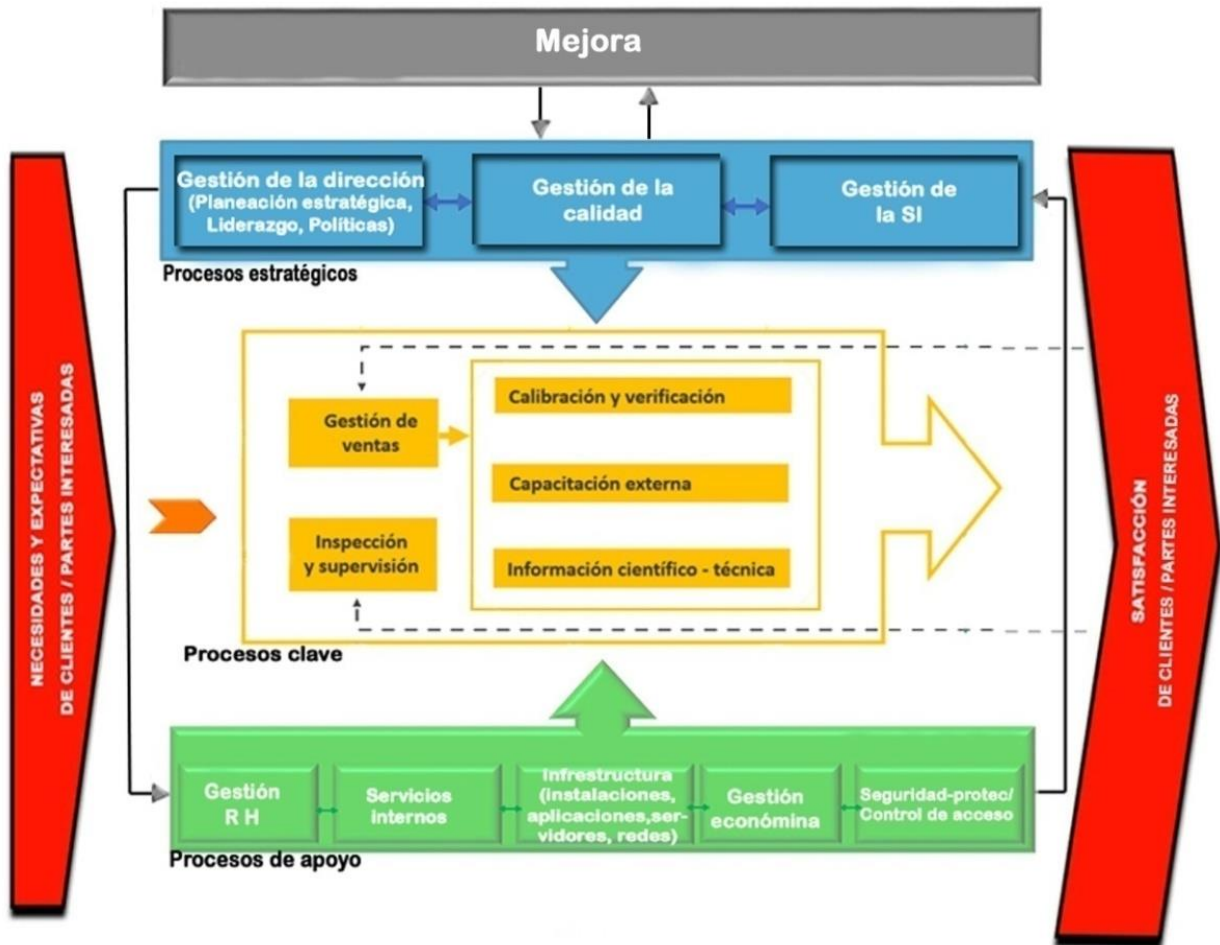
### Anexo 11: Plan de capacitación comité de SI

Con el objetivo de preparar al comité de SI para que cumplan sus funciones en relación a la SI se desarrolla el siguiente plan.			
Temas de Capacitación	Ejecutor	Lugar	Duración
Curso interpretación y uso NC ISO/IEC 27001	Departamento de Normalización OTNH	Aula OTNH	24 horas
Taller técnicas de SI y herramientas de control	Departamento de Normalización OTNH	Aula OTNH	16 horas
Taller gestión de riesgo	Departamento de Normalización OTNH	Aula OTNH	16 horas
Conferencia seguridad y privacidad de la información	OSRI	Aula OTNH	2 horas
Conferencia conceptos, amenazas y vulnerabilidades de SI	OSRI	Aula OTNH	3 horas
Taller técnicas de auditoría	Departamento de Normalización	Aula OTNH	16 horas

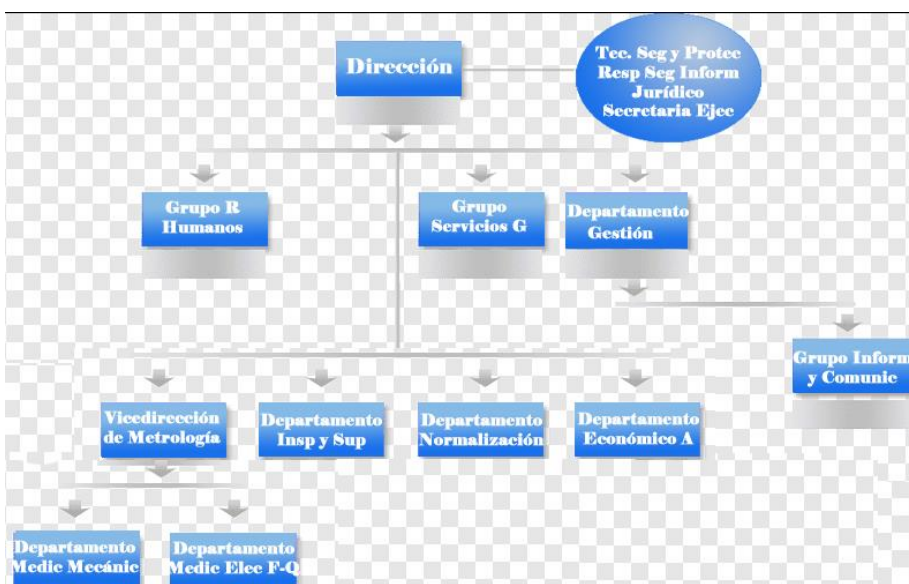
### Anexo 12: Plan de formación y concienciación

Temáticas	Objetivo	Participa	Medios	Resp
Divulgación de las políticas de: seguridad de operaciones, control de acceso, seguridad ante programas malignos, respaldo de información, gestión de incidentes, contraseñas	Identificar cuales comportamientos de SI se consideran correctos y cuales incorrecto	T/Trabajadores	Conferencia, intranet corporativa, correo electrónico	Recursos Humanos
Políticas mesas despejadas, clasificación de la información	Tener en cuenta que información debería ser protegida	Grupo 1 y 3	Charla	Recursos Humanos
Autoaprendizaje	Tomar conciencia en materia de SI	T/Trabajadores	Formación basada en la web	Jefe Inmediato
Obligaciones legales en SI	Conocer y cumplir legalmente lo establecido en SI	Grupo 1, 2 y 3	Conferencia (normas, decretos, resoluciones)	Recursos Humanos
Uso de dispositivos extraíbles	Aumentar su concienciación respecto a los riesgos asociados y los controles que se deberían implantar	T/Trabajadores	Charla, intranet, murales, correos electrónicos	Recursos Humanos
Principales amenazas	Tomar conciencia de las responsabilidades de SI	T/Trabajadores	Charla en matutinos, intranet, murales, correos electrónicos	Recursos Humanos

Anexo 13: Mapa de procesos propuesto de la Oficina Territorial de Normalización



Anexo 14: Nueva estructura de gestión de la actividad informática y la seguridad informática



### Anexo 15: Nivel de madurez de los requisitos NC ISO/IEC 27001

N.	ID	Cláusula	Valor	Nivel de madurez
1.	<b>4</b>	<b>Contexto de la organización</b>	3,25	Definido
2.	4.1	Comprender la organización y su contexto	4	Gestionado
3.	4.2	Comprensión de las necesidades y expectativas de las partes interesadas	4	Gestionado
4.	4.3	Determinación del alcance del sistema de gestión de seguridad de la información	4	Gestionado
5.	4.4	Sistema de gestión de seguridad de la información	1	Inexistente
6.	<b>5</b>	<b>Liderazgo</b>	4	Gestionado
7.	5.1	Liderazgo y compromiso	4	Gestionado
8.	5.2	Política	4	Gestionado
9.	5.3	Roles, responsabilidades y autoridades en la organización	4	Gestionado
10.	<b>6</b>	<b>Planificación</b>	2	Iniciado
11.	6.1	Acciones para tratar los riesgos y oportunidades	2	Iniciado
12.	6.2	Objetivos de SI y planificación para su consecución	2	Iniciado
13.	<b>7</b>	<b>SopORTE</b>	2,8	Definido
14.	7.1	Recursos	3	Definido
15.	7.2	Competencia	2	Iniciado
16.	7.3	Concienciación	4	Gestionado
17.	7.4	Comunicación	4	Gestionado
18.	7.5	Información documentada	1	Inexistente
19.	<b>8</b>	<b>Operación</b>	2,6	Iniciado
20.	8.1	Planificación y control operacional	2	Iniciado
21.	8.2	Apreciación de los riesgos de seguridad de información	3	Definido
22.	8.3	Tratamiento de los riesgos de seguridad de información	3	Definido
23.	<b>9</b>	<b>Evaluación del desempeño</b>	2	Iniciado
24.	9.1	Seguimiento, medición, análisis y evaluación	2	Iniciado
25.	9.2	Auditoría interna	2	Iniciado
26.	9.3	Revisión por la dirección	2	Iniciado
27.	<b>10</b>	<b>Mejora</b>	2	Iniciado
28.	10.1	No conformidad y acciones correctivas	2	Iniciado
29.	10.2	Mejora continua	2	Iniciado

**Anexo 16: Nivel de madurez Anexo A NC ISO/IEC 27001**

<b>5 Política</b>	<b>Nivel de madurez: 2</b>
<p>Observaciones:</p> <p>5.1.1 La política de SI a un nivel inferior se apoya en políticas sobre temas específicos para gestionar sus objetivos de SI, en las que se evidencian: No hay implantadas políticas para el uso adecuado de activos, puestos de trabajo despejados y pantallas limpias, información clasificada, teletrabajo o políticas de criptografía para la información clasificada, estas últimas de gran importancia a raíz de los nuevos cambios que sufren las organizaciones por la pandemia covid-19 con la incorporación de la modalidad de trabajo a distancia. Las políticas incluidas en el PSI no han sido comunicadas, ni están disponibles para los trabajadores, son tratadas como información clasificada.</p> <p>5.1.2 En auditorías internas y revisiones por la dirección se revisa el procedimiento “Uso de la computación” contemplado dentro del alcance del SIG, el mismo no contiene las políticas incluidas en PSI, definidas para el manejo de esta actividad, por lo que no hay evidencias que las mismas se revisen y se actualicen en caso de haber modificaciones.</p>	
<b>6 Organización de la seguridad de la información</b>	<b>Nivel de madurez: 2</b>
<p>Observaciones:</p> <p>6.1.1 Están definidas las responsabilidades generales en cuanto a la SI, pero no están definidos todos los activos y los procesos, por lo que quedan activos sin asignación de responsables.</p> <p>6.1.4 No se evidencian contactos con grupos de interés que brinden asesorías especializadas en SI.</p> <p>6.2.2 No existe una política para proteger la información accedida, tratada o almacenada en emplazamiento de teletrabajo (trabajo a distancia).</p>	
<b>7 Seguridad relativa a los recursos humanos</b>	<b>Nivel de madurez: 4</b>
<p>Observaciones: Se evidencia un nivel de implementación para los controles de este dominio, pero se debe continuar en el abordaje de la formación y ganar en conciencia sobre SI.</p>	
<b>8 Gestión de activos</b>	<b>Nivel de madurez: 2</b>
<p>Observaciones:</p> <p>8.1.1 No se realiza un correcto inventario de activos de SI, en el inventario incluido en el PSI no se incluyen activos como la información, equipamiento auxiliar, instalaciones, soportes de información, servicios o aplicaciones informáticas.</p> <p>8.1.2 El inventario se realiza a nivel de áreas por lo que no queda establecido un propietario por cada activo.</p> <p>8.2.1, 8.2.2, 8.2.3 Para el tratamiento de la información solo existe una lista maestra para clasificar y desclasificar la información, no existe un procedimiento donde se especifique su manejo y etiquetado.</p> <p>8.3.1 No existe una política o procedimiento para la gestión de los medios extraíbles, aunque se evidencia el uso de herramientas instaladas para bloquear los puertos USB, con el objetivo de que ninguna persona pueda introducir su dispositivo de almacenamiento extraíble y acceda a la información sin que se haya autenticado previamente y de ser así se guardan los registros de los mismos. Esta política no cumple objetivo ya que no se aplica en todas las computadoras.</p> <p>8.3.2 No existen implementadas políticas de eliminación y destrucción de soportes que</p>	

vayan a ser desechados por la organización y hayan contenido información confidencial.	
<b>9 Control de acceso</b>	<b>Nivel de madurez: 3</b>
Observaciones: 9.1.1 Existe un procedimiento de control de acceso incluida en el alcance del SIG, el mismo solo aborda la seguridad física, no hace referencia a las políticas para los controles de acceso lógicos que están incluidos en el PSI, ambos deberían considerarse conjuntamente.	
<b>10 Criptografía</b>	<b>Nivel de madurez: 1</b>
Observaciones: 10.1.1 No está implementada una política sobre el uso de los controles criptográficos, que incluya la gestión de claves criptográficas.	
<b>11 Seguridad física y del entorno</b>	<b>Nivel de madurez: 3</b>
Observaciones: 11.2.1 No existe instalación de tierra física y pararrayos para la protección de los equipos. 11.2.2 Los equipos no están protegidos con fuentes de respaldo en caso de fallos de suministro eléctricos. 11.2.9 No hay adoptada una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y política de pantalla limpia para los recursos de tratamiento de la información.	
<b>12 Seguridad de las operaciones</b>	<b>Nivel de madurez: 3</b>
Observaciones: 12.1.1 Existen adoptadas políticas para la seguridad de las operaciones, pero las mismas no están a disposición de los usuarios, ya que son tratadas como información clasificada, no cumpliendo su objetivo. 12.4.1, 12.4.3 No están configurados en todas las computadoras los registros de las actividades de usuarios, excepciones y eventos de SI. 12.6.1 Se evidencia que quedan fuera del inventario de riesgos amenazas vinculadas a la SI que no son tratadas; el inventario de riesgos no se realiza a partir de un inventario de activos, en el que deberían estar incluidos los activos de información. No están definidos los criterios de aceptación del riesgo, lo que impide efectuar una adecuada evaluación de los mismos.	
<b>13 Seguridad de las comunicaciones</b>	<b>Nivel de madurez: 3</b>
Observaciones: 13.2.1 No existe adoptada una política o procedimiento para el intercambio de información, el tema es tratado en el PSI como parte de otras políticas y de manera superficial.	
<b>14 Adquisición, desarrollo y mantenimiento de los sistemas de información</b>	<b>Nivel de madurez: 1</b>
Observaciones: 14.1.1 No hay evidencia que se tengan en cuenta los requisitos de SI para los nuevos sistemas de información. 14.1.2 y 14.1.3 Los servicios de aplicaciones en redes públicas con que cuenta la organización están hospedados fuera de sus instalaciones, las medidas de seguridad son de la entidad que ofrece el servicio de hosteo. 14.2.1, 14.2.2, 14.2.3, 14.2.4, 14.2.5, 14.2.6, 14.2.7, 14.2.8, 14.2.9, La organización no desarrolla aplicaciones o sistemas.	

<b>15 Relaciones con los Proveedores</b>	<b>Nivel de madurez: 1</b>
<p>Observaciones:</p> <p>15.1.1 No existe una política adecuada de cómo debe ser el tratamiento con los proveedores externos con respecto al acceso a la información.</p> <p>15.1.2 En los acuerdos contractuales con los proveedores que proporcionan componentes de la infraestructura, acceden, almacenan, comunican o tratan con la información, no están establecidos los requisitos de SI.</p> <p>15.1.3 No están incluidos en los acuerdos con los proveedores los requisitos para el tratamiento de los riesgos de SI.</p>	
<b>16 Gestión de Incidentes de la Seguridad de la Información</b>	<b>Nivel de madurez: 3</b>
<p>Observaciones:</p> <p>16.1.1, 16.1.2 Existe implantado un procedimiento para la gestión de incidentes incluido en el PSI, pero el mismo solo tiene en cuenta los incidentes relacionados a la seguridad de la información digital; no ha sido comunicado para que todos los trabajadores de la organización conozcan cómo proceder ante la materialización de un evento de esta índole, lo que conlleva a que no se haga uso del registro de incidentes cuando se produzca, por ejemplo, una contaminación por virus.</p>	
<b>17 Gestión de la Continuidad de Negocio</b>	<b>Nivel de madurez: 1</b>
<p>Observaciones:</p> <p>17.1.1 La organización no cuenta con un plan de continuidad del negocio o plan de recuperación de desastre, no están determinados los requisitos de SI en situaciones adversas, a partir de un análisis de impacto al negocio.</p> <p>17.1.2 No están implementados los controles de SI para la gestión de eventos disruptivos.</p> <p>17.2.1 Se deberían asegurar la disponibilidad de los recursos para el tratamiento de la información.</p>	
<b>18 Cumplimiento</b>	<b>Nivel de madurez: 2</b>
<p>Observaciones:</p> <p>18.1.2 La organización hace uso de productos de software patentados, como la utilización de sistemas operativos.</p> <p>18.1.4 No existe una política para la protección y privacidad de la información personal.</p> <p>18.1.5 No están implementados métodos criptográficos.</p> <p>18.2.1 En los procesos de auditoría interna y revisiones por la dirección no se tienen en cuenta objetivos, controles y políticas de SI, solo está dentro del alcance de estos procesos el procedimiento de utilización de la computación, el cual no hace referencia a las políticas y procedimientos incluidos en el PSI.</p>	

## Anexo 17: Gestión de activos

**Nombre del informe:** Valoración de activos

**Fecha:** 17/03/2021

No.	Dominio	Activo	Propietario	Conf.	Disp.	Integ.	Impacto
1	HW	Servidor de correo electrónico	Administrador de red	4	5	5	Crítico
2	HW	Servidor de internet	Administrador de red	3	2	3	Dañino
3	HW	Backup	Administrador de red	5	4	4	Severo
4	HW	Switch	Administrador de red	1	4	1	Menor
5	HW	Router	Administrador de red	1	4	1	Menor
6	HW	Firewall	Administrador de red	4	3	3	Dañino
7	HW	Periféricos (mause,teclado,speakers)	Administrador de red	1	4	1	Menor
8	HW	Computadora de trabajo	Administrador de red	4	5	5	Crítico
9	HW	Servidor de cliente ligero	Administrador de red	4	5	3	Severo
10	HW	Servidor de aplicaciones	Administrador de red	4	5	5	Crítico
11	HW	Servidor de dominio	Administrador de red	4	5	4	Severo
12	HW	Servidor de archivo	Administrador de red	5	5	5	Crítico
13	COM	Redes telefónicas	Etecsa	2	4	2	Dañino
14	COM	Red inalámbrica (wifi)	Administrador de red	2	4	2	Dañino
15	SW	Aplicación Normet	Administrador de red	3	5	3	Severo
16	SW	Aplicación Fastos	Jefe grupo recursos humanos	4	5	3	Severo

No.	Dominio	Activo	Propietario	Conf.	Disp.	Integ.	Impacto
17	SW	Aplicación Rodas	Jefe departamento económico	4	5	5	Crítico
18	SW	Aplicación Agenda express	Especialista de control interno	2	4	3	Dañino
19	SW	Intranet	Administrador de red	2	3	3	Dañino
20	SW	Sistemas operativos	Administrador de red	2	5	3	Dañino
21	SW	Antivirus	Responsable SI	4	4	4	Severo
22	SW	Mozilla firefox	Administrador de la red	2	4	3	Dañino
23	SW	Proxy(squid3)	Administrador de red	2	4	3	Dañino
24	SW	Wordclient	Administrador de red	2	4	2	Dañino
25	SW	Zimbra	Administrador de red	2	4	2	Dañino
26	P	Usuarios internos	Jefe grupo recursos humanos	4	2	2	Dañino
27	P	Administrador de sistemas	Administrador de red	2	2	2	Menor
28	P	Proveedores de servicios	Asesor jurídico	4	2	5	Severo
29	L	Local de servidores	Técnicos de seguridad y protección	5	5	5	Crítico
30	L	Local de información clasificada	Técnicos de seguridad y protección	5	5	5	Crítico
31	L	Edificio	Técnicos de seguridad y protección	4	2	2	Dañino
32	L	Instalaciones de respaldo	Técnico de seguridad y protección	4	4	4	Severo
33	S	Servicio de FTP	Administrador de red	4	3	2	Dañino



No.	Dominio	Activo	Propietario	Conf.	Disp.	Integ.	Impacto
34	Media	Info compartida	Administrador de red	2	4	2	Dañino
35	S	Active directory	Administrador de red	2	4	2	Dañino
36	D	Datos de la organización	Responsable SIG	5	4	5	Crítico
37	D	Datos clientes	Especialista principal de ventas	5	4	4	Severo
38	D	Datos clientes	Jefe departamento de inspección y supervisión	5	4	5	Crítico
39	D	Backup	Administrador de red	5	5	5	Crítico
40	D	Contraseñas	Administrador de red	5	5	4	Crítico
41	D	Logs	Responsable de SI	4	4	1	Dañino
42	AUX	Fibra óptica	Etecsa	2	3	2	Menor
43	AUX	Cableado	Operador	2	5	1	Dañino
44	AUX	Cable UTP	Administrador de red	2	5	3	Dañino
45	AUX	Archivos	Técnicos de seguridad y protección	2	2	2	Menor
46	AUX	UPS servidores	Administrador de red	1	4	1	Menor
47	AUX	Splits, aires acondicionados	Técnicos de seguridad y protección	1	4	1	Menor
48	AUX	Impresora	Jefa departamento de normalización	2	4	2	Dañino
49	D	Normas	Especialista gestión documental	5	5	5	Crítico
50	Media	Memorias USB	Jefe grupo recursos humanos	4	4	2	Dañino

No.	Dominio	Activo	Propietario	Conf.	Disp.	Integ.	Impacto
51	Media	Documentos del sistema	Responsable SIG	4	4	4	Severo
52	Media	Discos externos	Administrador de red	3	1	2	Menor
53	Media	DVD	Técnico de seguridad y protección	4	2	1	Menor
54	DP	Datos personales	Jefe grupo recursos humanos	3	2	3	Dañino

### Anexo 18: Análisis y evaluación de riesgos

Nombre del informe: Cálculo del riesgo

Fecha: 17/03/2021

Activo	Amenaza	Impacto de la amenaza	Valor	Probabilidad de ocurrencia	Valor	Total	Zona del riesgo
Servidor de correo electrónico	Fallos de hardware	Crítico	5	Probable	4	20	Extrema
	Acceso no autorizado	Crítico	5	Improbable	2	10	Alta
	Denegación de servicio	Dañino	3	Posible	3	9	Alta
Antivirus	Errores del administrador	Severo	4	Posible	3	12	Alta
	Difusión de software dañino	Crítico	5	Posible	3	15	Alta
	Errores de actualización de software	Crítico	5	Probable	4	20	Extrema
Administrador de sistemas	Deficiencias en la organización	Severo	4	Posible	3	12	Alta
	Extorsión	Crítico	5	Improbable	2	10	Alta
	Ingeniería social	Crítico	5	Improbable	2	10	Alta
Local de servidores	Acceso no autorizado	Crítico	5	Posible	3	15	Alta
	Incendio	Crítico	5	Posible	3	15	Alta

	Inundaciones	Crítico	5	Probable	4	20	Extrema
Local de información clasificada	Escapes de información	Crítico	5	Posible	3	15	Alta
	Acceso no autorizado	Crítico	5	Posible	3	15	Alta
	Modificación deliberada de la información	Crítico	5	Posible	3	15	Alta
Info compartida	Errores de los usuarios	Menor	2	Probable	4	8	Moderada
	Errores del administrador	Severo	4	Raro	1	4	Moderada
	Escapes de información	Insignificante	1	Improbable	2	2	Baja
Backup	Modificación deliberada de la información	Crítico	5	Probable	4	20	Extrema
	Destrucción de información	Crítico	5	Posible	3	15	Alta
Contraseñas	Escapes de información	Crítico	5	Improbable	2	10	Alta
	Errores de los usuarios	Crítico	5	Probable	4	20	Extrema
Cableado	Incendio	Crítico	5	Posible	3	15	Alta
	Inundaciones	Crítico	5	Casi seguro	5	25	Extrema
Impresoras	Fallos de hardware	Crítico	5	Probable	4	20	Extrema
	Robo	Crítico	5	Posible	3	15	Alta
Normas	Abuso de privilegios de acceso	Crítico	5	Posible	3	15	Alta
	Divulgación de información	Crítico	5	Probable	4	20	Extrema
Memorias USB	Degradación de los soportes de almacenamiento	Dañino	3	Casi seguro	5	15	Alta
	Fuga de información	Crítico	5	Posible	3	15	Alta
Documentos del sistema	Destrucción de información	Severo	4	Improbable	2	8	Moderada
	Modificación deliberada de la información	Crítico	5	Posible	3	15	Alta
	Divulgación de información	Severo	4	Posible	3	12	Alta
Datos personales	Divulgación de información	Dañino	3	Posible	3	9	Alta
	Deficiencias en la organización	Crítico	5	Posible	3	15	Alta