UNIVERSIDAD IBEROAMERICANA

Estudios con Reconocimiento de Validez Oficial por Decreto Presidencial
Del 3 de abril de 1981

LA VERDAD
NOS HARÁ LIBRES

UNIVERSIDAD
IBEROAMERICANA
CIUDAD DE MÉXICO ®

"PROPUESTA DE DEFINICIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BAJO EL ESTÁNDAR DE LA NORMA ISO/IEC 27001:2013 PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR EN NICARAGUA"

ESTUDIO DE CASO

Para obtener el grado de

MAESTRO EN GOBIERNO DE TECNOLOGÍA DE LA INFORMACIÓN

P r e s e n t a

CARLOS ALEJANDRO LOÁISIGA TÓRREZ

Director: Mtro. Guillermo Gómez Abascal
Asesor: Dr. Antonio Velasco Gómez
Lectores: Mtro. Guillermo Gómez Abascal
Dra. Tere Lucío Nieto

Ciudad de México, 2021

RESUMEN EJECUTIVO

La información en la actualidad es el activo más importante que tiene una organización, de ella depende el éxito o fracaso de la misma, se requiere análisis óptimo para protegerla de cualquier riesgo a la que está expuesta. Este antecedente permite realizar este estudio de caso, que trata sobre la gestión de la seguridad de la información basada en la norma ISO/IEC 27001:2013 y su incidencia en la información de las instituciones de educación superior en Nicaragua.

Se definirá un sistema de gestión de seguridad de la información para instituciones de educación superior en Nicaragua, que permita un mejor manejo de seguridad de la información, basada en la norma de seguridad ISO/IEC 27001:2013, que incorpora 14 dominios, 35 objetivos de control y 114 controles que facilitan el tratamiento, preservación, confiabilidad, integridad y disponibilidad de la información que gestiona toda organización.

La metodología utilizada se sustentó en el ciclo de mejora continua P.D.C.A. (Planear, Hacer, Chequear y Actuar), que está constituida por 4 fases, donde cada fase permite planificar, determinar, elaborar y valorar los activos de información.

El presente estudio de caso tendrá como enfoque principal la etapa I del ciclo P.D.C.A, ya que la fases de implementacion, de auditoría y acciones posteriores, no son parte del alcance.

Palabras Claves: Gestión, Seguridad de información, ISO/IEC 27001, sistema, vulnerabilidad, metodología, modelo, control, proceso, dominio, Tecnologías de la Información y Comunicación – TICS, Planear, Hacer, Chequear y Actuar -PDCA, riesgo.

ABSTRACT

Information is the most important asset that an organization has, its success or failure depends on it. An optimal analysis and security of informational data can protect organizations from any risk. This background allows us to carry out this case study, which deals with information security management based on the ISO / IEC 27001: 2013 standard and its impact on the information of higher education institutions in Nicaragua.

An information security management system will be defined for higher education institutions in Nicaragua, which allows better management of information security, based on the security standard ISO / IEC 27001: 2013, which incorporates 14 domains, 35 objectives of control and 114 controls that facilitate the treatment, preservation, reliability, integrity, and availability of the information that every organization manages.

The methodology is based on the continuous improvement cycle P.D.C.A. (Plan, Do, Check and Act), which is made up of 4 phases, each one allows planning, determining, elaborating, and evaluating the information assets.

The main focus of this case study is stage I of the P.D.C.A cycle, as the implementation, audit and subsequent actions phases are not part of the scope.

Keywords: Management, Information Security, ISO / IEC 27001, system, vulnerability, methodology, model, control, process, domain, Information and Communication Technologies - ICT, Plan, Do, Check and Act -PDCA, risk.

AGRADECIMIENTOS

Agradezco a Dios primeramente por permitirme culminar esta etapa de mi vida, por darme la fuerza, el tiempo, las condiciones físicas y mentales para el desarrollo de este trabajo.

A mis padres, por sus esfuerzos, tristezas y alegrías, asimismo el inculcarme a estudiar y superarme; además a las personas que estuvieron en este ciclo profesional de mi vida, les agradezco su amistad, consejo y apoyo.

Al Consejo Nacional de Universidades en Nicaragua, por su incondicional apoyo administrativo para la realización de esta importante Maestría.

Un agradecimiento especial a mi asesor el Dr. Antonio Velasco, por enseñarme que siempre se deben hacer las cosas bien y que cuando son difíciles, se valoran mucho más.

Al Maestro Guillermo Gómez Abascal, Coordinador de la Maestría en Gobierno de Tecnología de la Información y a mis maestros a lo largo de toda la maestría que desde el primer momento de mi llegada a la Universidad Iberoamericana me apoyaron en todo momento para ayudarme a culminar esté gran reto.

Agradezco al Gobierno de México, por medio de la Agencia Mexicana de Cooperación Internacional para el Desarrollo, en haberme otorgado la beca de excelencia académica, finalizando exitosamente mis estudios de Maestría.

ÍNDICE

TABLA DE ILUSTRACIONES

LISTA DE TABLAS

I. INTRODUCCIÓN

El presente estudio de caso está orientado a la definición de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013, donde se plantea como esta definición incide en el sistema de gestión de la información de las instituciones de educación superior en Nicaragua.

Dicha definición podría tener un impacto positivo y al mismo tiempo podría garantizar la seguridad en los diferentes servicios críticos que ofrecen las instituciones de educación superior en Nicaragua como es la parte académica, administrativa, registros, admisión, matriculación, contabilidad, informática entre otros servicios que prestan las instituciones de educación superior en Nicaragua. (Sevillano, 2016).

Es fundamental que las instituciones de educación superior en Nicaragua se enfoquen en el proceso de definir la seguridad de la información; ante estas circunstancias cabe destacar que el personal que toma decisiones dentro de las instituciones tengan la convicción y el conocimiento avanzado en el tema de seguridad de la información, además su apoyo será indispensable para llevar adelante las mejoras continuas (Isotools, 2018).

También se podría cambiar en algunos casos las modalidades de trabajo y algunas veces se modificarán procesos vitales institucionales, ya que se

implantarán nuevos controles de seguridad de la información para el uso correcto de la misma (Cruz Micán, Perea Sandoval & Ruiz López, 2018).

II. DESCRIPCIÓN DE LA ORGANIZACIÓN

Las instituciones de educación superior en Nicaragua, son instituciones estatales, autónomas, públicas, sin fines de lucro, que contribuye, desde la perspectiva del compromiso social universitario, así mismo existen universidades privadas dedicadas a la formación integral de profesionales bajo estándares nacionales e internacionales, desarrollando competencias a través de la docencia, la investigación y la extensión, con compromiso social y valores éticos.

Las instituciones de educación superior en Nicaragua, están comprometidas con la calidad, persiguen el mejoramiento continuo de forma sistemática consolidando su formación con principios éticos, humanísticos y ambientales, para que contribuyan al desarrollo sostenible del país y la región.

a. MISIÓN

La educación nicaragüense posee un subsistema que es responsabilidad del estado, bien público social, autónomo; tiene como finalidad la formación integral de profesionales de grado y posgrado; la generación y difusión de conocimientos a través de la investigación, la extensión, la innovación con calidad y la pertinencia educativa, con el fin de aportar a la sociedad nicaragüense un talento humano responsable, ético, solidario, reflexivo y crítico, capaz de mejorar: la calidad de vida, el respeto a la naturaleza, la institucionalidad del estado, la construcción de la identidad nacional y una sociedad multiétnica, democrática, solidaria, justa y próspera.

b. VISIÓN

La Educación Superior es un bien público y social de calidad, con reconocido liderazgo y prestigio en la sociedad, además es intercultural, articulado entre sí, que facilita la movilidad y el intercambio académico a nivel nacional e internacional, difundiendo el conocimiento y la cultura, potenciando el uso de los conocimientos y saberes locales, las tecnologías de la información y la comunicación, y que contribuye al desarrollo humano integral, científico y tecnológico del país.

III. ORGANIGRAMA

A continuación se muestra un modelo de organigrama estándar, donde las universidades de Educación Superior en Nicaragua, lo ocupan de ejemplo para poder realizar su estructura organizacional institucional:

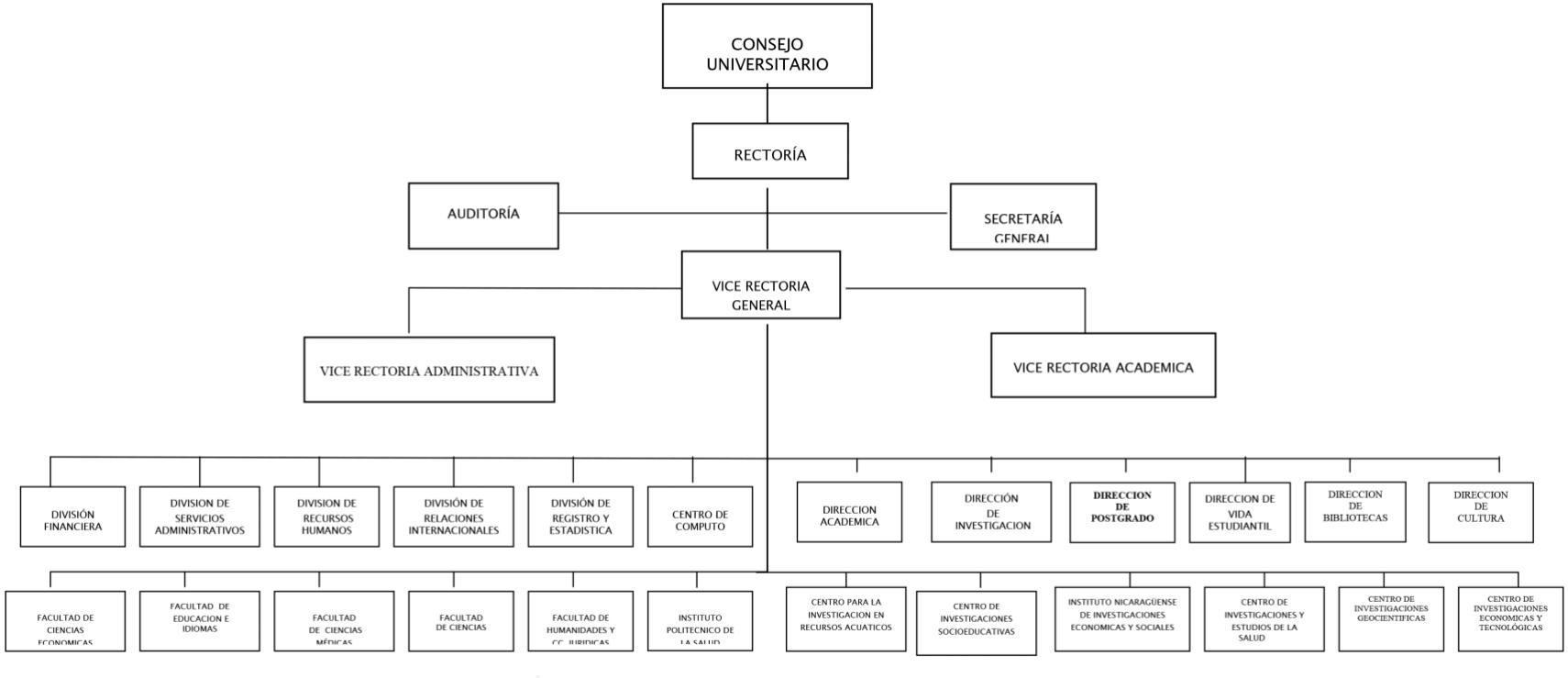

FIGURA 1. ORGANIGRAMA INSTITUCIONES DE EDUCACIÓN SUPERIOR

IV. SERVICIOS QUE OFRECEN

Las instituciones de educación superior, contribuyen a la formación de profesionales y técnicos, a nivel de grado y posgrado, con compromiso social, con valores éticos, morales y humanistas y en defensa del medio ambiente, líder en la producción de ciencia y tecnología, en la generación de modelos de aprendizajes pertinentes los cuales deben dirigir sus esfuerzos a satisfacer las demandas de la sociedad actual, siendo evidente la necesidad de formar seres humanos capaces de responder a estos modelos de aprendizajes, así mismo, a la superación de los retos nacionales, regionales e internacionales en las diferentes áreas de aprendizajes; constituyéndose en un espacio idóneo para el debate de las ideas y el análisis crítico constructivo de prácticas innovadoras y propuestas de mejoramiento humano y profesional permanente, contribuyendo a la construcción de una Nicaragua más justa y solidaria y, por lo tanto, más humana y en beneficio de las grandes mayoría.

<table>
<tr>
<td rowspan="2">Aliados Clave

Consejo Nacional de Universidades – CNU.

Ministerio de Educación – MINED.

Instituto Tecnológico Nacional – INATEC.

Gobierno de la República de Nicaragua.

Asociaciones de Universidades.

Enlaces académicos internacionales.</td>
<td>Actividades Clave

Enseñanza.
Bolsa de Trabajo.
Inscripción de materias, titulación.
Investigación, intercambio.</td>
<td rowspan="2">Propuesta de Valor

Ofrecer carreras técnicas, de nivel licenciaturas.
Ofrecer programas de maestrías y posgrados en todas las diferentes facultades académicas.
Experiencia académica y de calidad trabajando a favor de la educación en Nicaragua.
Modelo con enfoque sistémico en constante evolución.
Desarrollo de alianzas y convenios.</td>
<td>Relación con el Cliente

Estudiantes bachilleres y egresados como candidatos potenciales a las diferentes ofertas académicas.</td>
<td rowspan="2">Segmentos de Clientes

Estudiantes egresados de nivel bachillerato.

Estudiantes egresados de carreras de nivel técnico y licenciatura.

Estudiantes egresados de nivel maestría y doctorado.

Sociedad Nicaragüense</td>
</tr>
<tr>
<td>Recursos Clave

Profesores.
Personal administrativo.
Material didáctico.
Planes de estudio.
Infraestructura Tecnológica.
Salones de clases, laboratorios.</td>
<td>Canales

Medios Digitales.
Llamadas telefónicas.
Eventos educativos híbridos a causa del COVID19.</td>
</tr>
<tr>
<td colspan="3">Estructura de Costes

Costos de inmuebles e instalaciones.
Costos Administrativos.
Pago de aliados.</td>
<td colspan="2">Estructura de Ingresos

Partida presupuestaria del Gobierno de la República de Nicaragua.
Ingresos propios (Consultorías).
Captación de recursos económicos a través de proyectos.</td>
</tr>
</table>

TABLA 1: MODELO DE NEGOCIO DE LA ORGANIZACIÓN

V. PLANTEAMIENTO DEL PROBLEMA

En Nicaragua es, en parte, consecuencia de que los estudiantes tienen una desigualdad de insumos educativos, considerados críticos para facilitar el proceso de enseñanza-aprendizaje y que han demostrado tener una alta relevancia para mejorar la calidad y equidad de los aprendizajes. En gran parte del sector educativo es necesarios promover aprendizajes de buena calidad.

Las instituciones de educación superior en Nicaragua a través de sus máximas autoridades, personal docente y administrativo están realizando esfuerzos para reducir la burocracia en el manejo de la información lo que ha ocasionado problemas tanto para usuarios como para el personal que administra y procesa datos debido a la lentitud al momento de ingresar información.

Problemas muy comunes a nivel de software, hardware, desastres naturales e incluso el factor humano, ya sea por desconocimiento o por mal manejo. La pérdida o mal uso de información confidencial genera daños y repercusiones relacionados con la confidencialidad, integridad y disponibilidad de los archivos de la institución y a su vez para el titular del documento, incluso pérdida de credibilidad por parte de sus usuarios (estudiantes, comunidad educativa y público en general).

Por lo anterior se deben definir algunas políticas, lineamientos para el control, administración y manejo de información sobre la seguridad de la información dentro de las cuales es muy importante resaltar una política de riesgo, debido a que la

información es almacenada en dispositivos tanto lógicos como físicos los cuales no se encuentran localizados de manera estratégica, permitiendo así que la información sea vulnerable y como consecuencia de ello se genere un alto riesgo sobre la seguridad de la misma.

VI. **MARCO CONTEXTUAL** (IMPACTO ECONÓMICO Y SOCIAL)

El sistema educativo nicaragüense está constituido: i) educación básica, media y formación docente a cargo del Ministerio de Educación; ii) educación técnica y formación profesional a cargo del Instituto Nacional Tecnológico y el Ministerio de Educación; iii) educación superior bajo la coordinación del Consejo Nacional de Universidades (CNU); iv) educación extraescolar bajo la coordinación del Ministerio de Educación; y v) el Subsistema Educativo Autonómico Regional de la Costa Caribe Nicaragüense (SEAR), que es la responsabilidad de las regiones autónomas bajo la coordinación del Ministerio de Educación e Instituto Nacional Tecnológico.

El panorama de las carreras en los últimos años que ofrecen la educación superior nicaragüense se ha ampliado considerablemente, tanto en las universidades públicas como privadas. Sin embargo, no siempre la creación de carreras ha obedecido a estudios serios sobre las verdaderas necesidades y prioridades del país o mercado laboral, lo cual ha conducido a un crecimiento desordenado de las mismas en que se multiplica, exageradamente, el ofrecimiento de algunas carreras en determinada área del conocimiento.

La realidad impuesta al mundo por la pandemia del COVID–19 ha requerido la implementación de diversas opciones de educación. Según (Burns, M., 2020) el 91 % de los estudiantes a lo largo del mundo no está yendo a la escuela a causa de la crisis generada por el coronavirus. Frente a esto, gobiernos y organismos

internacionales y nacionales han implementado alternativas que han permitido que, según cálculos de varios medios de comunicación, cerca de 155 millones de niños y niñas alrededor del mundo continúen aprendiendo en casa.

Los centros educativos de Nicaragua han implementado opciones de educación a distancia. A pesar de los recursos y el acompañamiento cercano a maestros y tutores, el trabajo con esta modalidad ha sido complejo y difícil, y los resultados deberán ser evaluados en el futuro. Sin embargo, es preciso reconocer la agilidad con que los centros educativos encontraron soluciones y los ingentes esfuerzos que realizan todos los días para acompañar a estudiantes y sus familias y lograr que el aprendizaje continúe. Estas experiencias serán un importante aprendizaje para el país y ofrecerán alternativas que deberán ser analizadas en el futuro, para su implementación en el sistema de educación pública.

La situación de la educación en Nicaragua actualmente es crítica (Vijil, J & Castillo M, 2020), puesto que no se han alcanzado los objetivos básicos de universalización, hay altos niveles de ineficiencia y se ofrece una educación un poco deficiente que, lejos de constituirse como un mecanismo de movilidad social, está reproduciendo la pobreza y la desigualdad. Esta situación plantea desafíos estructurales universales, como los cambios de paradigmas educativos, y desafíos nacionales que en Nicaragua comienzan con el fortalecimiento de la democracia, y esto permita abrir las posibilidades de una mayor de participación ciudadana.

Un ámbito central es el abordaje y posicionamiento frente a la llamada “disrupción tecnológica” (Mateo y Rucci, 2019) y la educación a distancia, superando la falta de equidad, puesto que como dice (Burns, M., 2020) “la educación a distancia no puede verse simplemente como ‘una buena opción’, desarrollada junto con el sistema educativo existente; debe ser un componente esencial e integrado en el mismo”. Las nuevas tecnologías ofrecen un aspecto verdaderamente innovador que puede ayudar en la revolución educativa por su potencial para resolver muchos de los desafíos más importantes que enfrenta la educación, entre ellos, la atención a los diferentes ritmos y aprendizajes en una misma clase.

VII. **MARCO TEÓRICO** (DESCRIPCIÓN DE LAS HERRAMIENTAS A USAR)

Para el desarrollo de un sistema de gestión de seguridad de la información se utilizan conceptos referentes a la seguridad que aplican a cualquier tipo de entidad, públicas y/o privadas.

Sistema de Gestión de la Seguridad de la Información - SGSI: es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud de la información y sus métodos de proceso.
- Disponibilidad: 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.

A continuación se presentan conceptos fundamentales del estudio de caso con la revisión de la literatura, el estado del arte del tema y la fundamentación filosófica de dicha investigación:

i. ISO

La Organización Internacional de Estandarización (ISO) es una confederación de nivel global constituida por reglamentos de estandarización nacionales de 164 países, uno por cada país. La ISO es una institución que no depende de ningún gobierno, fundada en el año de 1947. La misión de la ISO es fomentar el desarrollo de la estandarización en el mundo relacionadas con esta norma, cuyo fin es ayudar permutando servicios y bienes, además de fomentar la cooperación en el campo intelectual, económico, científico, tecnológico.

ii. ANTECEDENTES DE LA NORMA ISO

La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa británica o no un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para obtener una certificación de parte de una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO, con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799. Esta última norma se le atribuyó como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En Marzo de 2006, posteriormente a la publicación de ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los Sistemas de Información.

Asimismo, ISO ha continuado, y continúa aún, desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificación dentro de la serie.

En la actualidad está vigente la ISO/IEC 27001 versión 2013, con un total de 14 dominios y 113 controles, además de contar con nuevos controles de seguridad.

iii. ISO 27001

(Portal ISO 27001, s.f.) es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una organización. La primera revisión se publicó en el año 2005 y fue desarrollada con base en el estándar británica BS 7799-2 (Bustamante Maldonado & Osorio Cano, 2017).

ISO 27001 puede ser implementada en toda organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información dentro de una organización. Permite que una empresa sea certificada; esto significa que una

entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización, en cumplimiento con la norma ISO 27000 (Bustamante Maldonado & Osorio Cano, 2017).

La norma ISO 27001 es una herramienta técnica de mejora continua basada en la metodología del ciclo PDCA, que permite implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para analizar y evaluar diferentes tipos de vulnerabilidades, riesgos o amenazas susceptibles que atenten contra la información de una organización, sea esta propia o datos de terceros (Excellence I, 2017).

En el anexo I se define todos los controles propuestos de la norma ISO27001.

iv. EVENTO DE SEGURIDAD DE LA INFORMACIÓN

Un evento de seguridad de la información, es la presencia reconocida de una condición de un sistema, servicio o inclusive red, que indica una potencial violación de la política de seguridad de la información o la falla de las contramedidas. Algunos ejemplos de eventos de seguridad de la información son; un empleado que se enlaza a un sistema, un intento errado de un empleado para acceder a un aplicativo, un Firewall que aprueba o bloquea un ingreso, una alerta de cambio de contraseña de un usuario, etc.

v. INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Un incidente de seguridad de la información se caracteriza por ser un evento o una serie de eventos de seguridad de la información, no esperados, que tienen una posibilidad mayor de comprometer las operaciones de la empresa y de comprometer la seguridad de la información. Cuando un evento comienza a registrar cualquier grado de impacto operativo, se convierte en un incidente. Por tanto, un incidente podría calificarse como un evento de cierta importancia, que genera un efecto significativo en los procesos del negocio.

Algunos casos de incidentes de seguridad de la información podrían ser; un acceso no permitido, el robo de contraseñas por parte de alguno de los usuarios, las diferentes prácticas de ingeniería social que se puedan presentar, la explotación de fallas en los procesos de autenticación para lograr accesos ilícitos, el robo de información, el borrado de información de terceros, la alteración de la información de terceros, el abuso y/o mal uso de los servicios informáticos internos o externos de una organización.

vi. DIFERENCIA ENTRE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD INFORMÁTICA

Es importante tener clara la diferencia entre la seguridad de la información y la seguridad informática, la primera abarca muchas más áreas, debido a que la información puede encontrarse en diferentes medios y formas, mientras la segunda se dedica exclusivamente de la protección de las infraestructuras de tecnologías de

la información y la comunicación que soportan las organizaciones. Por consiguiente la seguridad de la información cubre la seguridad informática.

vii. ACTIVO

El principal activo que tienen las organizaciones es la información, la cual debe ser protegida frente a riesgos y amenazas para asegurar el adecuado funcionamiento de la empresa. Esta información que es necesaria asegurar se denomina activo de seguridad de la información. Para identificación completa de los activos es necesario ampliar la visión y tener en cuenta más elementos que sólo hardware y software, puesto que contiene información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

viii. VULNERABILIDAD

Los activos de seguridad de la información pueden tener vulnerabilidades, es decir, circunstancias o características que representan una debilidad, permitiendo la materialización de ataques que comprometan la confidencialidad, integridad o disponibilidad del mismo.

Dicho de otra manera, la incapacidad de resistencia cuando se presenta un fenómeno amenazante es conocida como vulnerabilidad. Por ejemplo, un equipo será vulnerable a los virus si no tiene un programa antivirus instalado. Las vulnerabilidades pueden estar ligadas a aspectos organizativos (procedimientos mal definidos o sin actualizar, ausencia de políticas de seguridad), al factor humano

(falta de formación y/o de sensibilización del personal con acceso a los recursos del sistema), a los propios equipos, a los programas y herramientas lógicas del sistema, a los locales y las condiciones ambientales del sistema (deficientes medidas de seguridad física, escasa protección contra incendios, mala ubicación de los locales con recursos críticos para el sistema, etc.)

ix. AMENAZA

Aclarando el término de amenaza mencionado en la definición de vulnerabilidad, una amenaza es un evento o incidente provocado por una entidad natural, humana o artificial que aprovechando una o varias vulnerabilidades de un activo, pone en peligro la confidencialidad, la integridad o la disponibilidad de ese activo. Por tal motivo, se puede afirmar que una amenaza explota la vulnerabilidad del activo.

Una amenaza actúa de formas inesperadas para aprovecharse de las vulnerabilidades de los sistemas, servicios o redes de información y tiene el potencial de causar incidentes no deseados a los activos expuestos por las vulnerabilidades. Las amenazas pueden ser clasificadas de acuerdo al elemento que las provoca, bien sean personas, amenazas lógicas o amenazas físicas. De manera intencionada o accidental, las personas son las responsables de la mayoría de ataques a los sistemas, causando cuantiosas pérdidas.

x. RIESGO

Si una amenaza aprovecha una vulnerabilidad en los sistemas de información para causar daño, se habla de riesgo. Un riesgo es la apreciación del grado de

exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. Por lo tanto, el riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente.

xi. PROBABILIDAD

En la gestión de riesgos, es muy importante el concepto de probabilidad, ya que le permite a la organización determinar cuál de los escenarios de riesgos son más proclives a materializarse dado su entorno. Este aspecto resulta de gran utilidad posteriormente cuando la organización comienza el proceso de priorización de sus actividades de mitigación de riesgos.

xii. IMPACTO

Junto con la probabilidad, el impacto es un elemento fundamental en la gestión de riesgos. La NTC-ISO/IEC 27005, define el impacto como “el cambio adverso en el nivel de los objetivos del negocio logrados”. El impacto se refiere a la medición y valoración del daño que podría producir a la organización un incidente de seguridad.

xiii. POLÍTICAS DE SEGURIDAD

Se define la política y objetivos de seguridad de la información, es decir que la política de seguridad muestre lo que la organización planea realizar con relación a la seguridad de la información, los objetivos que aspira lograr, considerando las condiciones legales y reglamentarios aplicables y teniendo presente el compromiso de la Dirección de la organización para obtenerlos.

Una política es una directiva que apoya la ejecución de los objetivos, definida en función del alcance, y está considerada como el primer control de la norma ISO/IEC 27002. Es importante tener presente que la política de seguridad de información de una organización es una sola, y luego partiendo de esta política general establecida se pueden definir las distintas políticas determinadas en los diferentes niveles, por ejemplo: política de acceso a equipos y usuarios, política de uso de equipos informáticos y dispositivos móviles, política de respaldos de base de datos, entre otras políticas.

xiv. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Si una organización es víctima de alguno de estos ataques, su estabilidad y el cumplimiento de sus objetivos corporativos podrían verse afectados de manera significativa, por lo que es necesario adaptar un método que garantice que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Para lograr este fin, se implementa un Sistema de Gestión de Seguridad de la Información, el cual fomenta que una organización conozca los riesgos a los que está expuesta su información y los trate mediante una metodología definida, documentada y conocida por todos, que se revisa y mejora constantemente.

El Sistema de Gestión de Seguridad de la Información salvaguarda la confidencialidad, la integridad y la disponibilidad de la información, por medio de la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas al gestionar adecuadamente los riesgos.

El objetivo principal de un Sistema de Gestión de Seguridad de la Información es que las diferentes actividades afines con la gestión de la seguridad de la información, como pueden ser la declaración de objetivos, la planificación de actividades relacionadas al mejoramiento de la seguridad de la información, la implantación de controles, que pueden ser adaptados de normas como son ISO27001:2013 ITIL O COBIT, el análisis y la reacción ante incidentes y eventos, se puedan definir, repetir, medir y optimizar, implantando un proceso de mejora continua y dotando a las organizaciones del concepto de calidad a la seguridad.

Es un error considerar que el aseguramiento de los sistemas de información de una organización es función del área de TI, debido a que las acciones de todos los miembros que la componen pueden afectar de manera representativa la seguridad. Es por ello que la implementación exitosa de un Sistema de Gestión de Seguridad de la Información requiere el compromiso de todos, especialmente la alta dirección, comprendiendo y aceptando sus responsabilidades.

xv. GESTIÓN DEL CAMBIO

El cambio es una constante en las organizaciones de hoy. Ya sea un cambio en los procesos, nuevas tecnologías, en la estructura organizacional o en otros aspectos, generalmente estos impactan la forma en que las personas en una organización hacen su trabajo. El éxito del cambio, depende del éxito de la gestión del cambio para ayudar a las personas a aceptar, adoptar y utilizar los cambios requeridos.

Las organizaciones no cambian, las personas sí. No importa qué tan grande sea el proyecto que está asumiendo, el éxito de ese proyecto depende en última instancia de que cada empleado haga su trabajo de manera diferente, multiplicado por todos los empleados impactados por el cambio.

La gestión del cambio organizacional aprovecha las herramientas y metodologías que ayudan a las personas a realizar cambios que contribuyen a alcanzar los objetivos de la organización. Con una perspectiva de gestión del cambio organizacional, surge un proceso sobre cómo escalar las actividades de gestión del cambio y cómo utilizar el conjunto completo de herramientas disponibles para los líderes de proyectos y los gerentes de negocio.

VIII. OBJETIVOS

OBJETIVO GENERAL

Proponer la definición de un sistema de gestión de seguridad de la información para instituciones de Educación Superior en Nicaragua, basado en los estándares de la norma ISO 27001:2013, para incrementar la confianza, reducir los riesgos y garantizar la confidencialidad, integridad y disponibilidad de la información.

OBJETIVOS ESPECÍFICOS

- Establecer una metodología para definir un modelo de seguridad para la gestión de la seguridad de la información basada en la norma ISO/IEC 27001 dentro de las diferentes instituciones de educación superior en Nicaragua.
- Identificar riesgos existentes en las instituciones de educación superior en Nicaragua como base para el Sistema de Gestión de Seguridad de la Información.
- Evaluar los diferentes parámetros de confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación de las instituciones de educación superior en Nicaragua.
- Formalizar el Sistema de Gestión de Seguridad de la Información, mediante la documentación de las políticas, programas y procedimientos necesarios para gestionar los riesgos de seguridad de información de las instituciones de educación superior en Nicaragua.
- Coadyuvar a la difusión del conocimiento de la norma ISO 27001:2013 en las diferentes instituciones de educación superior en Nicaragua con el fin de apropiarse de los conceptos y metodologías para su correcta aplicación.

IX. ALCANCE

Definir un sistema de gestión de seguridad de la información para instituciones de educación superior en Nicaragua, para permitir un mejor manejo de seguridad de la información, con el objetivo de definir políticas, normas, lineamientos y estándares enfocados a las necesidades de la organización, posteriormente poder realizar un concienzudo y real análisis de la identificación de los riesgos que lleven a una futura implementación del sistema de gestión de seguridad de la información, de esta manera se facilitará entender al entorno organizacional, evaluar la situación actual de la seguridad de información e identificar las expectativas a través de las partes interesadas.

Se considera incluir la definición de una estrategia de gestión del cambio para la implantación del Sistema de Gestión de Seguridad de la Información en las instituciones de educación superior en Nicaragua, que consistirá en ofrecer formación, tanto a responsables como a empleados, de la aplicación de acciones de mejora en la documentación de los procesos y mostrándoles como utilizarlos, para obtener un mayor beneficio de los mismos y que permita favorecer a la organización para el cumplimiento de los objetivos.

Además, se creará en función de la organización y de su localización, que puede englobar un proceso, un conjunto de procesos, un servicio o un conjunto de servicios y oportunamente ser definido para prevenir confusiones y determinar la definición de un proyecto alcanzable en términos de tiempo y recursos.

El desarrollo del trabajo comprende proponer la definición para un sistema de gestión de seguridad de la información en instituciones de educación superior en Nicaragua. Todo lo anterior, soportado con la norma ISO/IEC 27001:2013, este trabajo no incluye implementación, mantenimiento y revisión del Sistema de Gestión de Seguridad de la Información en instituciones de educación superior en Nicaragua.

A continuación se presenta la metodología a usar en la primera fase del ciclo PDCA, el presente estudio de caso tiene un enfoque aplicado porque busca encontrar estrategias, políticas y mecanismos que permitan definir la seguridad de la información en las instituciones de educación superior en Nicaragua.

X. METODOLOGÍA

La metodología propuesta para la implantación de un Sistema de Gestión de Seguridad de la Información, se detallan en las fases que componen el ciclo de mejora continua PDCA (Planear, Hacer, Chequear y Actuar), con sus respectivas etapas y actividades a ejecutarse para la gestión de la seguridad de la información, la misma que servirá como un modelo base de seguridad, para gestionar y mejorar la seguridad de la información de las instituciones de educación superior en Nicaragua.

Este modelo es muy usado para el inicio de sistemas de gestión, en este caso un sistema de gestión de seguridad de información, ya que permite una efectiva organización y documentación.

FIGURA 2. CICLO PDCA

En la fase de *Planificación (Plan)* se realiza una evaluación de la organización donde se evalúa el estado en seguridad, el resultado de este estudio definirá las

medidas que se deben implementar en respuesta a las necesidades detectadas. La información tiene diferentes valores y diferentes tipos de riesgos, lo cual conlleva a que se deba realizar un análisis de riesgos que valore los activos de la información. Así mismo es necesario realizar una gestión de los riesgos detectados y reducirlos en la medida de lo posible, el resultado final después de aplicar el análisis y la gestión de riesgo, son una seria de controles necesarios para reducir los riesgos.

En la fase de *Hacer (Do)* del Modelo PDCA se realiza la implementación de los controles de seguridad seleccionados por la organización en la fase anterior, estos controles hacen referencia a fenómenos más técnicos como son la documentación necesaria. De igual forma en esta fase se realiza uno de los elementos vitales en el proceso y son las campañas de concientización y formación que permite dar a conocer a todos los actores de la organización qué se está haciendo y por qué.

En la fase de *Chequear;* en ella se valora la validez de los controles implementados, de ahí radica la importancia de contar con todos los registros e indicadores desarrollados al momento de definir y desarrollar los controles en las fases anteriores.

Se finaliza con la fase de *Actuar;* en ella se realizan las actividades relacionadas con el mantenimiento del sistema, si en el desarrollo de la fase anterior, la fase de verificar se detectó algún problema, ese problema es mejorado y corregido en esta fase del proceso. Al terminar la ejecución de las cuatros fases

se tienen en cuenta los resultados de la última fase y se inicia nuevamente con la primera.

Fase	Ciclo PDCA	Actividades (Etapas)
1	**PLANEAR** (Definir)	Definir alcance del SGSI. Definir política de seguridad. Metodología para evaluación de control de riesgo. Identificar el riesgo. Analizar y evaluar los riesgos. Identificar y evaluar opciones de tratamiento de riesgo. Seleccionar controles para el tratamiento de riesgo. Declaración de aplicabilidad.
2	**HACER** (Implementar y operar el SGSI)	Definir plan de tratamiento de riesgos. Implantar el plan de tratamiento de riesgos. Implementar controles. Definir un sistema de métricas. Formar y concientizar. Gestionar recursos del SGSI. Implantar procedimiento
3	**CHEQUEAR** (Monitorizar y revisar el SGSI)	Monitorear y Revisar el SGSI Revisar y medir la efectividad de los controles del SGSI (métricas del SGSI). Revisar los riesgos residuales. Realizar auditorías internas del SGSI. Revisar el SGSI por parte de la dirección

		Implementar mejoras al SGSI.
4	**ACTUAR** (Mantener y mejorar el SGSI)	Realizar acciones preventivas y correctivas. Evaluar sugerencias y definir la implementación de mejoras. Comunicar acciones y mejoras del SGSI. Asegurar alcanzar los objetivos previstos.

TABLA 2: CICLO PDCA

La seguridad absoluta no es posible y no existe un sistema totalmente seguro, por lo que el factor de riesgo siempre es latente sin importar las medidas que se tomen. Para tratar de mitigar esa realidad, la seguridad de la información se ha definido como un proceso continuo que se debe actualizar, refinar y mejorar constantemente, permitiendo a cada organización utilizar los instrumentos que considere oportunos para medir y controlar la mejora del sistema.

MODELO ADKAR

Este modelo de gestión del cambio orienta sus etapas inicialmente en un cambio individual, porque perciben que sí se realiza inicialmente el cambio individual será más fácil que se lleve el cambio organizacional. “El ciclo de vida de ADKAR comienza después de que se haya identificado un cambio. Desde este punto de partida, el modelo proporciona un marco y secuencia para manejar el cambio lateral de las personas” (Hiatt, 2006, pág. 3). Después de identificar el cambio, se llevan a cabo 5 etapas en el orden establecido, para cumplir con éxito el propósito del cambio, en la siguiente ilustración se detallan las 5 etapas:

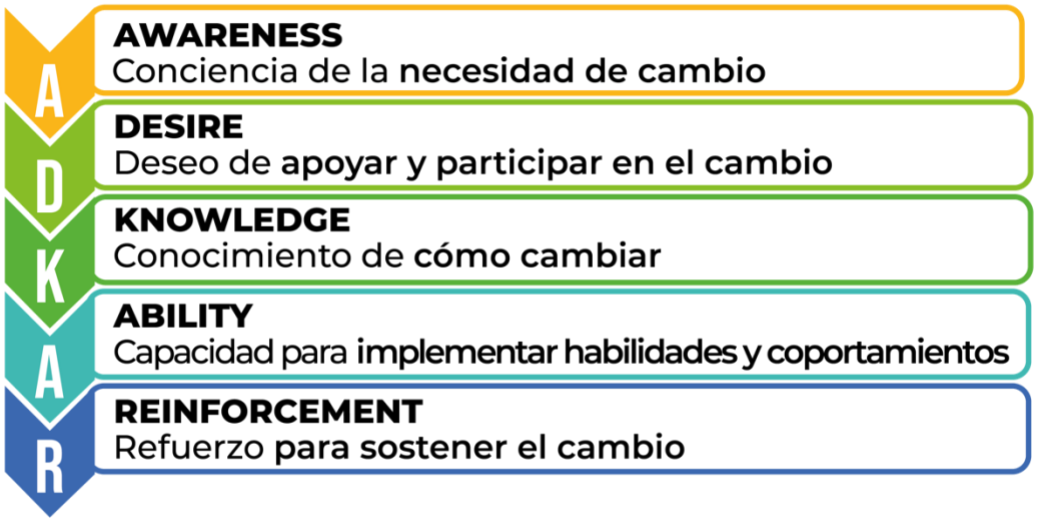

FIGURA 3: MODELO ADKAR- GESTIÓN DEL CAMBIO

En alguna de las etapas se puede encontrar el tipo de personas frente al cambio ó elementos que pueden intervenir para que las etapas no se desarrollen de acuerdo a lo establecido y que no se cumpla con el objetivo del cambio. A continuación, se hará una breve descripción de las etapas del modelo ADKAR y los elementos que pueden influir en cada una de ellas.

AWARENESS (CONCIENCIA)

El objetivo de esta etapa es crear conciencia en el personal sobre la necesidad del cambio y que riesgos puede traer tanto personalmente como en la organización no realizarlo, es decir, en esta etapa el personal debería entender el origen del cambio y por qué es necesario. (Hiatt, 2006, págs. 9-10) menciona que

en esta etapa se pueden presentar cinco factores que pueden influir en la conciencia de la necesidad del cambio, es decir, que pueden ocasionar resistencia al cambio.

DESIRE (DESEO)

En esta segunda etapa el objetivo es motivar al personal a participar y sensibilizarlos frente a la importancia de apoyar el cambio y el impacto que puede generar su participación en el mismo, se puede presentar resistencia al cambio, ya que “crear el deseo al cambio no está totalmente bajo el control de la organización” (Hiatt, 2006, pág. 18), sino que nace directamente en la persona apoyar los cambios o nuevos escenarios que se presenten. Según (Hiatt, 2006) en esta etapa se pueden presentar cuatro factores que influyen en el deseo de apoyar y participar en cambio a nivel personal o grupal, los cuales son:

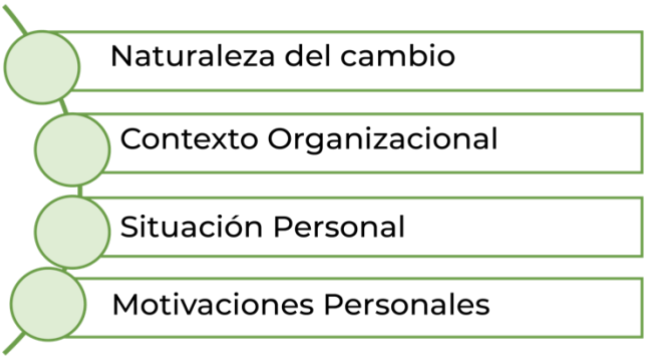

FIGURA 4: FACTORES QUE INFLUYEN EN EL DESEO AL CAMBIO

El primer factor es la naturaleza del cambio aquí es importante “la efectividad de la comunicación depende de cómo son recibidos e interiorizados los mensajes” (mypeople / Prosci)

El segundo factor es el contexto organizacional “la cultura de una organización desempeñaran un papel calve en la construcción del deseo de apoyar el cambio” (Hiatt, 2006).

El tercer factor es la situación personal, “comprender la situación personal individual es de gran ayuda para comprender su decisión de apoyar o resistirse a un cambio” (mypeople / Prosci), en este factor influyen elementos asociados al contexto interno del personal cómo las relaciones en el trabajo, su familia, situaciones del entorno, entre otras. Y por último las motivaciones personales, “las motivaciones personales son atributos inherentes que conducen nuestras decisiones y nos hacen únicos como individuos” (mypeople / Prosci).

KNOWLEDGE (CONOCIMIENTO)

“El conocimiento representa la información, la capacitación y el entrenamiento necesario para saber cómo cambiar” (mypeople / Prosci). En esta etapa, lo que se busca es que el personal conozca y se capacite para saber cómo cambiar o también que nuevos conocimientos adquiridos le permitirán adaptarse al cambio. Los factores que influyen en esta etapa de acuerdo al autor son: “capacidad de la persona para aprender, recursos disponibles para proporcionar educación y capacitación, acceso o existencia del conocimiento requerido y por último la base de conocimiento actual de una persona” (Hiatt, 2006, pág. 27).

ABILITY (HABILIDAD-CAPACIDAD)

El objetivo de esta etapa es fortalecer las habilidades que tenga el personal que logren nuevas conductas para cambiar, “en un proceso de cambio individual, los resultados y logros emergen por vez primera en el escenario de la habilidad. Los comportamientos se alcanzan de manera exitosa y el estado futuro comienza a tomar forma. Con la habilidad demostrada, el cambio se hace realidad” (mypeople / Prosci).

En esta etapa se puede presentar resistencia al cambio, por temor a lo desconocido, la incertidumbre que puede generar los nuevos cambios, costumbres o hábitos, las personas día a día tienen un hábito para desarrollar sus actividades y desarrollar nuevos hábitos puede generar un choque en las personas, la falta de tiempo o prioridades que tenga el individuo puede influir en el proceso de cambio, ya que para él habrá cosas más importantes que hacer.

REINFORCEMENT (REFUERZO)

El objetivo de esta etapa es mantener el cambio, dar continuidad a las acciones implementadas para que el cambio se cumpla con éxito. Organizacionalmente son aquellas herramientas o elementos que desarrolla la compañía para incentivar a que las personas siguen actuando bajo los cambios implementados y sensibilizar al personal del éxito que puede traer ejecutar los cambios si se trabaja continuamente

en ello. “Incluye acciones activas como reconocimientos, recompensas y celebraciones que estén unidas a la realización del cambio, así como también, la satisfacción interna de una persona con su logro” (mypeople / Prosci).

XI. CRONOGRAMA DE ACTIVIDADES

En esta sección se describe el cronograma de actividades, teniendo en cuenta que se han mencionados algunas propuestas de definiciones de políticas de seguridad de la información, se elaborarán y actualizarán los procedimientos de seguridad básicos para soportar el sistema de gestión de seguridad de la información, de acuerdo a los siguientes actividades:

- Definir el alcance del Sistema de Gestión de Seguridad de la Información en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- Definir una política de seguridad que:
    - Incluya el marco general y los objetivos de seguridad de la información de la organización;
    - Considere requerimientos legales o contractuales relativos a la seguridad de la información;
    - Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el Sistema de Gestión de Seguridad de la Información;
    - Establezca los criterios con los que se va a evaluar el riesgo;
    - Esté aprobada por la dirección.
- La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información que posee la ventaja de manifestar sus resultados en valores

cuantitativos, o sea en términos económicos, lo que facilita la toma decisiones y su validación por las máximas autoridades. Esta etapa está compuesta por los siguientes objetivos:

- Identificar activos: realizar una identificación y tasación de activos, que serán los elementos a proteger.
- Valorar activos: los activos deben contar con una valoración.
- Identificar amenazas: Identificar y valorar las amenazas a las que están expuestos los activos.
- Calcular el impacto: Se refiere al cálculo del daño que puede generar sobre el activo al ejecutarse la amenaza. Impacto = Valor del activo x Porcentaje de impacto.
- Calcular el riesgo: Después de calcular el impacto potencial, se calcula el riesgo potencial asociado. Riesgo = Frecuencia x Impacto.
- Selección apropiada de tratamiento: Identificados los riesgos, se debe evaluarse las acciones apropiadas.
- Reducción del riesgo y riesgos residual: en los riesgos tratados se ha restado el riesgo en un valor “X” quedando un riesgo menor a el inicial, al cual se llama riesgo residual.

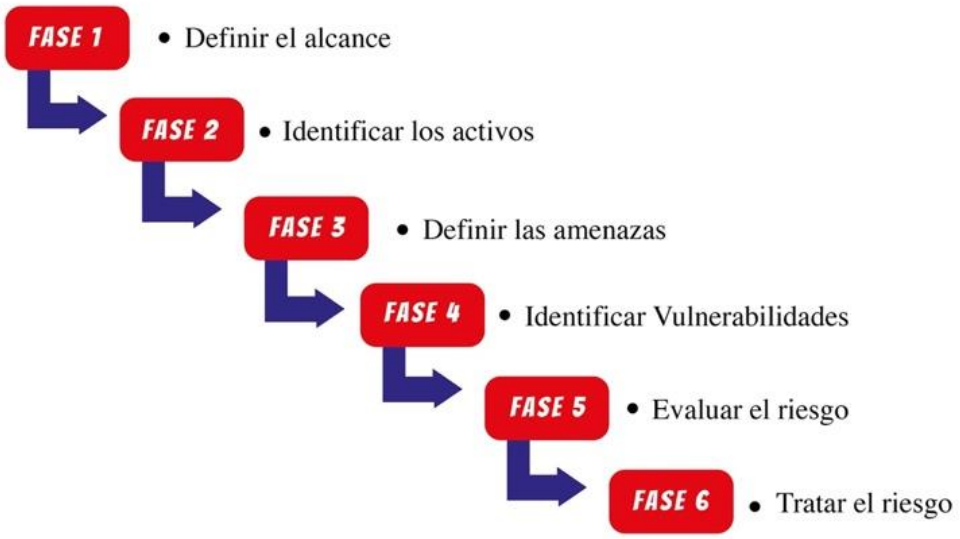

FIGURA 5. METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

- Identificar los riesgos (Identificar y Valorar activos):
    - Identificar los activos que están dentro del alcance del Sistema de Gestión de Seguridad de la Información y a sus responsables directos, denominados propietarios;
    - Identificar las amenazas en relación a los activos;
    - Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
    - Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

En esta etapa se ejecuta un inventario de activos señalando su localización, personal responsable y las funciones que estos llevan a cabo, facilitando un análisis

y valoración de los riesgos para establecer las amenazas, vulnerabilidades y efectos que presentan en las organizaciones.

Comprendiendo la norma ISO 27001:2013, se destaca como un activo de información, comprendiendo un activo como un elemento que represente valor para la organización, como por ejemplo activos de información tales como bases de datos, documentación, equipos informáticos, departamentos, manuales de usuario, software de aplicación y sistemas, contratos de equipo de comunicaciones, servicios informáticos, entre otros.

La clasificación general de los activos de información se puede visualizar en la siguiente Figura:

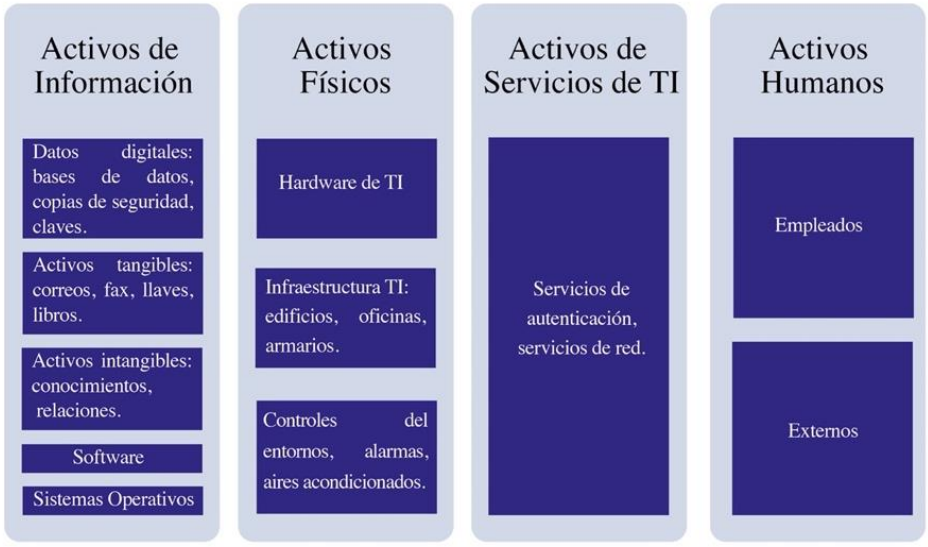

FIGURA 6. CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN.

- La información de los activos definidos anteriormente debe englobar los siguientes atributos:
    - Nombre de activo.
    - Descripción de activo.
    - Clase a la que pertenece (Equipo, aplicación, servicio, etc.).
    - Localización (Espacio físico donde se halla en la organización).
    - Propietario (Responsable del activo).
    - Es fundamental, una vez ejecutado el inventario de activo, considerar los siguientes principios:
        - Amenazas: Causas de alto grado de un incidente no previsto, por ejemplos daños a los sistemas de información y comunicación de la organización.
        - Vulnerabilidades: Debilidades de activos que pueden ser aprovechadas por otras amenazas.
- Analizar y evaluar los riesgos:
    - El análisis y evaluación de riesgos tiene como finalidad disponer una priorización de los riesgos de procesos y activos implicados en el alcance del Sistema de Gestión de Seguridad de la Información para su tratamiento siguiente. Esta etapa tiene que:
        - Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
        - Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas,

vulnerabilidades, impactos en los activos y los controles que ya estén implementados;

- Estimar los niveles de riesgo;
- Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

- Seleccionar los objetivos de control y los controles de la ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del Sistema de Gestión de Seguridad de la Información.
- Definir una declaración que incluya:
  - Los objetivos de control y controles seleccionados y los motivos para su elección;
  - Los objetivos de control y controles que actualmente ya están implantados;

El cronograma considera las actividades necesarias para la gestión del cambio, lo que implica un cambio de paradigmas en los actores que participarán en el Sistema de Gestión de Seguridad de la Información, así como la manera de ver y comprender la organización por parte de los miembros de la misma, pues las prácticas cotidianas en la gestión de la dinámica organizacional son mediadas por los significados construidos por las personas que la conforman y al instaurar un nuevo sistema de gestión, cambian las prácticas y los sistemas de trabajo, es por

eso que a continuación nombraremos las fases para la gestión del cambio provocado por la implantación del Sistema de Gestión de Seguridad de la Información en las instituciones de educación superior de Nicaragua:

FIGURA 7: FASES DEL PROCESO DE GESTIÓN DE CAMBIO

El proceso de gestión de cambio organizacional, se construye en tres fases en las autoridades superiores de la organización puede trabajar en los proyectos o iniciativas de transformación que está liderando. A continuación se describen cada fase del proceso de gestión de cambios para las organizaciones:

Fase 1 – Preparing for Change (preparándose para el cambio)

La primera fase del proceso, ayuda a los equipos de proyecto y cambio a prepararse para diseñar sus planes de gestión de cambio. Responde preguntas como:

¿Qué tanto en gestión de cambio necesita este proyecto?

¿A quiénes impacta esta iniciativa y de qué manera?

La primera fase proporciona el conocimiento de la situación que es crítico para crear planes de gestión de cambio efectivos.

Fase 2 – Managing Change (gestionando el cambio)

La segunda fase, se centra en la creación de planes que se integrarán con el plan de los diferentes proyectos que lleve acabo la organización.

Fase 3 – Reinforcing Change (reforzando el cambio)

El refuerzo, aunque igualmente crítico, la mayoría de veces se pasa por alto. La tercera fase lo ayuda a crear planes de acción específicos para garantizar que el cambio se mantenga. En esta fase, se desarrollan mecanismos para medir qué tan bien se está afianzando el cambio, ver si los empleados realmente están haciendo su trabajo de la nueva manera, identificar y corregir brechas y celebrar el éxito.

El cronograma de actividades de acuerdo a los tiempos posibles de cada una de las etapas del ciclo PDCA , incluyendo entre cada etapa las fases del proceso de gestión de cambio está descrito en la siguiente gráfica:

Actividades	ENERO				FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGO		
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3
Inicio y Planeación del proyecto.																															
Peparar el Cambio																															
PLAN Análisis de la Situación Actual																															
DO Implementación del SGSI																															
Gestionar el Cambio																															
CHECK Monitoreo del SGSI																															
ACT Mejorar Continua del SGSI																															
Reforzar el Cambio																															
Cierre del Proyecto																															

TABLA 3: CRONOGRAMA DE ACTIVIDADES

XII. GRUPOS DE TRABAJOS

La organización establece, implementa, mantiene y mejora continuamente un Sistema de Gestión de Seguridad de la Información, incluyendo los procesos necesarios y sus interacciones, de conformidad con los requisitos de esta Norma Internacional.

Es decir para cumplir con este control bastaría con sumar a las funciones de cada puesto aquellas funciones que tengan que ver con la seguridad de la información. Pero no basta con definirlas, también se debe comunicar a cada persona implicada en la seguridad de la Información sus roles y responsabilidades.

Se debe definir algunas propuestas de las responsabilidades de cada empleado o puesto de trabajo en relación a la seguridad de la información.

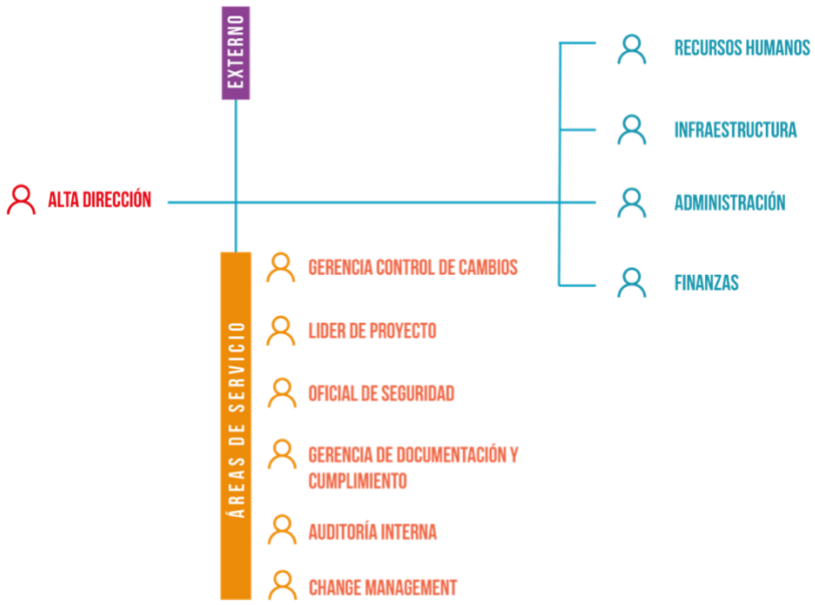

FIGURA 8. PROPUESTAS DE GRUPO DE TRABAJOS.

XIII. CONCLUSIONES

La definición de un Sistema de Gestión de Seguridad de la Información aplicado a cualquier institución de educación superior en Nicaragua, permitirá aumentar la probabilidad de alcanzar sus objetivos, fomenta la proactividad, ayudará a cumplir con los requisitos legales, normas y mejora la imagen de la institución educativa.

El desarrollo de políticas de seguridad mitiga y disminuye el impacto de que algún riesgo se materialice y ocasione pérdidas para la institución educativa, es de vital importancia que las políticas sean definidas, documentadas y publicadas para que todo el personal de la institución educativa las conozca y practique.

El contenido de la norma ISO 27001 está orientado a la gestión de la seguridad de la información mediante la evaluación y tratamiento de riesgos, peligros y vulnerabilidades a la que está expuesta la información de las instituciones de educación superior en Nicaragua, ya que esta norma describe paso a paso la manera adecuada de gestionar la seguridad de los activos de información dentro de las diferentes instituciones.

La propuesta diseñada es una oportunidad para las pequeñas y medianas empresas que deseen definir y posteriormente implementar un Sistema de Gestión de Seguridad de la Información o que deseen madurar sus procesos de seguridad

de la información; los diferentes elementos entregados se pueden adaptar y utilizar según las necesidades y los contextos de las empresas.

Las organizaciones están en la obligación, de certificarse y promover las mejores prácticas ofrecidas en las Normas Internacionales, estipuladas en la ISO 27000, ISO 27001 y la ISO 27002, cuyos estándares permitirán que las instituciones educativas obtengan un grado de confianza y solidez una vez se cuente con su correcta y verificada definición, implementación y puesta en marcha.

El modelo ADKAR proporciona estructura y dirección que ayudan a planear el cambio en las organizaciones de manera efectiva. El modelo es efectivo y fácil de entender. Si un cambio no está siendo exitoso, puede usar el modelo ADKAR para identificar cualquier brecha dentro de su proceso de gestión de cambio.

La gestión del cambio es un tema de preocupación en las organizaciones, principalmente en institución de educación superior de Nicaragua, para lo cual es preciso encontrar un alineamiento adecuado en el pensamiento estratégico de sus integrantes.

El esfuerzo de documentar y hacer expresar la estrategia en el seno de las instituciones d educación superior de Nicaragua, a través de los documentos de calidad o procesos, se basaría en evitar el aspecto coyuntural como origen de los cambios; logrando el progresos más estables, consolidados y que permitan a la institución ir avanzando en el tiempo y no a expensas únicamente del entorno.

Este modelo pretende ser una contribución para visibilizar la evolución del pensamiento estratégico de las instituciones de educación superior en Nicaragua, permitiendo orientar los avances de las mismas en aras a una mayor gestión de calidad.

XIV. REFERENCIAS BIBLIOGRÁFICAS

Aguirre, B. J. (2018). *Auditoria Informática*. Obtenido de http://fcasua.contad.unam.mx/apuntes/interiores/docs/98/8/audi_infor.pdf

Burns, M. (2020). *Cuatro opciones de enseñanza a distancia por considerar durante esta pandemina del COVID–19.* Obtenido de https://www.globalpartnership.org/fr/ blog/4-options-denseignement-distance-envisager-durant-cette-pandemie-de-covid-19

Bustamante Maldonado & Osorio Cano. (2017). Metodología de la seguridad de la información como medida.

Bustamante Maldonado & Osorio Cano. (2017). Metodología de la seguridad de la información como medida.

Cruz Micán, Perea Sandoval & Ruiz López. (2018). Análisis de riesgos en la gestión de proyectos. Aplicación de las TIC en los sectores económicos.

Excellence I. (2017). Obtenido de https://www.pmg-ssi.com/2015/07/que-es-sgsi/

Fundación Internacional para el Desafío Económico Global. (2018). Obtenido de http://fideg.org/wp-content/uploads/2018/09/INFORME-DE-RESULTADOS-2017.pdf.

Heinekn. (2016). Obtenido de Revista de Información a Directivos: http://www.sld.cu/sitios/infodir/temas.php?idv=1346

Hernández Figueroa, C. (2018). *Políticas de Seguridad*. Obtenido de http://www.spi1.nisu.org/recop/al01/javier/part4.html.

Hiatt, J. (2006). *ADKAR.*

ICONTEC. (2008). *Técnicas de Seguridad de la Información. Gestión de Riesgo en la seguridad de la Información.* Bogotá.

Isotools. (2018). *Descubre que es un SGSI y cuáles son sus elementos esenciales*. Obtenido de https://www.isotools.org/2016/02/16/descubre-que-es-un-sgsi-y-cuales-son-sus-elementos-esenciales/

Mateo y Rucci. (2019). *El futuro ya está aquí. Habilidades transversales en América Latina y el Caribe en el siglo XXI. Banco Interamericana de Desarrollo.* Obtenido de https://publications.iadb.org/publications/spanish/document/El_futuro_ya_est%C3%A1_aqu%C3%AD_Habilidades_transversales_de_Am%C3%A9rica_Latina_y_el_Caribe_en_el_siglo_XXI_es.pdf

mypeople / Prosci. (s.f.). Obtenido de www.mypeopleco.com

Portal ISO 27001. (s.f.). Obtenido de http://www.iso27000.es/iso27000.html.

Serrano Anton, J. C. (2017). *Seguridad de la Información*. Obtenido de https://www.fooddefensesoluciones.com/es/iso-27001-seguridad-de-la-informacion.

Sevillano. (2016). *Por qué implantar un SGSI basado en la norma ISO 27001?:*. Obtenido de https://www.pmg-ssi.com/2015/05/por-que-implantar-un-sgsi-basado-en-la-normaiso-27001/

Vijil, J & Castillo M. (2020). *Estamos ante una emergencia educativa, en la educación nos estamos jugando el presente y el futuro.*

XV. ANEXOS

En esta sección finalmente se incluyen los anexos que sustenta la investigación del estudio de caso para poder definir un sistema de gestión de seguridad de la información para instituciones de educación superior en Nicaragua:

a. ANEXO I

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

FIGURA 9: CONTROLES DE LA NORMA ISO 27002:2013

b. ANEXO II

TABLA 4: SISTEMAS DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

ISO/IEC 27001:2013 TECNOLOGÍAS DE INFORMACIÓN – TÉCNICAS DE SEGURIDAD

CLÁUSULAS		ENTREGABLE
4	**Contexto de la Organización**	
4.1	Inicio	Organigrama
4.2	Necesidades Expectativas	
4.3	Alcance	Plan de Comunicacion
		Plan de trabajo
4.4	Información del SGSI	Inicio y Planificacion
		Plan de Riesgos
		Manual del SGSI
5	**Liderazgo**	
5.1	Liderazgo y compromiso	Concretar reuniones
5.2	Política	Politica de Seguridad
5.3	Roles- Responsabailidades	Asignación de roles o cambios de los mismos.
6	**Planeación**	
6.1	Riesgos y oportunidades	Riesgos y Oportunidades

		Aceptación Niveles de riesgo
6.2	Objetivos de Seguridad y planes	SOA
		Plan de Riesgos
		Plan de Respuesta a riesgos
7	**Soporte**	
7.1	Recursos	Referencias laborales
7.2	Competencias	Descripción de Responsabilidades
		Descripción de Roles
		Listas de capacitación.
7.3	Sensibilización	Presentación SGSI.
		Tríptico SGSI.
		Capacitación al personal.
7.4	Comunicación	Plan de capacitación
		Plan de Difusión
		Procedimiento de Comunicación y Difusión
7.5	Gestión Documental	Documentación de Proceso
		Plantilla Agenda y Minuta
		Plantilla de lista Documentos

		Plantilla de lista de Registros
		Lista maestra de Documentos
		Lista maestra de Registros
		Política de Clasificación y Etiquetado de Información
		Repositorio
8	**Operación**	
8.1	Planeacion y control	Plan de trabajo
		Bitácora de Seguimiento
		Revisar lista de ISO 27001
		Reportes con la Gerencia
8.2	Evaluacion de riesgos	Utilizar información de resultados de la evaluación de riesgos.
8.3	Tratamiento de Riesgos	SOA
9	**Evaluación**	

9.1	Monitoreo Medición Analisis Evaluación	Definir de qué debe ser monitoreado, cómo, cada cuando, quien lo hace, cómo mide, cómo analiza medición y cómo evalua (resultados comparables y repetitivos)
		Información que evidencia el monitoreo y análisis.
9.2	Auditoria Interna	Manual de SGSI. Sección 9.2 Auditoría Definición de qué debe ser auditado, cómo, cada cuando, métodos, responsables, informes. quien lo hace, definir criterios de auditorías y alcance,
		Procedimiento de Auditorías Internas
		Política de Auditorías Internas
		Plan Anual de auditorias

		Agenda Para Auditoría Interna
		Lista de Asistencia de Apertura y Cierre de Auditorías
		Lista de Verificación
		Concentrado De Auditoria
		Informe Auditoría Interna
		Nombramiento Equipo Auditor
		Evaluación de Auditor Interno
		Información que de seguimiento a la ejecución de auditorías

9.3	Revisiones gerenciales	Los reportes deben incluir: estatus de accionesde revisiones previas a) Estatus de revisiones previas b) cambios en asuntos internos y externos que son relevantes para el SGSI. c) Retroalimentación del desempeño. d) Evaluación de riesgos. e) Mejora continua.
10	**Mejora Continua**	
10.1	No conformidad Acciones correctivas	Concentrado No Conformidades
		Formulario No Conformidades
		Politica No Conformidades
		Procedimiento No Conformidades
10.2	Mejora continua	Formato Mejora Continua
		Política Mejora Continua

		Procedimiento Mejora Continua
A.5	**A.5 Políticas de seguridad de la información**	
A.5.1	Directivas de la gestión para seguridad de la información	
A.5.1.1	Políticas para la seguridad de la información.	Politica de seguridad de la información
A.5.1.2	Revisión de políticas de seguridad de la información	Politica de seguridad de la información
A.6	**A.6 Organización de la seguridad de la información**	
A.6.1	Organización interna	
A.6.1.1	Funciones y responsabilidades de seguridad de la Información	Manual de SGSI.
A.6.1.2	Segregación de funciones	Manual de SGSI.
A.6.1.3	Contacto con autoridades	Contacto con las autoridades superiores.
A.6.1.4	Contacto con grupos de interés especial	Contacto con grupos de interés. Manual de SGSI.
A.6.1.5	Seguridad de la información en la administración de proyectos	Gestión de proyectos.
A.6.2	Dispositivos Moviles y Teletrabajo	
A.6.2.1	Política sobre dispositivos móviles	Política sobre dispositivos móviles
A.7	**Seguridad de los Recursos Humanos**	
A.7.1	Antes del Empleo	
A.7.1.1	Investigación	Referencias laborales
A.7.1.2	Términos y Condiciones de Contratación	Contrato individual de trabajo Reglamento interno de trabajo

		Compromiso de confidencialidad
		Aviso de privacidad
A.7.2	Durante el Empleo	
A.7.2.1	Gestión de las responsabilidades	Contrato individual de trabajo
		Actualización de Actividades
A.7.2.2	Sensibilización, Formación y Capacitación en seguridad de la información	Plan de Comunicación
		Presentación Inducción
		Política de concientización y capacitación
A.7.2.3	Procesos disciplinario	Procedimiento de conciliación y corrección
		Contrato Administrativo
		Acta de Conciliación
A.7.3	Durante el Empleo	
A.7.3.1	Cese o cambio de responsabilidades del empleo	Aviso de confidencialidad de la información.
		Gestión de altas y Bajas.
		Checklist de Alta
		Checklist de Baja
A.8	**Administración de Activos**	
A.8.1	Responsabilidad sobre los Activos	
A.8.1.1	Inventario de Activos	
A.8.1.2	Propiedad de los Activos	

A.8.1.3	Uso Aceptable de los Activos	Politica de uso aceptable de activos
A.8.1.4	Devolución de Activos	Politica de devolución de activos
A.8.2	Responsabilidad sobre los Activos	
A.8.2.1	Clasificación de la Información	Politica de clasificación, etiquetado y manejo de activos.
A.8.2.2	Etiquetado de la Información	Politica de clasificación, etiquetado y manejo de activos.
A.8.2.3	Manejo de Activos	Politica de clasificación, etiquetado y manejo de activos.
A.8.3	Manejo de los Medios	
A.8.3.1	Gestión de Medios Extraíbles	Politica de gestión de medios removibles.
A.8.3.2	Eliminación de Medios	Politica de eliminación y transeferencia segura de medios.
A.8.3.3	Transferencia de Medios Físicos	Politica de trasferencia de medios Procedimiento.
A.9	**Control de acceso**	
A.9.1	Requisitos del negocio para control de acceso	
A.9.1.1	Política de Control de Acceso	Política de control de acesos lógicos.
A.9.1.2	Acceso a Redes y a los Servicios de Red	Política de internet.
A.9.2	Gestión de Accesos de Usuario	

A.9.2.1	Registro de usuarios y des-registros	Proceso de registro y des-registro.
A.9.2.2	Provisión de acceso a usuario	Proceso de provisión de acceso a usuario(Gestion de roles y privilegios).
		Procedimiento de Gestión de altas y bajas.
A.9.2.3	Gestión de derechos de acceso privilegiado	Pólitica de control de acesos lógicos.
		Control de accesos privilegiados.
A.9.2.4	Gestión de información secreta de autentificación de los usuarios	Pólitica de gestión de contraseñas.
A.9.2.5	Revisión de los derechos de acceso a usuario	Pólitica de gestión de contraseñas.
A.9.2.6	Eliminación o ajuste de los derecho de acceso	Pólitica de gestión de contraseñas.
A.9.3	Responsabilidades del usuario	
A.9.3.1	Autentificación secreta	Pólitica de gestión de contraseñas.
A.9.4	Control del sistema y acceso a las aplicaciones	
A.9.4.1	Restricción del acceso de la información	Pólitica de gestión de contraseñas.
A.9.4.2	Procedimiento seguro de inicio de sesión	Procedimiento seguro de inicio de sesión.
A.9.4.3	Sistema de gestión de contraseñas	Sistema de gestión de contraseñas (Guía).

A.9.4.4	Uso de programas utilitarios privilegiados	Procedimiento para especificar. Monitoreo de uso de programas utilitarios privilegiados.
A.9.4.5	Control de acceso al código fuente de los programas	Politica de control de acceso al código fuente.
A.10	**Criptografía**	
A.10.1	Controles Criptográficos	
A.10.1.1	Política de Uso de Controles Criptográfico	Politica de controles criptográficos.
A.10.1.2	Gestión de Claves	Politica de controles criptográficos.
A.11	**Seguridad física y ambiental**	
A.11.1	Áreas seguras	
A.11.1.1	Perímetro de seguridad física	Procedimiento de Seguridad física.
A.11.1.2	Controles físicos de entrada	Procedimiento de Seguridad física.
A.11.1.3	Seguridad de oficinas, despachos e instalaciones	Procedimiento de Seguridad física.
A.11.1.4	Protección contra las amenazas externas y al medio ambiente	Procedimiento de Seguridad física.
A.11.1.5	Trabajo en áreas seguras	Procedimiento de Seguridad física.
A.11.1.6	Zona de entrega y de carga	Procedimiento de Seguridad física.

A.11.2	Equipamiento	
A.11.2.1	Emplazamiento y protección de equipos	Procedimiento de Equipamiento.
A.11.2.2	Instalaciones de soporte	Procedimiento de Equipamiento.
A.11.2.3	Seguridad del cableado	Procedimiento de Equipamiento.
A.11.2.4	Mantenimiento de los equipos	Procedimiento de Equipamiento.
A.11.2.5	Remoción de activos	Procedimiento de Equipamiento.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Procedimiento de Equipamiento.
A.11.2.7	Reutilización o retirada segura de equipos	Procedimiento de Equipamiento.
A.11.2.8	Equipo de usuario desatendido	Pólitica de equipo de usuario deseinformado.
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Política de pantalla y escritorio limpio.
A.12	**Seguridad en operaciones**	
A.12.1	Responsabilidades y procedimientos de operación	
A.12.1.1	Documentación de los procedimientos de operación	Gestión de desarrollo Procedimiento de Desarrollo.

		Gestión verificación y validación.
		Politicas Organizacionales.
A.12.1.2	Gestión de cambios	Solicitud de Cambio.
		Plan de datos y configuración.
A.12.1.4	Separación de los entornos de desarrollo, pruebas y producción	Aplicación de red.
		Plan de datos y configuración.
A.12.2	Protección contra malware	
A.12.2.1	Controles contra malware	Procedimiento.
		Politica de Antivirus.
A.12.3	Copia de seguridad	
A.12.3.1	Copia de seguridad de la información	Definir procedimiento, o actualizar en Plan de Datos y Configuración.
A.12.4	Registro y monitoreo	

A.12.4.1	Registro de eventos	Proceso de revisión de eventos de seguridad.
A.12.4.2	Protección de la información de registros	Procedimiento de protección.
A.12.4.3	Registros del administrador y operador	Proceso de revisión de eventos de seguridad.
A.12.5	Control de software en operación	
A.12.5.1	Instalación de Software en sistemas operativos	Procedimiento de instalación de software en sistemas operativos.
A.12.6	Gestión de vulnerabilidades técnicas	
A.12.6.1	Control de las vulnerabilidades técnicas	
A.12.6.2	Restricciones a la instalación de software	
A.12.7	Consideraciones sobre la auditoria de los sistemas de información	
A.12.7.1	Controles de auditoria de los sistemas de información	
A.13	**Seguridad en comunicaciones**	
A.13.1	Gestión de la seguridad de las redes	

A.13.1.1	Controles de red	Procedimiento para Seguridad en la red.
A.13.1.2	Seguridad de los servicios de red	Procedimiento para Seguridad en la red.
A.13.1.3	Segregación en las redes	Procedimiento para Seguridad en la red.
A.13.2	Transferencia de información	
A.13.2.1	Políticas y procedimientos de transferencia de la información	Políticas y procedimientos de transferencia de la información.
		Procedimiento de transferencia de informacón.
A.13.2.2	Acuerdos de transferencia de información	Contrato con Proveedores.
		Convenio de Confidencialidad.
		Procedimiento de seguridad de la información con proveedores. (Clausula de seguridad dentro de los acuerdo con los proveedores).
A.13.2.3	Mensajería electrónica	Política de mensajeria electrónica.
A.13.2.4	Confidencialidad o acuerdos de no divulgación	Contrato individual de trabajo.

A.14	**Adquisición, desarrollo y mantenimiento de sistemas**	
A.14.1	Requisitos de seguridad de los sistemas de información	
A.14.1.1	Análisis y especificación de los requisitos de seguridad de la información	Especificación de requiermientos
		Política de desarrollo seguro de software.
		Plan de administración de la configuración.
		Proceso de integración de componentes.
		Casos de uso indebido.
		Casos de uso.
		Gestion de Desarrollo.
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma operativa	Especificación de requiermientos.
		Solicitud de Cambio.doc.

A.14.2.4	Restricciones en los cambios de los paquetes de software	Procedimiento de desarrollo seguro.
		Especificación de requerimientos
		Solicitud de Cambio.doc
A.14.2.5	Principios de ingeniería de sistemas seguros	Gestión de desarrollo.
		Verificación y validación.
		Procedimiento de desarrollo seguro.
A.14.2.6	Entorno de desarrollo seguro	Aplicación de red.
		Plan de datos y configuración.
A.14.2.7	Desarrollo externalizado	
A.14.2.8	Pruebas de seguridad del sistema	Gestión verificación y validación.
		Estrategia de pruebas.
		Casos de prueba Integrales.
		Casos de prueba Unitarias.
		Matriz de Observaciones.

		Reporte de pruebas de uso indebido
A.14.2.9	Pruebas de aceptación del sistema	Gestión verificación y validación.
		Casos de Pruebas Aceptación.
A.14.3	Datos de prueba	
A.14.3.1	Protección de los datos de prueba	Estrategia de pruebas.
		Plan de datos y configuración.
A.15	**Relación con proveedores**	
A.15.1	Seguridad de la información en las relaciones con los proveedores	
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	Política de seguridad de la información para las relaciones con los proveedores.
A.15.1.2	Seguridad dentro de los acuerdo con los proveedores	Contrato con Proveedores.
		Convenio de Confidencialidad.

		Procedimiento de seguridad de la información con proveedores. (Clausula de seguridad dentro de los acuerdo con los proveedores).
A.15.1.3	Información y comunicación de la cadena de suministro de tecnología	Listado de proveedores.
A.15.2	Gestión de suministros de servicios del proveedor	
A.15.2.1	Monitoreo y revisión de los servicios de los proveedores	Procedimiento de seguridad de la información con proveedores.
		Lista de Servicios.
A.15.2.2	Gestión de cambios en los servicios prestados por proveedores	Procedimiento de seguridad de la información con proveedores.
A.16	**Administración de incidentes de seguridad de la información**	
A.16.1	Gestión de incidentes de seguridad de la información y mejoras	
A.16.1.1	Responsabilidades y procedimientos	Proceso de gestión de incidentes de seguridad
A.16.1.2	Notificación de los eventos de seguridad	Proceso de gestión de incidentes de seguridad

A.16.1.3	Informar sobre los puntos débiles de seguridad de la información	Proceso de gestión de incidentes de seguridad
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Proceso de gestión de incidentes de seguridad
A.16.1.5	Respuesta de incidentes de seguridad de la información	Proceso de respuesta a incidentes de seguridad
A.16.1.6	Aprendiendo de incidentes de seguridad de la información	Lecciones aprendidas
A.16.1.7	Recolección de evidencia	Proceso de gestión de incidentes de seguridad
A.17	**Aspectos de seguridad de la información en la administración de continuidad del negocio**	
A.17.1	Continuidad de la seguridad de la información	
A.17.1.1	Planificación de la continuidad de la seguridad de información	
A.17.1.2	Aplicar la continuidad de la seguridad de información	Plan de ejecución de continuidad de la seguridad de información.
A.17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de información	Plan de verficación, revisión y evaluación de la seguridad de información.
A.17.2	Redundancia	
A.17.2.1	Disponibilidad de instalaciones de tratamiento de la información	
A.18	**Aspectos de seguridad de la información en la administración de continuidad del negocio**	
A.18.1	Cumplimiento de requisitos legales y contractuales	

A.18.1.1	Identificación de la normativa aplicable y de los requisitos contractuales	Política de cumplimiento legal y regulatorio.
A.18.1.2	Derechos de propiedad intelectual (DPI)	Contrato de prestación de servicios para terceros.
		Contrato individual de prestación de servicios.
A.18.1.3	Protección de los registros	Política de protección de registros y privacidad de información de identificación personal.
A.18.1.4	Protección y privacidad de información de identificación personal	Política de protección de registros y privacidad de información de identificación personal
A.18.1.5	Regulación de controles criptográficos	
A.18.2	Revisiones de la seguridad de información	
A.18.2.1	Revisión independiente de la seguridad de la información	Politica de auditorias internas del SGSI.
		Procedimiento de auditorias internas del SGSI.
		Lista de verificación.
		Agenda de auditoria.
		Plan anual de auditoria.

A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Lista de verificación.
		Informe de auditoria interna.
		Concentrado de auditoria.
A.18.2.3	Revisión del cumplimiento de normas técnicas	Proceso de revisión del cumplimiento de normas técnicas.