UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:
INGENIERO EN SISTEMAS INFORMÁTICOS

INGENIERÍA EN SISTEMAS INFORMÁTICOS

TEMA:
DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA ISO 27000 PARA LA UNIDAD EDUCATIVA PARTICULAR SÉNECA.

AUTOR:
MARCO VINICIO BONILLA ORTIZ

TUTOR/A:
ING. TANNIA MAYORGA MG.

QUITO, ECUADOR
2018

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación certifico:

Que el trabajo de titulación **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA ISO 27000 PARA LA UNIDAD EDUCATIVA PARTICULAR SÉNECA**, presentado por MARCO VINICIO BONILLA ORTIZ, estudiante de la Carrera Ingeniería en Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D. M., 9 de abril de 2018

TUTOR

Ing. Tannia Mayorga MG.

AGRADECIMIENTO

A Dios, quien ha sido a través de sus lecciones y enseñanzas que he aprendido a levantarme y seguir creyendo en los sueños, aprendí con su amor a creer en mí y la capacidad que puedo tener para lograr cumplir mis objetivos.

A mi Madre Rita Bonilla, quién desde pequeño creyó en mí y jamás dejo de hacerlo, quién me ha apoyado siempre a pesar de no tener los recursos para hacerlo, sin embargo, el amor, la fe y sus oraciones, hacen que mi sueño sea el suyo.
Gracias madre por darme la vida y gracias por creer en mí.

A mis hermanos Byron y Edison, quienes me apoyaron en los momentos más difíciles que atravesaba, cuando no tenía los recursos para hacerlos, ellos estuvieron ahí para que pueda seguir mi camino, quizás sacrifique tiempo con mi familia, pido disculpas, pero ahora saben que el sacrificio valió la pena. Gracias hermanos, mi éxito es de la ustedes también.

A la familia Séneca: Paolita, Paulinita, Christian, Mariela, Mauricio y Pedrito quienes fueron y son amigos que además de un "sigue adelante" podía contar con ellos para una ayuda o un consejo, apoyo y sobre todo la amistad.

Mis compañeros y amigos de universidad Tyrone y Rony, con quienes hemos compartido risas, preocupaciones, sustos y demás anécdotas con un solo fin, disfrutar de este camino con sus altas y bajas llamado universidad.

A quienes llegaron a mi vida brindándome una oportunidad: Juano, Charito, Chiquita y Kattyta, quienes llegaron en el momento preciso cuando no creía en mí, y lo único que dijeron fue "adelante, tú si puedes y eres capaz de hacerlo", basto esas palabras para emprender y continuar este viaje que ha sido duro, sacrificado, pero de mucha alegría.

A mis profesores, quienes han aportado con su conocimiento y sabiduría en especial al Ing. Christian Vaca quien considero el mejor profesor de la universidad y gracias a sus clases fue una inspiración para la realización de este proyecto. A la Ing. Tannia Mayorga quien me guiado durante el proceso de la tesis sus consejos y exigencias que en oportunos momentos me dio ánimos para continuar a que llegue a cumplir los objetivos planteados para la finalización del proyecto, y por último al Ing. Pablo Recalde por su colaboración oportuna en momentos precisos, reitero mi más grande agradecimiento

DEDICATORIA

Quiero dedicar primeramente a Diosito por permitirme cumplir uno de mis más grandes sueños, el amor y el agradecimiento hacia él son incomparables y cada día hago mención de eso, “gracias por todo lo que me has dado”. Te amo mucho.

A mi Madre y hermanos, “Negro, eres el mejor hermano que podía tener y gracias por estar siempre pendiente de mí, eres mi ídolo”.

También quiero dedicar a una persona que llego a mi vida de la nada, que de apoco fue involucrándose en mi mundo y quién jamás permitió que este sueño lo abandonará, nunca dejo que algo tan simple como un pasaje impidiera que siga el camino hacia mi sueño.
¡Usted sabe de quién hablo! Gracias por su apoyo.

TABLA DE CONTENIDOS

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

El diseño de un Sistema de Gestión de Seguridad de la Información “SGSI” permitirá fomentar las buenas prácticas de protección y Seguridad de la Información dentro de la Unidad Educativa Particular Séneca por medio de la asociación entre los activos tecnológicos y de información y quienes lo manipulan.

Para el análisis y evaluación de riesgos se creó varias matrices de acuerdo a los criterios de valoración entre las amenazas y vulnerabilidades con el propósito de conocer el nivel de riesgo que los activos poseen, sus resultados sirvieron para realizar el tratamiento de riesgo y sugerir controles para dar respuesta a los riesgos que posee la Unidad Educativa Particular Séneca.

Para la identificación del mal uso de los equipos y la poca protección de los mismos se realizó el levantamiento de activos de toda la institución educativa utilizando un formato en la que describe el tipo de activo, su ubicación, propiedad y responsabilidad, se realizó el análisis de brecha entre los requisitos de la norma ISO 27001 numerales 4-10 enfocándose en el cumplimiento, de la misma manera para conocer el nivel de cumplimiento de los Dominios relacionados con la norma ISO 27002 en conjunto con el Anexo A de la norma ISO 27001 se realizó otro análisis de brecha, mismo que comprende el numeral 5-18. Los resultados permitieron conocer los tipos de activos, así como la situación inicial de la institución.

La identificación de activos generó la gestión documental que por medio de una guía que describe la codificación de documentos, activos, áreas y políticas de seguridad de información con la finalidad de identificar la documentación con mejor precisión. Los resultados permitieron la organización de documentos según las actividades.

PALABRAS CLAVES*:* SGSI, Estándar ISO/27000, Metodología de Riesgos, Controles, Activos, Políticas, Seguridad, Información, Amenazas, Vulnerabilidades, Riesgo, Impacto, Educación.

ABSTRACT

The design of an Information Security Management System SGSI will allow the promotion of good protection practices and "Information Security" within the Séneca Individual Educational Unit through the association between technological and information assets and those who they manipulate it.

For the analysis and evaluation of risks, several matrices were created according to the evaluation criteria between the threats and vulnerabilities in order to know the level of risk that the assets possess, their results served to perform the risk treatment and suggest controls for respond to the risks that the UEP has Seneca.

For the identification of the misuse of the equipment and the little protection of the same ones, the asset survey of the whole educational institution was carried out using a format in which it describes the type of asset, its location, property and responsibility, the analysis was carried out of gap between the requirements of ISO 27001 numerals 4-10 focusing on compliance, in the same way to know the level of compliance of the domains related to ISO 27002 in conjunction with Annex A of ISO 27001 performed another gap analysis, which includes the number 5-18. The results allowed knowing the types of assets, as well as the initial situation of the institution.

The identification of assets generated the document management through a guide that describes the codification of documents, assets, areas and policies of information security in order to identify the documentation with better accuracy. The results allowed the organization of documents according to the activities.

KEYWORDS: ISMS, ISO / 27000 Standard, Risk Methodology, Controls, Assets, Policies, Security, Information, Threats, Vulnerabilities, Risk, Impact, Education.

INTRODUCCIÓN

Antecedentes de la situación objeto de estudio

La Seguridad de la Información se basa en el proceso que se relaciona la tecnología con la información, así como también los sistemas que los procesan y dependiendo del tipo de empresa u organización, estas deben tener como prioridad y buenas prácticas de seguridad la protección y cuidado de los activos de manera interna y externa.

La protección de los activos no solamente se trata de equipos o sistemas que gestionen seguridad, a su vez se trata también de cómo se puede evitar riesgos de posibles amenazas hacia sus activos pudiendo ser estos, humanos o tecnológicos.

El Laboratorio de Computación de la Unidad Educativa Particular Séneca, es el área que administra la red y el servicio de internet, así también es la encargada de dar soporte a los equipos informáticos, sin embargo, no cuenta con un organigrama de TI, ya que sólo está considerada como un aula de clase, por ende, las autoridades desconocen la importancia que tiene el proteger los recursos tecnológicos y de información que se encuentra en esta área.

El presente proyecto tiene como finalidad proponer el diseño de un Sistema de Gestión de Seguridad de la Información para la Unidad Educativa Particular Séneca mediante la aplicación de la Norma IOS/IEC 27000 versión 2014.

Planteamiento

El siguiente proyecto se enfocará en el Laboratorio de Computación de la institución, este será la base para el Sistema de Gestión de Seguridad de la Información propuesto, dicha área está a cargo de gestionar los recursos tecnológicos y velar por el funcionamiento y soporte del servicio de red e internet en toda la unidad educativa particular Séneca.

El alcance de este proyecto comprende el diseño que se sugiere para mejorar en el control de los procesos y administración de activos tecnológicos en el Laboratorio de Computación.

Formulación

La tecnología es una expansión sin medida en todas las áreas y su conexión permanente se entiende a través de todo tipo de objetos, esto hace que los expertos en seguridad se preocupen por proteger la información que se procesa, ahora no sólo las empresas deben preocuparse por la seguridad de los activos, sino también las instituciones educativas, en el caso de la Unidad Educativa Particular Séneca existe poco control en la gestión de los recursos tecnológicos lo que permite la manipulación de equipos informáticos sin restricciones y cuentas de usuarios gestionadas con las medidas de seguridad apropiadas.

Una de las complicaciones principales dentro de la institución para la gestión de recursos de tecnología se debe a la falta de un área responsable de administrar, gestionar, designar y controlar el manejo de recursos tecnológicos, servicio de internet, acceso a los activos, etc., esta responsabilidad fue designada al Laboratorio de Computación siendo en la actualidad el área principal relacionada con TI.

La manipulación directa de los equipos informáticos puede provocar la infección de *software* malicioso que amenace la confidencialidad, integridad y disponibilidad de la información, la problemática también existe en la transmisión y flujo de datos, relacionándose con el deterioro de cables, conexiones eléctricas en mal estado, conectores rotos, varios dispositivos conectados, sistemas operativos desactualizados y acceso al internet sin previa autorización, estos son factores que provocan el mal funcionamiento de los equipos y la inestabilidad del servicio de red e internet.

A través de este análisis se puede mostrar que la institución carece de una política o procedimiento que permita gestionar los recursos de tecnología y de información, la misma que está expuesta a ser vulnerable contra intrusos informáticos y humanos.

Justificación

El nivel de ataque mundial es muchas veces perpetrado en diferentes organizaciones o empresas sin importar su giro de negocio o tamaño, hace que de apoco tomen la debida importancia acerca del cuidado y protección que deben tener con los activos de información. A pesar de tener poco o suficiente conocimiento acerca del peligro que se tiene cuando se utiliza los recursos tecnológicos, aun no logran comprender cómo se puede llegar a mitigar aquellos riesgos que pueden perjudicar a nivel; administrativo, financiero, académico o de comunicación, esto con el tiempo puede causar daños leves, graves e incluso irreparables, pues al no poseer una guía, política, norma, metodología o simplemente una cultura de proteger la información, la amenaza siempre estará latente (Pascual, 2013, p. 18).

Este proyecto, planea diseñar un SGSI utilizando la norma ISO/IEC 27000; con la que se pretende concientizar y evidenciar los riesgos que posee la Unidad Educativa Particular Séneca con el propósito de elaborar guías o políticas que ayuden a gestionar los activos mediante los resultados del análisis y evaluación de riesgos que a su vez sirve de base para sugerir controles se adecuen a loa activos críticos que se encuentran en la institución.

Objetivo General

Diseñar un Sistema de Gestión de Seguridad de la Información que permita la gestión correcta de los recursos tecnológicos y de información, así como la clasificación de activos para el análisis y evaluación de riesgos, por medio de la ISO 27000 y su familia para que la institución tenga una mejor administración y control de recursos.

Objetivos Específicos

- Realizar una revisión bibliográfica del marco legal y de buenas prácticas para la elaboración de un SGSI.
- Examinar la situación actual de la Unidad Educativa Particular Séneca por medio de un análisis de brecha.

- Realizar el análisis y evaluación del riesgo identificando los recursos a proteger (activos) en Laboratorio de Computación de la institución.
- Determinar y sugerir algunos mecanismos de control que permitan minimizar las vulnerabilidades que se encuentran durante el análisis de riesgo.
- Elaborar Políticas de Seguridad de la Información y sugerir controles basado en los resultados obtenidos anteriormente.

Alcance

El alcance del proyecto únicamente incluye las siguientes actividades:

Inventario de activos de tecnología e información con la finalidad de clasificar, ubicar y etiquetar, definiendo el nivel de riesgo de acuerdo a su valoración.

Utilizar las directrices que recomienda la ISO 27005 para el análisis y evaluación de riesgos, así como su tratamiento.

Diseñar políticas que permitan minimizar el acceso y manipulación de recursos tecnológicos proponiendo controles que definan responsabilidad sobre dichos recursos que pertenecen a la institución.

Recomendar controles que se adapten a las necesidades de acuerdo a los resultados obtenidos que permitan dar respuesta a los niveles de riesgo críticos.

CAPÍTULO I

FUNDAMENTACIÓN TEÓRICA

1.1. Introducción

Muchas veces las organizaciones consideran que asegurar o proteger la información es adquirir *hardware* o *software* costoso sin tomar en cuenta que, al carecer de una política o procedimiento, ésta se vuelve vulnerable ante amenazas ya sea interna o externa, esto se puede evitar teniendo una cultura organizacional de buenas prácticas de seguridad de la información.

Para conseguir una buena gestión sobre la Seguridad de la Información es indispensable conocer una metodología o norma que pueda satisfacer los objetivos y necesidades de la institución, misma que permita documentar, registrar y definir todo evento relacionado con la protección de activos y los riesgos que puedan aparecer ante amenazas de tipo humanas y no humanas.

Dentro de las metodologías o normas que ofrecen guías para la protección de activos de información, en el siguiente proyecto se utilizará la familia de la norma ISO/IEC 27000, que es un conjunto de estándares internacionales que hablan sobre la "Seguridad de la Información" sugiriendo como cultura institucional las buenas prácticas de protección a los recursos de tecnología e información, siendo sus aliados principales las normas ISO/IEC 27001, 27005 y 27002 (27000, ISOTools, s.f.).

1.2. Marco Legal

Tabla 1. Marco Legal

LEY DE PROTECCIÓN DE DATOS PERSONALES	LEY DE COMERCIO ELECTRÓNICO
Según la BASE CONSTITUCIONAL en el Ar. 66 de la constitución de la República del Ecuador. *"Se reconoce y garantizará a las personas: El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos de información requerirán la autorización del titular y el mandato de la ley"*	De acuerdo con el capítulo I Principios Generales, en al Art. 5. *"Confidencialidad y reserva. - Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia"* (Jurídico, s.f.). En el Art. 9 que se encuentra en [4] dispone que: *"Protección de datos. - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.* *La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente".*

Fuente: (DerechoEcuador, 2011).

1.3. Marco Contextual

1.3.1. Unidad Educativa Particular Séneca

La Unidad Educativa Particular "Séneca", ubicada en la Urb. Iñaquito Alto, calle Juan Díaz sector OE-9 con una población aproximada de 280 y un personal administrativo y docentes de 38 personas.

La Unidad Educativa Particular "Séneca" es una entidad que brinda una educación con principios y valores desde una perspectiva familiar en la que ha venido creciendo desde hace 24 años, cuyo propósito es ofrecer oportunidades únicas de formación y desarrollo, basadas en la consideración de que cada ser humano es una identidad irrepetible de alma, cuerpo y mente no susceptible de generalizaciones absolutas.

Misión

Ser una comunidad educativa particular, pluralista que apoye a la Nación en la tarea formadora de las nuevas generaciones, bajo una filosofía integrativa, humanista y sistemática optimizando la calidad humana a través de los modelos de honestidad, creatividad, cooperación, tolerancia asertividad; con adecuado autoconocimiento, valoración e imagen que generen un YO interno apto para contribuir al desarrollo de la sociedad.

Visión

Ser una institución líder en educación integradora donde se prioriza el respeto a la diversidad y la atención a las necesidades educativas particulares de sus educandos.
Cumplir armoniosamente su misión formadora conociendo, comprendiendo y amando a quienes integran la comunidad educativa, a través de conducir, es decir, acompañar a los estudiantes en sus esfuerzos formativos y realizar ajustes oportunos mediante métodos adecuados y eficientes (Séneca, s.f.).

Organigrama

La Unidad Educativa Particular Séneca, presenta su organigrama.

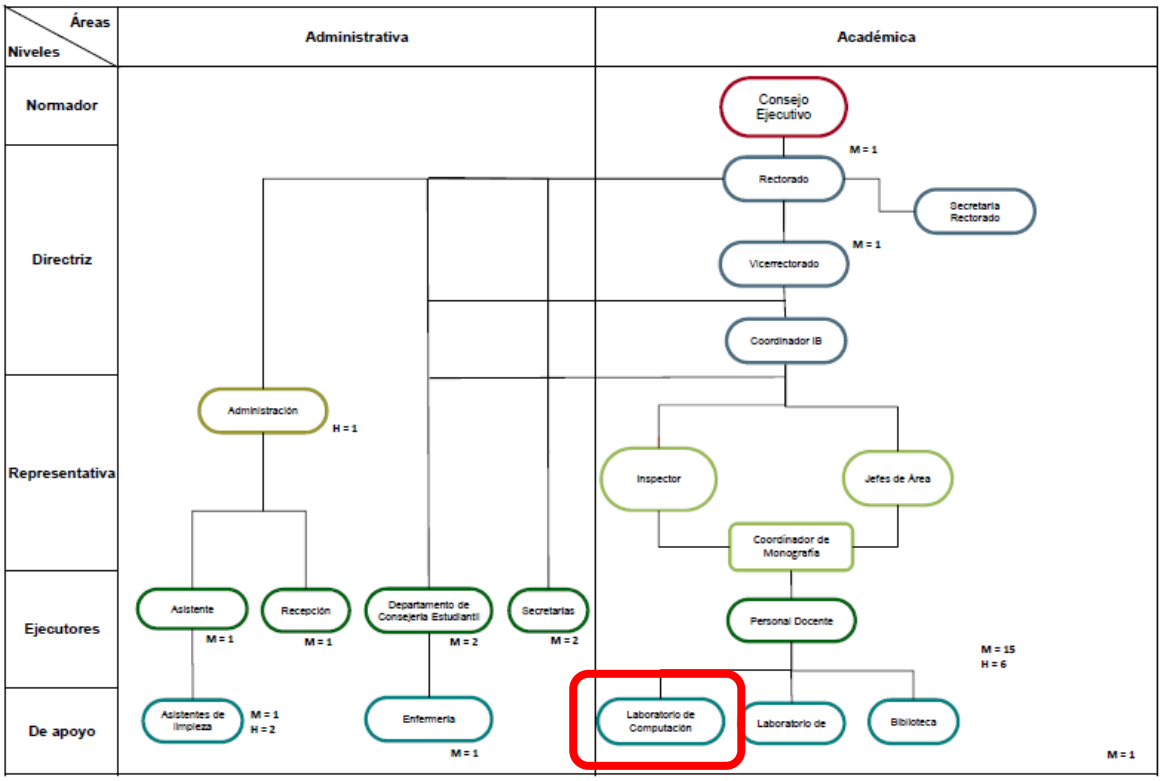


Figura 1. Organigrama de la Unidad Educativa Particular Séneca

Fuente: U.E.P. Séneca http://www.seneca.edu.ec/nuestras-políticas/

Laboratorio de Computación

El Laboratorio de Computación es el área que asumió la responsabilidad de gestionar los recursos de tecnología e información, así como el soporte y administración de la red y servicio de internet. Como se muestra en el organigrama de la institución el laboratorio no es un área de TI, sin embargo, actualmente es el área encargada de administrar los recursos.

Actualmente el responsable del Laboratorio de Computación es el profesor de informática, quién fue designado por parte de la administración.

Infraestructura

La U.E.P. Séneca posee una infraestructura la cual soporta la parte académica y administrativa, tiene el cableado estructurado en las oficinas, así como también la cobertura de internet de forma inalámbrica dividida en dos secciones: primaria y secundaria.

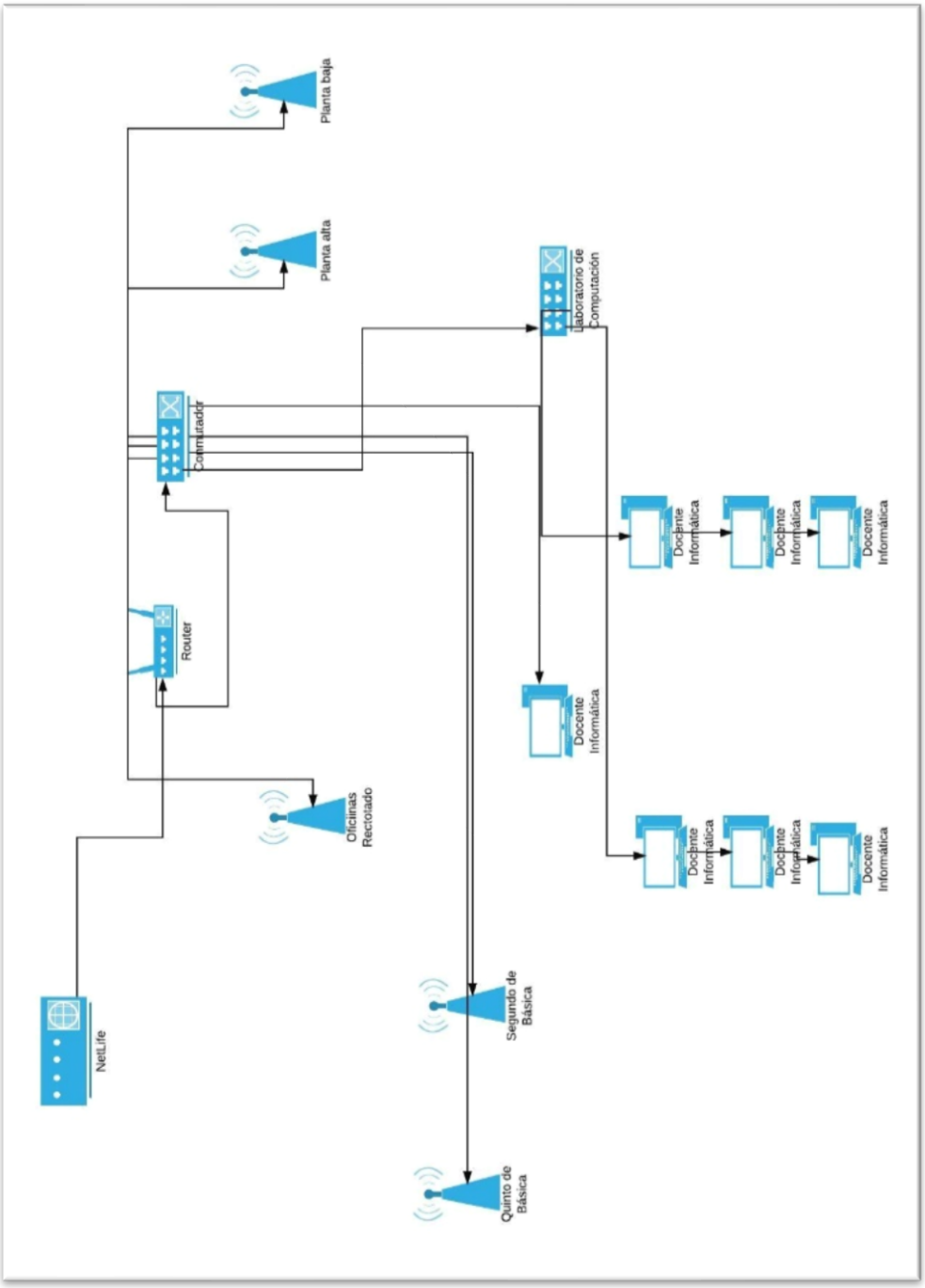


Figura 2. Red de la Unidad Educativa Particular Séneca

Elaborado por el Autor.

1.4. Normas

En la actualidad y durante el año pasado, muchas organizaciones y empresas han tenido que admitir que sus sistemas de información poseen vulnerabilidades en las que permitieron que información privada se filtrara hacia el público. Una de las tendencias de mayor trascendencia fue la del secuestro de *software* a través de programas como: *WannaCry* o *NoyPeyta*, mismas que impedían que las empresas tengan acceso a su información pidiendo a su vez un rescate para devolver el acceso a sus computadoras (Estéfano, 2017).

Hay factores por las cuales las empresas ignoran el hecho de proteger la información siendo una de estas la falta de cultura acerca de los riesgos que puede ocasionar la mala manipulación o gestión de activos de información y/o recursos de tecnología, sin embargo, tratan de proteger a su manera, es decir, sin un procedimiento adecuado lo cual les lleva a hacer grandes inversiones de equipos sofisticados con el fin de proteger sus activos de ataques, intrusión a sistemas, divulgación de información, acceso sin autorización, desastres naturales, etc.

Cuando se habla de amenazas se pueden mencionar que estas se pueden formar de la siguiente manera:

- Amenazas de carácter humano, provocando a las computadoras la infección directa o indirectamente de *malware* (*software* malicioso), acceso sin autorización a equipos, acceso, modificación, eliminación o robo de información, así como la divulgación de la misma, etc.
- Las amenazas de tipo tecnológicas, en la que generalmente no existen controles para acceder a equipos informáticos, inestabilidad en la red por descuido en el cableado, conexiones eléctricas defectuosas o descuidadas, falta de ups, etc.
- Amenazas naturales, ubicación incorrecta de los equipos los cuales pueden estar expuestos al polvo, a la humedad, al agua, incendios, temblores, etc.

Para elegir una norma o metodología, a continuación, se mostrará una tabla comparativa entre ITIL, COBIT e ISO 7000.

Tabla 2. Metodologías de seguridad de información.

ITILv3	COBIT.5	ISO 27000
ITIL es un marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos. ITIL se creó como un modelo que incluye información sobre las metas, entradas y salidas de procesos, actividades generales que pueden incorporar las áreas de TI. Versiones: - ITIL v1. Constituida en diez libros que se refiere a Soporte al Servicio y Entrega del servicio. - ITIL V2. Se redujo a siete los libros reconocido ahora como "estándar de facto" para la administración de Servicios de TI. - ITIL v3. Conformándose en cinco libros enfocándose en el ciclo de vida del servicio (Acevedo, 2016).	Cobit (Control Objectives for Information and related Technology) es una buena práctica para el control de información de TI y los riesgos que se utiliza para implementar el gobierno de TI. Versiones: Su primera versión aparece en el año de 1996, seguida por la segunda en 1998, 2000 (edición on-line en 2003), la cuarta en 2005 y la actualmente 4.1 en mayo del 2007. - COBIT 4.1. Contiene 34 procesos cubriendo 20 objetivos de control detallados en cuatro dominios (Planificación, Adquisición Entrega y Soporte, y Supervisión). - COBIT 5. La cual proporciona una visión empresarial del Gobierno de TI. Principios: - Satisfacer las necesidades de los accionistas. - Considerar la empresa de punta a punta. - Aplicar un único modelo de referencia. - Posibilitar un enfoque holístico. - Separar gobierno de la gestión (Soto, 2016).	Es un conjunto de estándares internacionales sobre la seguridad de información que brinda buenas prácticas para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información, siendo sus bases las ISO 27001 y 27002. La familia de la norma ISO 27000 posee un alcance amplio y es aplicable a distintas empresas en cualquier sector. Beneficios: - Asegurar los activos fijos. - Administrar los riesgos. - Mantener y mejorar la confianza con el cliente. - Demostrar conformidad con mejoras prácticas internacionales. - Evitar pérdidas, daños de imagen o posibles multas regulatorias. (Bustamante, 2014).

Elaborado por el Autor

1.4.1. JUSTIFICACIÓN DE USO DE LA NORMA ISO 27000

Como se muestra en la tabla 2, ITIL que está enfocada en la administración de servicio de TI la cual proporciona metas y actividades generales en el marco de administración de procesos, mientras que COBIT es una buena práctica para el control de información y los riesgos que se utiliza para implementar el gobierno de TI en cambio la ISO 27000 brinda buenas prácticas para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información, siendo sus bases las ISO 27001 y 27002, trabajando en conjunto con el fin de garantizar la seguridad de la información.

Por esta razón el siguiente proyecto utilizará la norma ISO 27000, ya que inicia la elaboración de SGSI creando buenas prácticas de seguridad de la información, brindado apoyo sobre la gestión de riesgos y la recomendación de controles.

La norma ISO 27000 y su familia se muestran a continuación en la siguiente figura.

Figura 3. Familia ISO 27000
Fuente: (ISO 2. , 2015)
Elaborado por el Autor.

Para conseguir el objetivo principal de la norma ISO 27000, ésta se basa en diez ítems importantes que se describen en la siguiente estructura:

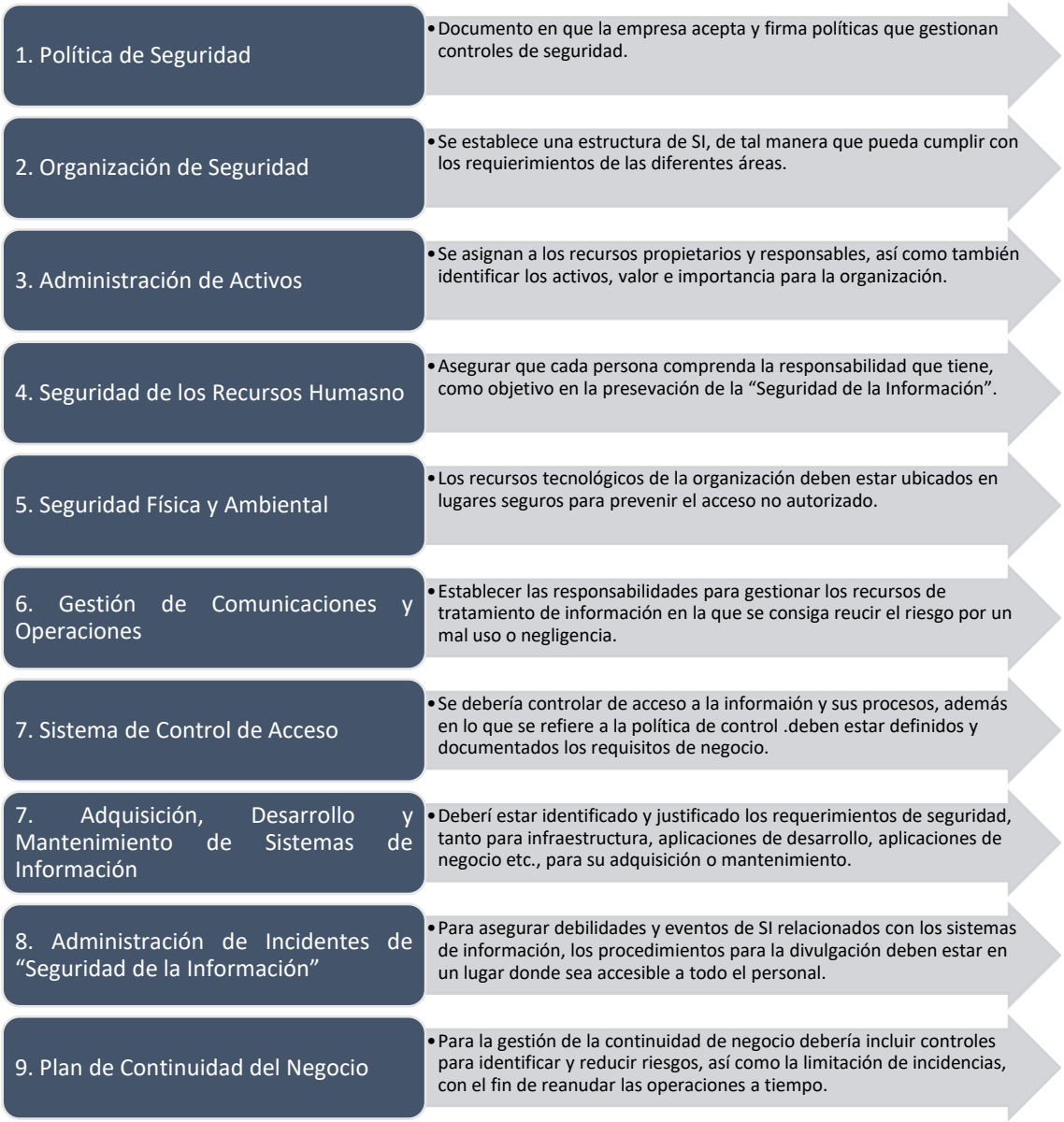


Figura 4. Estructura de la ISO 27000: 2014
Fuente: (Martínez, 2015)

Como se pudo notar anteriormente en la (Figura 3) su estructura muestra ocho normas que posee la ISO/IEC 27000, y para este proyecto se utilizará la ISO 27001, ISO 27005 e ISO 27002, que se describen a continuación:

1.4.2. NORMA ISO/IEC 27001: 2013

Es una norma que proporciona los requisitos para un SGSI, éstas están determinadas de acuerdo con los objetivos y necesidades de cualquier empresa u organización (27001:2013 I. , s.f.).

Atributos de la información

Confidencialidad, integridad y disponibilidad, son los atributos que posee un activo de información, a continuación, se muestra el detalle de cada una.

Tabla 1. Atributos de la información.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
La confidencialidad de la información es muy importante y ésta debe estar accesible para quienes estén autorizadas.	La información debe mantenerse inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización.	Trata de que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos.

Fuente: (Pmg-ssi, 2018)

Elaborado por el Autor.

Para gestionar la Seguridad de la Información es necesario definir los objetivos de acuerdo a las necesidades, así como también políticas, guías o documentos lo que permitirá fomentar buenas prácticas de seguridad (PCWorld, 2014).

Un Sistema de Gestión de Seguridad de la Información es parte de la familia IS0 27000 siendo uno de los pilares fundamentales para su elaboración. La norma 27001 garantiza la confidencialidad, integridad y disponibilidad de la seguridad de la información en los activos (PMG S. , 2015).

La siguiente (Tabla 3) muestra la estructura de un SGSI con los siguientes componentes:

Tabla 3. Estructura de la norma ISO/IEC 27001: 2013

SECCIÓN	ÍTEM	OBJETIVO
S. 1	Alcance	Permite de designación de un área u proceso para la elaboración de un SGSI.
S. 2	Referencias normativas	Proporcionan según las normas la terminología y definiciones para su elaboración.
S. 3	Términos y definiciones	Referente a la ISO/IEC 27000.
S. 4	Contexto de la organización	Situación que define la empresa u organización para definir un “SGSI”.
S. 5	Liderazgo	Define las responsabilidades, roles, apoyo y seguimiento sobre la elaboración de un SGSI.
S. 6	Planificación	Según los objetivos aquí se realiza la planificación de actividades por realizar según las etapas de la norma.
S. 7	Apoyo	Total, apoyo a la gestión de un SGSI disponiendo recursos, comunicando y documentado las etapas según se finalice.
S. 8	Operación	Tratamiento de riesgos e implementación de controles que son necesarios para el cumplimiento.
S. 9	Evaluación del desempeño.	Analizar, medir, monitorear, evaluar y realizar una auditoría que sea interna por parte de las autoridades.
S. 10	Mejora	Correcciones del “SGSI”, sus medidas correctivas apropiadas y la mejora continua del negocio.
	Anexo A	Proporciona una lista en la que consta de 114 controles distribuidos en 14 secciones (secciones A.5 a A.18).

Fuente: (Advisera, s.f.).

El ciclo continúo llamado Ciclo de Deming PHVA, es muy importante para el desarrollo de un Sistema de Gestión de Seguridad de la Información ya que son las fases para su elaboración la cual se detalla a continuación: (PMG, SGSI, 2015).

Tabla 4. Ciclo continuo de Deming (PHVA)

FASE	OBJETIVO	DESCRIPCIÓN
1. Planificar	Establece un SGSI	Establecer políticas, objetivos, procesos y procedimientos, siendo este pertinente a la gestión de riesgos para mejorar la Seguridad de la Información obteniendo resultados.
2. Implementar	Implementa y opera un SGSI	Implementa y opera la política, controles, procesos y procedimientos de un SGSI.
3. Medir	Monitorea y revisa un SGSI	Evalúa y mide el rendimiento del proceso, objetivos y práctica, informando los resultados para su revisión.
4. Mejorar	Mantiene y mejora el SGSI	Tomar acciones preventivas y correctivas, basados estos en los resultados de las auditorías internas.

Fuente: ISO 27001: Ciclo de Deming
Elaborado por el Autor.

Para el proyecto de un SGSI propuesto para la unidad educativa particular Séneca se realizará sólo en la fase (planear).

Una característica principal de la norma ISO 27001 es que es certificable y por esta razón las empresas que realizan la actividad de auditoria requieren documentos que se les haya entregado a las autoridades de manera obligatoria, los cuales se muestran en la siguiente (véase tabla 5) a continuación:

Tabla 5. Documentos obligatorios para la norma ISO/IEC 27001: 2013

DOCUMENTO	DESCRIPCIÓN GENERAL	CAPÍTULO (ISO/IEC 27001: 2013)
Alcance de un "SGSI".	Es la limitación que tendrá el "SGSI".	4.3
Políticas y Objetivos de "Seguridad de la Información".	Documento con nivel alto que detalla los objetivos del "SGSI" relacionadas con la SI.	5.2, 6.2
Metodología de Evaluación y Tratamiento de Riesgos.	Directrices que permite hacer un análisis, evaluación y tratamiento de riesgos.	6.1.2
Declaración de Aplicabilidad	Por medio de esta fase se sugieren controles basándose en el Anexo A.	6.1.3d
Plan de Tratamiento del Riesgo.	Plan de acción sobre cómo implementar controles que fueron definidos en (6.1.3).	6.1.3e, 6.2
Informe sobre la evaluación y tratamiento de riesgo	Aunque no se específica una estructura para el plan, éste debe ser formulado a partir de las salidas de 6.1.3a, c.	8.2, 8.3
Definir funciones y responsabilidades de seguridad.	Se determina la creación de funciones y responsabilidades para gestionar la "Seguridad de la Información".	A.7.1.2, A.13.2.4
Inventario de Activos	Documento en la que consta los activos de información que pertenecen a la U.E.P. Séneca.	A.8.1.1
Uso aplicable de los activos	Se define el tratamiento que se brindará a los activos que no han sido incluidos.	A.8.1.3
Política de Control de Acceso	Se refiere a las políticas para el control tanto físico como lógico.	A.9.1.1
Procedimientos operativos para la gestión de TI	Se genera un documento que describe (gestión de cambios, copias de seguridad, seguridad en la red, etc.)	A.12.1.1
Principios de ingeniería para sistema seguro	son técnicas incorporadas de seguridad se la realiza específicamente en las capas de	A.14.2.5

	arquitectura: datos, aplicaciones, negocio y tecnología.	
Política de seguridad para proveedores	Política específicamente para contratistas.	A.15.1.1
Procedimiento para gestión de incidentes	Se detalla cómo se clasifica maneja e informa eventos o incidentes de seguridad.	A.16.1.5
Procedimiento de la continuidad del negocio	Son planes de continuidad detalladamente acerca del negocio, también posee respuesta ante cualquier incidente que pueda afectar, así como también la recuperación de negocio.	A.17.1.2
Requisitos legales, normativos y contractuales	Normativa que posee la institución en la que debe cumplir.	A.18.1.1

Fuente: (EPPS, 2014)
Elaborado por el Autor.

1.4.3. NORMA ISO/IEC 27002: 2013

Esta norma sugiere y recomienda una guía para establecer controles los cuales se muestran a continuación (ISO, 2013).

Tabla 6. Dominios y Controles ISO/IEC 27002: 2013

DOMINIOS	CONTROLES
5. Políticas de la Seguridad de la Información.	2
6. Organización de la Información de la Seguridad.	7
7. Seguridad de los recursos humanos.	6
8. Gestión de activos.	10
9. Control de acceso.	14
10. Criptografía.	2
11. Seguridad Física y del Entorno.	15
12. Seguridad de las operaciones.	14
13. Seguridad de las Comunicaciones.	7
14. Adquisición, Desarrollo y Mantenimiento de Sistemas.	13
15. Relación con los proveedores.	5
16. Gestión de incidentes de la Seguridad de la Información.	7
17. Aspectos de Seguridad de la Información de la Gestión de la Continuidad de negocio.	4
18. Cumplimiento.	8

Fuente: (27002, s.f.)
Elaborado por el Autor.

1.4.4. METODOLOGÍA DE ANÁLISIS Y EVALUACIÓN DE RIESGOS

Para el análisis y evaluación de riesgos, se observa la siguiente tabla comparativa donde se analiza algunas opciones de evaluación como Magerit, ISO 31000 e ISO 27005. Esta comparación permitirá elegir la metodología o norma que mejor se adapte a este proyecto.

Tabla 7. Tabla comparativa para el Análisis y Evaluación de Riesgos.

MAGERIT	ISO 31000	ISO 27005
Es una metodología de Análisis y Gestión de Riesgos de los sistemas de información. MAGERIT implementa un marco de trabajo basado en el proceso de Gestión de Riesgos para que las organizaciones puedan tomar decisiones tomando en cuenta los riesgos que posee el uso de las tecnologías de información. Recomienda las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados. Objetivos: - Concientizar de la existencia de los riesgos y la necesidad de gestionarlos. - Obtener un método persistente para el análisis de riesgos obtenidos por el uso de las TIC. - Ayudar a mantener el control de riesgo a través del tratamiento oportuno. - (ENS, 2012).	Es una norma para la Gestión de Riesgos proporcionando principios exhaustivos, se adpata a empresas públicas o privadas ya que incluye una planeación, operaciones y procesos de comunicación, recomienda mejores técnicas de gestión para garantizar la seguridad de la información ayudando a fomentar el desempeño de seguridad y salud. Ventajas: - Mejorar de forma proactiva la eficacia operativa. - Genera confianza entre partes interesadas. - Aplica controles de sistemas de gestión para analizar los riesgos. - Responde a cambios de forma eficaz y protege la empresa mientras crece (BSI, 2018).	No es una metodología, sino una norma en la que contiene diferentes recomendaciones y directrices generales para la gestión de riesgo, su relación con la ISO 27001 la hace compatible como soporte para la aplicación de un SGSI basado en el enfoque de gestión de riesgo. Esta norma es aplicable para todo tipo de organización y está dependerá principalemente del alcance de un SGSI, así mismos los usuarios podrán elegir el método que mejor se adpate, por ejemplo para la evaluación de riesgos de alto nivel y análisis en profundidad sobre las áreas de mayor riesgo. Ventajas: - Incluye seis Anexos (A-F) de carácter informativo y no normativo que permite desde la identificación de activos, amenazas, vulnerabilidades e impactos, hasta el análisis de riesgo. - Apoyar la tarea del análisis de gestión de riesgos en el marco de un SGSI (Sampedro, 2009).

Elaborado por el Autor

1.4.5. JUSTIFICACIÓN PARA EL USO DE LA NORMA ISO 27005

La tabla 7 hace referencia a otras metodologías o normas que pueden ser utilizadas para la gestión de riesgos; MAGERIT propone un marco de trabajo basado en el proceso de Gestión de Riesgos para que las organizaciones puedan tomar decisiones tomando en cuenta los riesgos que posee el uso de las tecnologías de información, es decir, se trabaja dentro de una gestión de riesgos, mientras que la ISO 31000 recomienda mejores técnicas de gestión para garantizar la seguridad de la información ayudando a fomentar el desempeño de seguridad y salud, y por último la ISO 27005 que no es una metodología, sino una norma en la que contiene diferentes recomendaciones y directrices generales para la gestión de riesgo, su relación con la ISO 27001 la hace compatible como soporte para la aplicación de un SGSI basado en el enfoque de gestión de riesgo.

Las dos primeras se basan en la gestión propia de los riesgos partiendo ya desde un análisis y evaluación anteriormente definida y gestionada, en cambio, la ISO 27005 se alinea con la implementación de un SGSI, lo cual es el objetivo de este proyecto.

1.4.6. NORMA ISO/IEC 27005: 2011

La norma 27005 brinda directrices con la finalidad de apoyar a la realización de un análisis y evaluación de riesgo como uno de los requisitos que recomienda la norma 27001. La desventaja de esta norma es que no ofrece una metodología, sin embargo, es considerada para la elaboración de un SGSI (27005, ISO, s.f.).

La estructura está definida según se muestra (véase fig. 5) la cual apoya a los conceptos definidos en la ISO 27001 que mediante su enfoque está diseñada para una aplicación satisfactoria del sistema de información.

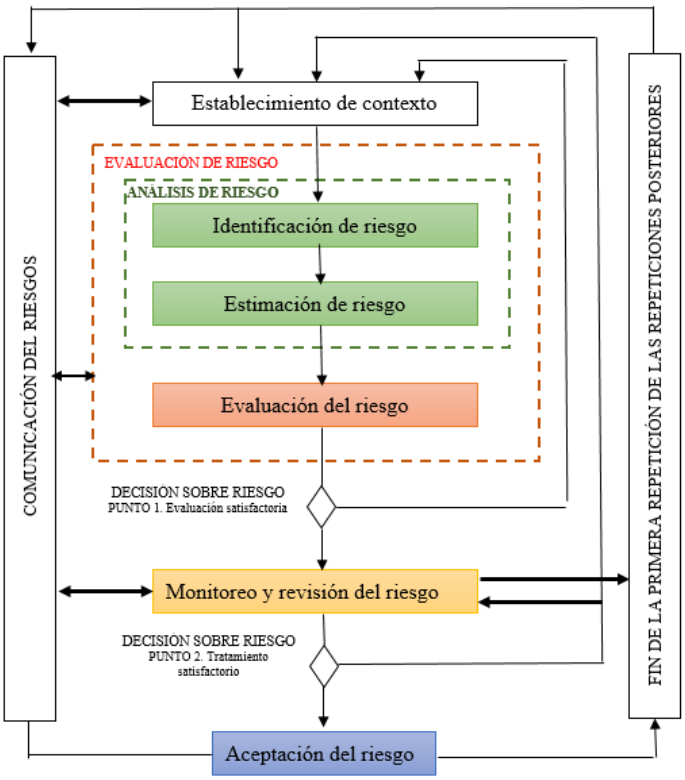


Figura 5. Estructura de la ISO 27005: 2011
Fuente: IEC/ITS 27005, 2008, pág. 5

1.4.6.1. Inventario de activos

Los activos son la parte fundamental para diseñar un SGSI, estos constan de:

- Identificación del activo (código)
- Tipo de activo
- Descripción
- Ubicación
- Propietario
- Responsable

En la siguiente figura se indica el modelo a utilizar para el inventario de activos de la unidad educativa particular Séneca.

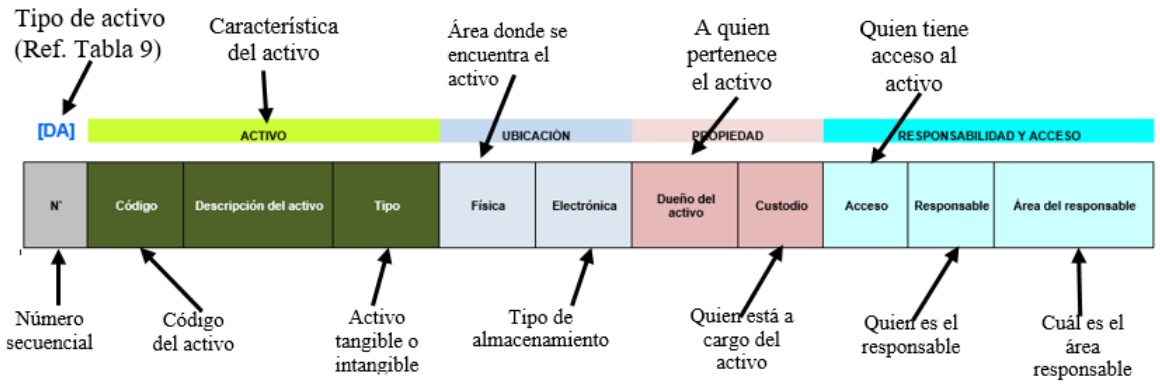


Figura 6. Instructivo para la clasificación de activos.
Elaborado por el Autor.

Descripción de ítems:

a) DA Datos / Información
   a. Número secuencia; 1, 2, 3, 4……n.
b) Activo
   a. Código, código generado para identificar el activo, ejemplo; DA_FAC que corresponde a Datos de facturación.
   b. Descripción, los datos corresponden a las facturas que se generan.
   c. Tipo, si es tangible (se puede ver y tocar) o intangible (no se puede tocar).
c) Área dónde se encuentra el archivo:
   a. Física, lugar dónde está ubicado el activo (equipo o recurso tecnológico).
   b. Electrónico, equipo o dispositivo donde se aloja la información.
d) Propiedad:
   a. Dueño del activo, a quién pertenece el activo.
   b. Custodio, quien está a cargo del activo.
e) Responsabilidad y acceso:
   a. Acceso, quien es el usuario que puede acceder al activo.
   b. Responsable, el usuario que se hará responsable del activo.
   c. Área del responsable, área en la que se encuentra el activo.

En la siguiente figura se muestra un ejemplo de tipo de activo con su detalle.

DATOS/INFORMACIÓN

[D]	ACTIVO			UBICACIÓN		PROPIEDAD		RESPONSABILIAD Y ACCESO		
N`	Código	Descripción del activo	Tipo	Física	Electrónica	Dueño del activo	Custodio	Acceso	Responsable	Área del responsable
1	D_BCK	Copias de Seguridad del Sistema Financiero.	INTANGIBLE	ADM	Equipo de computo	ADM	ADM	ADM-CON	ADM	Administración
2	D_FAC	Facturación	INTANGIBLE	ADM	Equipo de computo	RR-HH-ADM	ADM	ADM-CON	ADM	RR-HH

Figura 7. Ejemplo de activo y su detalle.
Elaborado por el Autor

Ver formato en el Anexo E.

1.4.6.2. Identificación de activos

Para hacer la valoración de activos, estos tienen que ser identificados de acuerdo al tipo de activo que posee la institución, en la siguiente figura se muestra el detalle.

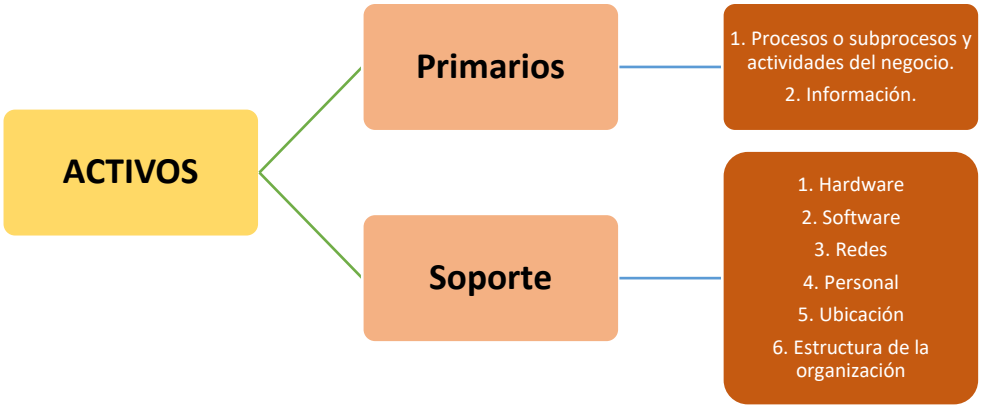


Figura 8. Tipos de Activos
Fuente: (ISO/IEC 2. , 2011)

1.4.6.3. Valoración del activo

La norma ISO 27005 en el Anexo B2; dice que después de identificar los activos hay que estimar un valor que posee para la institución educativa, se considera qué activo puede resultar con daño en cuanto a la disponibilidad, integridad y confidencialidad.

Según la norma se puede utilizar la escala cuantitativa (valor económico) o cualitativa (bajo, medio, alto) o también un determinado rango numérico (0-10).

Los criterios que se toman en cuenta parta la evaluación de posibles consecuencias como la pérdida de la confidencialidad, integridad y disponibilidad. Entre otras son:

- Incumplimiento de la legislación y/o reglamentación
- Pérdidas económicas
- Interrupción de servicios
- Alteración de la operación interna
- Efecto negativo en la reputación

1.4.6.4. Identificación de amenazas

Esta etapa comprende según la ISO 27005 la identificación de amenazas (Anexo C) y las posibles vulnerabilidades (Anexo D) que pueden tener los activos.

Tabla 8. Tipos de amenazas.

LITERAL	SIGNIFICADO	DESCRIPCIÓN
D	Deliberadas	Se utiliza para todas las acciones deliberadas que tienen como objetivo los activos de la información.
A	Accidentales	Son acciones humanas que pueden dañar accidentalmente los activos de información
E	Ambientales	Son incidentes que no se basa en las acciones humanas.

(NTC 27005, pág. 69)

Elaborado por el Autor

1.4.6.5. Valoración e Impacto

Para valorar el impacto se debe conocer que un incidente relacionado con la seguridad de la información puede tener un impacto en uno o varios activos, esto está vinculado con el grado de éxito de dicho incidente, por lo tanto el impacto se considera como un efecto inmediato o futuro operacional, misma que incluyen gastos financieros y de mercado (NTC, 2014).

El impacto inmediato puede ser directo o indirecto:

Tabla 9. Valoración de impacto.

DIRECTO	INDIRECTO
El valor financiero del reemplazo del activo perdido (o parte de este activo).	Costos de la oportunidad (nuevos recursos financieros necesarios para reemplazar o reparar un activo se podrían haber utilizado en otra parte).
El costo de adquisición, configuración e instalación del activo nuevo o de su copia de soporte.	El costo de las operaciones interrumpidas.
El costo de las operaciones suspendidas debido al incidente hasta que se restaure el servicio prestado por el (los) activo (s).	El potencial de la mala utilización de la información obtenida a través de una brecha en la seguridad.
El impacto tiene como resultado una brecha en la seguridad de la información.	Incumplimiento de las obligaciones estatutarias o reglamentarias.

(NTC 27005, 2008, pág. 72)

1.4.6.6. Estimación de riesgo

.

Villavicencio Andrés, en su proyecto Diseño y propuesta técnica-económica de la red con voz IP y datos apoyados en la norma ISO/IEC 27001: 2013, pág. 45 dice que para la tasación de la probabilidad de que la amenaza explore la vulnerabilidad, la escala elegida es la cuantitativa con valores del 1 al 3 correspondiente a bajo, medio y alto respectivamente

Así también Sosa Johanna en su trabajo Estándares para la administración de riesgos menciona que una de las ventajas de utilizar la escala cuantitativa es que proporciona medidas de impacto que pueden ser utilizadas en análisis costo-beneficio.

CAPÍTULO II

MARCO METODOLÓGICO

1.1.Metodología de desarrollo

Se utilizará como metodología de investigación que, a través de la definición y formulación del problema, ayudando a enfocarse en el proceso sobre el cual se realizará la mencionada investigación, relacionándose principalmente con la Seguridad de la Información de la Unidad Educativa Particular Séneca.

Tipos de Investigación que utilizar:

1.1.1. **Investigación Exploratoria,** permite acercarse a lo que se pretende investigar para conocer, recoger e identificar toda aquella información antecedente que permita a través de números y cuantificaciones documentar experiencias que no han sido tomadas en cuenta. Como instrumentos de investigación se utilizará la entrevista, la observación y cuestionarios, mismos que pretende levantar datos que permitan dar un primer diagnóstico sobre el tratamiento de la información.

1.1.2. **Investigación Descriptiva:** Permite la delimitación de los hechos que conforman el problema de investigación a través de la descripción de actividades por realizar (Noticias, 2017).

1.1.3. **Técnicas de recolección de información:** la recolección de datos es una de las etapas más sensibles de la investigación en la que depende de acuerdo al tipo de investigación los resultados, en este proyecto se utilizará el cuestionario.

El cuestionario es una de las técnicas más universales que se utiliza, para este caso se lo hará de forma individual a distintas personas y áreas de la institución.

1.2.Fases para el diseño de un SGSI

Para el diseño de un SGSI en la Unidad Educativa Particular Séneca se llevará a cabo una serie de fases que permitirá llegar a cumplir los objetivos propuestos en este proyecto, en la siguiente (Figura 8) se muestra cada fase a realizar.

Figura 8. Fases para el diseño de un SGSI.

Elaborado por el Autor

Cada una de las fases detalla las actividades y procedimientos que se deberán realizar, siendo estas:

1.2.1. Fase 1: Situación Actual

- Soporte de la Dirección
- Alcance
- El análisis diferencial

1.2.2. Fase 2: Gestión Documental

- Políticas de Seguridad de la Información
- Revisión por parte de las autoridades
- Roles y responsabilidades

1.2.3. Fase 3: Metodología de Análisis y Evaluación de Riesgos

- Inventario de activos
- Valoración de activos
- Identificación de amenazas por activos
- Evaluación de activos por amenazas y vulnerabilidades
- Identificación y criterios de impacto para valoración de riesgos
- Evaluación de riesgos (amenazas y vulnerabilidades)
- Evaluación de riesgos (amenaza y vulnerabilidad con impacto)
- Evaluación de riesgos con probabilidad e impacto
- Calculo de riesgos

1.2.4. Fase 4: Declaración de Aplicabilidad

- Declaración de aplicabilidad

1.2.5. Fase 5: Tratamiento de Riesgo

- Tratamiento de Riesgo

1.3.Codificación de documentos

Con la finalidad de identificar los activos, sus propietarios y responsabilidades, así como también diferenciar entre instructivos, formatos, registros y documentos para los cuales se generarán códigos de acuerdo con las actividades realizadas.

1.3.1. Introducción

La siguiente guía describe la manera cómo se asignarán los diferentes códigos de acuerdo con los activos, áreas, responsables y documentos con el propósito de identificar fácilmente cada documento y su relación con la seguridad de la información.

1.3.2. Procedimiento

Los procedimientos que se emitan en las políticas, instructivos, formatos o registros utilizarán un identificador que está conformada por una numeración alfanumérica para cada uno, y su estructura será la siguiente:

1.3.3. Código de documentos

En la siguiente tabla se muestra el detalle de cómo se codificará los documentos.

Tabla 10. Código de documentos.

CÓDIGO	FUNCIÓN	DESCRIPCIÓN
I	Instructivo	Escrito en el que se define los pasos para realizar una actividad determinada.
F	Formato	Escrito en el que se registra resultados de una actividad.
P	Políticas	Escrito en el que se define los lineamientos que se debe cumplir en la U.E.P. Séneca.
D	Documento	Escrito que describe un compromiso.
R	Registro	Escrito que registren actividades acerca de la manipulación de activos.

Elaborado por el Autor

1.3.4. Código de áreas

Detalle del código que identifica el área o encargado utilizando los tres caracteres siguientes.

Tabla 11. Código de áreas.

CÓDIGO	ÁREAS
ADM	Administración
SCR	Secretaria de Rectorado
DEC	Departamento de Consejería Estudiantil
CBI	Coordinador de Bachillerato Internacional
PRV	Proveedor
RRH	Recursos Humanos
SCA	Secretaria Académica
LBC	LABORATORIO DE COMPUTACIÓN
REC	Rectorado
VIC	Vicerrectorado
CON	Contabilidad
OFI	Oficinas
AIN	Área de internet
AUL	Aulas
DOC	Docentes
INS	Inspección
COP	Comité Paritario
RLC	Responsable de laboratorio de computación
EOF	Encargado de oficina
NAC	Notas Académicas
MAT	Matrículas

Elaborado por el Autor.

1.3.5. Códigos de la clasificación de activos

A continuación, se mostrará los códigos propuestos para la identificación de activos.

Tabla 12. Tipos de activos de información

INICIAL	GRUPO	DESCRIPCIÓN
DA	Datos /Información	Activo principal de la institución
HW	*Hardware*	Equipo físico que alojan datos e información.
SW	*Software*	Sistemas operativos / ofimática.
COM	Comunicaciones	Equipos que permiten el intercambio de datos e información entre activos.
INS	Instalaciones	Lugares físicos, ubicación de los equipos informáticos.
PER	Personal	Quienes gestionan todos los activos.
SSC	"Sistemas de seguridad y control de acceso"	Equipos que proporcionan seguridad en las instalaciones.

Elaborado por el Autor.

Códigos de los activos de información clasificados de acuerdo a la tabla 13, que pertenecen a la unidad educativa particular Séneca.

Tabla 13. Código de los activos (Datos y/o Información).

CÓDIGO	DESCRIPCIÓN
DA_BCK	Copias de Seguridad del Sistema Financiero.
DA_FAC	Facturación
DA_RDP	Roles de pago
DA_CNT	Contratos
DA_HLB	Historial Laboral
DA_NAC	Notas académicas
DA_DEC	Admisión DECE
DA_MAT	Matriculación
DA_DRT	Documentos de registros tecnológicos

Elaborado por el Autor

Tabla 14. Código de los activos (Software).

CÓDIGO	DESCRIPCIÓN
SW_SOP	Sistemas Operativos
SW_OFI	Ofimática
SW_CONT	Contabilidad
SW_ANT	Software Antivirus
SW_STD	Software Estándar

Elaborado por el Autor

Tabla 15. Código de los activos (Hardware).

CÓDIGO	DESCRIPCIÓN
HW_HOST	Servidor
HW_CPP	Computadoras portátiles de uso institucional.
HW_CPE	Computadoras de escritorio de uso institucional.
HW_PRT	Impresoras
HW_ROU1	Router principal de la Institución
HW_ROU2	Router secundario de Administración
HW_MOD1	Modem principal de la institución
HW_MOD2	Modem secundario de Administración
HW_SWH	Switch
HW_UPS	Sistema de Alimentación Ininterrumpida
HW_HUB	Hub o concentrador
HW_ACP	Puntos de Acceso Inalámbricos
HW_PRO	Proyectores
HW_DMP	Dispositivos móviles personales

Elaborado por el Autor

Tabla 16. Código de los activos (Comunicaciones).

CÓDIGO	DESCRIPCIÓN
COM_INT	Internet
COM_LAN	Red de Área Local
COM_WIF	Conectividad Inalámbrica
COM_WEB	Página web

Elaborado por el Autor

Tabla 17. Código de los activos (Instalaciones).

CÓDIGO	DESCRIPCIÓN
INS_LBC	Laboratorio de Computación
INS_OFR	Oficina Rectorado
INS_OFV	Oficina Vice rectorado
INS_OFC	Oficina Coordinador BI
INS_OFA	Oficinas Administrativas
INS_OFR	Oficinas Recepción
INS_DEC	Oficinas DECE
INS_OFI	Oficina Inspección
INS_SEC	Aulas Secundaria
INS_PRI	Aulas Primaria

Elaborado por el Autor

Tabla 18. Código de los activos (Personal).

CÓDIGO	DESCRIPCIÓN
PER_ADM	Administrador de la Institución
PER_DOC	Personal Docente
PER_CON	Personal de conserjería
PER_ATI	Administrador de TI
PER_EST	Estudiantes

Elaborado por el Autor

Tabla 19. Código de los activos (Sistema de Control y Seguridad).

CÓDIGO	DESCRIPCIÓN
SSC_SEN	Sensores de movimiento
SSC_ALA	Alarma
SSC_CAM	Cámaras de seguridad
SSC_SBI	Sistema Biométrico
SSC_EXT	Extintores

Elaborado por el Autor

1.3.6. Códigos para documentos de apoyo

Documentos de apoyo para la Unidad Educativa Particular Séneca y su gestión de activos y recursos.

Tabla 20. Códigos de las políticas de información.

CÓDIGO	DESCRIPCIÓN
PSI	Políticas de seguridad de la información
PDS	Propuesta de Sistema de Gestión de la Información
ALC	Alcance y limitación
MAE	Metodología de Análisis y Evaluación de Riesgos
CAI	Clasificación de Activos de Información
TRI	Tratamiento de Riesgo
DAP	Declaración de Aplicabilidad
DAC	Documento de acuerdo de confidencialidad
IIA	Instructivo para inventario de activos
FSE	Formato para solicitar salida de equipos fuera de la Institución
RRE	Reporte de solicitud de revisión de equipos informáticos.
FAW	Formato de solicitud de acceso a sitios web
FRT	Formato de utilización de recursos tecnológicos.
ICP	Instructivo para revisión de cumplimiento de “Políticas de seguridad”.

Elaborado por el Autor.

1.3.7. Ejemplos

En el siguiente ejemplo se muestra cómo se codifica los documentos, registros, instructivos, etc.

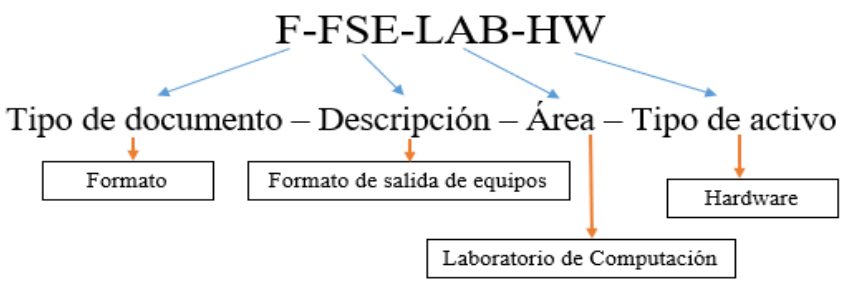


Figura 9. Ejemplo de codificación de documentos.
Elaborado por el Autor.

Ejemplo de codificación de Políticas de Seguridad de la Información.

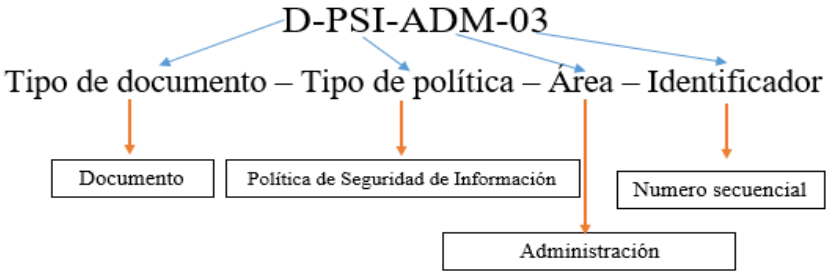


Figura 10. Codificación de Políticas de "Seguridad de la Información".
Elaborado por el Autor.

Como aporte para la institución se crearon documentos (formatos) de apoyo para una mejor gestión de recursos tecnológicos y de información, estos se encuentran en el Anexo E.

1.4.Cuestionarios realizados a la institución

Con el propósito de iniciar con algunas referencias sobre la seguridad existente a nivel de tecnología, a continuación, se presentan cuatro cuestionarios que se realizó a diferentes personas miembros de la institución.

1.4.1. Cuestionario 1. Seguridad de la Información a nivel general.

Resultados

De acuerdo a las preguntas sobre la seguridad de la información a nivel general la figura 11 muestra que solamente el 17% cumple o conoce el tema, mientras que el 83% desconocen o no hay cumplimiento (Anexo 1).

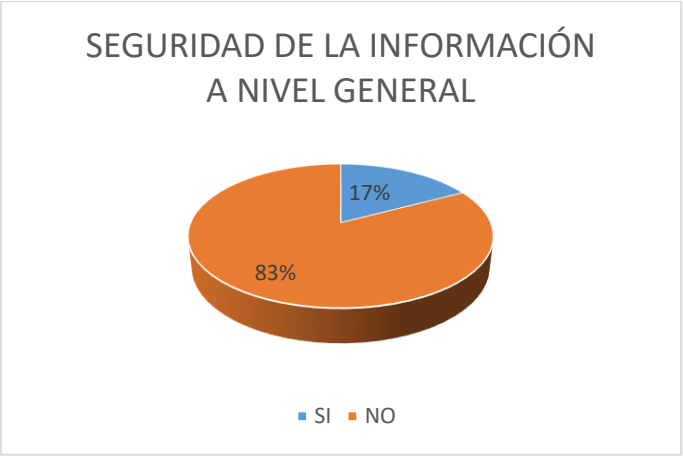


Figura 11. Representación gráfica del Cuestionario 1.
Elaborado por el Autor

1.4.2. Cuestionario 2. Red y mantenimiento

Resultados

En la figura 12 se puede muestra que el 21% tiene algún tipo de información relacionado con la función de la red, equipos y mantenimiento, el 36% no sabe sobre los temas y el 43% desconoce del tema tratado (Anexo 2).

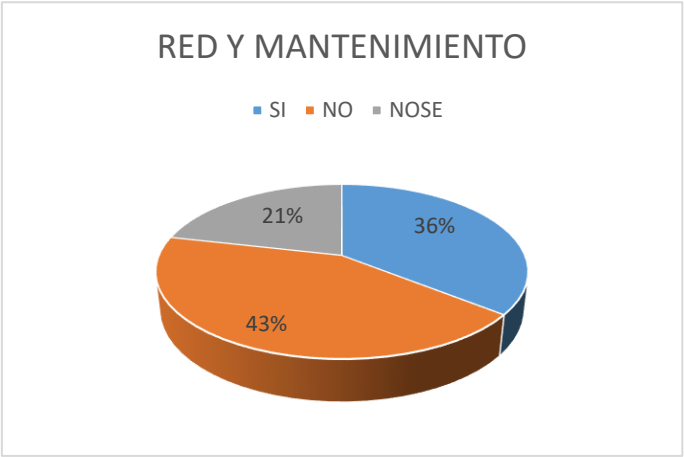


Figura 12. Representación gráfica del Cuestionario 2.
Elaborado por el Autor

1.4.3. Cuestionario 3. Seguridad Física

Resultados

En la siguiente figura 13 se puede notar que el 11% desconoce del tema en cuanto a la seguridad física, el 33% no se aplica alguna seguridad física, y el 56% si sabe y aplica medidas relacionado a la seguridad física (Anexo 3).

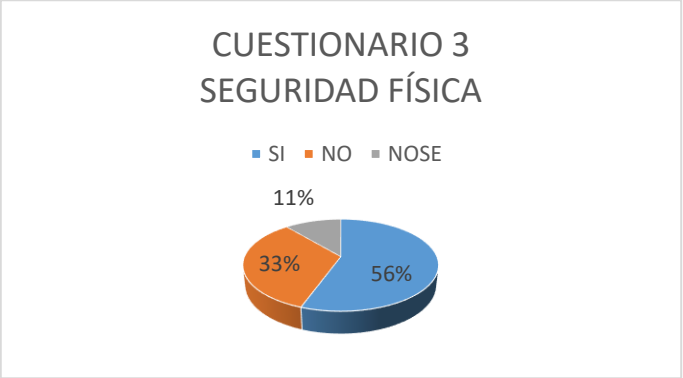


Figura 13. Representación gráfica del Cuestionario 3.
Elaborado por el Autor

1.4.4. Cuestionario 4. Gestión de TI.

Resultados

En la figura 14 se puede notar que el 5% desconoce del tema en cuanto a conocimiento de TI, el 40% no existe planes o guías sobre la Gestión de TI, y el 55% si sabe y se administra algún tipo de control relacionado a TI.

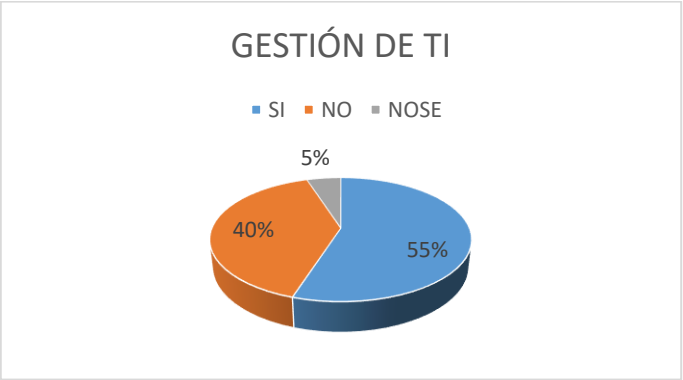


Figura 14. Representación gráfica del Cuestionario 4.
Elaborado por el Autor

CAPÍTULO III

PROPUESTA

3.1. Fase 1: Situación Actual

Para la Unidad Educativa Particular Séneca es un cambio de paradigma el conocer sobre las amenazas y riesgos que tienen sus activos. En la actualidad es claro que ahora no solamente se escucha en las noticias o a través de redes sociales varios tipos de hackeos a nivel mundial sin excepción alguna del tamaño o giro de negocio que tenga una empresa u organización, ahora hay que preocuparse de la computadora que está en las aulas, oficinas, hogares, etc., es ahí por medio de la manipulación inconsciente o a propósito del ser humano se puede dañar y/o comprometer la información.

La institución al estar ligada a la educación no quiere decir que no posea información importante, el intercambio o almacenamiento de esta en las computadoras hace que sea accesible a cualquier persona creando amenazas por mala manipulación del equipo provocadas con o sin intención.

La información que se maneja en la institución requiere que sea protegida ante cualquier evento de amenaza sea humano o por naturaleza, pues puede comprometer la confidencialidad, integridad y disponibilidad de la información, así como la inestabilidad de sus procesos.

Por estas razones es que nace la idea de proponer un SGSI para la Unidad Educativa Particular Séneca basado en la norma ISO/IEC 27000 y su familia.

3.1.1. Soporte de la Dirección

UNIDAD EDUCATIVA PARTICULAR SÉNECA

PROPUESTA DE UN DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN BASE A LA ISO/IEC 27000.

Código del documento	**D-PDS-ADM-01**
Versión	1.0
Fecha de versión	2018-05-04
Creador por	Marco V. Bonilla Ortiz
Aprobado por	Dra. Paulina Jaramillo (Administradora)
Nivel de confidencialidad	Alto

Historial de cambio

Fecha:	**Versión:**	**Creado por:**	**Descripción del cambio**
2018-05-04	1.0	Marco Bonilla	Versión inicial

Para dar inicio con esta fase de elaboración de un SGSI primeramente se coordinará una reunión con la administradora de la Unidad Educativa Particular Séneca para plantear el proyecto que se pretende investigar, definiendo los objetivos y beneficios que obtendrá con el diseño de un SGSI y así obtener la aprobación y seguimiento correspondiente durante la elaboración del proyecto.

Propósito

La siguiente propuesta tiene a fin hacer conocer acerca de los beneficios y ventajas que tiene implementar un SGSI en la Unidad Educativa Particular Séneca, sin embargo, en este proyecto se realizará sólo el diseño lo cual permitirá que un futuro se llegue a concretar este proyecto. Como se planteó anteriormente en las fases que tendrá la elaboración del SGSI, a continuación, se iniciará con el desarrollo de las mismas.

Nota: Proceso que genera el documento Alcance del Sistema de Gestión de "Aprobación" que requiere la ISO/IEC 27001.

Estructura y duración del proyecto

Tabla 21. Actividades de Planeación

N°	ACTIVIDAD	FECHA DE INICIO	FECHA FINAL
1	Inventario de Activos	16-abril-18	30-abril-18
2	Metodología de Análisis y Evaluación de Riesgos	7-mayo-18	18-mayo-18
3	Declaración de Aplicabilidad	21-mayo-18	25-mayo-18
4	Plan de Tratamiento de Riesgos	28-mayo-18	30-jun-18
5	Seleccionar Controles de seguridad	2-jul-18	13-jul-18
6	Políticas de "Seguridad de la Información"	16-jul-18	27-jul-18

Elaborado por el Autor

3.1.2. Alcance del SGSI

UNIDAD EDUCATIVA PARTICULAR SÉNECA

ALCANCE

Código del documento	**D-ALC-ADM-02**
Versión	1.0
Fecha de versión	2018-04-13
Creador por	Marco V. Bonilla Ortiz
Aprobado por	Dra. Paulina Jaramillo (Administradora)
Nivel de confidencialidad	Alto

Historial de cambio

Fecha:	Versión:	Creado por:	Descripción del cambio
2018-05-04	1.0	Marco Bonilla	Versión inicial

Propósito

Una de las ventajas del SGSI es que se puede definir el alcance y para este proyecto el área designada es el LABORATORIO DE COMPUTACIÓN, área considerada para la administración de recursos tecnológicos e información.

Nota: Proceso que genera el documento Alcance del Sistema de Gestión de Seguridad de la Información que requiere la ISO/IEC 27001.

Activos que posee la institución

La Unidad Educativa Particular Séneca cuenta con diferentes áreas como son: la primaria, secundaria, oficinas de recepción, administración, rectorado, vicerrectorado, coordinación académica y de BI, y DECE (Departamento de Consejería Estudiantil), cada área posee un computador de escritorio o portátil, su conexión dependiendo el equipo está conectado al servicio de internet por medio de cable o wifi, el laboratorio de computación, área designada para este proyecto se encuentra en el segundo piso de la secundaria y es el área que gestiona los recursos de tecnología y servicio de internet.

3.1.3. Análisis de brecha

Para obtener información relevante es necesario hacer un análisis de brecha para determinar el estado de situación actual que se encuentra el Laboratorio de Computación tomando como referencia los numerales 4 a 10 de los dominios de la ISO/IEC 27001 los cuales son obligatorios como requisito para la norma.

El autor Nieto, Juan Pablo en su trabajo Plan de implementación de la ISO/IEC 27001, realizó un análisis diferencial GAP en la que evalúa el grado de cumplimiento con respecto a la norma ISO 27001 siendo una ventaja el poco tiempo en que se realiza y permite anticiparse a acciones de mejora.

Tanto el análisis de brecha con la ISO 27001 (situación actual) e ISO 27002 (controles y Anexo A de la ISO 27001) se realiza tomando en cuenta el estado inicial, es decir, las áreas donde se puede valorar la madures, por consiguiente se asigna una escala del 0 al 5 como se muestra en la siguiente tabla (Nieto, 2013).

Tabla 22. Nivel de cumplimiento

VALOR	NOMBRE	DESCRIPCIÓN
0	No existe	No existe evidencia (documento) o práctica en la institución.
1	Etapa inicial	Tiene prácticas informales sin seguimiento
2	Repetible	Tiene un enfoque direccionado, sin embargo, no está documentado.
3	Definido	Tiene un enfoque direccionado, está documentado, pero no tiene seguimiento.
4	Administrado	Hay seguimiento con mejoras continuas.
5	Optimizado	Existe cumplimiento con buenas prácticas.

Elaborado por el Autor

Tabla 23. Nivel de cumplimiento ISO 27001.

NIVEL DE CUMPLIMIENTO					
ISO 27001					
Numeral	Dominio	Cumple Escala 0-5	Equivale sobre 100	No cumple Escala 0-5	Equivale sobre 100
4	Contexto	1,00	20,00	4,00	80,00
5	Liderazgo	1,67	33,33	3,33	66,67
6	Planificación	0,25	5,00	4,75	95,00
7	Soporte	1,63	32,50	3,38	67,50
8	Operación	0,00	0,00	5,00	100,00
9	Evaluación de desempeño	0,00	0,00	5,00	100,00
10	Mejora	1,00	20,00	4,00	80,00
	TOTAL	**5,54**	**15,83**	**4,21**	**84,17**

Elaborado por el Autor

El análisis de brecha del Laboratorio de Computación de la institución identifica el nivel de cumplimiento de acuerdo con los valores definidos en la (Tabla 22) en la que se le da un valor entre 0 y 5. Los resultados de este análisis se muestran en el Anexo B.

Figura 15. Nivel de cumplimiento ISO 27001.
Elaborado por el Autor

Análisis

El primer resultado que muestra el análisis de brecha, se observa que existe liderazgo y compromiso por parte de la institución hacia el laboratorio de computación, también hay soporte, sin embargo, esto no puede garantizar una buena gestión para los recursos de tecnología e información.

El siguiente análisis de brecha se hará con el fin de conocer el cumplimiento de los Dominios, Objetivos de Control y Controles de Seguridad de la ISO 27002 y el Anexo A de la ISO 27001.

Compresión de resultados

Para calcular los resultados con el rango (0-5) propuesto, cada literal, ejemplo A6 (primer nivel) contiene A.6.1 (segundo nivel) y A.6.1.1, A.6.1.2 (tercer nivel) etc., los de tercer nivel obtendrán un promedio que se coloca en el del segundo nivel, en caso de haber más de segundo nivel se sumarán y su resultado se coloca en el de primer nivel y para obtener el promedio general, se suman todos los de primer nivel.

Primer nivel →	A.6	Aspectos organizativos de la seguridad de la información	**20,00**	**80,00**
Segundo nivel →	A.6.1	Organización interna	**1,00**	
Tercer nivel →	A.6.1.1	Asignación de responsabilidades para la seguridad de la información.	1	
	A.6.1.2	Segregación de tareas	2	
	A.6.1.3	Contacto con las autoridades	2	
	A.6.1.4	Contactos con grupos de interés especial	0	
	A.6.1.5	Seguridad de la información en la gestión de proyectos	0	

Tabla 24. Cumplimiento de controles por dominio.

NIVEL DE CUMPLIMIENTO DOMINIOS DE LA ISO 27002 Y ANEXO A DE LA ISO 27001			
Numeral	**Dominio**	**Cumplimiento**	**No cumple**
A.5	A.5 Políticas de seguridad	0,0	100,0
A.6	A.6 Aspectos organizativos de la seguridad de la información	20,0	80,0
A.7	A.7 Seguridad ligada a los recursos humanos	53,3	46,7
A.8	A.8 Gestión de activos	25,0	75,0
A.9	A.9 Control de accesos	20,0	80,0
A.10	A.10 Cifrado	0,0	100,0
A.11	A.11 Seguridad física y ambiental	53,3	46,7
A.12	A.12 Seguridad en la operativa	0,0	100,0
A.13	A.13 Seguridad en las telecomunicaciones	86,7	13,3
A.14	A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información	6,7	93,3
A.15	A.15 Relaciones con suministradores	0,0	100,0
A.16	A.16 Gestión de incidencias en la seguridad de la información	5,7	94,3
A.17	A.17. Aspectos de seguridad de la información en la gestión de la continuidad de negocio	0,0	100,0
A.18	A.18 Cumplimiento	28,0	72,0
TOTAL		**21,34**	**78,66**

Elaborado por el Autor

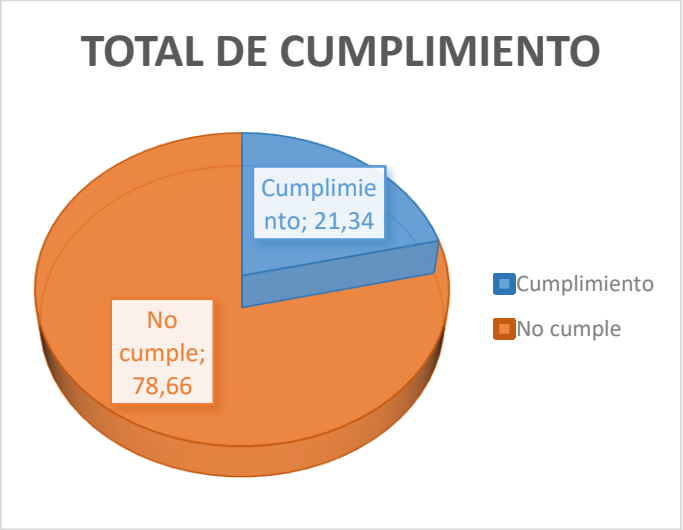


Figura 16. Controles de seguridad existentes

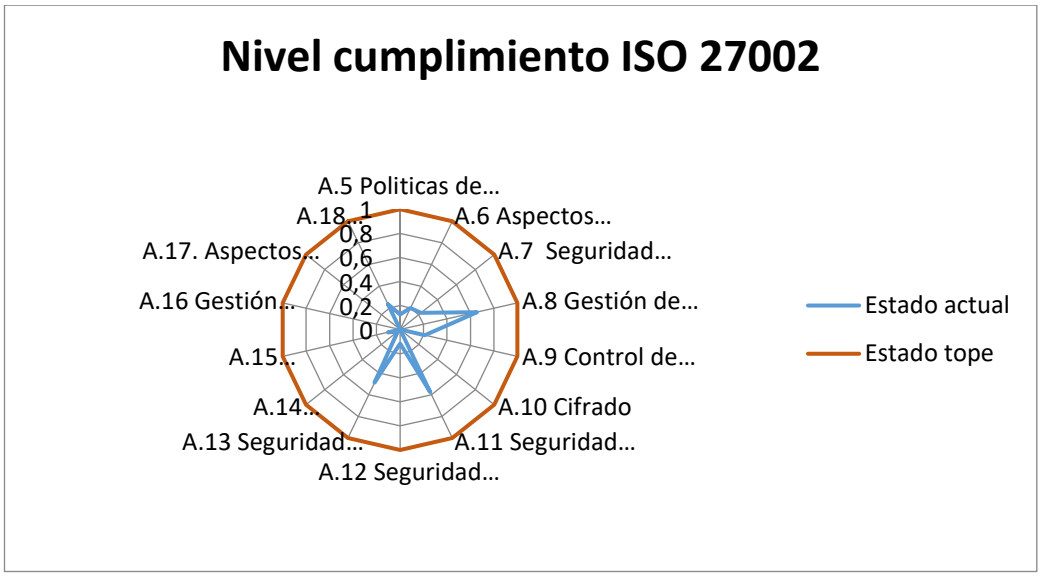


Figura 17. Nivel de cumplimiento.
Elaborado por el Autor

Análisis

Los resultados obtenidos en la tabla 24, muestra los valores de cumplimiento sobre los controles según la norma ISO 27002 y el Anexo de la ISO 27001, es muy claro que la institución muestra falencias en varios controles y en algunos como: políticas, cifrado, seguridad en la operativa, relación con los suministradores y aspectos de seguridad de la información su resultado es cero, quizás se justifica el desconocimiento en cuanto a la protección de los recursos de tecnología e información por medio de controles o no se ejecuta.

3.2. Fase 2: Gestión Documental

Cuando se realiza la implementación o diseño de un SGSI en cualquier empresa u organización, es muy importante generar documentos para futuras auditorias, modificaciones o actualizaciones incluso su seguimiento, en esta fase se desarrollará las políticas de seguridad de la información para la Unidad Educativa Particular Séneca.

3.2.1. Políticas de Seguridad de la Información

UNIDAD EDUCATIVA PARTICULAR SÉNECA

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Código del documento	**D-PSI-ADM-03**
Versión	1.0
Fecha de versión	2018-06-16
Creador por	Marco V. Bonilla Ortiz
Aprobado por	Dra. Paulina Jaramillo (Administradora)
Nivel de confidencialidad	Baja

Historial de cambio

Fecha:	Versión:	Creado por:	Descripción del cambio
2018-05-04	1.0	Marco Bonilla	Versión inicial

La creación de políticas de SI se basa en las necesidades y objetivos que propone la unidad educativa particular Séneca, estas deben contener un documento con una declaración que manifieste su compromiso y apoyo a los propósitos para gestionar la Seguridad de la Información.

Nota: Proceso que genera el documento Políticas de la Seguridad de la Información que requiere la ISO/IEC 27001: 2013, mismo que debe ser comunicado.

Propósito

El Laboratorio de Computación de la unidad educativa particular Séneca tenga el compromiso junto con el área de Administración para garantizar la protección de la Seguridad de la Información, así como de los recursos tecnológicos, permitiendo el cumplimiento eficaz de sus funciones, operaciones y actividades diarias.

Objetivos generales

Con la finalidad de cumplir el compromiso entre las dos áreas mencionadas anteriormente a continuación, se describen los objetivos generales sobre las políticas de seguridad de la información:

- Garantizar la Seguridad de la Información de la Unidad Educativa Particular Séneca relacionada con actividades académicas, administrativas y estudiantiles.
- Definir controles de acceso a los equipos informáticos y servicio de red o internet con cuenta de usuarios y contraseñas registradas individualmente para cada docente.
- Garantizar que la información académica esté disponible, así como el servicio internet, siempre y cuando este con permiso autorizados para su uso.

Alcance

Las Políticas de Seguridad de la Información que se elaborarán en la siguiente fase sólo se aplican para el LABORATORIO DE COMPUTACIÓN de la unidad educativa particular Séneca.

Descripción

El Laboratorio de Computación es el área que brinda soporte operativo y tecnológico, así como también la protección de los equipos informáticos, por este motivo es trascendental cumplir de manera objetiva las Políticas de Seguridad de la Información que se establecerán en este documento.

Definiciones

Con el propósito de entender el siguiente documento, a continuación, se mencionará términos para su mejor comprensión:

- **Activo**, es todo aquello que posee un valor para cualquier organización u empresa, ésta incluye información que se encuentre escrita, impresa, digital y se transmita por cualquier medio electrónico o se encuentre almacenada en equipos de cómputo.
- **Confidencialidad**, se trata de prevenir la divulgación sin intención o mal intencionada de la información a personas ajenas a la institución.
- **Integridad**, se refiere a los datos que permanecen intactos, es decir, libres de modificación o alteración alguna realizado por terceras personas.
- **Disponibilidad**, este quizás es el más importante, ya que de mantenerse segura e integra no será de utilidad si no está disponible para el usuario o sistema que lo requiera (PMG, ISO/IEC 27001: 2013, 2017).
- *Access point***:** dispositivo que interconecta dispositivos de comunicación inalámbrica para extender la señal de internet.
- **Red:** red de computadoras, es un conjunto de equipos conectados a través de cables, señales u ondas de transmisión de datos que comparten información.

- **Sistema Operativo:** *software* que se encarga de organizar, asignar, manejar y comunicar una operación en la computadora con el usuario.
- **Usuario:** es la persona que usa algo para una función específica.
- *Password***:** autenticación por parte de un usuario final a un sistema informático.
- **Vulnerabilidad:** estado que afecta negativamente a las propiedades de la información CID de cualquier personal o sistema informático.
- **Amenaza:** evento o circunstancia que tiene el potencial de causar daño a un sistema informático.
- ***Software* malicioso:** diseñado para ingresar al sistema de la computadora con el fin de ingresar en otro momento de acuerdo con sus intenciones.
- **Virus:** programa informático creado para alterar el estado de una computadora.
- **Antivirus:** programa que se utiliza para contra restar el efecto de un virus.
- *Spam***:** mensaje que es destinado a una audiencia en general por medio de un email de manera anónima en la que puede contener publicidad o virus.
- **Correo electrónico:** servicio que permite enviar y recibir mensajes entre usuarios mediante sistemas de comunicación.
- **Chat:** comunicación simultánea (audio y vídeo) entre dos o más usuarios a través de internet.
- **Seguridad informática:** es encargada de proteger la infraestructura computacional vinculada con la información.
- **Riesgo informático:** evento que se refiere a que una amenaza puede materialice utilizando la vulnerabilidad de un activo para su posterior ataque.
- **"Política de seguridad Informática":** es una forma de comunicarse con los usuarios y autoridades, estableciendo un canal del comportamiento del personal con los recursos y servicios de tecnología de la institución.

Condiciones generales

Para que las políticas de Seguridad de la Información tengan una usabilidad correcta se debe tomar en balance lo siguiente:

- Las políticas de seguridad de la información deberán estar disponibles para toda la comunidad educativa, ésta debe estar disponible de forma física y digital.

- El Laboratorio de Computación en conjunto con la oficina de Administración serán los entes quienes deberán difundir las Políticas y Lineamientos que permitirán velar por su cumplimiento.

Lineamientos

Las autoridades en conjunto con el Laboratorio de Computación deben trabajar con los lineamientos que a continuación se describe:

- Brindar apoyo tecnológico a las funciones o actividades que requiera de institución.
- Diseñar políticas para el uso de equipos de tecnología, las cuales deben ser cumplidas por todo el personal de la Unidad Educativa Particular Séneca.
- Mantener el compromiso con las autoridades sobre el cambio cultural al personal acerca del manejo y uso de recursos tecnológicos que ofrece la institución a su comunidad.
- Asegurar la conectividad y el servicio de internet para la institución y su entorno.
- Coordinar con la administración la adquisición de equipos, insumos y recursos asociados a las tecnologías de información en caso de requerirlos.
- Coordinar con las autoridades académicas para realizar una capacitación en la que se muestre la importancia de proteger la información que manejan a través de la tecnología y conozcan las obligaciones y responsabilidades sobre los activos de información.
- Se deberá actualizar las políticas de seguridad de la información establecidas de la institución si así lo amerita el caso.

Las políticas de seguridad de la información se encuentran en el Anexo C.

3.2.1. Revisión por parte de las autoridades

Es importante que las autoridades tengan el seguimiento apropiado en la elaboración de las políticas de seguridad de la información y para esto esta actividad se genera un documento con la declaración y aprobación por parte de las autoridades para su gestión.

3.2.2. Roles y responsabilidades

Cuando se implementa un Sistema de Gestión de la Seguridad de la Información es fundamental crear un comité de seguridad dentro de la empresa u organización, esto con el fin de mantener y supervisar el mismo, además se recomienda que un miembro sea una autoridad de la alta dirección con el propósito de agilitar las decisiones y aprobarlas.

Dentro de las funciones que tendría el comité de seguridad se menciona las siguientes:

- Motivar el uso de las buenas prácticas de seguridad de la información.
- Asignar responsabilidades y funciones.
- Realizar un seguimiento al Sistema de Gestión de Seguridad de la Información.
- Aprobar cambios y mejoras a las políticas de seguridad de la información.
- Comunicar de los riesgos, así como de sus controles.

La conformación del comité de seguridad de la unidad educativa particular Séneca son:

- La administradora
- Inspector General
- Coordinadora académica
- Profesor de Informática

3.3.Fase 3: Metodología de Análisis y Evaluación de Riesgos

UNIDAD EDUCATIVA PARTICULAR SÉNECA

METODOLOGÍA PARA EL ANÁLISIS Y EVALUACIÓN DE RIESGOS

Código del documento	**D-MER-ADM-04**
Versión	1.0
Fecha de versión	2018-05-07
Creador por	Marco V. Bonilla Ortiz
Aprobado por	Dra. Paulina Jaramillo (Administradora)
Nivel de confidencialidad	Alta

Historial de cambio

Fecha:	Versión:	Creado por:	Descripción del cambio
2018-05-04	1.0	Marco Bonilla	Versión inicial

Para realizar el análisis y evaluación de riesgos se utilizarán las guías y directrices de la norma ISO 27005 que se eligió para el desarrollo de esta actividad como se muestra en la tabla 7 y se justifica en el literal 1.4.5.

Nota: Proceso que debe generar el documento Metodología de Evaluación de Riesgos y el Tratamiento de Riesgos, que requiere la ISO/IEC 27001: 2013.

Propósito

El siguiente escrito tiene como finalidad mostrar la utilidad de la metodología de evaluación de riesgos basado en la norma 27005 y los beneficios que ésta tiene al momento de aplicar, mostrando resultados sobre los activos de la institución.

Alcance

El análisis y evaluación se aplicará a todos los activos de la institución, sin embargo, para definir los controles sólo se tomará en cuenta el área designada que en este caso es el Laboratorio de Computación.

Términos y definiciones

Consecuencia: Resultado de un evento en la que puede ser cierto o incierto y en el contexto de la SI suele ser negativa.
Controlar: medida que es la modificación del riesgo, también conocida como salvaguarda o contramedida.
Evento: ocurrencia o cambio de un conjunto en particular de ocurrencias (algo que sucede).
Contexto externo: ambiente externo en la institución busca alcanzar sus objetivos (cultural, social, político, jurídico, normativo, financiero, económico, tecnológico, etc.)
Contexto interno: ambiente interno en la institución busca alcanzar sus objetivos (gobierno, estructura organizativa roles y responsabilidades).
Nivel de riesgo: magnitud expresada en términos de combinación de consecuencias y probabilidades.
Probabilidad: posibilidad de que suceda u ocurra algo.
Riesgo: efecto en la incertidumbre (desviación positiva o negativa) en los objetivos.

Análisis de riesgo: comprender el riesgo, es decir, su naturaleza para determinar el riesgo con su respectivo nivel.

Evaluación de riesgos: proceso general de identificación de riesgo, análisis de riesgo y evaluación de riesgo.

Criterios de riesgo: términos de referencia contra la cual el significado de un riego se evalúa.

Evaluación de riesgo: resultados obtenidos a partir del análisis realizado siendo estos aceptables, mitigados, tolerables o eliminados.

Identificación de riesgo: proceso de encontrar, reconocer y describir los riesgos.

Gestión de riesgos: actividad para dirigir y controlar una organización con respecto al riesgo.

Tratamiento de riesgo: proceso para modificar el riesgo (27000, ISO, s.f.).

3.3.1. Inventario de activos

El levantamiento de activos es la parte fundamental dentro de la institución en la que se clasificará de acuerdo al detalle en el literal 1.4.6.1 y figura 9, así como también la generación de códigos según la tabla 13, y para clasificación desde la tabla 14 hasta la 20.

Tabla 25. Clasificación de activos (Datos/Información).

[DA]	ACTIVO			UBICACIÓN		PROPIEDAD		RESPONSABILIDAD Y ACCESO		
N`	Código	Descripción del activo	Tipo	Física	Electrónica	Dueño del activo	Custodio	Acceso	Responsable	Área del responsable
1	DA_BCK	Copias de Seguridad del Sistema Financiero.	INTANGIBLE	ADM	Equipo de computo	ADM	ADM	ADM-CON	ADM	Administración
2	DA_FAC	Facturación	INTANGIBLE	ADM	Equipo de computo	RR-HH-ADM	ADM	ADM-CON	ADM	RR-HH
3	DA_RDP	Roles de pago	INTANGIBLE	ADM	Archivador	RR-HH-ADM	ADM	ADM-CON	ADM	RR-HH
4	DA_CNT	Contratos	INTANGIBLE	ADM	Archivador	RR-HH-ADM	ADM	ADM-SCA	ADM	RR-HH
5	DA_HLB	Historial Laboral	INTANGIBLE	ADM	Archivador	ADM	ADM	ADM	ADM	
6	DA_NAC	Notas académicas	INTANGIBLE	SCA	Equipo de computo	SCA	SCA	SCA	SCA	Secretaría Académica
7	DA_DEC	Admisión DECE	TANGIBLE	DECE	Equipo de computo	DECE	DECE	DECE	DECE	DECE
8	DA_MAT	Matriculación	TANGIBLE	ADM	Equipo de computo	ADM	ADM	AD	ADM	Administración
9	DA_DRT	Documentos de registros tecnológicos	INTANGIBLE	LBC	Equipo de computo	ADM	LBC	RLBC	RLBC	LBC

Elaborado por el Autor

Tabla 26. Clasificación de activos (Software).

[SW]	ACTIVO			UBICACIÓN		PROPIEDAD		RESPONSABILIDAD Y ACCESO		
N`	Código	Descripción del activo	Tipo	Física	Electrónica	Dueño del activo	Custodio	Acceso	Responsable	Área del responsable
1	SW_SOP	Sistemas Operativos	INTANGIBLE	Institución	Equipo de computo	Microsoft	ADM	RLBC	RLBC	LBC
2	SW_OFI	Ofimática	INTANGIBLE	Institución	Equipo de computo	Microsoft	ADM	RLBC	RLBC	LBC
3	SW_CONT	Contabilidad	INTANGIBLE	Administración	Equipo de computo	ADM	ADM	ADM-CON	ADM-CON	Administración
4	SW_ANT	Software Antivirus	INTANGIBLE	Institución	Equipo de computo	Terceros	RLBC	RLBC	RLBC	LBC
5	SW_STD	Software Estándar	INTANGIBLE	Institución	Equipo de computo	Terceros	RLBC	RLBC	RLBC	LBC

Elaborado por el Autor

Tabla 27. Clasificación de activos (Hardware).

[HW]	ACTIVO			UBICACIÓN		PROPIEDAD		RESPONSABILIDAD Y ACCESO		
N`	Código	Descripción del activo	Tipo	Física	Electrónica	Dueño del activo	Custodio	Acceso	Responsable	Área del responsable
1	HW_HOST	Servidor	TANGIBLE	Administración	Equipo de computo	Administración	ADM	ADM-CON	ADM	Administración
2	HW_CPP	Computadoras portátiles de uso institucional.	TANGIBLE	LBC	Equipo de computo	Institución	RLBC	RLBC	RLBC	LBC
3	HW_CPE	Computadoras de escritorio de uso institucional.	TANGIBLE	OFI	Equipo de computo	Institución	OFI	EOF	EOF	EOF
4	HW_PRT	Impresoras	TANGIBLE	OFI		Institución	OFI	EOF	EOF	RLBC
5	HW_ROU1	Router principal de la Institución	TANGIBLE	AIN		Netlife	RLBC	RLBC	RLBC	LBC
6	HW_ROU2	Router secundario de Administración	TANGIBLE	Administración		TvCable	ADM	ADM	ADM	ADM
7	HW_MOD1	Modem principal de la institución	TANGIBLE	AIN		Netlife	RLBC	RLBC	RLBC	LBC
8	HW_MOD2	Modem secundario de Administración	TANGIBLE	Administración		TvCable	ADM	ADM	ADM	ADM
9	HW_SWH	Switch	TANGIBLE	AIN		Terceros	RLBC	RLBC	RLBC	LBC
10	HW_UPS	Sistema de Alimentación Ininterrumpida	TANGIBLE	AIN		Terceros	RLBC	RLBC	RLBC	LBC
11	HW_HUB	Hub o concentrador	TANGIBLE	AUL		Terceros	RLBC	RLBC	RLBC	LBC
12	HW_ACP	Puntos de Acceso Inalámbricos	TANGIBLE	AUL		Terceros	RLBC	RLBC	RLBC	LBC
13	HW_PRO	Proyectores	TANGIBLE	AUL		Institución	RLBC	DOC	DOC	LBC
14	HW_DMP	Dispositivos móviles personales	TANGIBLE	Institución	Dispositivos móviles	DOC	DOC	DOC	DOC	LBC

Elaborado por el Autor

Tabla 28. Clasificación de activos (Comunicaciones).

[COM]	ACTIVO			UBICACIÓN		PROPIEDAD		RESPONSABILIDAD Y ACCESO		
N`	Código	Descripción del activo	Tipo	Física	Electrónica	Dueño del activo	Custodio	Acceso	Responsable	Área del responsable
1	COM_INT	Internet	INTANGIBLE	AIN		Terceros	ADM	RLBC	RLBC	LBC
2	COM_LAN	Red de Área Local	INTANGIBLE	AIN		Institución	RLBC	RLBC	RLBC	LBC
3	COM_WIF	Conectividad Inalámbrica	INTANGIBLE	AIN		Terceros	RLBC	RLBC	RLBC	LBC
4	COM_WEB	Página web	INTANGIBLE	AIN		Terceros	ADM	ADM	ADM	ADM

Elaborado por el Autor

Tabla 29. Clasificación de activos (Instalaciones).

[INS]	ACTIVO			UBICACIÓN		PROPIEDAD		RESPONSABILIDAD Y ACCESO		
N`	Código	Descripción del activo	Tipo	Física	Electrónica	Dueño del activo	Custodio	Acceso	Responsable	Área del responsable
1	INS_LBCO	Laboratorio de Computación	TANGIBLE	Institución		Institución	RLBC	RLBC	RLBC	LBC
2	INS_OFR	Oficina Rectorado	TANGIBLE	Institución		Institución	ADM	REC	REC	REC
3	INS_OFV	Oficina Vice rectorado	TANGIBLE	Institución		Institución	ADM	VIC	VIC	VIC
4	INS_OFC	Oficina Coordinador BI	TANGIBLE	Institución		Institución	ADM	CBI	CBI	CBI
5	INS_OFA	Oficinas Administrativas	TANGIBLE	Institución		Institución	ADM	ADM	ADM	ADM
6	INS_OFR	Oficinas Recepción	TANGIBLE	Institución		Institución	ADM	SCA	SCA	SCA
7	INS_DEC	Oficinas DECE	TANGIBLE	Institución		Institución	ADM	DECE	DECE	DECE
8	INS_OFI	Oficina Inspección	TANGIBLE	Institución		Institución	ADM	INS	INS	INS
9	AUL_SEC	Aulas Secundaria	TANGIBLE	Institución		Institución	ADM	INS	INS	INS
10	AUL_PRI	Aulas Primaria	TANGIBLE	Institución		Institución	ADM	INS	INS	INS

Elaborado por el Autor

Tabla 30. Clasificación de activos (Personal).

[PER]	ACTIVO			UBICACIÓN		PROPIEDAD		RESPONSABILIDAD Y ACCESO		
N`	Código	Descripción del activo	Tipo	Física	Electrónica	Dueño del activo	Custodio	Acceso	Responsable	Área del responsable
1	PER_ADM	Administrador de la Institución	TANGIBLE	ADM		Institución	ADM	ADM	ADM	ADM
2	PER_DOC	Personal Docente	TANGIBLE	Institución		Institución	ADM	ADM	ADM	ADM
3	PER_CON	Personal de conserjería	TANGIBLE	Institución		Institución	ADM	ADM	ADM	ADM
4	PER_ATI	Administrador de TI	TANGIBLE	AIN		Institución	ADM	RLBC	RLBC	LBC
5	PER_EST	Estudiantes	TANGIBLE	Institución		Institución	Institución			

Elaborado por el Autor

Tabla 31. Clasificación de activos (Sistemas de Seguridad de Control).

[SSC]	ACTIVO			UBICACIÓN		PROPIEDAD		RESPONSABILIDAD Y ACCESO		
N`	Código	Descripción del activo	Tipo	Física	Electrónica	Dueño del activo	Custodio	Acceso	Responsable	Área del responsable
1	SSC_SEN	Sensores de movimiento	TANGIBLE	Institución		Institución	ADM	ADM	ADM	ADM
2	SSC_ALA	Alarma	TANGIBLE	Institución		Institución	ADM	ADM	ADM	ADM
3	SSC_CAM	Cámaras de seguridad	TANGIBLE	Institución		Institución	ADM	ADM	ADM	ADM
4	SSC_SBI	Sistema Biométrico	TANGIBLE	Institución		Institución	ADM	INS	INS	INS
5	SSC_EXT	Extintores	TANGIBLE	Institución		Institución	ADM	COP	COP	COP

Elaborado por el Autor

3.3.2. Fases de la metodología

Figura 18. Fases de la Metodología de Riegos

Fuente: (Iso 27001, 2012)

3.3.3. Valoración de activos

Para el siguiente paso es necesario establecer una escala como se menciona en el literal 1.4.6.3, por lo que para este proyecto se elige la escala cualitativa con sus criterios y valores respectivamente.

Tabla 32. Valoración de activos.

Criterio	Valor
Alto	3
Medio	2
Bajo	1

Elaborado por el Autor

Como dice Sosa Johanna en su trabajo Análisis de Riesgos "Estándares para la administración de riesgos", se debe tomar en cuenta la estimación cuantitativa y estimación cualitativa, siendo esta, los atributos calificados para describir la magnitud de consecuencias

potenciales (bajo, medio y alto) y la probabilidad que ocurran tomando en cuenta la confidencialidad, integridad y disponibilidad (Sosa, 2012, pág. 48).

Tabla 33. Preguntas para la valoración de activos.

ATRIBUTO	PREGUNTA
Confidencialidad	¿Qué importancia tendría que la información asociada al activo fuera conocida por personas no autorizadas?
Integridad	¿Qué importancia tendría que la información asociada al activo fuera modificada sin control?
Disponibilidad	¿Qué importancia tendría que el activo no estuviera disponible?

Elaborado por el Autor

Tabla 34. Valoración de activos (Datos/Información).

[D]	ACTIVO		CRITERIOS			VALORACIÓN	
N`	Código	Descripción del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Resultado	Valor
1	D_BCK	Copias de Seguridad del Sistema Financiero.	3	3	3	9	Alto
2	DA_FAC	Facturación	3	3	2	8	Medio
3	DA_RDP	Roles de pago	1	3	1	5	Bajo
4	DA_CNT	Contratos	2	3	1	6	Medio
5	DA_HLB	Historial Laboral	2	3	2	7	Medio
6	DA_NAC	Notas académicas	3	3	3	9	Alto
7	DA_DEC	Admisión DECE	3	3	3	9	Alto
8	DA_MAT	Matriculación	3	2	3	8	Medio
9	DA_DTR	Documentos de recursos tecnológicos	2	1	1	4	Bajo

Elaborado por el Autor

Tabla 35. Valoración de activos (Software).

[SW]	ACTIVO		CRITERIOS			VALORACIÓN	
N`	Código	Descripción del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Resultado	Valor
1	SW_SOP	Sistemas Operativos	1	3	3	7	Medio
2	SW_OFI	Ofimática	1	3	3	7	Medio
3	SW_CONT	Contabilidad	3	3	3	9	Alto
4	SW_ANT	Software Antivirus	2	3	1	6	Medio
5	SW_STD	Software Estándar	2	3	2	7	Medio

Elaborado por el Autor

Tabla 36. Valoración de activos (Hardware).

[HW]	ACTIVO		CRITERIOS			VALORACIÓN	
N`	Código	Descripción del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Resultado	Valor
1	HW_HOST	Servidor	3	3	3	9	Alto
2	HW_CPP	Computadoras portátiles de uso institucional.	3	3	3	9	Alto
3	HW_CPE	Computadoras de escritorio de uso institucional.	3	3	3	9	Alto
4	HW_PRT	Impresoras	2	3	1	6	Medio
5	HW_ROU1	Router principal de la Institución	3	3	3	9	Alto
6	HW_ROU2	Router secundario de Administración	3	3	3	9	Alto
7	HW_MOD1	Modem principal de la institución	3	3	3	9	Alto
8	HW_MOD2	Modem secundario de Administración	3	3	3	9	Alto
9	HW_SWH	Switch	1	2	2	5	Bajo
10	HW_UPS	Sistema de Alimentación Ininterrumpida	1	2	2	5	Bajo
11	HW_HUB	Hub o concentrador	2	1	2	5	Bajo
12	HW_ACP	Puntos de Acceso Inalámbricos	3	3	3	9	Alto
13	HW_PRO	Proyectores	1	1	1	3	Bajo
14	HW_DMP	Dispositivos móviles personales	3	3	3	9	Alto

Elaborado por el Autor

Tabla 37. Valoración de activos (Comunicaciones).

[COM]	ACTIVO		CRITERIOS			VALORACIÓN	
N`	Código	Descripción del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Resultado	Valor
1	COM_INT	Internet	3	3	3	9	Alto
2	COM_LAN	Red de Área Local	3	3	3	9	Alto
3	COM_WIF	Conectividad Inalámbrica	3	3	3	9	Alto
4	COM_WEB	Página web	1	3	1	5	Bajo

Elaborado por el Autor

Tabla 38. Valoración de activos (Instalaciones).

[INS]	ACTIVO		CRITERIOS			VALORACIÓN	
N`	Código	Descripción del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Resultado	Valor
1	INS_LBCO	Laboratorio de Computación	No aplica	No aplica	3	3	Bajo
2	INS_OFR	Oficina Rectorado	No aplica	No aplica	3	3	Bajo
3	INS_OFV	Oficina Vice rectorado	No aplica	No aplica	3	3	Bajo
4	INS_OFC	Oficina Coordinador BI	No aplica	No aplica	3	3	Bajo
5	INS_OFA	Oficinas Administrativas	No aplica	No aplica	3	3	Bajo
6	INS_OFR	Oficinas Recepción	No aplica	No aplica	3	3	Bajo
7	INS_DEC	Oficinas DECE	No aplica	No aplica	3	3	Bajo
8	INS_OFI	Oficina Inspección	No aplica	No aplica	3	3	Bajo
9	AUL_SEC	Aulas Secundaria	No aplica	No aplica	3	3	Bajo
10	AUL_PRI	Aulas Primaria	No aplica	No aplica	3	3	Bajo

Elaborado por el Autor

Tabla 39. Valoración de activos (Personal).

[PER]	ACTIVO		CRITERIOS			VALORACIÓN	
N`	Código	Descripción del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Resultado	Valor
1	PER_ADM	Administrador de la Institución	No aplica	No aplica	3	3	Bajo
2	PER_DOC	Personal Docente	No aplica	No aplica	3	3	Bajo
3	PER_CON	Personal de conserjería	No aplica	No aplica	3	3	Bajo
4	PER_ATI	Administrador de TI	No aplica	No aplica	3	3	Bajo
5	PER_EST	Estudiantes	No aplica	No aplica	3	3	Bajo

Elaborado por el Autor

Tabla 40. Valoración de activos (Sistema de Seguridad y Control).

[SSC]	ACTIVO		CRITERIOS			VALORACIÓN	
N`	Código	Descripción del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Resultado	Valor
1	SSC_SEN	Sensores de movimiento	3	3	3	9	Alto
2	SSC_ALA	Alarma	3	3	3	9	Alto
3	SSC_CAM	Cámaras de seguridad	3	3	3	9	Alto
4	SSC_SBI	Sistema Biométrico	3	3	3	9	Alto
5	SSC_EXT	Extintores	1	3	2	6	Medio

Elaborado por el Autor

3.3.4. Valoración de Impacto

En la norma ISO 27005 Anexo B, menciona que la valoración de impacto puede ser directo o indirecto, sus criterios se señalan en el literal 1.4.6.5 y en la tabla 9.

Tabla 41. Valoración de impacto (DA).

[D]	ACTIVO		CRITERIOS			VALORACIÓN		IMPACTO
N`	Código	Descripción del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Resultado	Valor	
1	D_BCK	Copias de Seguridad del Sistema Financiero.	3	3	3	9	Alto	DIRECTO
2	DA_FAC	Facturación	3	3	2	8	Medio	
3	DA_RDP	Roles de pago	1	3	1	5	Bajo	
4	DA_CNT	Contratos	2	3	1	6	Medio	
5	DA_HLB	Historial Laboral	2	3	2	7	Medio	
6	DA_NAC	Notas académicas	3	3	3	9	Alto	
7	DA_DEC	Admisión DECE	3	3	3	9	Alto	
8	DA_MAT	Matriculación	3	2	3	8	Medio	
9	DA_DTR	Documentos de recursos tecnológicos	2	1	1	4	Bajo	

Elaborado ´por el Autor

Tabla 42. Valoración de impacto (SW).

[SW]	ACTIVO		CRITERIOS			VALORACIÓN		IMPACTO
N`	Código	Descripción del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Resultado	Valor	
1	SW_SOP	Sistemas Operativos	1	3	3	7	Medio	DIRECTO
2	SW_OFI	Ofimática	1	3	3	7	Medio	
3	SW_CONT	Contabilidad	3	3	3	9	Alto	
4	SW_ANT	Software Antivirus	2	3	1	6	Medio	
5	SW_STD	Software Estándar	2	3	2	7	Medio	

Elaborado ´por el Autor

Tabla 43. Valoración de impacto (HW).

[HW]	ACTIVO		CRITERIOS			VALORACIÓN		IMPACTO
N`	Código	Descripción del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Resultado	Valor	
1	HW_HOST	Servidor	3	3	3	9	Alto	DIRECTO
2	HW_CPP	Computadoras portátiles de uso institucional.	3	3	3	9	Alto	
3	HW_CPE	Computadoras de escritorio de uso institucional.	3	3	3	9	Alto	
4	HW_PRT	Impresoras	2	3	1	6	Medio	
5	HW_ROU1	Router principal de la Institución	3	3	3	9	Alto	
6	HW_ROU2	Router secundario de Administración	3	3	3	9	Alto	
7	HW_MOD1	Modem principal de la institución	3	3	3	9	Alto	
8	HW_MOD2	Modem secundario de Administración	3	3	3	9	Alto	
9	HW_SWH	Switch	1	2	2	5	Bajo	
10	HW_UPS	Sistema de Alimentación Ininterrumpida	1	2	2	5	Bajo	
11	HW_HUB	Hub o concentrador	2	1	2	5	Bajo	
12	HW_ACP	Puntos de Acceso Inalámbricos	3	3	3	9	Alto	
13	HW_PRO	Proyectores	1	1	1	3	Bajo	
14	HW_DMP	Dispositivos móviles personales	3	3	3	9	Alto	

Elaborado ´por el Autor

Tabla 44. Valoración de impacto (COM).

[COM]	ACTIVO		CRITERIOS			VALORACIÓN		IMPACTO
N`	Código	Descripción del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Resultado	Valor	
1	COM_INT	Internet	3	3	3	9	Alto	DIRECTO
2	COM_LAN	Red de Área Local	3	3	3	9	Alto	
3	COM_WIF	Conectividad Inalámbrica	3	3	3	9	Alto	
4	COM_WEB	Página web	1	3	1	5	Bajo	

Elaborado ´por el Autor

Tabla 45. Valoración de impacto (INS).

[INS]	ACTIVO		CRITERIOS			VALORACIÓN		IMPACTO
N`	Código	Descripción del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Resultado	Valor	
1	INS_LBCO	Laboratorio de Computación	No aplica	No aplica	3	3	Bajo	INDIRECTO
2	INS_OFR	Oficina Rectorado	No aplica	No aplica	3	3	Bajo	
3	INS_OFV	Oficina Vice rectorado	No aplica	No aplica	3	3	Bajo	
4	INS_OFC	Oficina Coordinador BI	No aplica	No aplica	3	3	Bajo	
5	INS_OFA	Oficinas Administrativas	No aplica	No aplica	3	3	Bajo	
6	INS_OFR	Oficinas Recepción	No aplica	No aplica	3	3	Bajo	
7	INS_DEC	Oficinas DECE	No aplica	No aplica	3	3	Bajo	
8	INS_OFI	Oficina Inspección	No aplica	No aplica	3	3	Bajo	
9	AUL_SEC	Aulas Secundaria	No aplica	No aplica	3	3	Bajo	
10	AUL_PRI	Aulas Primaria	No aplica	No aplica	3	3	Bajo	

Elaborado ´por el Autor

Tabla 46. Valoración de impacto (PER).

[PER]	ACTIVO		CRITERIOS			VALORACIÓN		IMPACTO
N`	Código	Descripción del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Resultado	Valor	
1	PER_ADM	Administrador de la Institución	No aplica	No aplica	3	3	Bajo	INDIRECTO
2	PER_DOC	Personal Docente	No aplica	No aplica	3	3	Bajo	
3	PER_CON	Personal de conserjería	No aplica	No aplica	3	3	Bajo	
4	PER_ATI	Administrador de TI	No aplica	No aplica	3	3	Bajo	
5	PER_EST	Estudiantes	No aplica	No aplica	3	3	Bajo	

Elaborado ´por el Autor

Tabla 47. Valoración de impacto (SSC).

[SSC]	ACTIVO		CRITERIOS			VALORACIÓN		IMPACTO
N`	Código	Descripción del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Resultado	Valor	
1	SSC_SEN	Sensores de movimiento	3	3	3	9	Alto	INDIRECTO
2	SSC_ALA	Alarma	3	3	3	9	Alto	
3	SSC_CAM	Cámaras de seguridad	3	3	3	9	Alto	
4	SSC_SBI	Sistema Biométrico	3	3	3	9	Alto	
5	SSC_EXT	Extintores	1	3	2	6	Medio	

Elaborado ´por el Autor

3.3.5. Identificación de amenazas

Los diferentes tipos de amenazas se mencionan en el literal 1.4.6.4 y tabla 8, a continuación, se muestran las amenazas según la ISO 27005. Anexo C.

Tabla 48. Identificación de amenazas adaptadas al Anexo C.

Tipo	Amenaza	Origen
Daño Físico	Fuego	A, D, E
	Daño de agua	A, D, E
	Contaminación	A, D, E
	Accidente grave	A, D, E
	Destrucción de equipos o medios	E
	Polvo, corrosión, congelación	E
Eventos naturales	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundaciones	E
Pérdida de servicios esenciales	Peligro del aire acondicionado o sistema de abastecimiento de agua	A, D
	Falla en los equipos de telecomunicaciones	A, D
	Pérdida de energía eléctrica	A, D, E
	Robo de los medios de comunicación o documentos	D
	Robo de equipos	D
	Divulgación	A, D
	Datos de fuentes no confiables	D
	La manipulación del hardware	D
	La manipulación del software	D
Fallas técnicas	Daño en el equipo	A
	Malfuncionamiento del equipo	A
	Saturación del sistema de información	A, D
	Malfuncionamiento del software	A
	Incumplimiento del mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso de equipo no autorizado	D
	Copia de software fraudulento	D
	Uso de falsificación o software copiado	A, D
Funciones comprometedoras	Error en el uso	A
	Abuso de derechos	A, E, D
	Incumplimiento de la disponibilidad del personal	A, E, D

Fuente: (NTC 27005, 2008, pág. 69)

Las amenazas de tipo humano se recomiendan poner atención, ya que está comprobado que la mayor amenaza para la seguridad de la información es el ser humano.

Tabla 49. Identificación de amenazas humanas adaptadas al Anexo C.

Origen de la amenaza	**Motivación**	**Posibles consecuencias**
Criminal informático (hacker)	Reto Destrucción de la información Divulgación de información ilegal Chantaje Ganancia de dinero Alteración de datos no autorizados Venganza	Crimen por computador (espionaje cibernético). Soborno de la información Suplantación de identidad. Penetración y manipulación del sistema.
Intrusos (empleados descontentos, malintencionados, deshonestos o despedidos.	Destrucción de la información Espionaje económico Curiosidad Errores no intencionales y omisiones (ejemplo errores al ingresar datos, errores de programación)	Abuso del computador Fraude y robo Soborno de información Entrada de datos corruptos Intercepción de información Introducción de código malicioso (virus, bomba lógica, Troyanos, etc.). Venta de información Sabotaje del sistema.

Fuente: (NTC 27005, 2008, pág. 70)

Algunos ejemplos de vulnerabilidades y amenazas que pueden tomar ventaja de cualquier situación de riesgo se muestran en la siguiente tabla según la ISO 27005. Anexo D.

Tabla 50. Ejemplos de vulnerabilidades.

TIPOS	**VULNERABILIDADES**	**AMENAZAS**
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Falta de esquemas de reemplazo periódico.	Destrucción del equipo o los medios.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética.	Radiación electromagnética
	Falta de control de cambio con configuración eficiente.	Error en el uso
	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía

	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
	Falta o insuficiencia de la prueba del software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
Software	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Falta de pruebas de auditoría	Abuso de los derechos
	Distribución errada de los derechos de acceso	Abuso de los derechos
	Software de distribución amplia	Corrupción de datos
	Utilización de los programas de aplicación a los datos errados en términos de tiempo	Corrupción de datos
	Interface de usuario complicada	Error en el uso
	Falta de documentación	Error en el uso

(NTC 27005, 2008, pág. 72)

A continuación, se define las vulnerabilidades que poseen los activos de la institución.

Tabla 51. Identificación de vulnerabilidades (DA).

ACTIVO		AMENAZA Descripción	VULNERABILIDADES
DATOS/INFORMACIÓN			
DA_NAC	Notas académicas	Daños a equipos	Los estudiantes acceden a las computadoras lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
DA_DRT	Documentos de recursos tecnológicos	Daños a equipos	Los estudiantes acceden a las computadoras lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.

Elaborado por el Autor

Tabla 52. Identificación de vulnerabilidades (SW).

ACTIVO		AMENAZA Descripción	VULNERABILIDADES
SOFTWARE			
SW_SOP	Sistemas Operativos	Daños a equipos	Los estudiantes acceden a las computadoras lo que conlleva el acceso al internet e información descargable.
		Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
SW_OFI	Ofimática	Daños a equipos	Los estudiantes acceden a las computadoras lo que conlleva el acceso al internet e información descargable.
		Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
SW_ANT	Software Antivirus	Daños a equipos	
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
SW_STD	Software Estándar	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.

Elaborado por el Autor

Tabla 53. Identificación de vulnerabilidades (HW).

ACTIVO		AMENAZA Descripción	VULNERABILIDADES
HARDWARE			
HW_CPP	Computadoras portátiles de uso institucional.	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
HW_CPE	Computadoras de escritorio de uso institucional.	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
HW_PRT	Impresoras	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
HW_ROU1	Router principal de la Institución	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.

Table 53 (cont.)

HARDWARE			
HW_MOD1	Modem principal de la institución	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
HW_UPS	Sistema de Alimentación Ininterrumpida	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
HW_HUB	Hub o concentrador	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
HW_ACP	Puntos de Acceso Inalámbricos	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Interrupción de servicios Acceso a las computadoras	No existe protección para el acceso a los equipos.

Elaborado por el Autor

Tabla 54. Identificación de vulnerabilidades (COM).

ACTIVO		AMENAZA Descripción	VULNERABILIDADES
COMUNICACIONES			
COM_INT	Internet	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
COM_LAN	Red de Área Local	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
COM_WIF	Conectividad Inalámbrica	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.

Elaborado por el Autor

Tabla 55. Identificación de vulnerabilidades (INS).

ACTIVO		AMENAZA Descripción	VULNERABILIDADES
INSTALACIONES			
INS_LBCO	Laboratorio de Computación	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Daños físicos	Acceso de agua provocado por las lluvias.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.

Elaborado por el Autor

Tabla 56.Identificación de vulnerabilidades (PER).

ACTIVO		AMENAZA Descripción	VULNERABILIDADES
PERSONAL			
PER_DOC	Personal Docente	Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
PER_CON	Personal de conserjería	Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
PER_ATI	Administrador de LB	Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
PER_EST	Estudiantes	Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.

Elaborado por el Autor

Tabla 57. Identificación de vulnerabilidades (SSC).

ACTIVO		AMENAZA Descripción	VULNERABILIDADES
SISTEMA DE SEGURIDAD Y CONTROL DE ACCEO			
SSC_SEN	Sensores de movimiento	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
SSC_ALA	Alarma	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
SSC_CAM	Cámaras de seguridad	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
SSC_SBI	Sistema Biométrico	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.
SSC_EXT	Extintores	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.
		Interrupción de servicios	Falta de protección en las conexiones eléctricas.
		Información errónea	Falta de control en el manejo de datos.
		Acceso a los archivos	Los archivos no son administrados con permiso de usuario.
		Acceso a las computadoras	No existe protección para el acceso a los equipos.

3.3.6. Probabilidad que una amenaza explote una vulnerabilidad

En el literal 1.4.6.6 se habla sobre la probabilidad de que una amenaza sea exitosa aprovechando de vulnerabilidades, así como también la definición de la escala cuantitativa que se muestra en la siguiente tabla.

Tabla 58. Probabilidad de que la amenaza explote la vulnerabilidad.

Criterio	Valor
Alto	3
Medio	2
Bajo	1

Elaborado por el Autor

La calificación del nivel de riesgo se la da multiplicando el valor de la probabilidad por el valor de impacto (P x I), de esta manera se obtiene el resultado en las siguientes tablas.

Accidentales (A)	Deliberadas (D)	Ambientales (E)

Tabla 59. Calificación del Riesgo (DA).

ACTIVO		AMENAZA		VULNERABILIDADES	PROBABILIDAD	IMPACTO	VALOR	NIVEL DE RIESGO
		Descripción	Origen					
DATOS/INFORMACIÓN								
DA_NAC	Notas académicas	Daños a equipos	D, A. E	Los estudiantes acceden a las computadoras lo que conlleva el acceso al internet e información descargable.	3	3	9	Alto
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	2	2	4	Bajo
		Información errónea	D, A	Falta de control en el manejo de datos.	3	3	9	Alto
		Acceso a los archivos	D, A	Los archivos no son administrados con permiso de usuario.	2	2	4	Bajo
		Acceso a las computadoras	D	No existe protección para el acceso a los equipos.	3	3	9	Alto
DA_DRT	Documentos de recursos tecnológicos	Daños a equipos	D, A, E	Los estudiantes acceden a las computadoras lo que conlleva el acceso al internet e información descargable.	2	3	6	Medio
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	1	2	2	Bajo
		Información errónea	D, A	Falta de control en el manejo de datos.	1	2	2	Bajo
		Acceso a los archivos	D, A	Los archivos no son administrados con permiso de usuario.	1	1	1	Bajo
		Acceso a las computadoras	D	No existe protección para el acceso a los equipos.	1	1	1	Bajo

Elaborado por el Autor

Tabla 60. Calificación del Riesgo (SW).

ACTIVO		AMENAZA Descripción	AMENAZA Origen	VULNERABILIDADES	PROBABILIDAD	IMPACTO	VALOR	NIVEL DE RIESGO
SOFTWARE								
SW_SOP	Sistemas Operativos	Daños a equipos	D, A, E	Los estudiantes tienen acceso a la manipulación de los equipos así como a sus programas	3	3	9	Alto
		Información errónea	D, A	Falta de control en el manejo de datos.	1	1	1	Bajo
		Acceso a los archivos	D, A	Los archivos no son administrados con permiso de usuario.	2	3	6	Medio
		Acceso a las computadoras	D	No existe protección para el acceso a los equipos.	2	1	2	Bajo
SW_OFI	Ofimática	Daños a equipos	D, A, E	Los estudiantes tienen acceso a la manipulación de los equipos así como a sus programas	3	2	6	Medio
		Información errónea	D, A	Falta de control en el manejo de datos.	1	1	1	Bajo
		Acceso a los archivos	D, A	Los archivos no son administrados con permiso de usuario.	2	3	6	Medio
		Acceso a las computadoras	D	No existe protección para el acceso a los equipos.	2	1	2	Bajo
SW_ANT	Software Antivirus	Daños a equipos	D, A, E	Los estudiantes tienen acceso a la manipulación de los equipos así como a sus programas	3	2	6	Medio
		Acceso a los archivos	D	Los archivos no son administrados con permiso de usuario.	2	1	2	Bajo
		Acceso a las computadoras	D, A	No existe protección para el acceso a los equipos.	2	1	2	Bajo
SW_STD	Software Estándar	Daños a equipos	D, A, E	Los estudiantes tienen acceso a la manipulación de los equipos así como a sus programas	3	2	6	Medio
		Información errónea	D, A	Falta de control en el manejo de datos.	3	1	3	Bajo
		Acceso a los archivos	D	Los archivos no son administrados con permiso de usuario.	2	1	2	Bajo
		Acceso a las computadoras	D	No existe protección para el acceso a los equipos.	2	3	6	Medio

Elaborado por el Autor

Tabla 61. Calificación del Riesgo (HW).

ACTIVO		AMENAZA Descripción	AMENAZA Origen	VULNERABILIDADES	PROBABILIDAD	IMPACTO	VALOR	NIVEL DE RIESGO
HARDWARE								
HW_CPP	Computadoras portátiles de uso institucional.	Daños a equipos	D, A, E	Los equipos pueden ser manipulados por personal que no es autorizado	3	3	9	Alto
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	1	1	1	Bajo
		Información errónea	D, A	Falta de control en el manejo de datos.	1	3	3	Bajo
		Acceso a las computadoras	D	No existe protección para el acceso a los equipos.	3	3	9	Alto
HW_CPE	Computadoras de escritorio de uso institucional.	Daños a equipos	D, A, E	Los equipos pueden ser manipulados por personal que no es autorizado	3	2	6	Medio
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	1	2	2	Bajo
		Información errónea	D, A	Falta de control en el manejo de datos.	1	3	3	Bajo
		Acceso a las computadoras	D	No existe protección para el acceso a los equipos.	3	3	9	Alto
HW_PRT	Impresoras	Daños a equipos	D, A, E	Los equipos pueden ser manipulados por personal que no es autorizado	3	1	3	Bajo
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	1	1	1	Bajo
HW_ROU	Router	Daños a equipos	D, A, E	Los equipos pueden ser manipulados por personal que no es autorizado	3	3	9	Alto
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	2	3	6	Medio
		Acceso a Los equipos	D	No existe protección para el acceso a los equipos.	3	3	9	Alto

Tabla 61 (cont.)

HARDWARE								
HW_MOD	Modem principal de la institución	Daños a equipos	D, A, E	Los equipos pueden ser manipulados por personal que no es autorizado	3	3	9	Alto
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	3	3	9	Alto
		Acceso a los equipos	D	No existe protección para el acceso a los equipos.	3	3	9	Alto
HW_UPS	Sistema de Alimentación Ininterrumpida	Daños a equipos	D, A, E	Los equipos pueden ser manipulados por personal que no es autorizado	3	1	3	Bajo
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	3	1	3	Bajo
		Acceso a Los equipos	D	No existe protección para el acceso a los equipos.	3	1	3	Bajo
HW_HUB	Hub o concentrador	Daños a equipos	D, A, E	Los equipos pueden ser manipulados por personal que no es autorizado	3	3	9	Alto
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	1	3	3	Bajo
		Acceso a Los equipos	D	No existe protección para el acceso a los equipos.	3	3	9	Alto
HW_ACP	Puntos de Acceso Inalámbricos	Daños a equipos	D, A, E	Los equipos pueden ser manipulados por personal que no es autorizado	3	1	3	Bajo
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	1	1	1	Bajo
		Información errónea	D, A	Falta de control en el manejo de datos.	1	1	1	Bajo
		Acceso a Los equipos	D	No existe protección para el acceso a los equipos.	1	1	1	Bajo
HW_PRO	Proyectores	Daños a equipos	D, A, E	Los equipos pueden ser manipulados por personal que no es autorizado	1	1	1	Bajo
		Interrupción de servicios	A	No existe protección para el acceso a los equipos.	1	1	1	Bajo
		Acceso a Los equipos	D, A	No existe protección para el acceso a los equipos.	1	1	1	Bajo

Elaborado por el Autor

Tabla 62. Calificación del Riesgo (COM).

ACTIVO		AMENAZA Descripción	AMENAZA Origen	VULNERABILIDADES	PROBABILIDAD	IMPACTO	VALOR	NIVEL DE RIESGO
COMUNICACIONES								
COM_INT	Internet	Daños a equipos	D, A, E	Las computadoras portátiles son conectadas al internet y los estudiantes tienen acceso a la misma.	3	3	9	Alto
		Interrupción de servicios	A	No existe protección para el acceso a los equipos.	1	1	1	Bajo
		Acceso a Los equipos	D	No existe protección para el acceso a los equipos.	3	2	6	Medio
COM_LAN	Red de Área Local	Daños a equipos	D, A, E	El servicio de red tiene inestabilidad para el uso de toda la comunidad educativa.	1	3	3	Bajo
		Interrupción de servicios	A	No existe protección para el acceso a los equipos.	3	3	9	Alto
		Acceso a Los equipos	D	No existe protección para el acceso a los equipos.	3	3	9	Alto
COM_WIF	Conectividad Inalámbrica	Daños a equipos	D, A, E	El servicio de red inalámbrico tiene inestabilidad para el uso de toda la comunidad educativa.	1	3	3	Bajo
		Interrupción de servicios	A	No existe protección para el acceso a los equipos.	1	1	1	Bajo
		Acceso a Los equipos	D	No existe protección para el acceso a los equipos.	1	3	3	Bajo

Elaborado por el Autor

Tabla 63. Calificación del Riesgo (INS).

ACTIVO		AMENAZA Descripción	AMENAZA Origen	VULNERABILIDADES	PROBABILIDAD	IMPACTO	VALOR	NIVEL DE RIESGO
INSTALACIONES								
INS_LBCO	Laboratorio de Computación	Daños a equipos	D, A, E	Las computadoras portátiles son utilizadas por los docentes y estudiantes sin restricción alguna.	1	3	3	Bajo
		Daños físicos	D, A, E					
		Acceso a las computadoras	D, A	Acceso de agua provocado por las lluvias.	1	3	3	Bajo

Elaborado por el Autor

Tabla 64. Calificación del Riesgo (PER).

ACTIVO		AMENAZA Descripción	AMENAZA Origen	VULNERABILIDADES	PROBABILIDAD	IMPACTO	VALOR	NIVEL DE RIESGO
PERSONAL								
PER_DOC	Personal Docente	Información errónea	A	Falta de control en el manejo de datos.	1	3	3	Bajo
		Acceso a las computadoras	D	No existe protección para el acceso a los equipos.	4		0	Bajo
PER_CON	Personal de conserjería	Información errónea	A	Falta de control en el manejo de datos.	1	2	2	Bajo
		Acceso a las computadoras	D	No existe protección para el acceso a los equipos.	3		0	Bajo
PER_ATI	Administrador de LB	Información errónea	A	Falta de control en el manejo de datos.	1	3	3	Bajo
		Acceso a los archivos	D	Los archivos no son administrados con permiso de usuario.	1		0	Bajo
		Acceso a las computadoras	D	No existe protección para el acceso a los equipos.	1	3	3	Bajo
PER_EST	Estudiantes	Información errónea	A	Falta de control en el manejo de datos.	3		0	Bajo
		Acceso a las computadoras	D	No existe protección para el acceso a los equipos.	3	3	9	Alto

Elaborado por el Autor

Tabla 65. Calificación del Riesgo (SSC).

ACTIVO		AMENAZA Descripción	AMENAZA Origen	VULNERABILIDADES	PROBABILIDAD	IMPACTO	VALOR	NIVEL DE RIESGO
SISTEMA DE SEGURIDAD Y CONTROL DE ACCEO								
SSC_SEN	Sensores de movimiento	Daños a equipos	D, A, E	Los dispositivos están accesibles a la manipulación de personal no autorizado.	1	3	3	Bajo
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	1	3	3	Bajo
		Información errónea	A	Falta de control en el manejo de datos.	1	3	3	Bajo
		Acceso a los equipos	D, A	No existe protección para el acceso a los equipos.	1	3	3	Bajo
SSC_ALA	Alarma	Daños a equipos	D, A, E	Los dispositivos están accesibles a la manipulación de personal no autorizado.	1	3	3	Bajo
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	1	3	3	Bajo
		Información errónea	A	Falta de control en el manejo de datos.	3	2	6	Medio
		Acceso a los equipos	D, A	No existe protección para el acceso a los equipos.	2	3	6	Medio
SSC_CAM	Cámaras de seguridad	Daños a equipos	D, A, E	Los dispositivos están accesibles a la manipulación de personal no autorizado.	1	3	3	Bajo
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	1	3	3	Bajo
		Información errónea	A	Falta de control en el manejo de datos.	3	3	9	Alto
		Acceso a los equipos	D, A	No existe protección para el acceso a los equipos.	1	3	3	Bajo
SSC_SBI	Sistema Biométrico	Daños a equipos	D, A, E	Los dispositivos están accesibles a la manipulación de personal no autorizado.	1	3	3	Bajo
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	1	3	3	Bajo
		Información errónea	A	Falta de control en el manejo de datos.	3	3	9	Alto
		Acceso a los equipos	D, A	No existe protección para el acceso a los equipos.	3	3	9	Alto
SSC_EXT	Extintores	Daños a equipos	D, A, E	Los dispositivos están accesibles a la manipulación de personal no autorizado.	3	3	9	Alto
		Interrupción de servicios	A	Falta de protección en las conexiones eléctricas.	1	3	3	Bajo
		Información errónea	A	Falta de control en el manejo de datos.	1	3	3	Bajo
		Acceso a los equipos	D, A	No existe protección para el acceso a los equipos.	1	3	3	Bajo

Elaborado por el Autor

3.3.7. Representación gráfica de los riesgos

La representación gráfica de los resultados según el nivel de riesgo, es aquella que permite tener prioridad de eventos visualmente basándose en los niveles de riesgo obtenidos en las tablas de calificación.

3.3.8. Resultados

Los siguientes resultados son tomados a partir de la (tabla 69) en la cual muestra el nivel de riesgo de la Unidad Educativa Particular Séneca.

Tabla 66. Resultados

	Criterio			Nivel de riesgo
Valor	3		Alto	22
	2		Medio	12
	1		Bajo	60
Total activos				94

Elaborado por el Autor

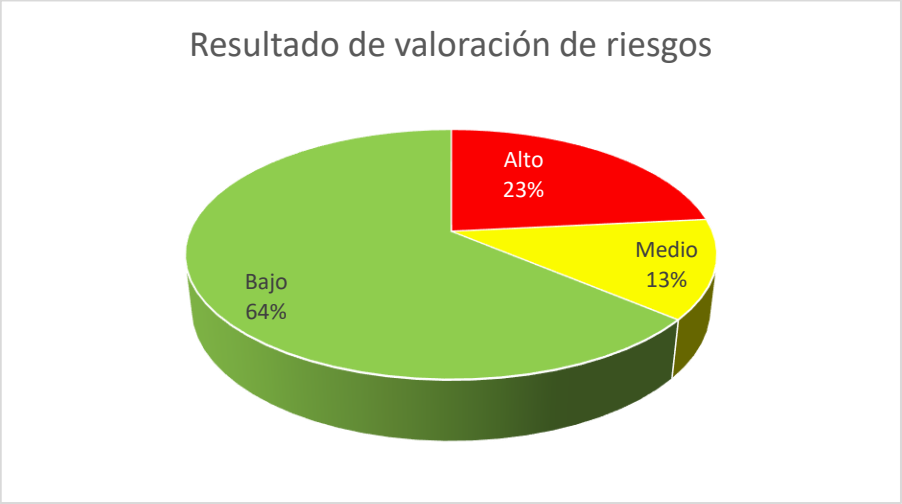


Figura 19. Representación gráfica de resultado total

Elaborado por el Autor

Análisis

A través de la representación gráfica de resultados sobe el nivel de riesgo se muestra que el 64% tiene un nivel bajo, es decir, no tiene mucho impacto sobre los activos, en cambio el 10% tiene nivel medio, aceptable, pero manteniendo un seguimiento continuo sobre su medición y por último tenemos el 30% de nivel alto en el cual hay que tomar en cuenta para sugerir controles de acuerdo a las necesidades de la empresa.

A continuación, se presenta el detalle de cada clasificación de activos:

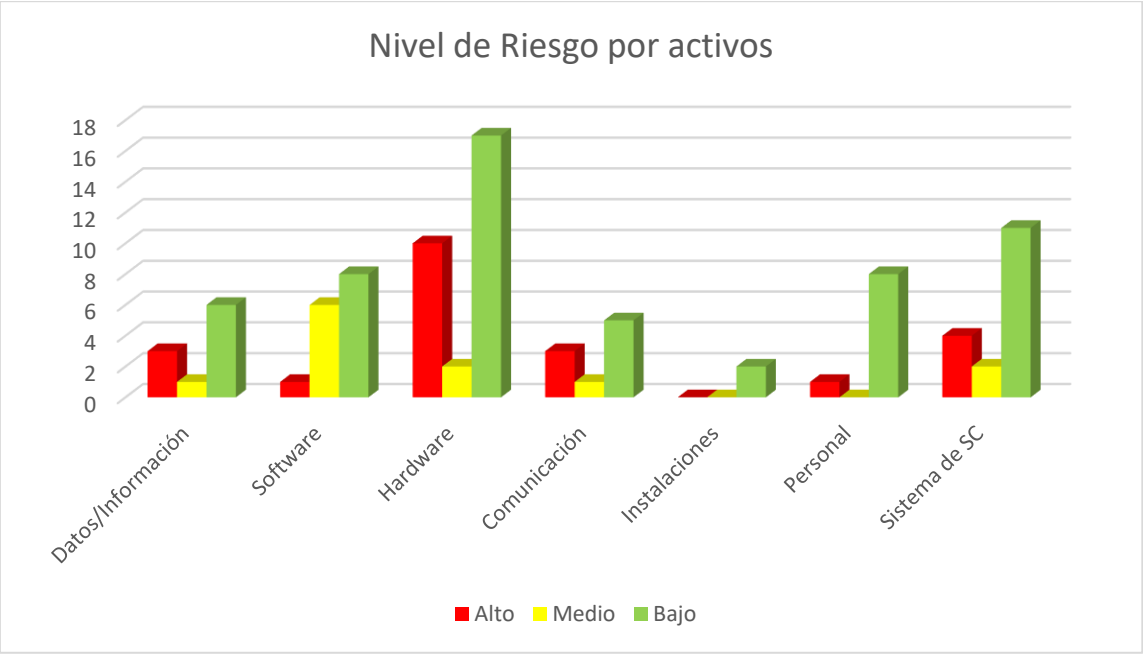


Figura 20. Nivel de riesgo por activos.
Elaborado por el Autor

3.4.Fase 4: Declaración de Aplicabilidad

UNIDAD EDUCATIVA PARTICULAR SÉNECA

DECLARACIÓN DE APLICABILIDAD

Código del documento	**D-DAP-ADM-05**
Versión	1.0
Fecha de versión	2018-05-21
Creador por	Marco V. Bonilla Ortiz
Aprobado por	Dra. Paulina Jaramillo (Administradora)
Nivel de confidencialidad	Media

Historial de cambio

Fecha:	**Versión:**	**Creado por:**	**Descripción del cambio**
2018-05-04	1.0	Marco Bonilla	Versión inicial

Para esta fase una vez analizado y evaluado los riesgos con su respectivo valor se pude definir la aplicabilidad de controles según la ISO/IEC 27002: 2013.

Nota: A partir del tratamiento de riesgo se debe generar el documento Declaración de Aplicabilidad y Plan de Tratamiento de Riesgos que requiere la ISO/IEC 27001: 2013, (véase tabla 6. 6.1.3d).

Propósito

En el siguiente documento se comprueba los controles que pueden ser apropiados para la implementación en el Laboratorio de Computación de la Unidad Educativa Particular Séneca, así también se describen los objetivos y controles respectivamente.

3.4.1. Aplicabilidad

Las siguientes tablas muestran la aplicabilidad de controles utilizando el Anexo A de la ISO/IEC 27001: 2013.

Tabla 67. Declaración de Aplicabilidad (Políticas de Seguridad de la Información).

A.5	POLITICAS DE SEGURIDAD DE LA INFORMACION			
A.5.1	Orientación de la dirección para la gestión de la seguridad de la información.	Control		
A.5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, en la que esté aprobada por la dirección, sí también comunicada y publicada a todo el personal interno y partes externas correspondientes.	**APLICA**	
			SI	**NO**
			Las políticas proveen un direccionamiento de acuerdo a los requerimientos de la institución y el cumplimiento de las leyes. Este documento es obligatorio para la ISO/IEC 27001: 2013.	
A.5.1.2	Revisión de las Políticas para la seguridad de la información	**Control:** Las políticas para la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continua.	**APLICA**	
			SI	**NO**
			Las políticas deben ser continuamente evaluadas con el propósito de actuar ante cambios de la institución.	

Elaborado por el Autor

Tabla 68. Declaración de Aplicabilidad (Organización de Seguridad de la Información).

Id Control	CONTROL	IMPLEMENTACION	APLICABLE	
A.6	ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION			
A.6.1	Organización interna			
A.6.1.1	Roles y Responsabilidades para la seguridad de la información	**Control:** Se debe definir y asignar todas las responsabilidades de la seguridad de la información.	APLICA	
			SI	NO
			La asignación de roles y responsabilidades en la institución es de mucha importancia ya que se debe cuidar los activos, así como sus procesos. Este documento es obligatorio en la Norma ISO/IEC 27001: 2013.	
A.6.1.2	Separación de deberes	**Control:** Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la institución.	APLICA	
			SI	NO
			Ninguna persona que pertenezca a la institución debería tener acceso a modificar los activos y/o información sin previa autorización.	
A.6.1.3	Contacto con las autoridades	**Control:** Se debe mantener contactos apropiados con las autoridades pertinentes.	APLICA	
			SI	NO
			Dentro de la institución debería haber procesos que permitan la comunicación con las autoridades en caso de repostar incidencias relacionadas con la seguridad de la información.	
A.6.1.4	Contracto con grupos de interés especial	**Control:** Se debería mantener contactos apropiados con grupos de interés especial u otros foros y asociados profesionales especializados en seguridad.	APLICA	
			SI	NO
A.6.1.5	Seguridad de la información en la gestión de proyectos	**Control:** La seguridad de la información se debe tratar en la gestión de proyectos independientemente del tipo de proyectos.	APLICA	
			SI	NO
			Para un proyecto de TI se debería tener una metodología para evaluar riesgos con el propósito de estar controlados.	
A.6.2	Dispositivos móviles y teletrabajo			
A.6.2.1	Políticas para dispositivos móviles	**Control:** Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	APLICA	
			SI	NO
			Todo dispositivo móvil es considerado un riesgo potencial para lo que tiene que ver con la seguridad de la información.	
A.6.2.2	Teletrabajo	**Control:** Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la se que tiene acceso, que es procesada o almacenada en los lugares en los que realiza el trabajo.	APLICA	
			SI	NO

Elaborado por el Autor

Tabla 69. Declaración de Aplicabilidad (Seguridad de los Recursos Humanos).

Id Control	CONTROL	IMPLEMENTACION	APLICABLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS		
A.7.1	Antes de asumir el riesgo		
A.7.1.1	Selección	**Control:** Las verificaciones de los antecedentes de todos los candidatos a un empleo se deban llevar a cado de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deban ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y los riesgos percibíos.	**APLICA** **SI** / **NO** Aparte de la profesionalidad, el personal debería ser ético, correcto y confiable en especial si va acceder a la información de la institución.
A.7.1.2	Términos condiciones del empleo	**Control:** Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las que la organización en cuanto a la seguridad de la información.	**APLICA** **SI** / **NO** Un contrato o acuerdo de los empleados debería tener clausulas relacionadas con la confidencialidad de la información.
A.7.2	Durante la ejecución del empleo		
A.7.2.1	Responsabilidades de la dirección	**Control:** La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la institución.	**APLICA** **SI** / **NO** Las autoridades aseguran que los roles y responsabilidades están definidas antes de brindar acceso confidencial, así como las del personal, sin embargo, no poseen políticas documentadas, siendo este un documento obligatorio.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	**Control:** Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, actualizaciones regulares sobre las políticas y procedimientos de la institución pertenecientes a su cargo.	**APLICA** **SI** / **NO** Mediante una charla relacionada a la seguridad de la información, el personal toma conciencia sobre la importancia de tener políticas mediante un SGSI.
A.7.2.3	Proceso disciplinario	**Control:** Se debe contar con un proceso formal, el cual debe ser comunicado para emprender acciones contra empleados que hayan cometido la violación a la seguridad de la información.	**APLICA** **SI** / **NO** Los procesos disciplinarios son en base a la responsabilidad del empleado.

Elaborado por el Autor

Tabla 70. Declaración de Aplicabilidad (Gestión de activos).

Id Control	CONTROL	IMPLEMENTACIÓN	APLICABLE
A.8	GESTIÓN DE ACTIVOS		
A.18.1	Responsabilidad por los activos		
A.8.1.1	Inventario de Activos	**Control:** Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se deben elaborar y mantener un inventario de estos activos.	APLICA SI / NO El inventario y su clasificación de activos permite conocer la importancia de los mismos y su impacto en la institución. Este documento es de carácter obligatorio.
A.8.1.2	Propiedad de los activos	**Control:** Los activos mantenidos en el inventario deben tener un propietario.	APLICA SI / NO Durante el ciclo de vida de los activos, es muy importante la responsabilidad de los propietarios. Este documento es de carácter obligatorio.
A.8.1.3	Uso aceptable de los activos	**Control:** Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con información e instalaciones de procesamiento de información.	APLICA SI / NO Todo el personal que tiene acceso al uso de los activos es responsable del mismo.
A.8.1.4	Devolución de activos	**Control:** Todos los empleados y usuarios de las partes externas deben devolver todos los activos de la organización que se encuentran a su cargo, al terminar su contrato.	APLICA SI / NO La devolución de activos debe ser formalizada al finalizar el contrato de un empleado, y su información debe ser transferida a la institución.
A.8.2	Clasificación de la información		
A.8.2.1	Clasificación de la información	**Control:** La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación autorizada.	APLICA SI / NO La clasificación de la información es muy importante para determinar el nivel y control de éste debería tener. Este documento es de carácter obligatorio.
A.8.2.2	Etiquetado de la información	**Control:** Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	APLICA SI / NO Durante el ciclo de vida de los activos, es muy importante la responsabilidad de los propietarios. Este documento es de carácter obligatorio.
A.8.2.3	Manejo de activos	**Control:** Se debe desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	APLICA SI / NO Para tener acceso a los activos, estos deberían restringirse de acuerdo a su clasificación.

Tabla 70 (cont.)

A.8.3	Manejo de medios			
A.8.3.1	Gestión de medios removibles	**Control:** Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación de la organización.	APLICA	
			SI	NO
			Los medios removibles deben tener el mismo tratamiento que cualquier otro activo de informático.	
A.8.3.2	Disposición de los medios	**Control:** Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	APLICA	
			SI	NO
			En los medios removibles se puede almacenar información confidencial y deben tener copias de seguridad y estar almacenados en lugares seguros.	
A.8.3.3	Transferencia de medios físicos	**Control:** Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	APLICA	
			SI	NO

Elaborado por el Autor

Tabla 71. Declaración de Aplicabilidad (Control de acceso).

Id Control	CONTROL	IMPLEMENTACIÓN	APLICABLE	
A.9	CONTROL DE ACCESO			
A.9.1	Requisitos del negocio para el control de acceso			
A.9.1.1	Política de control de acceso	**Control:** Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	APLICA	
			SI	NO
			El control de acceso con privilegios permite tener un control sobre el acceso físico y lógico de los activos a personas no autorizadas.	
A.9.1.2	Acceso a redes y a servicios de red	**Control:** Solo se debe permitir acceso a los usuarios a la red y a los servicios de red para los qe hayan sido autorizados especialmente.	APLICA	
			SI	NO
			La red y los servicios proveen acceso a diferentes servicios dentro de la institución a todo el personal.	
A.9.2	Gestión de acceso de usuarios			
A.9.2.1	Registro y cancelación de registro de usuarios	**Control:** Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	APLICA	
			SI	NO
A.9.2.2	Suministro de acceso de usuarios	**Control:** Se debe implementar un proceso de sumistro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	APLICA	
			SI	NO
A.9.2.3	Gestión de derechos de acceso privilegiado	**Control:** Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	APLICA	
			SI	NO
			Los accesos con privilegios a cualquier medio de información deberia estar asignado de acuerdo a las políticas de acceso.	
A.9.2.4	Gestión de información de autenticación secreta de usuarios	**Control:** La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	APLICA	
			SI	NO
			La autenticación del personal en los sistemas de información debería mentenerse de forma confidencial para así evitar la alteración y/o modificación de la información.	
A.9.2.5	Revisión de los derechos de acceso de usuarios	**Control:** Los propietarios de los activos deben revisar los derechos de acceso de usuarios, a intervalos regulares.	APLICA	
			SI	NO
			Estos derechos de acceso verifican lo que el usuario puede hacer sobre la información.	
A.9.2.6	Retiro o ajuste de los derechos de acceso	**Control:** Los derechos de acceso de todos los empleados y de usuarios externos a la información se deben retirar al terminar su empleo o ajustar cuando se hagan cambios.	APLICA	
			SI	NO
			La revocatoria de los derechos de acceso permite que si los empleados ya no ocupan el cargo no sigan teniendo el acceso a la información.	

A.9.3	Responsabilidades de los usuarios		
A.9.3.1	Uso de la información de autenticación secreta	**Control:** Se debe exigir a los usuarios que cumplan con ls prácticas de la institución para el uso de la información de autenticación secreta.	APLICA SI / NO La información confidencial sólo es accedida por personas autorizadas en la institución.

A.9.4	Control de acceso a sistemas y aplicaciones		
A.9.4.1	Restricción de acceso a la información	**Control:** El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	APLICA SI / NO El acceso a la información debe ser restringida en pro de evitar la revelación o acceso a personas no autorizadas.
A.9.4.2	Procedimiento de ingreso seguro	**Control:** Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	APLICA SI / NO El inicio de sesión seguro permite controlar el acceso a personas no autorizadas a ingresar a los sistemas de información.
A.9.4.3	Sistemas de gestión de contraseñas	**Control:** Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	APLICA SI / NO Una gestión de contraseñas se considera fuerte para la autenticación de usuarios, evitando la adivinanza de las mismas evitando ataques de fuerza bruta y/o diccionario.
A.9.4.4	Uso de programas utilitarios privilegiados	**Control:** Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener la capacidad de anular el sistema y lo controles de las aplicaciones.	APLICA SI / NO Para instalar programas utilitarios se debe tener mucho cuidado para que no afecten a los sistemas.
A.9.4.5	Control de acceso a códigos fuente de programas	**Control:** Se debe restringir el acceso a los códigos fuentes de los programas.	APLICA SI / NO

Elaborado por el Autor

Tabla 72. Declaración de Aplicabilidad (Criptografía).

Id Control	CONTROL	IMPLEMENTACIÓN	APLICABLE
A.10	CRIPTOGRAFIA		
A.10.1	Controles criptográficos		
A.10.1.1	Política sobre el uso de controles criptográficos	**Control:** Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	APLICA SI / NO
A.10.1.2	Gestión de llaves	**Control:** Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	APLICA SI / NO

Elaborado por el Autor

Tabla 73. Declaración de Aplicabilidad (Seguridad física y del entorno).

A.11	SEGURIDAD FÍSICA Y DEL ENTORNO		
A.11.1	Áreas Seguras		
A.11.1.1	Perímetro de seguridad física	**Control:** Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	APLICA SI / NO Un perímetro de seguridad física es la que impide a personas no autorizadas al acceso a los activos de información.
A.11.1.2	Controles de acceso físicos	**Control:** Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	APLICA SI / NO
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	**Control:** Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	APLICA SI / NO
A.11.1.4	Protección contra amenazas externas y ambientales	**Control:** Se debe diseñar y aplicar protección física contra desastres, ataques maliciosos o accidentes.	APLICA SI / NO La protección física debe ser ante desastres humanos y/o naturales.
A.11.1.5	Trabajo en áreas seguras	**Control:** Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	APLICA SI / NO
A.11.1.6	Áreas de despacho y carga	**Control:** Se deben controlar los puntos de acceso tales como la áreas de despacho y de carga, y otros puntos donde puedan entrar personas no autorizadas, y si es posible aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	APLICA SI / NO Los lugares de entrega están controlados y restringido al acceso.

Tabla 73 (cont.)

A.11.2	Equipos		
A.11.2.1	Ubicación y protección de los activos	**Control:** Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	APLICA SI / NO Los equipos deben estar protegidos de amenazas ambientales (fuego, agua) y humanas (acceso no autorizado).
A.11.2.2	Servicios de suministro	**Control:** Los equipos se debe proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	APLICA SI / NO Los suministros de energía y agua deberían estar de acorde a protección de equipos.
A.11.2.3	Seguridad del cableado	**Control:** El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinde soporte a los servicios de información se deben proteger contra interceptación, interferencias o daños.	APLICA SI / NO El cableado es a que que brinda la transmisión de datos o equipos o dispositivos.
A.11.2.4	Mantenimiento de equipos	**Control:** Los equipos se deben mantener correctamente para asegurar su disponibilidad en integridad continua.	APLICA SI / NO El mantenimiento de equipos proporciona garantía para su funcionamiento.
A.11.2.5	Retiro de activos	**Control:** Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	APLICA SI / NO El retiro de los equipos y/o eliminación de software debe ser realizado por personal autorizado de la institución.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	**Control:** Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de instalaciones.	APLICA SI / NO Los equipos de la institución deberían ser gestionados sólo por personal autorizado evitando la utilización de los mismos en áreas fuera de la institución.
A.11.2.7	Disposición segura o reutilización de equipos	**Control:** Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.	APLICA SI / NO Para la disposición o reutilización de equipos se debe tener un procedimiento para la eliminación o destrucción de la información almacenada.
A.11.2.8	Equipos de usuarios desatendido	**Control:** Los usuarios deben asegurarse de que los equipos desatendidos se les de la protección apropiada.	APLICA SI / NO Los usuarios deberían cerrar la sesión cuando no utilicen los equipos con contraseñas fuertes evitando el acceso no autorizado.
A.11.2.9	Políticas de escritorio limpio y pantalla limpia	**Control:** Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	APLICA SI / NO El almacenamiento de información que se confidencial no debe estar visible ante el público.

Elaborado por el Autor

Tabla 74. Declaración de Aplicabilidad (Seguridad de las operaciones).

Id Control	CONTROL	IMPLEMENTACIÓN	APLICABLE
A.12	SEGURIDAD DE LAS OPERACIONES		
A.12.1	Procedimientos operacionales y responsabilidades		
A.12.1.1	Procedimientos de operación documentadas	**Control:** Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	APLICA SI / NO Los procedimientos operacionales deberían estar documentados y disponibles, incluyendo copias de seguridad, encendido/apagado, configuración, etc. ***Este documento es de carácter obligatorio.***
A.12.1.2	Gestión de cambios	**Control:** Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	APLICA SI / NO Los controles de acceso físico son los que evitan el ingreso a personas no autorizadas a los activos de información.
A.12.1.3	Gestión de capacidad	**Control:** Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido por el sistema.	APLICA SI / NO Lo recursos deberían ser monitoreados con el propósito de gestionar la capacidad y rendimiento.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.	**Control:** Se deben separar los ambientes de desarrollo prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	APLICA SI / NO La separación de ambientes y desarrollo de pruebas reduce el riesgo no autorizada de operaciones.
A.12.2	Protección contra códigos maliciosos		
A.12.2.1	Control contra códigos maliciosos	**Control:** Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	APLICA SI / NO El software malicioso es un riesgo potencial para sistemas, provocando que operen de forma ineficiente permitiendo la captura de información.
A.12.3	Copias de respaldos		
A.12.3.1	Respaldo de la información	**Control:** Se deben hacer copias de respaldo de información, software e imágenes de los sistemas y ponerlos aprueba regularmente de acuerdo con una política de copias de respaldo acordadas.	APLICA SI / NO Las copias de seguridad e imágenes de sistemas pueden garantizar la recuperación del mismo después de haber fallas o desastres.
A.12.4	Registro y seguimiento		
A.12.4.1	Registro de eventos	**Control:** Se deben elaborar, conservar y revisar regularmente los registros a cerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	APLICA SI / NO Los logs (registros) almacenan información importante sobre eventos que ocurre durante la operación del sistema.
A.12.4.2	Protección de la información de registro	**Control:** Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	APLICA SI / NO Los registros de eventos deben ser registrados para posteriormente prevenir la modificación no autorizada.
A.12.4.3	Registro del administrador y del operador	**Control:** Las actividades del administrador y del operador de sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	APLICA SI / NO Los administradores tienen acceso privilegiado lo que les permite modificar la información de registros.
A.12.4.4	Sincronización de relojes	**Control:** Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	APLICA SI / NO La sincronización de los relojes permite mantener una referencia de tiempo.

Tabla 64 (cont.)

A.12.5	Control de software operacional		
A.12.5.1	Instalación de software en los sistemas operativos	**Control:** Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	APLICA SI / NO Se debe controlar la instalación de software.

A.12.6	Gestión de vulnerabilidad técnica		
A.12.6.1	Gestión de vulnerabilidades técnicas	**Control:** Se debe obtener oportunamente información acerca de vulnerabilidades técnicas de los sistemas de información que usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar medidas apropiadas para tratar el riesgo asociado.	APLICA SI / NO El inventario de activos debería estar actualizado, esto con el fin de determinar los riesgos asociados a las vulnerabilidades técnicas.
A.12.6.2	Restricción sobre la instalación de software	**Control:** Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	APLICA SI / NO Cualquier persona con acceso privilegiado podría instalar software en los equipos. Al tener un control apropiado podría afectar el funcionamiento del mismo con software malicioso.

A.12.7	Consideraciones sobre auditorias de sistemas de información		
A.12.7.1	Controles de auditorías de sistemas de información	**Control:** Los requisitos y actividades que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de negocio.	APLICA SI / NO

Elaborado por el Autor

Tabla 75. Declaración de Aplicabilidad (Seguridad de las comunicaciones).

Id Control	CONTROL	IMPLEMENTACIÓN	APLICABLE
A.13	SEGURIDAD DE LAS COMUNICACIONES		
A.13.1	Gestión de la seguridad de las redes		
A.13.1.1	Controles de redes	**Control:** Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	APLICA SI / NO Las redes deberían tener la protección debida para la transmisión de datos, garantizando la confidencialidad, integridad y disponibilidad.
A.13.1.2	Seguridad de los servicios de redes	**Control:** Se deben identificar los mecanismos de seguridad, los niveles de servicio y los registros de gestión de todos los servicios de red, e incluidos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o contraten externamente.	APLICA SI / NO Debería ser controlado y monitoreado los accesos a la red de proveedores.
A.13.1.3	Separación en las redes	**Control:** Los grupos de servicio de información, usuarios y sistemas de información se deben separar en las redes.	APLICA SI / NO Los usuarios distintos deberían estar separados de acuerdo a su labor.

Tabla 75 (cont.)

A.13.2	Transferencia de información		
A.13.2.1	Políticas y procedimientos de transferencia de información.	**Control:** Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	APLICA SI / NO Dichos procedimientos y controles ayudan a mantener seguro a la información cuando esta es transferida.
A.13.2.2	Acuerdos sobre trasferencia de información	**Control:** Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	APLICA SI / NO Se debería tener acuerdos para la transferencia de información con procedimientos.
A.13.2.3	Mensajería electrónica	**Control:** Los grupos de servicio de información, usuarios y sistemas de información se deben separar en las redes.	APLICA SI / NO Se debería proteger los mensajes enviados entre el personal docente.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	**Control:** Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	APLICA SI / NO Se debería tener acuerdos de confidencialidad con todo el personal.

Elaborado por el Autor

Tabla 76. Declaración de Aplicabilidad (Adquisición, desarrollo y mantenimiento de sistemas).

Id Control	CONTROL	IMPLEMENTACIÓN	APLICABLE
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 requisitos de seguridad de la información	**Control:** Los requisitos relacionados con la seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejorar los sistemas de información existentes.	APLICA SI / NO Los requerimientos de la seguridad de la información debería ser identificado de acuerdo con las políticas regulatorias.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	**Control:** La información involucrada en los servicios de las aplicaciones que pasen sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizada.	APLICA SI / NO La comunicación de los servicios y aplicaciones debería estar garantizada bajo esquemas de encriptación de datos.
A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones.	**Control:** La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada.	APLICA SI / NO La comunicación de los servicios y aplicaciones debería estar garantizada bajo esquemas de encriptación de datos.

Tabla 76 (cont.)

A.14.2	Seguridad en los procesos de desarrollo y soporte		
A.14.2.1	Política de desarrollo seguro	**Control:** Se deben establecer y aplicar las reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	APLICA SI / NO
A.14.2.2	Procedimiento de control de cambios de sistemas	**Control:** Los cambios de sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	APLICA SI / NO
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	**Control:** Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones de seguridad de la organización.	APLICA SI / NO
A.14.2.4	Restricciones en los cambios a los paquetes de software	**Control:** Se deben desalentar las modificaciones de los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	APLICA SI / NO
A.14.2.5	Principios de construcción de los sistemas seguros	**Control:** Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	APLICA SI / NO
A.14.2.6	Ambiente de desarrollo seguro	**Control:** Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	APLICA SI / NO
A.14.2.7	Desarrollo contratado externamente	**Control:** La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	APLICA SI / NO El software desarrollado externamente debería tener licencia, acuerdos y prácticas de desarrollo y pruebas seguros.
A.14.2.8	Pruebas de seguridad de sistemas	**Control:** Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de seguridad.	APLICA SI / NO
A.14.2.9	Pruebas de aceptación de sistemas	**Control:** Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados,	APLICA SI / NO Se deberían realizar pruebas de seguridad en base a los requerimientos de seguridad de la organización.
A.14.3	Datos de prueba		
Objetivo: Asegurar la protección de los datos usuados para pruebas.			
A.14.3.1	Protección de datos de prueba	**Control:** Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	APLICA SI / NO

Elaborado por el Autor

Tabla 77. Declaración de Aplicabilidad (Relación con los proveedores).

Id_Control	CONTROL	IMPLEMENTACIÓN	APLICABLE	
A.15	RELACIÓN CON LOS PROVEEDORES			
A.15.1	Seguridad de la información con los proveedores.			
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	**Control:** Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar y se deben documentar.	**APLICA**	
			SI	**NO**
			Los datos de prueba deberían ser seleccionados cuidadosamente y que no contengan ninguna información confidencial.	
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	**Control:** Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización..	**APLICA**	
			SI	**NO**
			Se deberían establecer acuerdos documentados entre la organización y los proveedores para el acceso a los activos.	
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	**Control:** Los acuerdos con los proveedores deben incluir requisitos para tratar los riesgos de seguridad de información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	**APLICA**	
			SI	**NO**
			Los suministros de los proveedores deberían estar acordes a las políticas de seguridad de la información de la institución.	
A.15.2	Gestión de la prestación de servicios a proveedores			
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.				
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	**Control:** Las organizaciones deben hacer seguimiento, revisar y auditar con la regularidad la prestación de servicios de los proveedores.	**APLICA**	
			SI	**NO**
			El monitoreo y acceso de los proveedores debería ser acorde las políticas de seguridad de la organización.	
A.15.2.2	Gestión de cambios en los servicios de los proveedores	**Control:** Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de riesgos.	**APLICA**	
			SI	**NO**
			Los cambios de los proveedores deberían estar acordes a los requerimientos de seguridad de la información de la institución.	

Elaborado por el Autor

Tabla 78. Declaración de Aplicabilidad (Gestión de incidentes de seguridad de la información).

Id_Control	CONTROL	IMPLEMENTACIÓN	APLICABLE	
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
A.16.1	Gestión de incidentes y mejoras de la seguridad de la información			
A.16.1.1	Responsabilidades y procedimientos	**Control:** Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	APLICA	
			SI	NO
			Los planes y procedimientos deberían estar documentados para gestionar los incidentes con la seguridad de la información.	
A.16.1.2	Reporte de eventos de seguridad de la información	**Control:** Los eventos de seguridad de la información se deben informar a través de los canales de gestión	APLICA	
			SI	NO
A.16.1.3	Reporte de debilidades de seguridad de la información	**Control:** Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	APLICA	
			SI	NO
			Se debería implementar mecanismos de reportes de incidentes de seguridad de la información en donde el personal debería reportar brechas de seguridad.	
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	**Control:** Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	APLICA	
			SI	NO
			El clasificar y priorizar los incidentes de seguridad ayudan a identificar el impacto que pueda tener la institución.	
A.16.1.5	Respuesta a incidentes de seguridad de la información	**Control:** Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	APLICA	
			SI	NO
			Deberían existir procedimientos documentados para dar respuesta a incidentes restableciendo la operación al nivel de seguridad aceptable lo más pronto posible.	
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	**Control:** El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto sobre incidentes futuros.	APLICA	
			SI	NO
			Se debería almacenar la información de los incidentes ocurridos con el propósito de prevenirlos en el futuro.	
A.16.1.7	Recolección de evidencia	**Control:** La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	APLICA	
			SI	NO

Elaborado por el Autor

Tabla 79. Declaración de Aplicabilidad (Aspectos de seguridad de la información).

Id_Control	CONTROL	IMPLEMENTACIÓN	APLICABLE	
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA			
A.17.1	Continuidad de seguridad de la información.			
A.17.1.1	Planificación de la continuidad de la seguridad de la información	**Control:** La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	APLICA	
			SI	NO
A.17.1.2	Implementación de la continuidad de la seguridad de la información	**Control:** La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	APLICA	
			SI	NO
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**Control:** La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	APLICA	
			SI	NO

Tabla 79 (cont.)

A.17.2	Redundancias		
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.			
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	**Control:** Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	**APLICA** **SI** / **NO**

Elaborado por el Autor

Tabla 80. Declaración de Aplicabilidad (Cumplimiento).

Id_Control	CONTROL	IMPLEMENTACIÓN	APLICABLE
A.18	CUMPLIMIENTO		
A.18.1	Cumplimiento de los requisitos legales y contractuales		
A.18.1.1	Identificación de la legislación aplicable a los requisitos contractuales	**Control:** Todos los requisitos estatuarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	**APLICA** **SI** / **NO** Los administradores deberían identificar toda la información legislativa aplicable a la organización con el fin de cumplir con los requerimientos del negocio.
A.18.1.2	Derechos de propiedad intelectual	**Control:** Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	**APLICA** **SI** / **NO**
A.18.1.3	Protección de registros	**Control:** Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	**APLICA** **SI** / **NO** Los registros deberían estar clasificados de acuerdo al esquema adoptado por la organización de acuerdo al nivel de confidencialidad.
A.18.1.4	Privacidad y protección de información de datos personales	**Control:** Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	**APLICA** **SI** / **NO**
A.18.1.5	Reglamentación de controles criptográficos	**Control:** Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes..	**APLICA** **SI** / **NO**
A.18.2	Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.			
A.18.2.1	Revisión independiente de la seguridad de la información	**Control:** El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	**APLICA** **SI** / **NO**
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	**Control:** Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	**APLICA** **SI** / **NO**
A.18.2.3	Revisión del cumplimiento técnico	**Control:** Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de información.	**APLICA** **SI** / **NO**

Elaborado por el Autor

3.4.2. Resultados

	APLICA		
	SI	NO	
Total	81	32	**113 Controles**
	71,68%	28,32%	

Figura 21. Suma total de controles.
Elaborado por el Autor

3.4.3. Representación gráfica

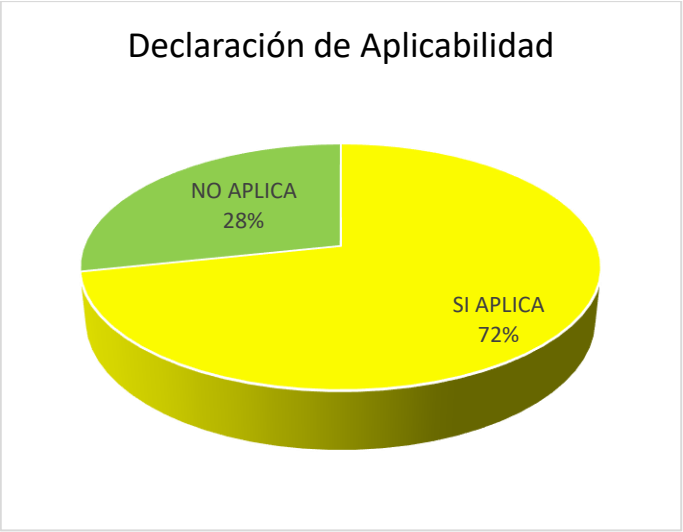


Figura 22. Representación gráfica de la Declaración de Aplicabilidad.
Elaborado por el Autor

3.5.Fase 5: Tratamiento de Riesgo

UNIDAD EDUCATIVA PARTICULAR SÉNECA

TRATAMIENTO DE RIESGOS

Código del documento	**D-TDR-ADM-07**
Versión	1.0
Fecha de versión	2018-05-28
Creador por	Marco V. Bonilla Ortiz
Aprobado por	Dra. Paulina Jaramillo (Administradora)
Nivel de confidencialidad	Bajo

Historial de cambio

Fecha:	Versión:	Creado por:	Descripción del cambio
2018-05-04	1.0	Marco Bonilla	Versión inicial

Propósito

La fase final es donde se determina qué tipo de controles son los apropiados una vez realizado la evaluación de riesgos y la aplicabilidad de controles en el Laboratorio de Computación de la Unidad Educativa Particular Séneca.

3.5.1. Tratamiento de riesgos

Según Villavicencio L., en su proyecto Diseño y propuesta técnica-económica de la red con voz sobre IP y datos apoyados en la norma ISO/IEC 27001: 2013, pág. 50 dice que para el plan de tratamiento de riesgo se lo puede hacer de distintas maneras, éste puede ser mediante el apoyo de las normas internacionales por medio de controles, también puede ser transfiriendo el riesgo a terceros, aceptando o evitando el riesgo.

Para este proyecto se utilizará la norma ISO 27002 y sus controles, sin embargo se tomará en cuenta los tratamientos mencionados dependiendo las necesidades de la institución.

Tabla 81. Tratamiento de riesgo

CÓDIGO	TRATAMIENTO	DESCRIPCIÓN
CS	Controles de seguridad (Anexo A) de la IOS/IEC 27001: 2013.	Esta norma sugiere varios tipos de controles, mismos que son basados de acuerdo con la evaluación realizada y sus resultados.
TR	Transferir el riesgo	Transfiere el riesgo a empresas externas de la institución.
ER	Evitar el riesgo	Se puede evitar el riesgo suspendiendo algunas actividades que provocan algún tipo de riesgo.
AR	Aceptar el riesgo	Puede ser viable cuando el coste a eliminar el riesgo es mayor que el daño que causará.

Fuente: (Corporativo, 2016)
Elaborado por el Autor

3.5.2. Aplicabilidad de controles de seguridad

Para el cumplimiento de los objetivos de la institución, en las siguientes tablas se muestra los controles y su tratamiento que se ha definido para los activos.

Tabla 82. Matriz de controles aplicables (Información).

CÓDIGO	ACTIVO	AMENZA	RIESGO	TRATAMIENTO	CONTROLES	ISO/IEC 27001: 2013
DATOS/INFORMACIÓN						
DA_NAC	Notas académicas		Normal		A.11.2.4	Mantenimiento de equipos
					A.12.3.1	Respaldo de la información
		A, D, E	Normal	CS	A.8.2.1	Clasificación de la Información
			Normal		A.8.2.2	Etiquetado de Información
DA_DRT	Documentos de recursos tecnológicos		Normal		A.11.2.4	Mantenimiento de equipos
		A, D, E	Normal	CS	A.12.3.1	Respaldo de la información
			Normal		A.8.2.1	Clasificación de la Información
			Normal		A.8.2.2	Etiquetado de Información

Elaborado por el Autor

Tabla 83. Matriz de controles aplicables (Software).

CÓDIGO	ACTIVO	AMENZA	RIESGO	TRATAMIENTO	CONTROLES	ISO/IEC 27001: 2013
SOFTWARE						
SW_SOP	Sistemas Operativos		Alta		A.12.2.1	Control contra código malicioso
					A.12.3.1	Respaldo de información
		A, D, E	Normal	CS	A.12.5.1	Instalación de software en los S.O
			Normal		A.12.6.2	Restricción sobre instalación de software
			Normal			
SW_OFI	Ofimática		Alta			
		A, D, E	Normal	CS	A.12.3.1	Respaldo de información
			Normal			
			Normal			
SW_ANT	Software Antivirus		Alta			
		A, D, E	Normal	CS	A.12.2	Protección contra códigos maliciosos
			Normal			
SW_STD	Software Estándar		Alta			
		A, D, E	Normal	CS	A.12.3.1	Respaldo de información
			Normal			
			Normal			

Elaborado por el Autor

Tabla 84. Matriz de controles aplicables (Hardware).

CÓDIGO	ACTIVO	AMENZA	RIESGO	TRATAMIENTO	CONTROLES	ISO/IEC 27001: 2013
HARDWARE						
HW_CPP	Computadoras portátiles de uso institucional.	A, D, E	Crítico Normal Normal Alta	CS	A.11.1.1 A.11.1.2 A.11.2.1	Perímetro de seguridad física Controles de acceso físico Ubicación y protección de activos
HW_CPE	Computadoras de escritorio de uso institucional.	A, D, E	Alta Normal Normal Alta	CS	A.11.1.1 A.11.1.2 A.11.2.1	Perímetro de seguridad física Controles de acceso físico Ubicación y protección de activos
HW_PRT	Impresoras	A, D, E	Normal Normal	AR	A.11.1.1 A.11.1.2 A.11.2.1	Perímetro de seguridad física Controles de acceso físico Ubicación y protección de activos
HW_ROU1	Router principal de la Institución	A, D, E	Crítico Normal Crítico	CS	A.11.1.1 A.11.1.2 A.11.2.1	Perímetro de seguridad física Controles de acceso físico Ubicación y protección de activos
HW_MOD1	Modem principal de la institución	A, D, E	Crítico Crítico Crítico	CS	A.11.1.1 A.11.1.2 A.11.2.1	Perímetro de seguridad física Controles de acceso físico Ubicación y protección de activos
HW_UPS	Sistema de Alimentación Ininterrumpida	A, D, E	Normal Normal Normal	CS	A.11.1.1 A.11.1.2 A.11.2.1	Perímetro de seguridad física Controles de acceso físico Ubicación y protección de activos
HW_HUB	Hub o concentrador	A, D, E	Crítico Normal Crítico	CS	A.11.1.1 A.11.1.2 A.11.2.1	Perímetro de seguridad física Controles de acceso físico Ubicación y protección de activos
HW_ACP	Puntos de Acceso Inalámbricos	A, D, E	Normal Normal Normal Normal	CS	A.11.1.1 A.11.1.2 A.11.2.1	Perímetro de seguridad física Controles de acceso físico Ubicación y protección de activos
HW_PRO	Proyectores	A, D, E	Normal Normal Normal	CS	A.11.1.1 A.11.1.2 A.11.2.1	Perímetro de seguridad física Controles de acceso físico Ubicación y protección de activos

Elaborado por el Autor

Tabla 85. Matriz de controles aplicables (Comunicaciones).

CÓDIGO	ACTIVO	AMENZA	RIESGO	TRATAMIENTO	CONTROLES	ISO/IEC 27001: 2013
COMUNICACIONES						
COM_INT	Internet	A, D, E	Alta Normal Alta	CS	A.9.1.2 A.11.2.3 A.13.1 A.13.2.1	Acceso a redes y a servicios de red Seguridad de cableado Gestión de la seguridad de redes Transferencia de información
COM_LAN	Red de Área Local	A, D, E	Normal Crítico	CS	A.9.1.2 A.11.2.3 A.13.1 A.13.2.1	Acceso a redes y a servicios de red Seguridad de cableado Gestión de la seguridad de redes Transferencia de información
COM_WIF	Conectividad Inalámbrica	A, D, E	Normal Normal Normal	CS	A.9.1.2 A.11.2.3 A.13.1 A.13.2.1	Acceso a redes y a servicios de red Seguridad de cableado Gestión de la seguridad de redes Transferencia de información

Elaborado por el Autor

Tabla 86. Matriz de controles aplicables (Instalaciones).

CÓDIGO	ACTIVO	AMENZA	RIESGO	TRATAMIENTO	CONTROLES	ISO/IEC 27001: 2013
INSTALACIONES						
INS_LBCO	Laboratorio de Computación	A, D, E	Normal Normal	AR	A.11.1	Áreas seguras

Elaborado por el Autor

Tabla 87.Matriz de controles aplicables (Personal).

CÓDIGO	ACTIVO	AMENZA	RIESGO	TRATAMIENTO	CONTROLES	ISO/IEC 27001: 2013
PERSONAL						
PER_DOC	Personal Docente	D, E	Normal Alta	AR	A.7	Seguridad de los recursos humanos
PER_CON	Personal de conserjería	D, E	Normal Alta	AR	A.7	Seguridad de los recursos humanos
PER_ATI	Administrador de LB	D, E	Normal Normal Normal	AR	A.7	Seguridad de los recursos humanos
PER_EST	Estudiantes	D, E	Alta Normal	AR	A.7	Seguridad de los recursos humanos

Elaborador por el Autor

Tabla 88- Matriz de controles aplicables (Sistema de seguridad y control de acceso).

CÓDIGO	ACTIVO	AMENZA	RIESGO	TRATAMIENTO	CONTROLES	ISO/IEC 27001: 2013
SISTEMA DE SEGURIDAD Y CONTROL DE ACCEO						
SSC_SEN	Sensores de movimiento	A, D, E	Normal Normal Normal Normal	CS	A.11	Seguridad física y del entorno
SSC_ALA	Alarma	A, D, E	Normal Normal Alta Alta	CS	A.11	Seguridad física y del entorno
SSC_CAM	Cámaras de seguridad	A, D, E	Normal Normal Alta Normal	CS	A.11	Seguridad física y del entorno
SSC_SBI	Sistema Biométrico	A, D, E	Normal Normal Alta Alta	CS	A.11	Seguridad física y del entorno
SSC_EXT	Extintores	A, D, E	Alta Normal Normal Normal	CS	A.11	Seguridad física y del entorno

Elaborado por el Autor

1 CONCLUSIONES Y RECOMENDACIONES

1.1 Conclusiones

- A medida que la información crece desmenuzablemente y se transporta sin alguna supervisión y mucho menos cuidado, por ende, sin control, las empresas u organizaciones están de acuerdo de apoco en aceptar que la información es hoy por hoy el activo más importante que proteger, es decir, tener una prioridad por encima del resto de activos, esto hará que su información esté garantizada cumpliendo con la confidencialidad, integridad y disponibilidad.
- Durante este proyecto la U.E.P. Séneca se involucró en varias actividades planificadas para su desarrollo, entre ellas se puede mencionar que ahora conocen los tipos de activos que poseen, los riesgos a los que pueden estar expuestos, los controles que pueden ser aplicables según su nivel de riesgo, además de los beneficios que aporta un "SGSI", es importante decir que a través de los análisis diferenciales se obtuvo la información con la que su conoció la situación en la que se encontraba la institución relacionados con la "seguridad de la información".
- Los activos son la parte principal y determinante a la hora de clasificarlos y etiquetarlos, el inventario de activos permite realizar el análisis, evaluación y tratamiento de riesgo donde se determina el nivel que estos tienen y el impacto negativo que podría tener si no tuvieran los controles que según la criticidad de activo estos ayudan a mitigar, trasferir, aceptar o eliminar dicho riesgo.

  De esta manera los beneficios de un "SGSI" son muchos, aunque no es implementado sino más bien un diseño, es una muestra de su eficacia al tratar con recursos tecnológicos y de información, su referente el Laboratorio de Computación que ahora cuenta con políticas para gestionar los activos pertenecientes a la U.E.P. Séneca.

1.2 Recomendaciones

- El propósito de la elaboración de un “SGSI” a través de este proyecto para la U.E.P. Séneca, es la de mostrar las ventajas de su aplicación, sin embargo, depende mucho de las autoridades para que llegue a su implementación y no quede como la propuesta que menciona este proyecto dentro del LABORATORIO DE COMPUTACIÓN. El paradigma y cultura organizacional con respecto al cuidado, responsabilidad y protección hacía los activos de información que posee, debería cambiar con el fin de cumplir objetivos propuestos para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Se recomienda también la capacitación al personal administrativo, docente, estudiantil, etc., sobre los riesgos que se pueden generar cuando se utiliza o manipula recursos de información sin las debidas precauciones para lo cual se entregará las “Políticas de seguridad”, formatos, instructivos y documentos que aporten a una mejor gestión sobre el uso de recursos tecnológicos y de información.
- Se recomienda el seguimiento y monitorización de las “políticas de seguridad de la información” y su cumplimiento, mismas que fueron creadas durante el desarrollo del proyecto, así como también la utilización de los formatos para la solicitud de recursos o servicios de tecnología. También se pone en consideración el asignar roles y responsabilidades acerca del manejo de las Tecnologías de Información, es decir, definir una o más personas que se dediquen especialmente a proteger el área que controla y administra los activos, la red, el servicio de internet, el soporte a los equipos y procesos de seguridad en toda la Unidad Educativa Particular Séneca.

REFERENCIAS BIBLIOGRÁFICAS

039-CG, A. (1 de 12 de 2009). *Desarrollo Amazónica.* Obtenido de http://www.desarrolloamazonico.gob.ec/wp-content/uploads/downloads/2014/05/NORMAS-DE-CONTROL-INTERNO-act.pdf

27000, I. (s.f.). *ISO*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

27000, I. (s.f.). *ISOTools*. Obtenido de https://www.isotools.cl/iso27000/.

27001, I. (7 de enero de 2014). *SGSI*. Obtenido de https://www.pmg-ssi.com/2014/01/proceso-de-implantacion-de-la-iso-27001-en-la-empresa/

27001:2013, I. (6 de abril de 2015). *SGSI*. Obtenido de https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

27001:2013, I. (s.f.). *International Organization for Standarization*. Obtenido de https://www.iso.org/standard/54534.html

27001-2013, I. (29 de 11 de 2015). *SGSI*. Obtenido de https://www.pmg-ssi.com/2015/09/gestion-cambios-sgsi-iso-iec-27001-2013/

27002, I. (s.f.). *iso27001*. Obtenido de http://www.iso27001security.com/html/27002.html.

27003, I. (17 de marzo de 2017). *Webstore.* Obtenido de https://webstore.iec.ch/preview/info_isoiec27003%7Bed2.0%7Den.pdf

27003, I. (s.f.). *iso27001*. Obtenido de http://www.iso27001security.com/html/27003.html

27004, I. (s.f.). *ISO27001Security*. Obtenido de http://www.iso27001security.com/html/27004.html

27005, I. (5 de 1 de 2017). *SGSI*. Obtenido de https://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/

27005, I. (s.f.). *ISO*. Obtenido de https://www.iso.org/standard/56742.html

A. Diaz, G. C. (s.f.). *konradlorenz.* Obtenido de http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf

Acevedo, H. (16 de junio de 2016). *Megazcitum*. Obtenido de http://www.magazcitum.com.mx/?p=50#.W53E3-hKjIU

Activa, C. (s.f.). *ActivaConocimiento*. Obtenido de http://activaconocimiento.es/matriz-probabilidad-impacto/

Advisera. (s.f.). *Advisera*. Obtenido de https://advisera.com/27001academy/es/que-es-iso-27001/

AENOR. (11 de 2014). *AENOR*. Obtenido de http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0053758#.WxaVfCAh29g

Alvarez A, G. L. (2012). *GUIA DE APLICACION DE LA NORMA UNE-ISO/IEC 27001 SOBRE SEGURIDAD EN SISTEMAS DE INFORMACION PARA PYMES.* Madrid: AENOR. ASOCIACION ESPAÑOLA DE NORMALIZACION Y CERTIFICACION.

BSI. (2018). *BSIgroup.* Obtenido de https://www.bsigroup.com/es-ES/ISO-31000-Gestion-de-Riesgos/

BSi, G. (s, f). *Holland, H.* Obtenido de https://www.bsigroup.com/LocalFiles/fr-fr/iso-iec-27001/ressources/BSI%20GROUP%20-%20ISO%2027001%20Implementation%20Guide.compressed.pdf

Buigues, M. J. (18 de 6 de 2015). *SlideShare*. Obtenido de https://es.slideshare.net/mariajosebuigues3/iso-27001-interpretacin-introduccin

Bustamante, G. &. (2014). *Cuaderno Activa.* Obtenido de http://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/202/206

Corporativo, B. (12 de abril de 2016). *ISOTools*. Obtenido de https://www.isotools.com.co/iso-27001-evaluacion-tratamiento-riesgos-6-pasos/

DerechoEcuador. (07 de febrero de 2011). Obtenido de https://www.derechoecuador.com/la-proteccion-de-datos-personales

Descalzo, F. (3 de 5 de 2014). *SlideShare*. Obtenido de https://es.slideshare.net/fabiandescalzo/270012013-seguridad-orientada-al-negocio

Editor. (10 de septiembre de 2010). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/

ENS. (octubre de 2012). *PAe.* Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?comentarioContenido=0#.W6BQrOhKjIU

EPPS. (02 de septiembre de 2014). *27001Academy*. Obtenido de http://info.advisera.com/hubfs/27001Academy/27001Academy_FreeDownloads/ES/Checklist_of_ISO_27001_Mandatory_Documentation_ES.pdf?t=1532726512471

Estéfano, D. (2017). El Comercio. *El 2017, un año de grandes 'hackeos'*, págs. El 2017, un año de grandes 'hackeos'.

Finder, L. (s.f.). *Política.* Obtenido de http://www.politica.gob.ec/wp-content/uploads/2017/04/EGSI.pdf

Franck, S. (28 de Mayo de 2013). *metadirectorio.* Obtenido de http://metadirectorio.org/bitstream/10983/866/2/Mantenimiento%20y%20Actualizacion%20de%20un%20sistema%20de%20gestion%20de%20seguridad%20de%20la%20informacion%20para%20ventas.pdf

Gómez, F. &. (2007). *Repositorio Institucional UNI.* Obtenido de http://cybertesis.uni.edu.pe/handle/uni/9764

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

IEC. (s.f.). *International Electrotechhnical Commission*. Obtenido de http://www.electropedia.org/iev/iev.nsf/index?openform&part=903

INCIBE. (20 de marzo de 2017). *Instituto Nacional de Ciberseguridad*. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Informatik. (s.f.). *Informatica2k*. Obtenido de http://www.informatica2k.com/cuestionario-seguridad-informatica-empresa.html

ISO. (10 de 2013). *Standardization, International Organization*. Obtenido de https://www.iso.org/standard/54533.html

Iso 27001, N. (8 de febrero de 2012). *Normas ISO y Preguntas frecuentes*. Obtenido de http://www.normas-iso.com/implantando-iso-27001/

ISO 27001:2013, S. (13 de abril de 2015). *SGSI*. Obtenido de https://www.pmg-ssi.com/2015/04/iso-27001-el-impacto-en-los-sistemas-de-gestion-de-seguridad-de-la-informacion/

ISO 27001:2013, S. (30 de marzo de 2015). *SGSI*. Obtenido de https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/

ISO, 2. (21 de enero de 2015). *IsoTools*. Obtenido de https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

ISO/IEC. (6 de 1 de 2011). *ISO.* Obtenido de http://mahdi.hashemitabar.com/cms/images/Download/ISO/iso-iec-27005-2011-english.pdf

ISO/IEC, 2. (01 de junio de 2011). *Mahdi.hashemitabar.* Obtenido de http://mahdi.hashemitabar.com/cms/images/Download/ISO/iso-iec-27005-2011-english.pdf

ISOTools. (20 de 1 de 2016). *ISOTools Excellence*. Obtenido de https://www.isotools.com.co/como-se-gestionan-los-cambios-segun-la-iso-27001/

ISOwin. (s.f.). *ISOWIN*. Obtenido de https://isowin.org/blog/amenazas-ISO-27001/

Izquierdo, S. (s.f.). *Colegio Séneca*. Obtenido de http://www.seneca.edu.ec/nosotros.html

J, S. (27 de enero de 2012). *Pegasus.* Obtenido de http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf

Jurídico. (s.f.). *OAS*. Obtenido de https://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf

Martin, M. R.-J. (2013). *Practical Assessment Through Data Collection and Analysis.* Obtenido de http://31.210.87.4/ebook/pdf/Information_Security_Risk_Assessment_Toolkit.pdf

Martínez, E. (3 de SEPTIEMBRE de 2015). *ISO 27000*. Obtenido de https://prezi.com/-80aj_hsfban/estructura-norma-iso-27000/

Maya, J. (9 de 8 de 2009). *Mailmax*. Obtenido de http://www.mailxmail.com/curso-comunicacion-informatica-historia-computacion/concepto-160-informacion-160-informatica

Mifsud, E. (26 de marzo de 2012). *Observatorio Tecnológico.* Obtenido de http://recursostic.educacion.es/observatorio/web/en/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

Namakforoosh. (2005). *Metodología de la Investigación.* México: https://books.google.es/books?hl=es&lr=&id=ZEJ7-0hmvhwC&oi=fnd&pg=PA219&dq=metodologia+de+investigacion&ots=i05zxUN84X&sig=yaaM4TRiqhNU9CVvPt-9HdeaV6M#v=onepage&q=metodologia%20de%20investigacion&f=false.

Nieto, J. P. (06 de junio de 2013). *Openaccess.* Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23054/1/Nieto_WP2013_PlanImplementacionISO2007.pdf

Noticias, C. (04 de abril de 2017). *Noticias Universidad Costa Rica*. Obtenido de http://noticias.universia.cr/educacion/noticia/2017/09/04/1155475/tipos-investigacion-descriptiva-exploratoria-explicativa.html.

NTC. (09 de diciembre de 2014). *Coursehero.* Obtenido de https://vdocuments.mx/iso-27005-558464a15252c.html

P, A. (s.f). *Seguridad Informática.* Madrid: Editex S.A.

Pascual, I. (2013). *UPM.* Obtenido de http://oa.upm.es/22176/1/PFC_IVAN_MATEOS_PASCUAL.pdf

PCWorld. (30 de 11 de 2014). *Los 10 principales riesgos de seguridad TI de las empresas españolas*. Obtenido de https://www.pcworld.es/articulos/seguridad/los-10-principales-riesgos-de-seguridad-ti-de-las-empresas-espanolas-392679/

PMG. (29 de SEPTIEMBRE de 2015). *SGSI.* Obtenido de https://www.pmg-ssi.com/2015/09/gestion-cambios-sgsi-iso-iec-27001-2013/

PMG. (04 de junio de 2015). *SGSI.* Obtenido de https://www.pmg-ssi.com/2015/06/iso-27001-ciclo-de-deming

PMG. (6 de julio de 2017). *ISO/IEC 27001: 2013*. Obtenido de https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

PMG, S. (13 de abril de 2015). Obtenido de SGSI: https://www.pmg-ssi.com/2015/04/iso-27001-el-impacto-en-los-sistemas-de-gestion-de-seguridad-de-la-informacion/

PMG, S. (13 de abril de 2015). *SGSI.* Obtenido de https://www.pmg-ssi.com/2015/04/iso-27001-el-impacto-en-los-sistemas-de-gestion-de-seguridad-de-la-informacion/

Pmg-ssi. (1 de febrero de 2018). *SGSI.* Obtenido de https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

PriteshGupta.com. (2005). *ISO 27000.es*. Obtenido de http://www.iso27000.es/iso27000.html

Sampedro, M. (27 de octubre de 2009). *Gestiopolis.* Obtenido de https://www.gestiopolis.com/riesgos-sistemas-informacion-iso-27005-vs-magerit-otras-metodologias/

Seneca. (2017). *Colegio Séneca*. Obtenido de http://www.seneca.edu.ec/index.html

Séneca, C. (s.f.). *Séneca*. Obtenido de http://www.seneca.edu.ec/quienes-somos/.

Serman. (22 de 10 de 2013). *Serman Recuperación de datos*. Obtenido de https://serman.com/blog-recuperacion-datos/que-es-el-ciclo-de-vida-de-la-informacion/

Sosa, J. (27 de enero de 2012). *Pegasus Javeriana.* Obtenido de http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf

Soto, D. (27 de septiembre de 2016). *Nextech.* Obtenido de https://nextech.pe/que-es-cobit-y-para-que-sirve/

Trentalance, J. I. (2009-2012). *Porto y Asociados.* Obtenido de http://www.portoyasociados.com.ar/manual_seginf_episodio1.pdf

Valenzuela, A. (6 de marzo de 2017). *SlideShare.* Obtenido de https://es.slideshare.net/ALEXMARIOVALENZUELA/leyes-en-ecuador-y-seguridad-informatica

ANEXOS A (Cuestionarios)

Cuestionario 1.

CUESTIONARIO GENERAL SOBRE LA SEGURIDAD DE LA INFORMACION

A NIVEL GENERAL

Nombre y cargo del entrevistado: Christian Bedoya / Coordinador

Dirección: Paseo de la Universidad y Juan Díaz

Fecha de inicio: 2018-06-12 Fecha de finalización: 2018-06-13

Nombre del entrevistador: Marco Bonilla

Objetivo: Obtener información general acerca de la seguridad de la información en la institución.

1 Seguridad General

¿La empresa tiene una solución de seguridad perimetral -un firewall- dentro o fuera de las instalaciones?	☐	Sí	☐	No	☐	n/s	
Los ordenadores de su empresa, ¿tienen instalado antivirus?	☐	Sí	☒	No	☐	n/s	
El antivirus que tienen instalado (si es el caso), ¿está actualizado con las últimas definiciones?	☐	Sí	☒	No	☐	n/s	
¿Se realiza un mantenimiento informático periódico sobre los ordenadores de la empresa?	☐	Sí	☒	No	☐	n/s	
¿La seguridad en los passwords de los usuarios cumple requisitos mínimos (combinación de mayúsculas, minúsculas, símbolos, etc.)?	☐	Sí	☒	No	☐	n/s	
¿De cuántos ordenadores dispone su empresa?	☐	1-20	☒	20-40	☐	+40	
¿Disponen de servidor central de datos en su empresa?	☒	Sí	☐	No			
Sobre dicho servidor, ¿se realiza un mantenimiento informático periódico?	☐	Sí	☒	No	☐	n/s	
¿Los datos empresariales están cubiertos por una copia de seguridad robusta y administrada regularmente?	☐	Sí	☒	No	☐	n/s	

¿En su empresa se trabaja desde algún ordenador externo, por conexión vía Internet?	☐ Sí	☐ No	☐ n/s
La web institucional, ¿cumple con las características de seguridad de su empresa (incluyendo la LOPD)?	☐ Sí	☐ No	☐ n/s
Si su empresa tiene conexión con cables, ¿utiliza las medidas de seguridad pertinentes para proteger dicha conexión (canaletas, etiquetas?	☐ Sí	☐ No	☐ n/s
Si su empresa tiene conexión sin cables (WIFI), ¿utiliza las medidas de seguridad pertinentes para proteger dicha conexión?	☐ Sí	☐ No	☐ n/s

3 Datos de la institución

¿Los ordenadores de trabajo tienen datos de la empresa almacenados dentro de su disco duro?	☐ Sí	☐ No	☐ n/s
¿Se realiza copia de seguridad de los datos de la empresa?	☐ Sí	☐ No	☐ n/s
En caso de que se realice copia de seguridad, con qué frecuencia	☐ diaria	☐ semanal	☐ otro
¿Dispone de alguna copia de seguridad (CD / DVD /, otro) fuera de la empresa?	☐ Sí	☐ No	☐ n/s
¿Se realiza un mantenimiento de las copias de seguridad de la empresa?	☐ Sí	☐ No	☐ n/s

5 Programas y Aplicaciones Informáticas

¿Los programas que se utilizan en su empresa, que almacenan datos, cumplen con las características de seguridad de su empresa (incluyendo la LOPD)?	☐ Sí	☒ No	☐ n/s
¿Algún técnico es el encargado de instalar/desinstalar los programas y aplicaciones informáticas en su empresa?	☐ Sí	☒ No	☐ n/s

6 Seguridad y control de acceso

¿Dispone de algún tipo de control de acceso en su institución)?	☐ Sí	☒ No	
En caso de si. ¿Este funciona apropiadamente?	☐ Sí	☒ No	☐ n/s
Hay algún responsable de administrar y dar mantenimiento al control	☐ Sí	☒ No	
¿Aparte de ese control tiene otro, el mismo que controla al personal de la institución?	☒ Sí	☐ No	☐ n/s
¿En la institución existe segregación de funciones para cada área?	☐ Sí	☒ No	

Ing. Christian Bedoya

CHRISTIAN BEDOYA

12 JUN 2018

REVISADO

COORDINADOR BI

Cuestionario 2.

CUESTIONARIO ACERCA DE LA RED

(INVENTARIO Y MANTENIMIENTO)

Nombre de la institución: Colegio Sinco

Dirección: URB. Iñaquito Alto.

Fecha de inicio: 11/06/2018 Fecha de finalización: 11/06/2018.

Nombre del entrevistador: Marco Bonilla.

Objetivo: Obtener datos específicos de la realización de mantenimiento e inventario de los recursos de tecnología de la institución.

1. ¿Tienen alguna bodega donde mantengan equipos viejos o nuevos? ¿Qué hacen con los equipos dañados?
   si
2. ¿Tienen algún plan en caso de que algún equipo no funcione correctamente?
   no
3. ¿Tienen algún tipo de acuerdo con alguna compañía distribuidora de equipos de informática?
   si
4. ¿Cuál es su ISP (Internet Service Provider)? ¿Por qué lo eligieron?
   netlife /
   ¿Hace cuánto tiempo trabajan con él?
   4 - 5 años
   ¿Miden la velocidad de transferencia de datos?
   no
   ¿Es la misma que el ISP (Internet Service Provider) estipula en el contrato?
   no sé
5. ¿Ha tenido problemas con la red?
   a veces.
6. ¿El proveedor alguna vez ha faltado a lo estipulado en el contrato?
   no.
7. ¿Cada cuánto renuevan contrato con él?
   c/ año.
8. ¿Cuáles fueron los criterios para adquirir los equipos de telecomunicaciones (red)?
   no sé
9. ¿Qué seguridad emplean para estos equipos?
   no se
10. ¿Hay planes de ponerles más seguridad en el futuro?
    si

14. ¿Poseen los manuales de usuario, documentación final y código de los sistemas adquiridos?

no sé

15. ¿Cuenta la empresa con las respectivas licencias y facturación del Software adquirido? (S.O, sistemas de aduana, Antivirus, etc.)

Si

16. ¿Está debidamente actualizado el software actual?

no

17. ¿Quién le proporciona los servicios de mantenimiento al software? ¿Una empresa externa o una persona interna?

persona interna.

18. ¿Las personas usuarias de los sistemas, tienen acceso a Internet libremente? O ¿utilizan los equipos únicamente para interactuar con el sistema que trabajan?

unicamente para interactuar.

19. ¿Con qué frecuencia de tiempo se le brinda mantenimiento al software?

Cada:

- 3 meses
- 6 eses
- Anualmente

20. ¿Existe algún registro de los mantenimientos que se realiza a los equipos?

no.

UNIDAD EDUCATIVA PARTICULAR SÉNECA ADMINISTRACIÓN

Cuestionario 3.

CUESTIONARIO SEGURIDAD FISICA

Nombre y cargo del entrevistado: Maria Arias Recepcionista

Dirección: Urb. Inaquito Alto

Fecha de inicio: 13/06/2018 Fecha de finalización: 13/06/2018

Nombre del entrevistador: Marco Bonilla.

Objetivo: Obtener información sobre la seguridad física en la institución para determinar los controles de acceso.

1. ¿Se han adoptado medidas de seguridad en la dirección de informática?
   Si
2. ¿Existe una persona responsable de la seguridad informática?
   Si
3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?
   No
4. ¿Existe personal de vigilancia en la institución?
   Si
5. ¿La vigilancia se contrata:
   a) Directamente ____
   b) Por medio de empresas que venden ese servicio X
6. ¿Se investiga a los vigilantes cuando son contratados directamente?
   No se
7. ¿Se controla el trabajo fuera del horario?
   No
8. ¿Existe vigilancia en la entrada a la institución durante las horas de trabajo?
   No
9. ¿Para registrar el ingreso a la instalación por parte del personal docente existe:
   a) lector biométrico X
   b) Libro de ingreso ____
   c) Tarjeta de control de acceso ____
   d) Nada ____
10. ¿Para controlar el ingreso de personal externo a la institución existe:
    a) Guardia ____
    b) Recepcionista X
    c) Tarjeta de control de acceso ____
    d) Nadie ____

12. ¿El lugar donde se encuentra el servidor está situado a salvo de:
    a) Inundación _____
    b) Terremotos _____
    c) Fuego _____
    d) Sabotaje ___X___
13. . ¿Existe alarma para:
    a) Detectar fuego /calor o humo) en forma automática _____
    b) Avisar en forma manual la presencia del fuego _____
    c) Detectar una fuga de agua _____
    d) Detectar magnetos _____
    e) No existe ___X___
14. ¿Esta alarma también está conectada?
    a) Al puesto de guardias _____
    b) A la estación de bomberos _____
    c) A ningún otro lado _____
    d) Otro _____

15. ¿Existen extintores de fuego?
    a) Manuales ___X___
    b) Automáticos _____
    c) No existen _____
16. ¿Se ha adiestrado el personal en el manejo de los extintores?
    Si
17. ¿Los extintores, manuales o automáticos a base de:
    a) Agua _____
    b) Gas _____
    c) Otros ___X___
18. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?
    Nota: Verifique el número de extintores y su estado.
    6 (bien)
19. Si es que existen extintores automáticos, ¿son activados por los detectores automáticos de fuego?
    ___
20. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?

COLEGIO SENECA
SECRETARIA

Cuestionario 4.

CUESTIONARIO ADMINISTRACION

Nombre de la institución: Colegio Séneca.

Dirección: ORB Tarquito Alto

Fecha de inicio: 08/06/2018 Fecha de finalización: 08/06/2018

Nombre del entrevistador: Marco Bonilla.

Objetivos: Recolectar información general y específica sobre los diferentes aspectos sobre cómo se maneja TI en la institución.

Obtener información crítica de los procesos informáticos que se manejan en el área de operaciones.

1. ¿Conoce lo que es TI?
   no
2. ¿Cuánto invierten en TI al año?
   3.000,00.
3. ¿Qué tan importante ha sido esa inversión? ¿Han sacado provecho de la inversión?
   Si
4. ¿Tienen planes futuros para TI?
   no sé
5. ¿Tienen algún manual interno para el manejo de TI (uso de PC, de software, hardware)?
   no
6. ¿Piden reportes del uso de TI? ¿Qué tan seguido?
   no
7. ¿Cómo controlan las TI en la empresa?
   Jefe de computación.
8. ¿Tienen respaldo de la información de sus clientes? ¿En qué manejan la información de sus clientes?
   Si
9. ¿Tienen algún plan para restablecer las operaciones si algo llegara a fallar?
   no
10. ¿Conoce lo qué es software libre? (Si usan software libre) ¿Cuál usan?
    Si
11. ¿Qué tipo de software usan (libre o con licencia)? (Si usan software con licencia) ¿Compraron la licencia?
    licencia. / Si compramos.
12. ¿Por qué usan ese software?
    Por que tiene seguridad y brindan soporte
13. ¿Tienen algún respaldo energético?
    no
14. ¿Alguna vez han experimentado fallas graves (no funcionan los sistemas o la red)? ¿Qué hacen en esos casos?
    Si / no sé
15. ¿Tienen una guía para casos como los antes mencionados?
    no
16. ¿Cuántas personas tienen acceso a las PC? ¿Cómo se identifican?

todos tenemos con usuarios.

17. ¿Qué tan capacitados están en el manejo de las redes (Solución de problemas)?
no mucho.

18. ¿Los equipos de telecomunicación son administrables? ¿Tienen contraseña? ¿Quién las maneja?
sí / sí / jefe computación.

19. ¿Cuánta gente tiene acceso a ellos? ¿Cómo se identifican?
solo computación.

20. ¿Cuál es el uso diario que le dan a los equipos?
Control de tiempo.

21. Si tiene WIFI
¿Quiénes tienen acceso al mismo? Solo computación.
¿Por qué? seguridad.
¿Cuáles son los requisitos para tener acceso? ser administrados.
¿Qué tipo de seguridad tiene? básica.

22. ¿Alguna vez han tratado de hacer la red? Si ha pasado ¿Qué hacen para evitarlo?
sí / contratamos a un tercero.

23. ¿Tienen algún manual o plan en caso de falla de la red en medio de operaciones importante?
no

24. ¿Quién toma las decisiones para modificar la red?
administración

25. ¿Tiene problemas relacionados al congestionamiento de la información?
no

26. ¿Cada persona tiene una cuenta para iniciar sesión en las máquinas o no?
sí

27. ¿En el sistema que utilizan estos tienen usuario y password? ¿Alguna vez han tenido problemas en el sistema al momento de ingresar datos? ¿Qué hacen en casos como estos?
sí / no tenemos problemas.

28. ¿Permiten que los usuarios inserten memorias USB a los equipos? O ¿deben pedir permiso? O ¿no está autorizado?
sí

29. El control de la información que se procesa en el sistema ¿se almacena en algún tipo de base de datos?
¿En qué software almacenan estos datos? (Excel, SQL, Access)
sí SQL

30. ¿Poseen un respaldo o replica de los datos que almacenan en caso de que pueda suceder cualquier percance en otro servidor para poder recuperarlos?
sí

31. ¿Poseen los usuarios del sistema restricciones en el uso del sistema operativo? Es decir, ¿se les permite hacer todo o no?
sí poseen.

32. ¿Cada cuánto se actualizan el nivel de los sistemas operativos y en que se basa esa decisión?
6 meses – 1 año

UNIDAD EDUCATIVA PARTICULAR SÉNECA ADMINISTRACIÓN

ANEXO B (Análisis de brecha)
ANÁLISIS DE BRECHA ISO 27001

ISO/IEC 27001 Análisis referencial			
Numeral	**Dominio o descripción**	**Cumplimiento**	**No cumple**
4.1	Contexto de la Organización	**1,00**	**4,00**
4.2	Comprensión de las necesidades y expectativas de las partes interesadas.	2,00	3,00
4.3	Determinación del alcance del "SGSI".	1,00	4,00
4.4	Sistema de la Gestión de la Seguridad.	0,00	5,00
5	**Liderazgo**	**1,67**	**3,33**
5.1	Liderazgo y compromiso	3,00	2,00
5.2	Política	0,00	5,00
5.3	Roles organizacionales, responsabilidades y autoridades.	2,00	3,00
6	**Planificación**	**0,25**	**4,75**
6.1.1	Generalidades	1,00	4,00
6.1.2	Evaluación de riesgos de seguridad de la información.	0,00	5,00
6.1.3	Tratamiento de los riesgos de seguridad	0,00	5,00
6.2	Objetivos de seguridad de información y la planificación para alcanzarlos.	0,00	5,00
7	**Soporte**	**1,63**	**3,38**
7.1	Recursos	3,00	2,00
7.2	Competencia	2,00	3,00
7.3	Conciencia	2,00	3,00
7.4	Comunicación	2,00	3,00
7.5	Información documentada	1,00	4,00
7.5.1	Generalidades	1,00	4,00
7.5.2	Creación y actualización	1,00	4,00
7.5.3	Control de la información documentada	1,00	4,00
8	**Operación**	**0,00**	**5,00**
8.1	Planificación y control operacional	0,00	5,00
8.2	Información de riesgos de seguridad	0,00	5,00
8.3	Tratamiento de riesgos de seguridad de la información	0,00	5,00
9	**Evaluación y desempeño**	**0,00**	**5,00**
9.1	Medición, análisis y evaluación	0,00	5,00
9.2	Auditoria interna	0,00	5,00
9.3	Revisión de gestión	0,00	5,00

10	**Mejora**	**1,00**	**4,00**
10.1	La no conformidad y acciones correctivas	1,00	4,00
10.2	Mejora continua	1,00	4,00

ANÁLISIS DE BRECHA ISO 27002 Y ANEXO A ISO 27001

Anexo A: ISO 27002: 2013 Análisis de brecha			
Numeral	**Dominio o descripción**	**Cumplimiento**	**No cumple**
A.5	Políticas de seguridad	**0,00**	**100,00**
A.5.1	Directrices de la dirección en seguridad de la información	0,00	
A.5.1.1	Documento de la política de seguridad de la información.	0	
A.5.1.2	Revisión de la política de seguridad de la información.	0	
A.6	Aspectos organizativos de la seguridad de la información	**20,00**	**80,00**
A.6.1	Organización interna	**1,00**	
A.6.1.1	Asignación de responsabilidades para la seguridad de la información.	1	
A.6.1.2	Segregación de tareas	2	
A.6.1.3	Contacto con las autoridades	2	
A.6.1.4	Contactos con grupos de interés especial	0	
A.6.1.5	Seguridad de la información en la gestión de proyectos	0	
A.7	Seguridad ligada a los recursos humanos	**53,33**	**46,67**
A.7.1	Antes de la contratación	**2,67**	
A.7.1.1	Investigación de antecedentes	3	
A.7.1.2	Términos y condiciones de contratación	3	
A.7.2	Uso aceptable de los activos	2	
A.7.2	Durante la contratación	**1,00**	
A.7.2.1	Directrices de clasificación	1	
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	1	
A.7.2.3	Proceso disciplinario	1	
A.7.3	Cese o cambio de puesto de trabajo	**1,00**	
A.7.3.1	Cese o cambio de puesto de trabajo	1	
A.8	Gestión de activos	**25,00**	**75,00**
A.8.1	Responsabilidades sobre los activos	**1,25**	
A.8.1.1	Inventario de activos	1	

A.8.1.2	Propiedad de los activos	1	
A.8.1.3	Uso aceptable de los activos	2	
A.8.3.4	Devolución de activos	1	
A.8.2	Clasificación de la información	**1,00**	
A.8.2.1	Directrices de clasificación	0	
A.8.2.2	Etiquetado y manipulación de la información	1	
A.8.2.3	Manipulación de activos	2	
A.9	Control de accesos	**20,00**	**80,00**
A.9.1	Requisito de negocio para el control de accesos	**1,00**	
A.9.1.1	Política de control de acceso	0	
A.9.1.2	Control de acceso a las redes y servicios asociados	2	
A.9.2	Gestión de acceso de usuario	**0,83**	
A.9.2.1	Gestión de altas y bajas en el registro de usuario	0	
A.9.2.2	Gestión de los derechos de acceso asignado a usuarios	1	
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	1	
A.9.2.4	Gestión de información confidencial de autenticación de usuarios	1	
A.9.2.5	Revisión de los derechos de acceso de los usuarios	1	
A.9.2.6	Retirada o adaptación de los derechos de acceso	1	
A.9.3	Responsabilidades del usuario	**0,90**	
A.9.3.1	Uso de la información confidencial	1	
A.9.4	Control de acceso a sistemas y aplicaciones	**0,80**	
A.9.4.1	Restricción de acceso a la información	2	
A.9.4.2	Procedimientos seguros de inicio de sesión	1	
A.9.4.3	Gestión de contraseñas de usuario	1	
A.9.4.4	Uso de herramientas de administración de sistemas	0	
A.9.4.5	Control de acceso al código fuente de los programas	0	
A.10	Cifrado	**0,00**	**100,00**
A.10.1	Controles criptográficos	0,00	
A.10.1.1	Política de uso de los controles criptográficos	0	
A.10.1.2	Gestión de claves	0	
A.11	Seguridad física y ambiental	**53,33**	**46,67**
A.11.1	Áreas seguras	2,67	
A.11.1.1	Perímetro de seguridad física	3	
A.11.1.2	Controles físicos de entrada	2	
A.11.1.3	Seguridad de oficinas, despachos y recursos	3	
A.11.1.4	Protección contra las amenazas externas y ambientales	3	
A.11.1.5	El trabajo en áreas seguras	3	
A.11.1.6	Áreas de acceso público, carga y descarga	2	
A.11.2	Seguridad de los equipos	2,00	

A.11.2.1	Protección de equipos	2	
A.11.2.2	Instalaciones de suministro	2	
A.11.2.3	Seguridad de cableado	3	
A.11.2.4	Mantenimiento de los equipos	4	
A.11.2.5	Salida de activos fuera de la institución	1	
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	1	
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	2	
A.11.2.8	Equipo informático de usuario desatendido	1	
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	2	
A.12	Seguridad en la operativa	**0,00**	**100,00**
A.12.1	Responsabilidades y procedimientos de operación	**0,00**	
A.12.1.1	Documentación de procedimientos de operación	0	
A.12.1.2	Gestión de cambios	0	
A.12.1.3	Gestión de capacidades	0	
A.12.1.4	Separación de entornos de desarrollo	0	
A.12.2	Protección contra código malicioso	**3,00**	
A.12.2.1	Controles contra el código malicioso	3	
A.12.3	Copias de seguridad	**0,50**	
A.12.3.1	Copias de seguridad de la información	2	
A.12.4	Registro de actividad y supervisión	**0,00**	
A.12.4.1	Registro y gestión de eventos de actividad	0	
A.12.4.2	Protección de los registros de información	0	
A.12.4.3	Registros de actividad del administrador y operador del sistema	0	
A.12.4.4	Sincronización de relojes	0	
A.12.5	Control del software en explotación	**3,00**	
A.12.5.1	Instalación del software en sistemas en producción	3	
A.12.6	Gestión de la vulnerabilidad técnica	**2,00**	
A.12.6.1	Gestión de las vulnerabilidades técnicas	1	
A.12.6.2	Restricciones a la instalación de software	3	
A.12.7	Consideraciones de las auditorias de los sistemas de información	0,00	
A.12.7.1	Controles de auditoria de los sistemas de información	0	
A.13	Seguridad en las telecomunicaciones	**86,67**	**13,33**
A.13.1	Gestión en la seguridad en las redes	**4,33**	
A.13.1.1	Control de la red	4	
A.13.1.2	Mecanismos de seguridad asociados al servicio de red	4	
A.13.1.3	Segregación de redes	5	
A.13.2	Intercambio de información con partes externas	**0,00**	

A.13.2.1	Políticas y procedimientos de intercambio de información	0	
A.13.2.2	Acuerdos de intercambio	0	
A.13.2.3	Mensajería electrónica	0	
A.13.2.4	Acuerdos de confidencialidad y secreto	0	
A.14	Adquisición, desarrollo y mantenimiento de los sistemas de información	**6,67**	**93,33**
A.14.1	Requisitos de seguridad de los sistemas de información	**0,33**	
A.14.1.1	Análisis y especificación de los requisitos de seguridad	1	
A.14.1.2	Seguridad de las telecomunicaciones en servicios accesibles por redes públicas	0	
A.14.1.3	Protección de las transacciones por redes telemáticas	0	
A.14.2	Seguridad de los procesos de desarrollos y soporte	**0,00**	
A.14.2.1	Política de desarrollo seguro de software	0	
A.14.2.2	Procedimientos de control de cambios en los sistemas	0	
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	0	
A.14.2.4	Restricciones a los cambios en los paquetes de software	0	
A.14.2.5	Uso de principios de ingeniería en protección de sistemas	0	
A.14.2.6	Seguridad en entornos de desarrollo	0	
A.14.2.7	Externalización del desarrollo del software	0	
A.14.2.8	Prueba de funcionalidad durante el desarrollo de los sistemas	0	
A.14.2.9	Pruebas de aceptación	0	
A.14.3	Datos de prueba	**0,00**	
A.14.3.1	Protección de los datos utilizados en pruebas	0	
A.15	Relaciones con suministradores	**0,00**	**100,00**
A.15.1	Seguridad de la información en las relaciones con suministradores	**0,00**	
A.15.1.1	Política de seguridad de la información para suministradores	0	
A.15.1.2	Tratamiento de riesgo dentro de acuerdo de suministradores	0	
A.15.1.3	Cadena de suministro en tecnología de información y comunicación	0	
A.15.2	Gestión de la prestación del servicio por suministradores	**2,00**	
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros	2	
A.15.2.2	Gestión de cambios en los servicios prestados por terceros	2	
A.16	Gestión de incidentes en la seguridad de la información	**5,71**	**94,29**
A.16.1	Gestión de incidentes de seguridad de la información y mejoras	**0,29**	

A.16.1.1	Responsabilidades y procedimientos	1	
A.16.1.2	Notificación de los eventos de seguridad de la información	1	
A.16.1.3	Notificación de puntos débiles de la seguridad	0	
A.16.1.4	Valoración de eventos de la seguridad de la información y toma de decisiones	0	
A.16.1.5	Respuesta a los incidentes de seguridad	0	
A.16.1.6	Aprendizaje de los incidentes de seguridad de información	0	
A.16.1.7	Recopilación de evidencias	0	
A.17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio	**0,00**	**100,00**
A.17.1	Continuidad de la seguridad de la información	**0,00**	
A.17.1.1	Planificación de la continuidad de la seguridad de la información	0	
A.17.1.2	Implantación de la continuidad de la seguridad de la información	0	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	0	
A.17.2	Redundancias	**0,00**	
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	0	
A.18	Cumplimiento	**28,00**	**72,00**
A.18.1	Cumplimiento de los requisitos legales y contractuales	**1,40**	
A.18.1.1	Identificación de la legislación aplicable	1	
A.18.1.2	Derechos de propiedad intelectual (DPI)	1	
A.18.1.3	Protección de los registros de la organización	2	
A.18.1.4	Protección de los datos y privacidad de la información personal	3	
A.18.1.5	Regulación de los controles criptográficos	0	
A.18.2	Revisiones de la seguridad de la información	**1,67**	
A.18.2.1	Revisión independiente de la seguridad de la información	4	
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	1	
A.18.2.3	Comprobación del cumplimiento	0	

ANEXO C (Políticas)
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

	POLÍTICAS DE SEGURIDAD GENERAL	Código: P-PSI-ADM-01
		Fecha:
		Versión: 01
		Nivel:
Elaborado por: _____	Aprobado por: _____	

La U.E.P Séneca reconoce que el activo más importante es la *información* por lo que se comprometerá a mantener de forma segura de acuerdo con su valoración y sensibilidad del lugar o medio que se encuentre, a continuación, se detalla algunas de las políticas a nivel general.

- Todo recurso y servicio de tecnología suministrada por la institución al personal docente, deberá ser estrictamente para uso de actividades académicas.
- Es responsabilidad de la institución garantizar los recursos materiales y humanos que son necesarios para su mantenimiento o actualización de recursos o servicios tecnológicos.
- La asignación de recursos de tecnología e información asignados al personal docente estará sujeta a la aprobación del área de administración y el LABORATORIO DE COMPUTACIÓN.
- La asignación de recursos de tecnología estará sujeta de acuerdo con la disponibilidad y capacidad con la que cuenta la institución.
- Se negará o restringirá la asignación de recursos de tecnología e información a personas ajenas a la institución sin una autorización escrita por parte del área administrativa.
- Los usuarios (personal docente) que utiliza los recursos tecnológicos serán los responsables del uso correcto, mismo que debe ser ético, moderado y legal.
- Para el acceso a los equipos informáticos con programas bajo licencia legal, el docente debe tener la responsabilidad de tener un usuario y contraseña designada para su uso personal.
- Todos los equipos deberán disponer de una licencia legal del *software* de ofimática (Word, Excel, PowerPoint) que permita su uso adecuado.
- Los servicios y recursos de tecnología deberán estar administrados por la persona responsable o encargada del LABORATORIO DE COMPUTACIÓN, mismo que estará autorizado para: instalar, configurar, modificar y actualizar los sistemas alineándose a las Políticas de la U.E.P Séneca.

Para los servicios de tecnología e información que presta a la U.E.P. Séneca se tomarán las siguientes consideraciones:

Usuario (docente)

- Es del docente la responsabilidad solicitar de forma individual el usuario y contraseña para utilizar los recursos en la institución.
- Para solicitar un servicio o recurso, el usuario (docente) deberá hacerlo con el formato designado para esta actividad y en caso de no cumplirse esto, dicha solicitud será rechazada.
- El usuario (docente) debe estar sometido a los acuerdos, formatos o instructivos de compromisos según el servicio o recurso a solicitar.

Administrador

- El Laboratorio de Computación es el área que administra los accesos a los equipos informáticos y servicios de internet en la U.E.P. Séneca.
- En el uso de los equipos y servicios de internet los usuarios deben solicitar el formato designado y tener la responsabilidad del o los recursos.
- Con la finalidad de proteger los activos de información y tecnología, en caso de requerir algún programa o innovar el mismo, se deberá realizar pruebas y así evitar cualquier efecto negativo sobre dichos activos.
- Para controlar y llevar un registro del uso de los equipos por parte del personal docente, se debe utilizar los formatos elaborados para la gestión y beneficio de la U.E.P. Séneca.

Tabla 89. "Políticas de seguridad" de los activos de información.
Elaborado por el Autor

	POLÍTICAS DE SEGURIDAD DE LA ADMINISTRACIÓN DE USUARIOS DE LOS SISTEMAS DE INFORMACIÓN	Código: P-AUS-ADM-02
		Fecha:
		Versión: 01
		Nivel:
Elaborado por: _____	Aprobado por: _____	

Política en la que define la administración de usuarios y la creación de cuenta y contraseñas para el ingreso autorizado a los activos de tecnología e información.

- **Administrar privilegios a usuarios.**

  - Los equipos de la institución que se encuentran en las oficinas deberán tener acceso solo quienes posean una cuenta y contraseña con privilegios de administrador y no se sugiere tener más cuentas para evitar accesos no autorizados.

- Para la utilización de los equipos, el Laboratorio de Computación será el encargado de generar una cuenta con privilegios de administrador y otras cuentas con su respectiva contraseña para los docentes que requieran acceder al equipo en sus horas de materia.

- **Administración y uso de contraseñas.**

  - Se asignará una contraseña para acceder a los equipos institucionales (docentes), evitando así el uso de contraseñas que no poseen los lineamientos descritos a continuación.

Lineamientos para crear una contraseña segura.

- Las contraseñas no deben tener números consecutivos.
- La contraseña deberá tener un máximo de seis caracteres entre los cuales debe ser alfanuméricos (números y letras, mayúsculas – minúsculas y caracteres especiales (@/#).
- La contraseña no debe relacionarse con el nombre del usuario, vida personal, fechas de cumpleaños, entre otras.
- No debe ser las mismas que usan frecuentemente.

  - En caso de olvido de la contraseña por parte del docente, éste deberá reportar con un escrito al Laboratorio de Computación para ser restablecida o generar una nueva.
  - Se prohíbe que los usuarios (docentes, administrativos, autoridades) tengan de manera escrita en su área de trabajo y de forma visible contraseñas escritas en papel, *stickers*, cinta adhesiva, etc., así como también correos electrónicos abiertos, documentos accesibles, etc., esto con la finalidad de evitar que personas ajenas a la institución pueda tener acceso a dicha información.
  - Todo usuario (docente) que sospeche que la contraseña de su equipo a cargo ha sido identificada por personal ajeno, tendrá la obligación de realizar el cambio inmediatamente o informar para la generación de una nueva.

Tabla 90. "Políticas de seguridad" de la Administración de usuarios.
Elaborado por el Autor

	POLÍTICAS DE SEGURIDAD PARA EL PERSONAL	Código: P-PSP-ADM-03
		Fecha:
		Versión: 01
		Nivel:
Elaborado por: _____	Aprobado por: _____	

Uno de los eslabones débiles considerados para la "Seguridad de la Información" es el humano, y es muy importante tomar en cuenta su vinculación a la institución, ésta debe realizar un proceso de selección bajo lineamientos orientados a los cargos y funciones que deberá desempeñar.

- La Administración como área de Talento Humano tendrá la responsabilidad y obligación de verificar y validar la documentación del candidato que está postulando para trabajar en la U.E.P. Séneca.
- El área de Administración es el ente encargado de hacer firmar un Acuerdo de Confidencialidad y de Admisión de las Políticas de "Seguridad de la Información" al personal de la institución con el fin de informar sus compromisos con los objetivos de proteger la "Seguridad de la Información" de la U.E.P. Séneca.
- Estos acuerdos deben estar anexados en conjunto con la carpeta de documentos de la persona en ocupación al cargo designado.

Tabla 91. "Políticas de seguridad" para el personal.
Elaborado por el Autor

	POLÍTICA DE GESTIÓN DE ACTIVOS DE LA INFORMACIÓN	Código: P-GAI-ADM-04
		Fecha:
		Versión: 01
		Nivel:
Elaborado por: _____	Aprobado por: _____	

La U.E.P. Séneca como institución educativa la cual genera información académica es la única propietaria por su uso y manipulación, la información generada durante el año lectivo ya sea física o digital que a través del Laboratorio de Computación y la Administración serán quienes otorguen responsabilidades sobre los activos de información.

- El inventario de activos se realizará por cada área o aula utilizando el formato I-IIA-ADM-DOC.
- Todos los recursos de tecnología e información que se ha designado al personal docente estarán sujetos a revisiones ocasionales sobre el cumplimiento de su uso y manipulación a través de la Administración y el Laboratorio de Computación.
- El Laboratorio de Computación es está facultado para adquirir, instalar, modificar o eliminar programas instalados si fuese necesario con una previa revisión y justificación de tal motivo.
- El Laboratorio de Computación tiene la responsabilidad de preparar los equipos de cómputo (desktop y portátiles) para el uso del personal de la institución al inicio de cada año lectivo.
- Los recursos de tecnología e información (equipos, servicio de internet, etc.) deben ser utilizados de acuerdo con las políticas estipuladas y no deben ser utilizados para fines propios o ajenos a las actividades de la institución.

Tabla 92. Política de Gestión de Activos de Información
Elaborado por el Autor

	POLÍTICA DE CONTROL DE ACCESO	Código: P-CAC-ADM-05
		Fecha:
		Versión: 01
		Nivel:
Elaborado por: _____	Aprobado por: _____	

El Laboratorio de Computación tiene como obligación la administración y protección de la red y el servicio de internet contra accesos no autorizados.

- Entre las responsabilidades principales del Laboratorio de Computación es la de controlar el acceso no autorizado, así como también garantizar la eficiencia de las redes inalámbricas verificando su intensidad del usuario a través del Registro de dispositivos móviles con el siguiente formato R-RDM-LAB-HW.
- Todo el personal debe tener los equipos tecnológicos a utilizar registrados según los formatos con su respectiva cuenta y contraseña designadas por la Laboratorio de Computación, además se les recuerda sobre la responsabilidad sobre los mismos a través del acuerdo de confidencialidad firmado y otorgado por la Administración.

Tabla 93. Documento de Políticas de Control de Acceso.
Elaborado por el Autor

Por medio de este documento a continuación se detalla sobre la importancia y responsabilidad de la seguridad física y de medio ambiente como entorno de U.E.P. Séneca.

- **Autoridades y su responsabilidad**

Los docentes encargados de su área o quienes utilicen ocasionalmente deberán garantizar el cuidado y protección de los activos que están a su disposición tomando en cuenta los siguientes puntos:

  - Se debe verificar que el equipo bajo su responsabilidad esté conectado a un tomacorriente en buen estado, caso contrario notificar para su respectiva reparación.
  - El docente debe verificar que en él toma corriente donde está conectado el equipo no tenga más conexiones de las debidas con la finalidad de no saturar su funcionamiento. En caso de necesitar más conexiones, el docente deberá iniciar el proceso según los formatos para la adquisición de recursos a través del LABORATORIO DE COMPUTACIÓN.

- **Seguridad en la red**

  - El Laboratorio de Computación es el área encargada de revisar, mantener y garantizar el funcionamiento de: cableado de red de las oficinas, swiches, router, access point, computadoras, impresoras, servicio de internet, etc., es decir, velar por el funcionamiento óptimo de los recursos de red existentes.
  - **Equipos (inventario)**

  - Los equipos que pertenecen a la institución y equipos personales deberán ser inventariados de acuerdo con el formato I-IIA-ADM-DOC con la finalidad de asegurar los accesos a los recursos tecnológicos y de información.

- **Mantenimiento de equipos (preventivo y correctivo).**

  - Como medida de cuidado y protección de los equipos informáticos se deberá elaborar un cronograma anual (año lectivo) por parte del Laboratorio de Computación para el mantenimiento de los equipos.

- Una vez definida la fecha de mantenimiento se debe informar a quienes sean los encargados sobre la actividad a realizar.
- Antes de realizar el mantenimiento, se deberá comunicar a los docentes como respaldar su información.
- En caso de requerir el mantenimiento o revisión fuera del cronograma estipulado, el docente a cargo deberá solicitar mediante el registro R-MDE-LAB-HW para su respectivo proceso.
- Para la entrega del equipo después de realizar el mantenimiento el docente deberá acercarse al Laboratorio de Computación para constatar el funcionamiento del equipo, así como la información respaldada.
-

- **Seguridad de equipos informáticos (virus).**
  -
  - Como parte del mantenimiento el equipo, éste tendrá su propio programa de protección (Windows defender), el cual será actualizado y ejecutado de acuerdo con el cronograma establecido para mantenimiento preventivo.

- **Protección y respaldo**
  -
  - La disponibilidad de la información es importante y puede ser compartida con una autorización debida para la manipular y modifica su contenido.
  - Los usuarios (docentes y administrativos) son los únicos responsables de la información que manejen o manipulen utilizando los recursos de tecnología e información que pertenecen a la U.E.P. Séneca.
  - El respaldo de la información por parte de los docentes debe ser obligatoria para de esa manera prevenir la pérdida o modificación.

- ***Software* (adquisición e instalación).**

  - Si el docente requiere la instalación de algún tipo de *software* con fines educativos, deberá solicitar al Laboratorio de Computación el registro R-IDS-LAB-HW para su revisión, verificación, aprobación o negación de esta.
  - Se tomará como una falta grave a los docentes que instalen cualquier tipo de *software* en las computadoras que no esté autorizado por el Laboratorio de Computación y su registro correspondiente.

- **Acceso físico (controles).**

  - Ingreso a la institución.
  - La U.E.P. Séneca deberá proveer de un carné a los estudiantes, docentes y empleados que laboren dentro de la institución con el propósito de ser reconocidos e identificados.
  - Las personas ajenas a la institución (padres de familia, proveedores, visitas, capacitadores, etc.) deberán dejar un documento de verificación de sus datos y portar un identificador de visita para el ingreso a la institución.

- **Ubicación de los equipos.**
  -
  - Los docentes no deberán mover o reubicar equipos, así como instalar o desinstalar programas o dispositivos, ni retirar etiquetas de identificación sin previa autorización por parte de Laboratorio de Computación.
  - Los equipos de cómputo asignados a cada docente deberán ser utilizados sólo para fines laborales dentro de la Unidad Educativa Particular Séneca.
  - El docente tiene la responsabilidad de solicitar cualquier tipo de capacitación en cuento al manejo de programas o herramientas instaladas en el equipo, con el propósito de evitar daños por mal uso.
  - El docente debe asegurar la conexión del equipo, evitando que el cable sea pisado o este, bajo algún sobre peso.
  - En caso de pérdida o robo, el docente encargado debe reportar inmediatamente al Laboratorio de Computación para su correspondiente proceso.

- **Daño a los equipos de cómputo.**

  - Mientras se utiliza la computadora no se puede consumir alimentos o ingerir bebidas en cualquier aula, área u oficina.
  - El docente es responsable tanto del equipo de cómputo como de cualquier recurso tecnológico a utilizar, y si éste sufre algún daño por mala manipulación, descuido o negligencia, y si ésta es comprobada, el docente deberá cubrir la reparación o reposición del equipo o accesorio.

Tabla 94. "Políticas de seguridad" Física y del Medio Ambiente.
Elaborado por el Autor

	POLÍTICAS DE SEGURIDAD EN LA RED E INTERNET	Código: P-SR-ADM-07
		Fecha:
		Versión: 01
		Nivel:
Elaborado por:	Aprobado por:	

El internet es la puerta hacia todo tipo de información, así como también la posible infección por la descarga de archivos o programas que tengan *software* malicioso, por esta razón hay que proteger el acceso al internet y a la red.

- **Protección de la información**
  - Toda información relacionada con actividades académicas debe estar disponible para quienes necesiten usarla de acuerdo con sus requerimientos.
  - Los docentes son dueños de la información generada, así como también ser responsables de proteger.

- Es de total responsabilidad de los docentes y administrativos identificar riesgos en su lugar de trabajo para informar y tomar medidas o acciones que sean necesarias para mitigar o eliminar dichos riesgos.
- Durante los días laborables, los docentes deberán tener el escritorio de trabajo limpio de cualquier tipo de información expuesta, así como también los elementos de almacenamiento como: pendrive, Cd, memorias, etc., estos deben estar guardados en cajones con seguro.
- Los docentes deberán cerrar o bloquear la sesión cuando termine su hora clase para que no puedan acceder al equipo sin su autorización.
- Los docentes tienen la responsabilidad de proteger la información a su cargo, por lo que debe apagar y entregar el equipo luego de terminar la jornada laboral.

- **Protección (*software* malicioso)**
  - Si algún equipo se muestra sospechoso en su comportamiento, los docentes deben comunicar al Laboratorio de Computación con el registro designado para su revisión o mantenimiento con el propósito de proceder con la desinfección del virus.
  - Los docentes no deben utilizar *software* descargado del internet diferente a los que se encuentran ya instalados, en caso de requerir otro programa seguir el procedimiento y formato de solicitud al LABORATORIO DE COMPUTACIÓN.

- **Protección (navegación en internet)**

La U.E.P. Séneca brinda el acceso al servicio de internet con el propósito de facilitar las labores académicas y administrativas, los cuales acceden de acuerdo a las políticas expuestas para su utilización.

- Los docentes deberán aceptar las restricciones realizadas por la institución y el Laboratorio de Computación a páginas web o sitios que comprometan o afecten la productividad educativa.
- Para todo el personal miembro de la comunidad educativa se prohíbe la divulgación de cualquier tipo de información sobre la institución en sitios no autorizados o fuera de la misma.
- El personal docente no debe utilizar la navegación en internet para participar en grupos de chat o redes sociales a menos que sea exclusivamente con fines educativos y autorizados.
- El personal docente no debe utilizar las redes sociales durante sus labores diarias (hora clase) y tampoco hacer algún comentario sobre la institución o algún evento educativo de carácter privado con personas ajenas a la misma.

Tabla 95. Documento de Política de seguridad en la Red e Internet.
Elaborado por el Autor

Los sistemas o programas informáticos que se utilice para gestionar la información académica o administrativa es de uso exclusivo de los usuarios autorizados que la manejen, por lo tanto, se prohíben el uso indebido fuera de horario de trabajo, teniendo como una sanción de acuerdo a su falta.

- **Privacidad.**
  - La U.E.P. Séneca no se responsabiliza por garantizar la información personal del docente, ya que el mismo es responsable de cómo lo manipule, publique o divulgue.
- **Seguridad (correo electrónico).**

La información de tipo confidencial no debería ser transferida por correo a menos que quien lo haga sea una autoridad pertinente.

- La generación de cuentas de correo de docentes será emitida por la administración, será responsabilidad del docente cambiar su contraseña.
- Las cuentas de correo electrónico (docentes y estudiantes) serán creadas de forma individual teniendo un formato, primer nombre y apellido separado con un punto finalizando con el dominio de la institución.
- Los docentes no deben utilizar otras cuentas que no sean las de la institución para tratar temas netamente de la comunidad educativa y sus actividades.
- Todo mensaje electrónico debe contener un membrete personalizado con los datos personales, cargo y número de contacto.
- Para la eliminación de una cuenta de correo (docentes o estudiantes) se hará la constatación de su permanencia en la institución, la cual debe ser notificado por escrito la inhabilitación de la cuenta para que no se envié correos o mensajes tanto internos como externos.

La U.E.P. Séneca deberán, comunicar a los usuarios (docentes) que el medio de comunicación (correo electrónico) es solamente de uso exclusivo con propósitos institucionales.

- Los docentes no podrán enviar mensajes utilizando el correo electrónico que puedan generar un ambiente hostil, algún comentario respecto a la raza, nacionalidad, género, orientación sexual, religión, política o discapacidad.
- Los mensajes enviados con carácter informativo deben contener el tipo de nivel en el pie de página.

Tabla 96. Documento de Política de Control y manejo de acceso a sistemas de información.
Elaborado por el Autor

ANEXO D (Aprobación de documentos)

Aprobación para la elaboración de un Sistema de Gestión de Seguridad de la Información

UNIDAD EDUCATIVA PARTICULAR SÉNECA

APROBACIÓN

ELABORACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

DECLARACIÓN

A través del presente documento se hace constancia la aprobación de la elaboración de un Sistema de Gestión de Seguridad de la Información para la U.E.P. Séneca, el cual permitirá conocer los diferentes tipos de activos para su etiquetado, análisis, evaluación y tratamiento de riesgos con la finalidad de proteger los recursos tecnológicos y de información, tomando como referencia el Laboratorio de Computación.

A los 09 días del mes de abril del 2018.

UNIDAD EDUCATIVA PARTICULAR SÉNECA ADMINISTRACIÓN

Mg. Paola Jaramillo

Coordinadora Académica y de Bachillerato Internacional

UNIDAD EDUCATIVA PARTICULAR SÉNECA

Aprobación del Alcance para la elaboración de un SGSI.

UNIDAD EDUCATIVA PARTICULAR SÉNECA

APROBACIÓN

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

DECLARACIÓN

A través del presente documento se hace constancia la aprobación del alcance que tendrá el Sistema de Gestión de Seguridad de la Información para la U.E.P. Séneca, en la que figura como área designada el Laboratorio de Computación,

A los 13 días del mes de abril del 2018.

UNIDAD EDUCATIVA PARTICULAR SÉNECA

Mg. Paola Jaramillo

Coordinadora Académica y de Bachillerato Internacional

UNIDAD EDUCATIVA PARTICULAR SÉNECA

Aprobación para realizar el inventario de activos.

UNIDAD EDUCATIVA PARTICULAR SÉNECA

APROBACIÓN

INVENTARIO DE ACTIVOS DE INFORMACIÓN

DECLARACIÓN

A través del presente documento se hace constancia de la aprobación sobre la realización del Inventario de Activos para la U.E.P. Séneca, el cual permite conocer y clasificar de manera detallada para una mejor gestión.

A los 16 días del mes de abril del 2018.

Mg. Paola Jaramillo

Coordinadora Académica y de Bachillerato Internacional

UNIDAD EDUCATIVA PARTICULAR SÉNECA

Aprobación de la Metodología de Evaluación de Riesgos.

UNIDAD EDUCATIVA PARTICULAR SÉNECA

APROBACIÓN

METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

DECLARACIÓN

A través del presente documento se hace constancia la aprobación de la Metodología de Evaluación y Tratamiento de Riesgos para la U.E.P. Séneca, el cual permitirá realizar un análisis de los activos sobre las amenazas a las que están expuestas identificando las vulnerabilidades y el impacto negativo que éstas tendrían a través de los resultados obtenidos.

A los 07 días del mes de mayo del 2018.

Mg. Paola Jaramillo

Coordinadora Académica y de Bachillerato Internacional

UNIDAD EDUCATIVA PARTICULAR SÉNECA

Aprobación de la Declaración de Aplicabilidad.

UNIDAD EDUCATIVA PARTICULAR SÉNECA

APROBACIÓN

DECLARACIÓN DE APLICABILIDAD

DECLARACIÓN

A través del presente documento se hace constancia la aprobación de la Declaración de Aplicabilidad para la U.E.P. Séneca, el cual basándose en los resultados de la fase anterior (evaluación de riesgos) se sugiere ciertos controles según el Anexo A los cuales pueden ser aplicables.

A los 21 días del mes de mayo del 2018.

Mg. Paola Jaramillo

Coordinadora Académica y de Bachillerato Internacional

UNIDAD EDUCATIVA PARTICULAR SÉNECA

Aprobación del Plan de Tratamiento de Riesgos.

UNIDAD EDUCATIVA PARTICULAR SÉNECA

APROBACIÓN

PLAN DE TRATAMIENTO DEL RIESGO

DECLARACIÓN

A través del presente documento se hace constancia la aprobación del Plan de Tratamiento del Riesgo para la U.E.P. Séneca, el cual crea un plan de acción sobre cómo implementar controles que fueron identificados en etapas anteriores.

Las autoridades a través del siguiente proyecto podrán determinar cómo tratar los riesgos encontrados y definir controles de acuerdo con sus objetivos.

A los 28 días del mes de mayo del 2018.

UNIDAD EDUCATIVA PARTICULAR SÉNECA ADMINISTRACIÓN

Mg. Paola Jaramillo

Coordinadora Académica y de Bachillerato Internacional

UNIDAD EDUCATIVA PARTICULAR SÉNECA

Aprobación en la selección de controles.

UNIDAD EDUCATIVA PARTICULAR SÉNECA

APROBACIÓN

INFORME SOBRE LA EVALUACIÓN Y TRATAMIENTO DE RIESGO – SELECCIÓN DE CONTROLES

DECLARACIÓN

A través del presente documento se hace constancia la aprobación del Informe sobre la Evaluación y Tratamiento de Riesgo para la U.E.P. Séneca, el cual se genera a través de los resultados sobre el análisis y evaluación de riesgos proponiendo controles en los que puedan ser evitados, transferidos, aceptados o eliminados.

A los 18 días del mes de junio del 2018.

Mg. Paola Jaramillo

Coordinadora Académica y de Bachillerato Internacional

UNIDAD EDUCATIVA PARTICULAR SÉNECA

Aprobación para la elaboración de Políticas de Seguridad de la Información.

UNIDAD EDUCATIVA PARTICULAR SÉNECA

APROBACIÓN

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

DECLARACIÓN

A través del presente documento se hace constancia la aprobación de la elaboración de las Políticas de Seguridad de la Información para la U.E.P. Séneca, el cual permitirá documentar, registrar y utilizar para las diferentes actividades académicas, en las que dichas políticas deberán ser comunicadas al personal para su cumplimiento y seguimiento.

A los 02 días del mes de julio del 2018.

Mg. Paola Jaramillo

Coordinadora Académica y de Bachillerato Internacional

UNIDAD EDUCATIVA PARTICULAR SÉNECA

Aprobación para la definición de responsabilidades.

UNIDAD EDUCATIVA PARTICULAR SÉNECA

APROBACIÓN

DEFINIR FUNCIONES Y RESPONSABILIDADES DE SEGURIDAD

DECLARACIÓN

A través del presente documento se hace constancia la aprobación sobre Definir funciones y responsabilidades de Seguridad de la Información para la U.E.P. Séneca, el cual se debe puntualizar acerca de quiénes serán los responsables de proteger y velar por la seguridad de la información tanto de los recursos tecnológicos como los de información.

A los 23 días del mes de julio del 2018.

Mg. Paola Jaramillo

Coordinadora Académica y de Bachillerato Internacional

UNIDAD EDUCATIVA PARTICULAR SÉNECA

ANEXO E (Documentos de apoyo)

Formato para la salida de recursos de tecnología fuera de la institución.

	FORMATO DE SALIDA DE RECURSOS TECNOLÓGICOS	Código:	F-FSE-LAB-HW
		Fecha:	
		Área:	

Solicita:	Aprueba:
Motivo de préstamo de equipo:	Pedido N°
Fecha de salida:	Fecha de devolución:
Observaciones:	

DESCRIPCIÓN DEL RECURSO TECNOLÓGICO			
Código	**Equipo**	**Descripción**	**Cantidad**

Atentamente

Recibí conforme

Formato para la solicitud de acceso a la web.

	FORMATO DE SOLICITUD DE ACCESO A SITIOS WEB	Código:	F-FAW-ADM-HW
		Fecha:	
		Área/Grado-curso:	

Fecha de inicio:	Solicitud #
Nombre del solicitante:	Autorizado por:
Observaciones:	

PÁGINAS A LAS QUE SOLICITA ACCESO			
Descripción de la página	**Justificación**	**Link**	**Equipo para acceder**

Atentamente

Recibí conforme

Formato para la utilización de recursos tecnológicos.

	FORMATO DE UTILIZACIÓN DE RECURSOS TECNOLÓGICOS	Código:	F-FRT-LAB-HW
		Fecha:	
		Área:	

Solicita:	Aprueba:
Motivo de uso del equipo:	Periodo de uso:
Compromiso de uso:	Componentes extras del equipo:
|Observaciones del docente al responsabilizarse del equipo:	

DESCRIPCIÓN DEL EQUIPO INFORMÁTICO			
Código	**Equipo**	**Descripción**	**Cantidad**

Atentamente

Recibí conforme

INSTRUCTIVOS

Instructivo para el inventario de activos.

	INSTRUCTIVO PARA EL INVENTARIO DE ACTIVOS	Código:	I-IIA-ADM-DOC
		Fecha:	
		Área:	
Responsable:		Aprobado por:	

ACTIVO	UBICACION	PROPIEDAD	RESPONSABILIAD Y ACCESO	GESTION

N'	Código	Descripción del activo	Tipo	Fisica	Electrónica	Dueño del activo	Custodio	Acceso	Responsable	Area del responsable	Fecha de ingreso del Activo	Fecha de salida del Activo
1	AUL-HW	Computadora portátil	INTANGIBLE	AULA	Equipo de computo	ADM	ADM	DOC	DOC	LBC	26/4/2018	
2												
3												
4												
5												
6												
7												
8												

Instructivo para la revisión de cumplimiento de las Políticas de la Información.

	INSTRUCTIVO PARA REVISIÓN DE CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD	Código:	I-ICP-ADM-DA
		Fecha de inicio:	
		Fecha de finalización	

Política	**Efectividad**				**Observación**
	Excelente	Buena	Mala	Pésima	
P-SG-ADM-01					
P-AU-ADM-02					
P-SP-ADM-03					
P-GA-ADM-04					
P-CA-ADM-05					
P-SF-ADM-06					
P-SR-ADM-07					
P-CM-ADM-08					
D-AC-ADM-09					

REGISTROS Y REPORTES

Registro para los dispositivos móviles.

	REGISTRO DE DISPOSITIVOS MÓVILES	Código:	R-RDM-LAB-HW
		Fecha:	
		Área/Grado-curso:	

Propietario	Tipo dispositivo	Marca	MAC	Fecha de registro	Firma

Registro para realizar mantenimiento a los equipos informáticos.

	REGISTRO DE MANTENIMIENTO DE EQUIPOS	Código:	R-MDE-LAB-HW
		Fecha:	
		Área/Grado-curso:	

Fecha de inicio:	Solicitud #
Nombre del solicitante:	Autorizado por:
Observaciones por la cual se hará el mantenimiento del equipo:	

DETALLE DEL EQUIPO

Docente a cargo	Equipo N°	N° serie	Accesorios del equipo

Atentamente

Recibi conforme

Registro para la instalación de software en los equipos.

	REGISTRO PARA LA INSTALACIÓN DE SOFTWARE	Código:	R-IDS-LAB-HW
		Fecha:	
		Área/Grado-curso:	

Fecha de solicitud:	Solicitud #
Nombre del solicitante:	Autorizado por:
Motivo para la instalación de software solicitado:	

DETALLE DEL EQUIPO

Docente a cargo	Equipo N°	N° serie	Nombre del o los programas

Atentamente

Recibí conforme

REGISTROS Y REPORTES

Reporte de solicitud de revisión de equipos informáticos.

	REPORTE DE SOLICITUD DE REVISIÓN DE EQUIPOS	Código:	F-RRE-LAB-HW
		Fecha:	
		Área/Grado-curso:	

Fecha de solicitud: Hora:	Solicitud #
Nombre del solicitante:	Autorizado por:
Observaciones:	

DETALLE PARA LA REVISIÓN O REPARACIÓN

Docente a cargo	Equipo	Defecto o daño a revisar

Atentamente

Recibí conforme

ANEXOS F (Fotografías)
FOTOGRAFIAS

Reunión con las autoridades de la U.E.P. Séneca

Gráfico: F1. Reunión sobre la aprobación del SGSI para la Unidad Educativa Particular Séneca.

Muestra de ejemplos de un SGSI y sus beneficios

Gráfico: F2. Beneficios de un SGSI previo a la aprobación

Laboratorio de computación

Gráfico: F3. Área designada para el SGSI.

Conexiones descuidadas

Gráfico: F4. Las conexiones de internet no tienen el cuidado respectivo.

Verificación de conexión wifi.

Gráfico: F5: Chequeo de puntos de acceso a la red wifi.

Platos para extender la señal de wifi

Gráfico: F6. *Access point* para extender la señal de wifi a otras áreas.

Colocación de *Access point* en la sala de profesores.

Gráfico: F7. Ubicación de punto de acceso inalámbrico en la sala de profesores.

Configuración de nuevo punto de acceso inalámbrico.

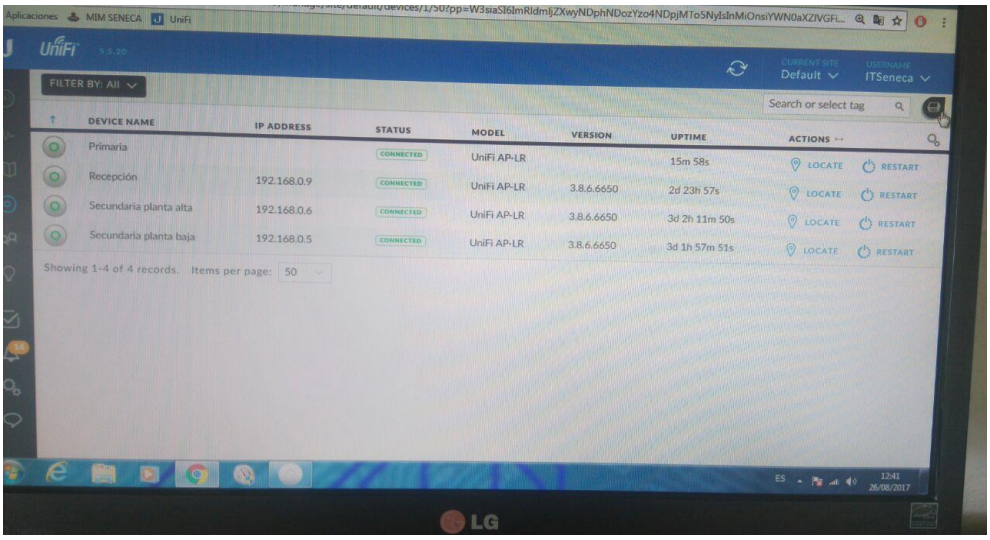


Gráfico: F8. Configuración del punto de acceso inalámbrico.

Comprobación del acceso a internet en otras áreas.

Gráfico: F9. Verificación del acceso a internet en la recepción.

Firma de la aprobación del proyecto de tesis

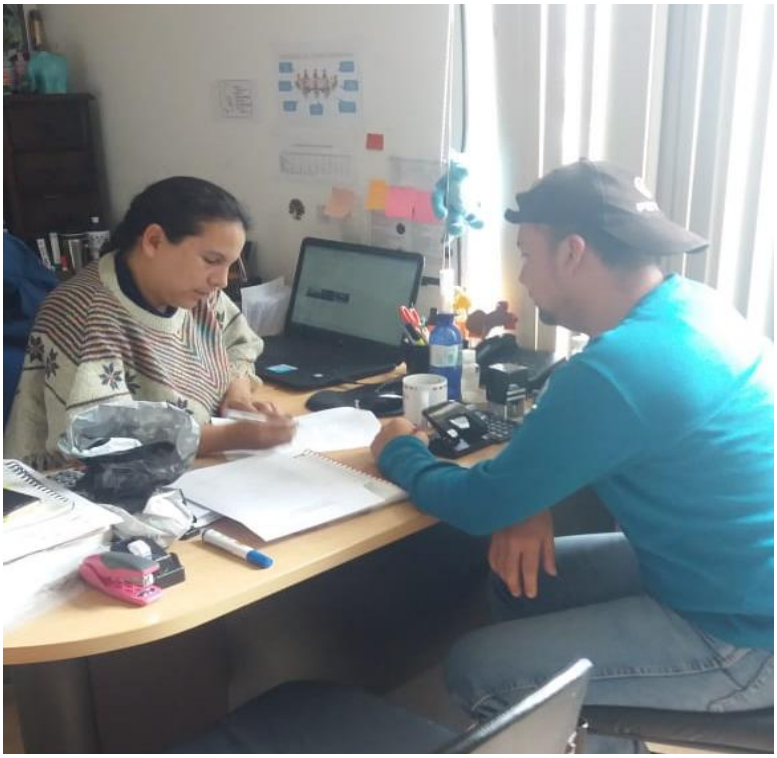
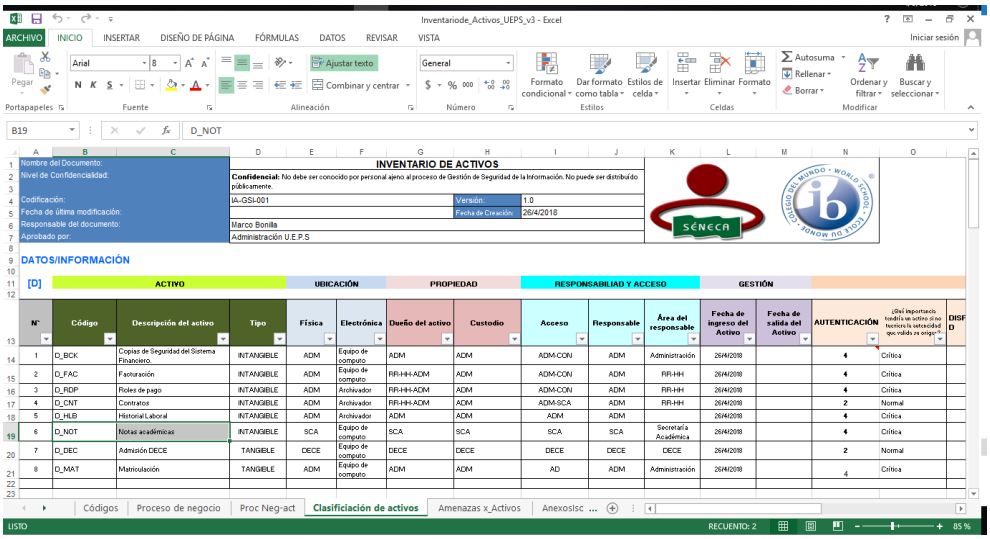


Gráfico: F10. Aprobación y firma del “SGSI” para la U.E.P. Séneca.

Clasificación de activos

Gráfico: F11. Muestra sobre la aprobación de la clasificación de activos

Clasificación de activos (información).



Inventariode_Activos_UEPS_v3 - Excel

Nombre del Documento:
Nivel de Confidencialidad:
Codificación: IA-GSI-001
Fecha de última modificación:
Responsable del documento: Marco Bonilla
Aprobado por: Administración U.E.P.S

INVENTARIO DE ACTIVOS

Confidencial: No debe ser conocido por personal ajeno al proceso de Gestión de Seguridad de la Información. No puede ser distribuido públicamente.

Versión: 1.0
Fecha de Creación: 26/4/2018

DATOS/INFORMACIÓN

[D]	ACTIVO			UBICACIÓN		PROPIEDAD		RESPONSABILIAD Y ACCESO			GESTIÓN			
N°	Código	Descripción del activo	Tipo	Física	Electrónica	Dueño del activo	Custodio	Acceso	Responsable	Área del responsable	Fecha de ingreso del Activo	Fecha de salida del Activo	AUTENTICACIÓN	¿Qué importancia tendría un activo si no tuviera la autenticidad que valida su origen?	DISP D
1	D_BCK	Copias de Seguridad del Sistema Financiero.	INTANGIBLE	ADM	Equipo de computo	ADM	ADM	ADM-CON	ADM	Administración	26/4/2018		4	Crítica	
2	D_FAC	Facturación	INTANGIBLE	ADM	Equipo de computo	RR-HH-ADM	ADM	ADM-CON	ADM	RR-HH	26/4/2018		4	Crítica	
3	D_RDP	Roles de pago	INTANGIBLE	ADM	Archivador	RR-HH-ADM	ADM	ADM-CON	ADM	RR-HH	26/4/2018		4	Crítica	
4	D_CNT	Contratos	INTANGIBLE	ADM	Archivador	RR-HH-ADM	ADM	ADM-SCA	ADM	RR-HH	26/4/2018		2	Normal	
5	D_HLB	Historial Laboral	INTANGIBLE	ADM	Archivador	ADM	ADM	ADM	ADM		26/4/2018		4	Crítica	
6	D_NOT	Notas académicas	INTANGIBLE	SCA	Equipo de computo	SCA	SCA	SCA	SCA	Secretaría Académica	26/4/2018		4	Crítica	
7	D_DEC	Admisión DECE	TANGIBLE	DECE	Equipo de computo	DECE	DECE	DECE	DECE	DECE	26/4/2018		2	Normal	
8	D_MAT	Matriculación	TANGIBLE	ADM	Equipo de computo	ADM	ADM	AD	ADM	Administración	26/4/2018		4	Crítica	

Códigos | Proceso de negocio | Proc Neg-act | Clasificación de activos | Amenazas x_Activos | Anexosisc

Gráfico: F12. Muestra del formato para la clasificación de activos.

Muestra de las amenazas en los activos

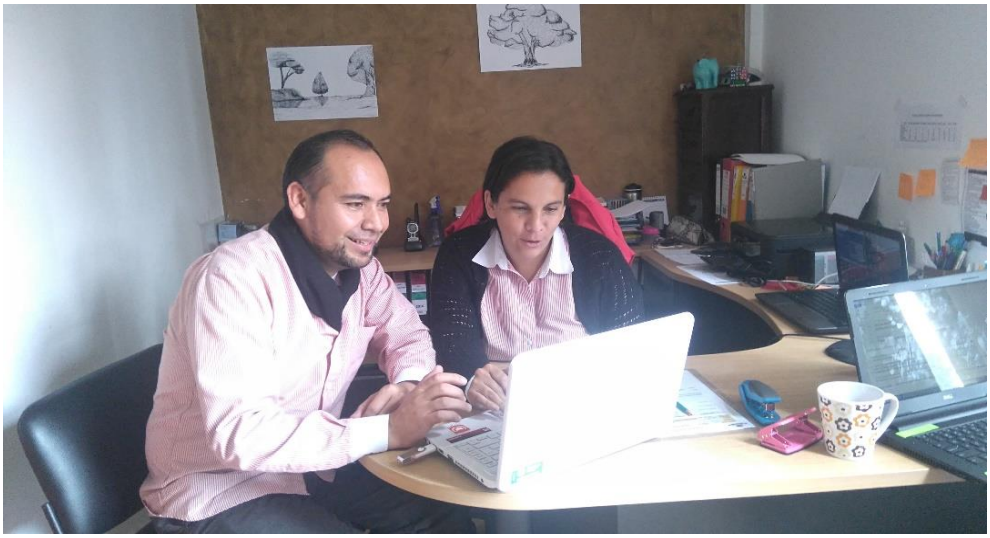


Gráfico: F13. Los activos y sus amenazas que poseen.

Valoración de los activos

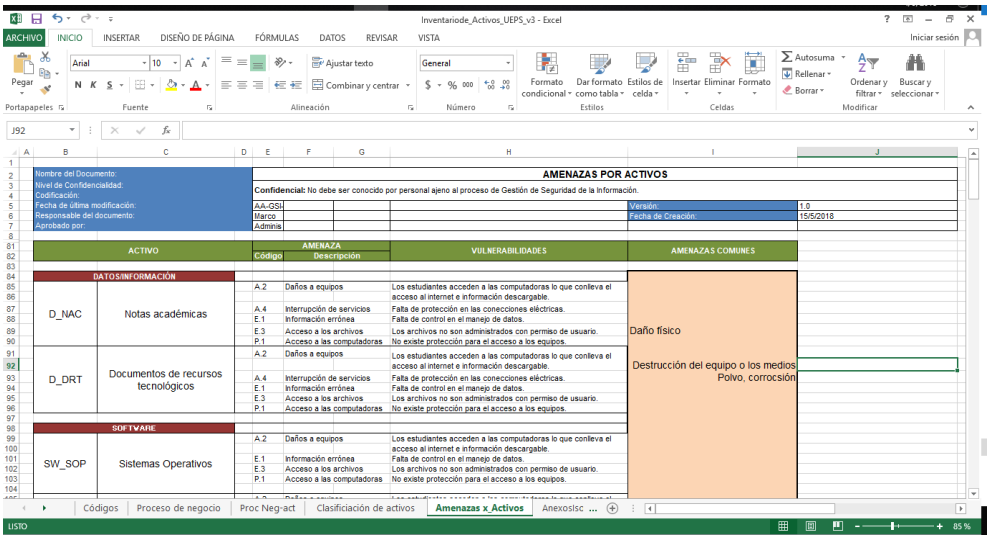
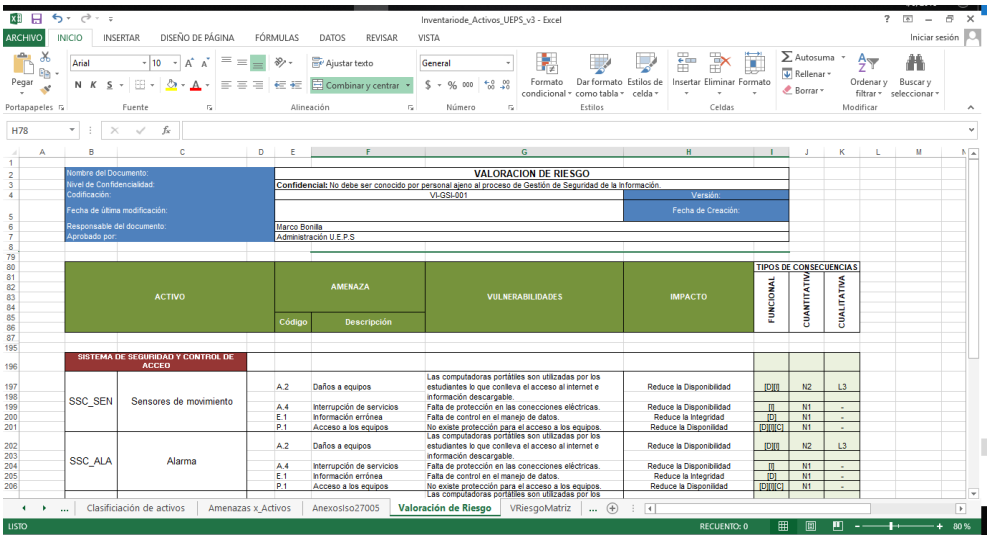


Gráfico: F14. Muestra de los activos con amenazas y vulnerabilidades.

Socialización acerca de la valoración de riesgo

Gráfico: F15. Muestra de la valoración de riesgos

Muestra de la valoración de riesgos.



Nombre del Documento:	VALORACION DE RIESGO							
Nivel de Confidencialidad:	Confidencial: No debe ser conocido por personal ajeno al proceso de Gestión de Seguridad de la Información.							
Codificación:	VI-GSI-001					Versión:		
Fecha de última modificación:						Fecha de Creación:		
Responsable del documento:	Marco Bonilla							
Aprobado por:	Administración U.E.P.S							

ACTIVO		AMENAZA		VULNERABILIDADES	IMPACTO	TIPOS DE CONSECUENCIAS		
		Código	Descripción			FUNCIONAL	CUANTITATIVA	CUALITATIVA
SISTEMA DE SEGURIDAD Y CONTROL DE ACCEO								
SSC_SEN	Sensores de movimiento	A.2	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.	Reduce la Disponibilidad	[D][I]	N2	L3
		A.4	Interrupción de servicios	Falta de protección en las conecciones eléctricas.	Reduce la Disponibilidad	[I]	N1	-
		E.1	Información errónea	Falta de control en el manejo de datos.	Reduce la Integridad	[D]	N1	-
		P.1	Acceso a los equipos	No existe protección para el acceso a los equipos.	Reduce la Disponilidad	[D][I][C]	N1	-
SSC_ALA	Alarma	A.2	Daños a equipos	Las computadoras portátiles son utilizadas por los estudiantes lo que conlleva el acceso al internet e información descargable.	Reduce la Disponibilidad	[D][I]	N2	L3
		A.4	Interrupción de servicios	Falta de protección en las conecciones eléctricas.	Reduce la Disponibilidad	[I]	N1	-
		E.1	Información errónea	Falta de control en el manejo de datos.	Reduce la Integridad	[D]	N1	-
		P.1	Acceso a los equipos	No existe protección para el acceso a los equipos.	Reduce la Disponilidad	[D][I][C]	N1	-
				Las computadoras portátiles son utilizadas por los				

Gráfico: F16. Muestra de la valoración de los riesgos.

Concientización sobre la seguridad de la información de la Unidad Educativa Particular Séneca.

Gráfico: F17. Capacitación al personal.

Concientización sobre la “seguridad de la información” en el aula de computación.

Gráfico: F18. Taller sobre la “seguridad de la información”.

Socialización de los beneficios de un SGSI en otras áreas.

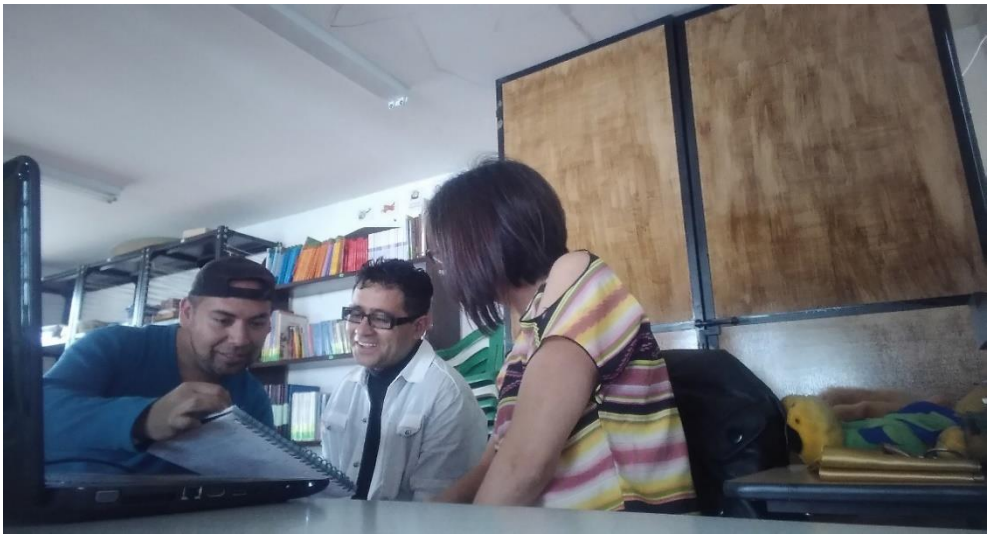


Gráfico: F19. Seguridad de la Información en la biblioteca de la institución.

Etiquetado de activos

Gráficos: F20-21. Etiquetados de los activos y sus recursos.

Finalización de actividades

Gráficos: F22-23. Finalización de actividades y firma de documentos de aprobación de un diseño de “Sistema de Gestión de Seguridad de la Información”.

MG. Paola Jaramillo: Coordinadora Académica y del Bachillerato Internacional.

Marco Bonilla: Estudiante de la Universidad Tecnología Israel

Dr. Paulina Jaramillo: Administradora de la Unidad Educativa Particular Séneca.