UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
Propuesta de un modelo de Sistema de Gestión seguridad de la Información para la Unidad Educativa Fray Jodoco Ricke bajo la norma ISO 27001
Línea de Investigación:
Seguridad Informática
Campo amplio de conocimiento:
Tecnologías de la Información y Comunicación
Autor:
Jonathan Bryan Cueva Quintana
Tutor:
Mg. Christian Patricio Vaca Benalcázar CPA

Quito – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, CHRISTIAN PATRICIO VACA BENALCÁZAR con C.I: 1719368555 en mi calidad de Tutor del proyecto de investigación titulado PROPUESTA DE UN MODELO DE SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD EDUCATIVA FRAY JODOCO RICKE BAJO LA NORMA ISO 27001.

Elaborado por: JONATHAN BRYAN CUEVA QUINTANA, de C.I: 0503972598, estudiante de la Maestría: SEGURIDAD INFORMÁTICA, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito viernes, 09 septiembre de 2022

_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, JONATHAN BRYAN CUEVA QUINTANA con C.I: 0503972598, autor/a del proyecto de titulación denominado: PROPUESTA DE UN MODELO DE SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD EDUCATIVA FRAY JODOCO RICKE BAJO LA NORMA ISO 27001. Previo a la obtención del título de Magister en SEGURIDAD INFORMÁTICA.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2022

_____

Firma

ORCID: 0000-0001-7032-9088

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Se presenta aspectos de la seguridad de la información “aplicados a la educación media (colegio)”, en donde se analiza mediante un bosquejo los peligros de la red, además se revisa como las acciones de los usuarios que no conocen de los modos de operación de los hackers pueden obtener información privada, las mismas que son las causantes de vulnerar los sistemas. Por ende, deben existir espacios seguros con medidas y protocolos a seguir para manejar la información con responsabilidad y cambiar la forma de administrar estos activos.

Hoy en día, según (Sánchez, 2020), el uso de Internet se ha generalizado y con ello, el correo electrónico, la nube, el intercambio de archivos, la educación virtual, la banca virtual e incluso los servicios de las redes sociales son ampliamente utilizados, no solo a nivel individual, comunitario y familiar, sino también en instituciones, entidades, empresas, etc.

Con la globalización y la difusión de los servicios de red, en el campo del sector educativo, con lo cual los beneficios y conveniencias que brinda internet son ciertos, sin embargo, hacerlo sin las respectivas medidas de seguridad hace que este expuesto a diversas vulnerabilidades en la red que incluso puede llevar al robo, pérdida, fraude y delitos informáticos.

Para hablar de cuestiones esenciales de seguridad de información, se tiene en cuenta el impulso del trabajo de los usuarios de la Unidad Educativa Fray Jodoco Ricke en el campo del desempeño de la vida digital a través de los diversos dispositivos que hacen uso, se puede observar los riesgos más comunes que provocan la inseguridad y que se puede hacer para evitarlos, de esta forma con una metodología se podrá solventar el peligro de la comunidad educativa digital y sobre todo con la adquisición de una serie de rutinas que darán seguridad a las acciones.

Se debe considerar técnicas de cooperación seguras y sobre todo de cómo se puede disfrutar de las grandes posibilidades que brinda la red evitando sus peligros para que en un futuro sea un espacio compartido de información con responsabilidad.

Sin embargo, al seguir normas de seguridad a las que se tiene en otros lugares, no es suficiente, hay que generar conciencia en los usuarios, ya que se encuentran las personas rodeadas por la tecnología que crece con rapidez y el constante cambio al que se enfrentan diariamente los ciudadanos en el ecosistema digital, esto con el propósito de dar seguridad y a la vez favorecer la reflexión ante ese nuevo sistema.

Problema de investigación

La falta de procedimientos ocasiona que se haga un inadecuado uso de los laboratorios, ya que tampoco existe seguridad en la segregación de páginas web del servidor principal. Esto ocasiona que los estudiantes ingresen a sitios prohibidos cómo pornografía y redes sociales. Por lo que se puede evidenciar que no se ha configurado de una forma adecuada los equipos de laboratorio. También hace falta de usuarios para la administración de sesiones en las computadoras, ya que el proceso de instalación de programas no se solicita la autorización del administrador principal a esto también se puede agregar qué es necesario un programa para congelar la producción de archivos en los discos duros.

El internet no solamente favorece nuestra vidas, sino también da cabo suelto al uso con diferentes dispositivos permitiendo el intercambio de información con las personas que se encuentran alrededor, las tendencias hoy en día se transmiten con enorme rapidez y es una tarea de todos hacer un uso creativo, dinámico y respetuoso de estas nuevas herramientas, en la educación este campo es especialmente importante ya que los usuarios de la Unidad Educativa Fray Jodoco Ricke han tenido acceso a los recursos tecnológicos desde el momento que ingresaron al establecimiento, sin recibir indicaciones o advertencias sobre el buen uso de los mismos.

El uso de equipos de computación, los medios de comunicación como las redes sociales, la colaboración en tiempo real a través de la web, entre otras, no siempre se dan de forma adecuada, para trabajar tanto docentes como estudiantes, llegando al punto de adentrarse en un entorno virtual, donde empiezan a manipular los recursos que la Institución les provee de manera experimental, ya que en ocasiones no han recibido formación académica o a su vez hacen mal uso de las mismas, teniendo que enfrentarse a unas herramientas que no siempre conocen, por tal motivo intercambiar información con los diferentes usuarios sin tomar las debidas precauciones que estas involucran. Los usuarios del entorno podrían estar inmiscuidos buscando vulnerabilidades, para posteriormente hacer uso de la información que obtuvieron, ya sea para beneficio propio o ajeno lo cual se convierte en una forma de delinquir o extorsionar a dichos usuarios.

Mediante la propuesta que se presenta como el diseño de un modelo de sistemas de seguridad de información para la Unidad Educativa Fray Jodoco Rick bajo norma ISO 27001, ayudará a enmendar las situaciones que anteriormente se mencionan, para ello la normativa permite gestionar la seguridad de información en las organizaciones con diferentes enfoques, en la que se favorece a la protección de los usuarios ante amenazas, el uso correcto de los recursos, el manejo de políticas de seguridad y otros, con la finalidad de fomentar la: confidencialidad, integridad y la disponibilidad de la información, por cuanto el proyecto pretende mejorar el estado actual del tratamiento de la información de la comunidad educativa.

Objetivo general

Diseñar un modelo de sistema de gestión de seguridad de información utilizando como referencia la normativa ISO 27001, para proteger la información de los usuarios, de la Unidad Educativa Fray Jodoco Ricke.

Objetivos específicos

- Contextualizar sobre fundamentos teóricos y las formas que actualmente se están vulnerando a nivel de información en Ecuador y la Unidad Educativa, con la finalidad de lograr identificar riesgos en común, para posteriormente recomendar mecanismos de control en la propuesta.
- Determinar el uso de recursos tecnológicos que son el medio de vulnerabilidad al que están expuestos en la seguridad de la información, mediante el sondeo de una encuesta a los usuarios de la Unidad Educativa Fray Jodoco Ricke.
- Identificar las brechas de seguridad que presenta el laboratorio de la Unidad Educativa Fray Jodoco Ricke, con la finalidad de proponer controles que mitiguen el inadecuado uso por parte de los estudiantes.
- Diseñar una guía para la gestión de seguridad de la información, utilizando como referencia la normativa ISO 27001, para asegurar los datos de los usuarios de la Unidad Educativa Fray Jodoco Ricke, con la finalidad de innovar la infraestructura impulsando el acceso igualitario a la información.

Vinculación con la sociedad y beneficiarios directos:

En el diseño de un sistema de gestión de seguridad de información con la normativa ISO 27001 se pretende fomentar la: confidencialidad, integridad y la disponibilidad de los datos en usuarios de la Unidad Educativa Fray Jodoco Ricke, para el uso de los recursos tecnológicos en dicha institución.

La unidad educativa al tomar en cuenta este referente del sistema de gestión seguridad de la información bajo la normativa ISO 27001 ayudará a resolver los inconvenientes de seguridad y el uso de los equipos con el propósito de salvaguardar la información de usuarios en la Institución, adoptando tecnologías y procesos limpios logrando que todos los recursos se usen de forma eficiente.

Beneficiarios directos:

La comunidad educativa que está conformada por administrativos, docentes y estudiantes que hacen uso de recursos tecnológicos con los cuales intercambian información.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

Según (Mayorga, 2014) dice que el Ecuador tiene una gran debilidad en materia de seguridad, en las Unidades de educativas no preexiste un sistema de políticas de seguridad, dejando a la juventud expuesta a riesgos. Ya en la educación primaria hay alumnos que usan laptops o móviles sin ningún tipo de seguridad, lo que implica muchos riesgos. Es necesario aplicar normas que acompañen las políticas puestas en marcha, definir los roles, las responsabilidades para que cada uno asuma su responsabilidad.

Según (Ortiz, 2021) menciona que, en el Ecuador hubo: más de 51000 detecciones relacionadas con criptomonedas, aproximadamente 140000 exploits, 6000 detecciones de ransomware y casi 1000 detecciones de spyware, estos son datos que incluyen ciertos tipos de malware.

Ransomware es un malware creado en Brasil, es el país donde se producen más virus de Latinoamérica. Este ha causado daños a empresas públicas y privadas en Ecuador. Según ESET, Ecuador ocupó el sexto lugar entre los países latinos con el mayor número de detecciones de malware en 2021, después de Brasil, México, Argentina, Colombia y Perú (Cuvi, 2019, p. 25).

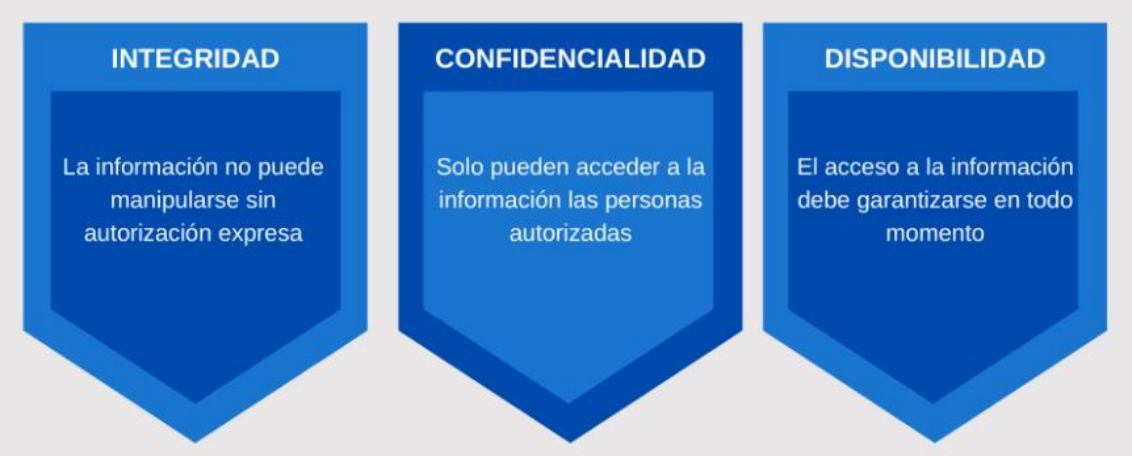
El Ecuador es uno de los países con menor certificaciones en cuanto a las normas ISO 27000, según la encuesta nacional. Sin embargo, esta normativa tiene diferentes campos de aplicación como, por ejemplo: el sector militar, farmacéutico, público y educativo (Cuvi, 2019, p. 26).

Seguridad de la Información

La seguridad de los datos es uno de los principales intereses ya que responde a las necesidades para determinar la forma de trabajo y ejecución de las acciones institucionales de acuerdo con los objetivos planteados por cada organización (Acurio, 2019, p. 25).

En el presente, por lo general las empresas, usan principalmente el Internet y los avances tecnológicos; provocando un aumento en las amenazas y dando paso a las vulnerabilidades en las organizaciones, esto resulta un riesgo en los datos y la seguridad de las mismas. Sin embargo, estas tienen que mantener la: disponibilidad, integridad y confidencialidad (Areitio, 2018).

Figura 1
Objetivos de la seguridad de la información



Nota: Adaptado de Objetivos de la Seguridad de la Información, Seguridad de la información: Aspectos a tener en cuenta. (2020, Julio 14). Ayuda Ley Protección Datos. (https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/).

Importancia de la seguridad de los datos

Es evidente que la protección tiene como objetivo asegurar y prevenir cualquier tipo de incidente con respecto a los datos guardados por las empresas, ya que la información hoy en día es de gran importancia, para el trabajo en muchos campos, como el análisis de datos para implementar campañas de marketing con base en esta información. (Berumen & Arriaza, 2008).

Dinámica de la protección de datos.

Consiste en asegurar los datos generados por el medio de mercado en el que se encuentre el negocio como los números de teléfono de los clientes potenciales, pero así también pretende la seguridad de los demás implementos tecnológicos como: infraestructura, cableados, dispositivos, servidores de comunicaciones y otros que forman parte de los activos en las empresas. (Suárez & Ávila, 2015). A continuación, algunos puntos de conocimiento.

- Privacidad de datos con estado de disponibilidad de solo usuarios, procesos y dispositivos autorizados.
- Asegurar la integridad es particularmente importante cuando la información es de gran valor y no debe perderse, así como cuando los datos pueden modificarse intencionalmente para desinformar al destinatario.
- La accesibilidad es la provisión de un acceso rápido y confiable a la información y los servicios de información.
- La autenticidad es la capacidad de identificar información de manera única.

Gestión y seguridad de datos.

Las formas disponibles para que las empresas administren la seguridad de la información es configurar un sistema de administración de seguridad de los datos como el sistema de detección de intrusos. La protección se basa en la identificación de los riesgos que pueden presentarse en la organización, según lo determinado por la ISO 27000, ya que esto requiere apoyo como un sistema jerárquico automatizado para el control de intrusos (Ormella, 2017).

Gestión de Seguridad de Información

La norma ISO 27001 establece las mejores prácticas para configurar un sistema de gestión de la información. Esto le permite no solo proteger los datos de su organización, sino también crear una cultura de mayor confianza entre sus clientes, proveedores, empleados. A continuación los implicados en la Gestión de la información.

- Las personas manipulan y procesan la información.
- Estos pueden ser empleados, reguladores, autoridades, clientes, proveedores de servicios y contratistas.
- Los procesos son las actividades desempeñadas por el personal a cargo de la empresa, pero la mayoría de estos presentan vulnerabilidades.
- La tecnología se ocupa de servicios e infraestructura en la empresa, para la gestión y desarrollo de la información, además, proporciona la capacidad de: almacenar, recuperar, difundir y retener datos valiosos.

Procedimientos para asegurar los datos bajo normas vigentes.

Debido a la importancia de proteger la información se implementan sistemas en contra de los eventos que ponen en peligro las actividades comerciales, por ende, existen varios estándares que implementan procesos de gestión de seguridad de la información para garantizar las mejores prácticas enfocadas en los diferentes modelos de negocio como se muestra en la figura 2, un resumen de las normativas existentes y el número de controles que contiene cada uno de estos.

Figura 2
Normativas de gestión de seguridad y riesgos de la información.

ITIL

Organización

- Information Technology Infrastructure Library

Descripción

- Dispone de un conjunto de publicaciones que mejoran las buenas prácticas para gestión de servicios de tecnologías de información con asesoramiento sobre proveedores de servicios de de calidad.

Organización

PCI Security Standasds Conuncil

Descripción

- Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) para cada organización que acepta tarjetas de crédito, puede asegurar sistemas críticos y proteger los datos confidenciales del titular de la tarjeta.

Controles de seguridad

CIS critical Security Controls

Organización

- Center for Internet Security (CIS)

Descripción

- Creado en el 2008 por el Centro de Seguridad de Internet para la proteccion efectiva, los que son acciones para la ciberdefensa de ataque potentes.

Controles de seguridad

- 20 Controles de CIS

OWASP

Organización

- Open web Application Security Project

Descripción

- Es una organizacion sin fines de lucro efocada para mejorar las seguridades de las aplicaciones web, para los profesionales de desarrollo para fortalecer las seguridades del entorno.

Controles de seguridad

- 10 controles.

NIST 800 series

Organización

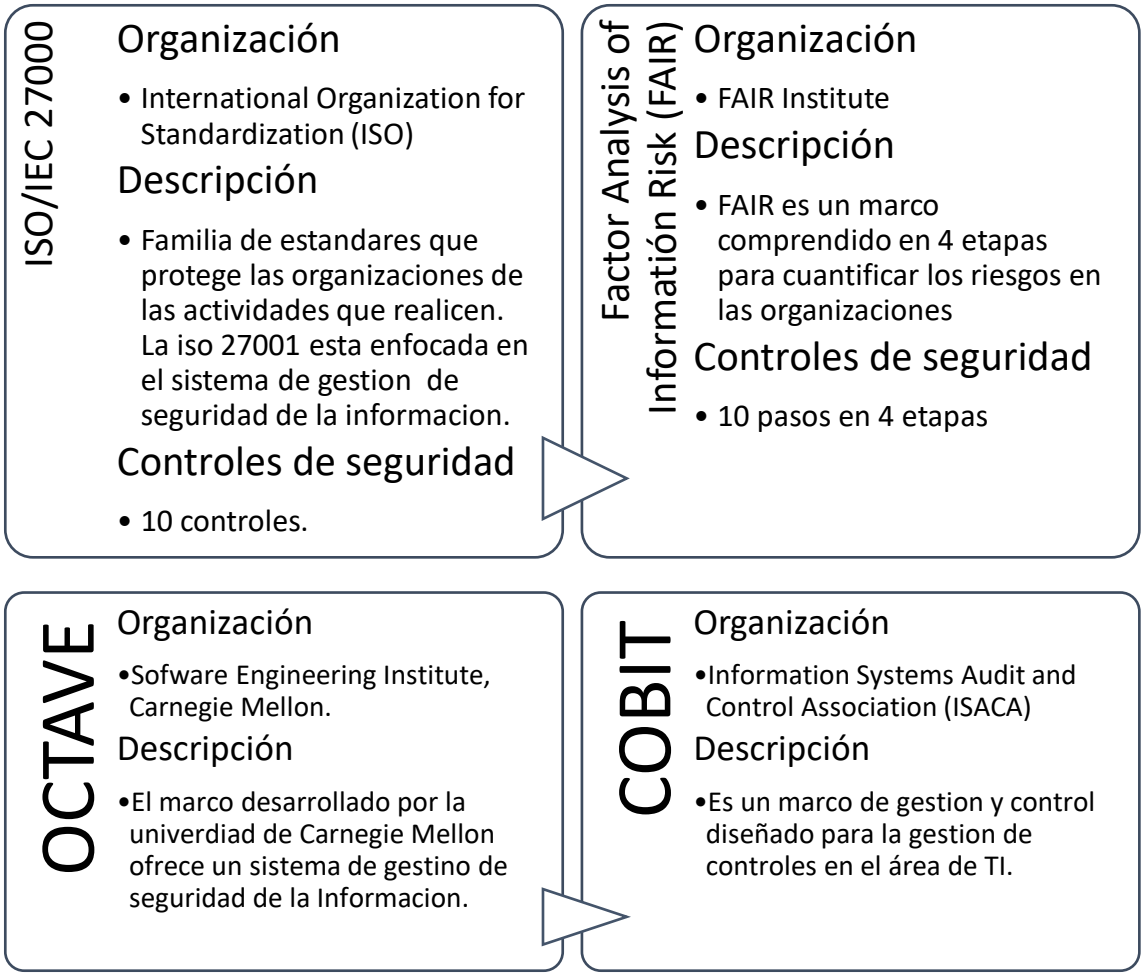
- International Organización for Standardization (ISO)

Descripción

- Varios controles para monitorear y tomar deciciones de seguridad en la organizacion. Pero también está la NIST-171 que tiene un solo enfoque, proteger datos de contratistas y sistemas de informacion no federales.

Controles de seguridad

- NIST 800-53 y 800-171



Nota: Adaptado de Normativas de gestión de seguridad y riesgos de la información, Propuesta metodológica de gestión de riesgos de Tecnología de información y comunicación (TIC): Patiño Rosado, S. G. (2018).

Metodología MAGERIT

Esta es una metodología de análisis y riesgo que fue desarrollada en su momento por el Consejo Superior de Electrónica y actualmente es administrada por la Secretaría General de Gobierno Digital, MAGERIT es una metodología pública que puede ser utilizada sin necesidad de autorización previa. Es de interés de los sujetos al aplicar el Esquema Nacional de Seguridad, respetar la gestión de seguridad basada en el análisis y la gestión de riesgos relacionados con la dependencia de la información (PAe, 2015).

Serie ISO/IEC 27000

De acuerdo a Valencia y Orozco (2017), dicen que La serie de normas internacionales ISO/IEC 27000, ISO/IEC 27001, 27002, ISO/IEC 27005, publicada por la Organización Internacional para la Estandarización Electrónica Internacional, explica cómo la seguridad de la información debe ser

manejada en una organización y los conceptos relacionados con los sistemas de gestión, los requisitos del SGSI, los controles y la gestión de la seguridad con la familia ISO/IEC se presentan en la Tabla 9.

Tabla 9

Familia serie ISO/IEC

Normativa	Contenido
ISO/IEC 27000	Contiene una perspectiva general y los conceptos que se manejan.
ISO/IEC 27001	Contiene requisitos para implementar un SGSI es una norma certificable.
ISO/IEC 27002	Contiene buenas prácticas, describen los objetivos de control de seguridad.
ISO/IEC 27003	Define consejos de implementación de un SGSI de acuerdo ISO/IEC 27001.
ISO/IEC 27004	Contiene una guía para determinar métricas para medir un SGSI.
ISO/IEC 27005	Contiene una guía para realizar la gestión del riesgo en un SGSI.
ISO/IEC 27006	Contiene requisitos y provee guía para auditoría y certificación del sistema.
ISO/IEC 27007	Aporta un marco de seguridad para el desarrollo, implantación y para mantener especificaciones de los Sistemas de Gestión de la SI.
ISO/IEC 27008	Dispone de plataforma estratégica de implementación y operación de controles según el tipo de organización.
ISO/IEC 27009	Contiene interpretación de requisitos acorde a la organización donde se implementará.
ISO/IEC 27010	Determina la forma del traslado e intercambio de información con referencia al funcionamiento interno de la organización.

Nota: Esta tabla describe la familia ISO/IEC para gestión de seguridad de la información.

ISO/IEC 27001:2013

Este es un estándar internacional publicado por la Organización Internacional que describe cómo se debe administrar la seguridad de la información dentro de una empresa. La primera revisión fue publicada en 2005 y basada en la norma británica BS 7799-2. La ISO 27001 puede aplicarse a cualquier organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está escrito por los principales expertos mundiales en el tema y proporciona una metodología para poner en la gestión de seguridad de la información, también permite que una empresa sea certificada (Nieves, 2017).

Tabla 10

ISO/IEC 27001: 2013.

Sección	Descripción
1	Introducción: objetivo de la norma.
2	Alcance: Puede ser aplicada a todo tipo de organización.

3	Referencias normativas: hace referencia a la ISO/IEC 27000.
4	Términos y definiciones: define los términos más utilizados.
5	Contexto de la organización: determina la organización, partes interesadas, requisitos y alcance del SGSI.
6	Liderazgo: apoyo de directivos al SGSI, estableciendo roles y responsabilidades y aprobando la política de seguridad de la información.
7	Planificación: realizar la gestión de riesgos, llenar la declaración de aplicabilidad, plantear los objetivos de seguridad de la información.
8	Apoyo: contar recursos financieros, difusión y control de documentos.
9	Funcionamiento: implementación de la gestión de riesgos, y de los controles y procesos para cumplir con los objetivos de seguridad.
10	Evaluación del desempeño: monitoreo, medición, análisis, evaluación, auditoría interna del funcionamiento del SGSI.
11	Mejora: para una mejora continua identifica como realizar las medidas correctivas.
Anexo A	Controles de seguridad con dominios de seguridad.

Nota: Esta tabla describe como está conformada ISO/IEC 27001: 2013.

Normativa ISO/IEC 27001

Menciona Vegas (2019), que se tiene en cuenta dentro del marco regulatorio la seguridad de la información está en el corazón del gobierno de TI. Es parte de la familia 27000 y cubre varios tipos de enfoques. Especifica los requisitos para establecer, implementar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información documentado en el contexto del negocio al que se refiere. También especifique los requisitos para aplicar controles de seguridad en función de las necesidades de la organización.

Activos de la información

Según ISOTools (2017), Los activos de información pueden entenderse como un conjunto de: personas, tecnologías y procesos, los que conforman un ciclo de vida dentro de la empresa. Pero en el caso del procesamiento de información se almacenan los equipos o servidores.

Valoración de Activos

Para valorar activos de información, se define una escala a utilizar criterios para cada valor, los criterios están delimitados en la tabla 13, con referencia a la norma ISO/IEC 27005.

Tabla 13

Escala de valoración de activos

Valor	Impacto	Detalle	Total
1	Muy Bajo	No afecta ni produce pérdidas de la institución.	1-3
2	Bajo	Afecta en niveles bajos, pero no produce pérdidas de la institución.	4-6
3	Medio	Afecta el funcionamiento y puede producir pérdidas o afectar la reputación de la institución.	7-9
4	Alto	Afecta su funcionamiento, produce pérdidas también se ve afectada la reputación de la institución e incumplimiento de obligaciones legales.	10-12
5	Muy Alto	Afecta el funcionamiento, produce grandes pérdidas económicas, pérdida de reputación, incapacidad para cumplimientos de obligaciones legales.	13-15

Nota: Elaborado por Jonathan Cueva, 2022, Fuente: propia. Describe como afecta las perdidas según el nivel de impacto en activos en las instituciones.

Vulnerabilidades

Estas fallas pueden ser explotadas por un agente causal una condición favorable a un evento negativo, es decir, la vulnerabilidad es la fragilidad de un activo o uno de estos, que puede ser explotada por una o más amenazas que inciden en el incumplimiento de uno o más principios de seguridad. Las vulnerabilidades están presentes en los propios activos, es decir, son inherentes a los mismos y pueden ser de carácter tecnológico, procesual y ambiental (Joya & Sacristán, 2017).

Amenazas

Las amenazas siempre han existido y tienen orígenes más diversos y, a medida que avanza la tecnología, pueden aparecer nuevas formas de exponer la información. Sin embargo, muchos que no reconocen la importancia de la seguridad de la información terminan dejando los activos de información desatendidos, los cuales requieren de protecciones que contribuyen a la ocurrencia de la seguridad de incidentes (Fache, 2016).

Probabilidades

Según (Konzen, 2013), es la probabilidad de que ocurra un evento, vinculando una escala de 0 a 1 a uno puede vincularse a la frecuencia de ocurrencia o la confianza de que ocurrirá un evento.

Para identificar amenazas y vulnerabilidades que generan riesgos en los activos de información se tienen en cuenta criterios: la disponibilidad, seguridad e integridad de los activos en función de la probabilidad y el impacto. Para evaluar las amenazas y vulnerabilidades de seguridad, se ha establecido una escala según ISO/IEC 27005, que se encuentra en la tabla 15.

Tabla 15

Escala de valoración de probabilidad

Valoración	Probabilidad	Detalle
1	Poco probable	Riesgo mínimamente probable
2	Improbable	Riesgo que se puede producir eventualmente
3	Moderado	Riesgo que se presenta de manera moderada.
4	Probable	Riesgo que puede producir habitualmente.
5	Muy probable	Riesgo que se produce recurrentemente.

Nota: Elaborado por Jonathan Cueva, 2022, Fuente: propia. Muestra una escala de valoración en la probabilidad de riesgo ante un evento.

Impacto

Konzen (2013), define el impacto como la extensión del daño causado por una seguridad a uno o más procesos de negocio, en términos, se refiere al posible daño que un incidente de seguridad de la información puede comunicar directamente a la empresa. Estos daños pueden significar pérdidas: económicas, calidad de los servicios prestados, insatisfacción de clientes, recursos, entre otros.

Definir en el siguiente orden: 1.-la probabilidad, 2.-la escala de impacto. La misma se presenta en la tabla que muestra la evaluación del nivel de impacto sobre el producto si ocurre un riesgo en común y con la valoración de P= probabilidad, I= impacto. Para el cálculo del riesgo sumar el valor de la probabilidad más el impacto.

Tabla 16

Escala de valoración de impacto

Valoración	Impacto	Detalle
1	Insignificante	No afecta ni produce pérdidas de la institución.
2	Bajo	Afecta el funcionamiento, pero no produce pérdidas de la institución.
3	Medio	Afecta el funcionamiento, y puede producir pérdidas y afecta la reputación de la institución.
4	Alto	Afecta el funcionamiento, produce pérdidas y se ve afectada la reputación de la institución e incumplimiento de obligaciones legales.
5	Crítico	Afecta el funcionamiento, produce grandes pérdidas económicas y de reputación, pérdida de reputación, incapacidad para cumplimientos de obligaciones legales.

Nota: Elaborado por Jonathan Cueva, 2022, Fuente: propia. Muestra una escala sobre el impacto en el funcionamiento, ya sea con pérdidas de información o discontinuidad del negocio.

Incidentes de seguridad

De acuerdo con García Cruz (2020), Un incidente de seguridad de la información registrado es un evento múltiple inesperado o imprevisto que tiene algún grado que afecta las operaciones o los procesos comerciales y la seguridad de la información. También se conceptualiza como una acción de amenaza que revela una o más vulnerabilidades.

Se presentan a continuación los cuatro tipos de incidencias que son las siguientes:

- Suplantación de identidad o enmascaramiento: ocurre cuando una entidad ataca la identidad de otra entidad, este tipo de incidentes suelen incluir otro tipo de ataque escondido.
- Repetición: implica recopilar pasivamente unidades de datos y retransmitirlos.
- Editar mensaje: implica editar parte o todo el mensaje.
- Denegación de servicio: estos problemas a menudo impiden ciertos servicios de comunicación.

Gestión de Riesgos en la Seguridad de la Información

Sobre la base de lo anterior, se observa que las organizaciones a menudo están en riesgo. La presencia de estos implica que tienen que llevar aspectos de evaluación para: identificar, analizar, evaluar si estos riesgos deben ser tratados o no.

Según Gómez (2017), el proceso de gestión de riesgos se refiere a la planificación, seguimiento y control, con base en la información producida por la actividad de análisis de riesgos, lo que hace que el proceso se divida en seis pasos distintos.

- Planificación y estrategia: se caracteriza por la planificación de la acción y la creación de estrategias de evaluación.
- Identificación: creación de procedimientos para la correcta identificación de
- Evaluación: evaluación de amenazas y vulnerabilidades.
- Cuantificación: puntuación del nivel de riesgo.
- Impactos y respuestas: establecer procedimientos que determinen un riesgo particular y la respuesta que se debe
- Seguimiento y control: definición de los procedimientos de seguimiento de los riesgos y de las medidas adoptadas para minimizarlos.

Tratamiento del riesgo

El tratamiento del riesgo permite tomar decisiones de actuar frente a riesgos analizados, a continuación, se describen los criterios de tratamiento de riesgos:

- Aceptar riesgo: se acepta el riesgo sin realizar ninguna acción, ya que los costos de solución podrían ser mayores al origen del riesgo.
- Reducir riesgo: se toman acciones para minimizar y reducir la probabilidad de que se provoque el riesgo.
- Evitar el riesgo: tratar de eliminar las actividades que tomen riesgo.
- Transferir riesgo: trasladar el riesgo a terceros en este caso se lo hace a: especialistas, empresas, u otras entidades que conocen el tratamiento de riesgo.

Para el tratamiento de riesgos hay que definir criterios de valoración en base a una escala, que se presentan en la Tabla 18.

Tabla 18

Escala de tratamiento de riesgo

Valoración	Riesgo	Detalle
1 – 3	Mínimo	Asumir el riesgo
4 – 5	Bajo	Reducir el riesgo
6 – 8	Medio	Evitar el riesgo
9-10	Alto	Transferir el riesgo

Nota: Elaborado por Jonathan Cueva, 2022, Fuente: propia.

1.2. Proceso investigativo metodológico

Dentro del proyecto se utiliza una investigación aplicada, ya que se recolecta información cuantitativa y cualitativa, pero la investigación es metodología de tipo no experimental.
También se utiliza la investigación descriptiva para determinar la situación actual de la Unidad Educativa, en donde se identifica: activos, riesgos e incidentes.

Población

Se desarrolla una encuesta a todos los directivos, docentes y estudiantes de la Unidad Educativa Fray Jodoco Ricke, donde se centrará el flujo de información recolectada para el éxito de la investigación.

Muestra

En la muestra se obtiene la cantidad de los componentes de la investigación que conforman la comunidad educativa son un total de 567 en los que están comprendidos cinco directivos, veintidós docentes y quinientos cuarenta estudiantes, en base a la encuesta se podrá identificar las situaciones de inseguridad que tiene la institución al no contar con un esquema de seguridad de información. Para el cálculo de la muestra se procede a utilizar la fórmula que se muestra en la figura 3, sin embargo, el sitio web SurveyMonkey proporciona la herramienta para determinar el número de encuestas. La población es de 567 de lo cual se procede a utilizar el 95% de nivel de confianza y un margen de error del 5%, obteniendo el resultado del tamaño de la muestra de 230 como se muestra en la Figura 4.

Figura 3

Fórmula de la muestra

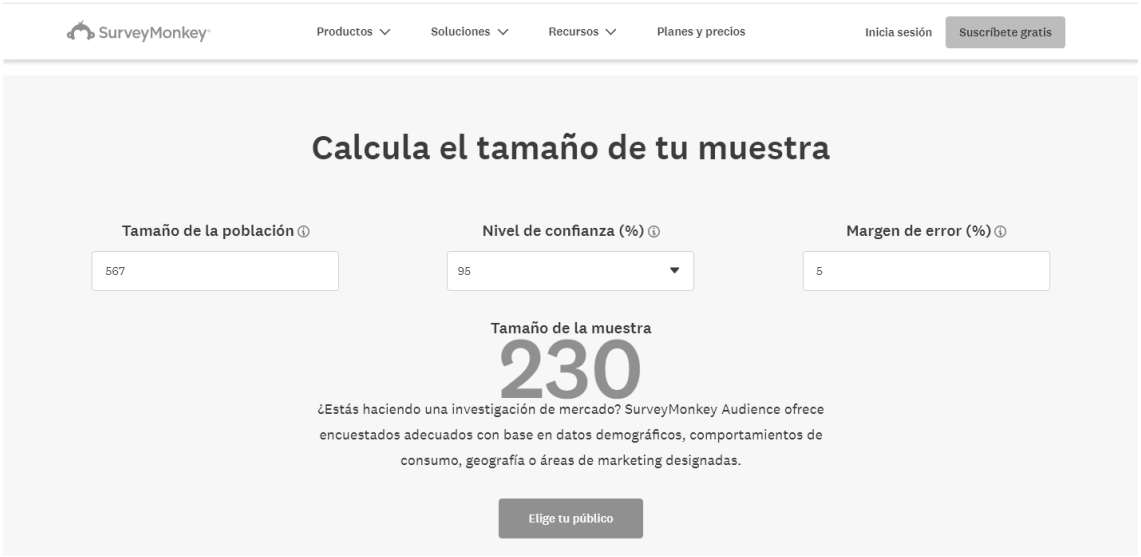
$$n = \frac{Z^2 . p . q . N}{NE^2 + Z^2 \ p . q .}$$

Z=Nivel de confianza
N=Población-Censo
p= Probabilidad a favor
q= Probabilidad en contra
e= error de estimación
n= Tamaño de la muestra

Nota: (UNIDAD DE EMPRENDIMIENTO VIRTUAL, 2015) Fuente: http://hachepe57.blogspot.com/2010/05/l-calculo-del-tamano-de-la-muestra.html. Fórmula para calcular la muestra de una población finita.

Figura 4

Cálculo de tamaño de muestra.



Nota: (Momentive, 2022) Fuente: https://es.surveymonkey.com/mp/sample-size-calculator/. Según el resultado de SurveyMonkey se aplica 230 encuestas.

Técnicas e instrumentos

Se recolecta la información con base en las revisiones de información y documentación de la encuesta aplicable a la Unidad Educativa, donde se recolecta toda la información pertinente que servirá como base para identificar aspectos de seguridad de información al no contar con algún sistema de gestión.

Encuesta

Se encuesta con la herramienta en línea, de la web de QuestionPro, y posteriormente se tabula los datos obtenidos, el formato de la encuesta se lo puede ver en el Anexo 1, dicha encuesta determina la seguridad de la información que se maneja en el uso de dispositivos y la conexión a internet de los usuarios de la Unidad Educativa Fray Jodoco Ricke.

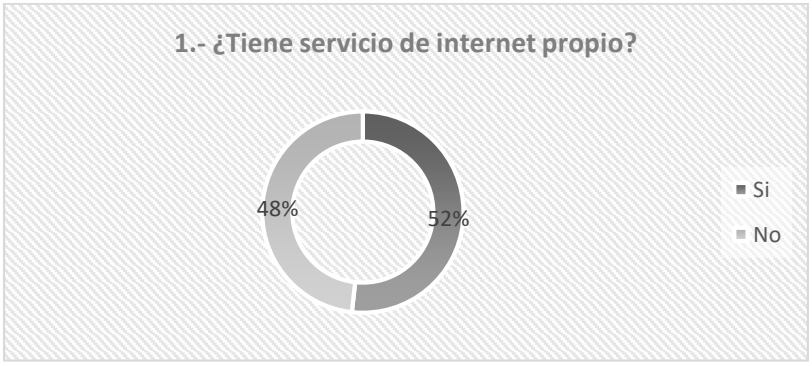
1.3. Análisis de resultados

En los resultados se muestra la recolección de los datos de la encuesta, los cuales son la fuente de información necesaria para la realización del presente proyecto, esta permite obtener un mejor panorama con respecto a los conceptos de gestión de seguridad de la información, permitiendo identificar los problemas. Con la herramienta en línea QuestionPro, se refleja la estadística de los datos para su tabulación.

Tabla 1
Tabulación de resultados obtenidos de la pregunta 1.

1.- ¿Tiene servicio de internet propio?			
	Si	119	52%
	No	111	48%
Total		**230**	**100%**

Figura 5
Tabulación de resultados obtenidos de la pregunta 1.



Fuente: propia

Elaborado por: Jonathan Cueva

En la Figura 2 se observa que el 52% de los encuestados tiene servicio de internet propio, a diferencia del 48%, entonces no dispone del servicio propio, lo cual da a entender que para acceder a internet lo hace mediante internet compartido de otros usuarios.

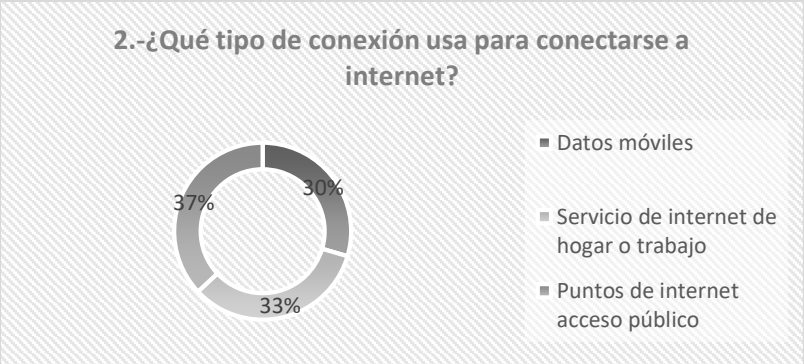
Tabla 2

Tabulación de resultados obtenidos de la pregunta 2.

2.-¿Qué tipo de conexión usa para conectarse a internet?		
Datos móviles	68	30%
Servicio de internet de hogar o trabajo	77	33%
Puntos de internet acceso público	85	37%
Total	**230**	**100%**

Figura 6

Tabulación de resultados obtenidos de la pregunta 2.



En la Figura 3 se observa que el 37% de los encuestados tiene accede a internet, por medio de puntos de acceso público, siendo esto un riesgo de vulnerabilidad, seguido por el 33% que utilizan el servicio de internet contratado en casa o trabajo, a diferencia del 30 % que usa su conexión de datos móviles mediante el teléfono celular.

Tabla 3

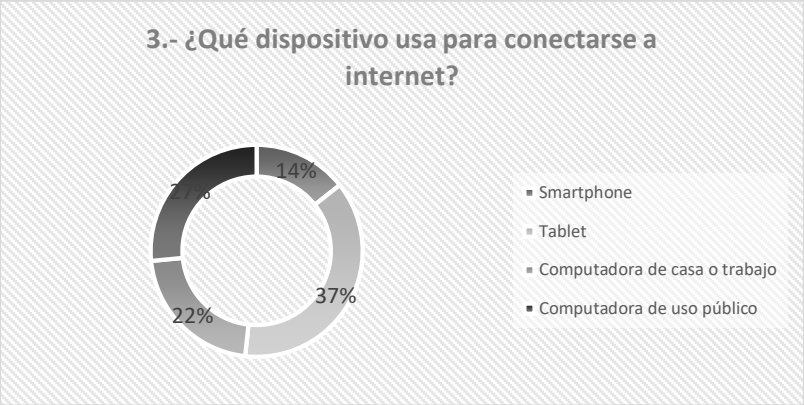
Tabulación de resultados obtenidos de la pregunta 3

3.- ¿Qué dispositivo usa para conectarse a internet?		
Tablet	33	14%
Smartphone	86	37%
Computadora de casa o trabajo	50	22%
Computadora de uso público	61	27%

Total	**230**	**100%**

Figura 7

Tabulación de resultados obtenidos de la pregunta 3.



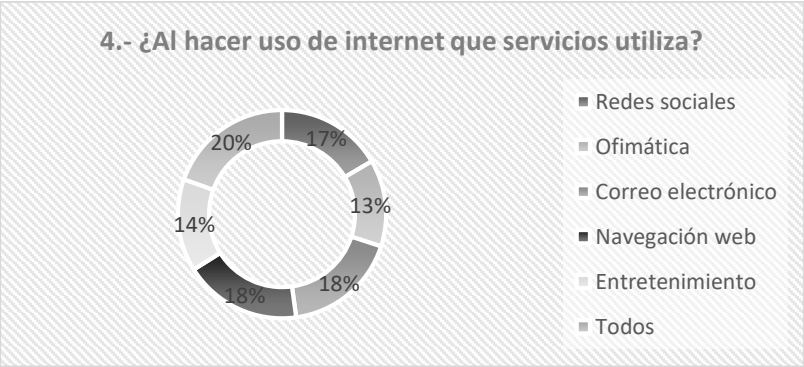
En la Figura 4 se observa que el 37% de los encuestados usa un Smartphone para acceder a internet, lo cual podría ser un objetivo en común para vulnerar, mientras que el 27% usan un computador público, en donde no se mantiene precauciones para navegar en internet siendo un blanco fácil para los ciberdelincuentes, por otro lado, el 22% usa una computadora ya sea de casa o trabajo esto da a entender que la usan en su casa o en la Institución a la que asisten y finalmente el 14% usa el Tablet que se destinaria a entretenimiento o redes sociales, también se podría convertir en un dispositivo a vulnerar.

Tabla 4

Tabulación de resultados obtenidos de la pregunta 4.

4.- ¿Al hacer uso de internet que servicios utiliza?		
Redes sociales	38	17%
Ofimática	31	13%
Correo electrónico	41	18%
Navegación web	42	18%
Entretenimiento	33	14%
Todos	45	20%
Total	**230**	**100%**

Figura 8
Tabulación de resultados obtenidos de la pregunta 4.



En la Figura 5 se observa que el 20% de los encuestados usan recursos tecnológicos para realizar diferentes tareas, mientras que el 18% en común usan para entretenimiento, navegar en la web y para correos electrónicos, seguidamente por el 17% que hace uso para redes sociales y finalmente el 13% usa para herramientas de ofimática, por lo tanto da a entender que la mayor parte de los encuestados están en constante uso de los servicios, siendo esto un riesgo de seguridad si no se usa correctamente.

Tabla 5
Tabulación de resultados obtenidos de la pregunta 5.

5.- ¿Conoce de algún protocolo de seguridad para la protección de datos?			
	Si	121	53%
	No	109	47%
Total		**230**	**100%**

Figura 9
Tabulación de resultados obtenidos de la pregunta 5.

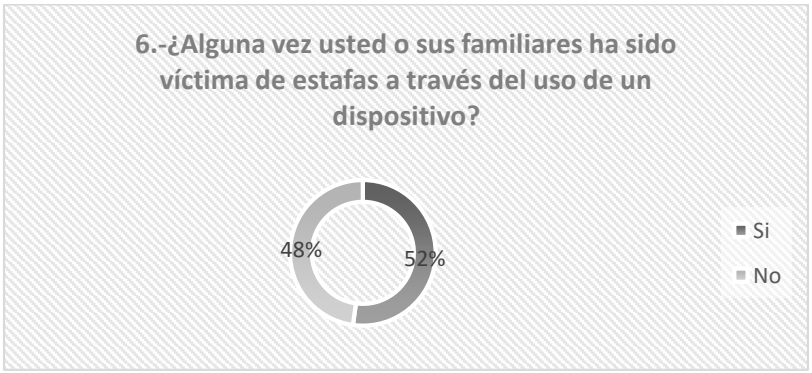
En la Figura 6 se observa que el 53% de los encuestados tiene conocimiento de algún protocolo de seguridad, a diferencia del 47% que no conoce de medidas de seguridad para protección de los datos

siendo esto una estadística importante ya que esto generaría múltiples formas de inseguridad cuando hacen uso de algún recurso tecnológico.

Tabla 6
Tabulación de resultados obtenidos de la pregunta 6.

6.- ¿Alguna vez usted o sus familiares ha sido víctima de estafas a través del uso de un dispositivo?			
	Si	120	52%
	No	110	48%
Total		**230**	**100%**

Figura 10
Tabulación de resultados obtenidos de la pregunta 6.



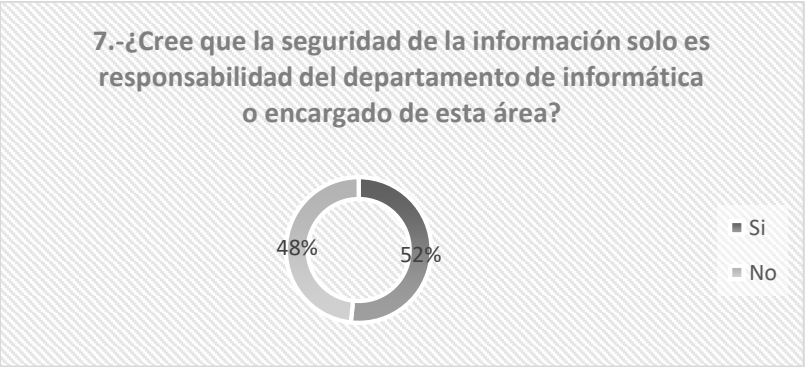
En la Figura 7 se observa que el 52% de los encuestados en algún momento han sido víctima de estafa ya sea el usuario o su familiar, mediante el uso de algún dispositivo, mientras que el 48% dice que no han sufrido algún incidente de inseguridad, esto evidencia que la mitad de los encuestados en algún momento su información que intercambiaron fue vulnerada y usada para cometer algún acto de perjuicio en su contra, esto ya sea por su inadecuado uso de los recursos tecnológicos.

Tabla 7
Tabulación de resultados obtenidos de la pregunta 7.

7.- ¿Cree que la seguridad de la información solo es responsabilidad del departamento de informática o encargado de esta área?			
	Si	119	52%
	No	111	48%
Total		**230**	**100%**

Figura ***11***

Tabulación de resultados obtenidos de la pregunta 7.



En la Figura 8 se observa que el 52% de los encuestados dice que la responsabilidad de la seguridad de la información le corresponde al departamento de informática a donde asisten, sin embargo, el 48% indica que no sería responsabilidad del departamento de informática, dando a entender que la seguridad de la información es responsabilidad de todos los que conforman la Institución a la que asisten.

Resumen de la recolección de los datos

Después de haber obtenido los resultados y tabulado de los datos se ha llegado a la conclusión de que la mayoría de los encuestados utilizan el servicio de internet para uso de varias actividades, también se ha identificado que usan más de un recurso tecnológico para intercambiar información y finalmente se ha identificado que más de la mitad de los usuarios no conocen de algún protocolo de seguridad para la información con base a esto, se evidencia que han sido víctimas de estafas por el mal uso de los dispositivos y de igual manera piensan que la responsabilidad es solo del departamento de informática cosa que no sería cierta, la responsabilidad es de todos los usuarios que son parte de la Institución a la que pertenecen y en si hay que tener conciencia del uso y la información que se comparte en esta era tecnológica de la que somos parte. Esta técnica de recolección de datos ha sido esencial ya que permitió identificar aspectos de seguridad de información de la Unidad Educativa en la que se plantea el proyecto, por lo cual sería factible la propuesta que se plantea en el siguiente capítulo del presente documento.

CAPÍTULO II: PROPUESTA

1.1. Descripción de la propuesta

En el documento se plantea la propuesta de un modelo de sistema de gestión de seguridad de la información para la Unidad Educativa Fray Jodoco Ricke, utilizando como referente la norma ISO 27001, tiene el propósito mitigar situaciones de seguridad de la información las cuales comprende la protección de los usuarios para fortalecer la confidencialidad, integridad y disponibilidad de la información, para que a futuro se pueda tener un ambiente responsable, seguro y de conformidad para compartir información.

a. Estructura general

A continuación, se muestra en la figura 10 la estructura en la que se ha diseñado la propuesta. La propuesta se va a hacer según el diagrama que se encuentra en la figura 10 la misma que contine las siguientes fases. Y cuyo entregable se encuentra en el anexo

Figura 12
Diagrama de la estructura general de la propuesta.

Nota: Adaptado de Objetivos de la ISO 27001, Seguridad de la información: ISO 27001 Paso a paso - Implementación del SGSI.(https://normaiso27001.es/fase-6-implementando-un-sgsi/)

b. Explicación del aporte

Para el desarrollo de la propuesta se toma como referencia la normativa ISO/IEC 27001:2013 en donde se plantea un modelo de sistema de gestión de seguridad de la información, sugiriendo algunos controles de seguridad que contiene la normativa los cuales son los mas adecuados para la Unidad Educativa “Fray Jodoco Ricke”.

- **Descripción de la Institución**

La Unidad Educativa Fray Jodoco Ricke es una institución de educación media de bachillerato del sector público, con un tamaño de población conformado por 567, cuenta con alrededor de 5 directivos 22 docentes en el Colegio y 540 estudiantes alumnos. Tiene alrededor de 5 años de labor y se encuentra ubicada en la ciudad de Quito sector El Comité del Pueblo en la Av. La Bota y 28 de mayo.

- **Análisis DAFO**

En la Tabla 8 se presenta un análisis de las brechas de seguridad y la situación de la Unidad Educativa Fray Jodoco Ricke, se procede a utilizar la matriz DAFO en donde se puede identificar las Debilidades, Amenazas, Fortalezas y Oportunidades, en el ámbito de la seguridad de la información.

Tabla 8

Matriz DAFO

DEBILIDADES	FORTALEZAS
• No se cuenta con servidor alterno, para respaldos. • Algunos de los equipos no cuentan con licencias de software, solo usuarios específicos cuentan con licencia activa, pocos equipos cuentan con software de uso libre. • Carecen de conocimiento sobre la seguridad de la información. • El acceso al área de equipos de red o de telecomunicaciones no se encuentra organizada y baja protección es evidente al público. • Ausencia de planes de contingencia en caso de pérdida de la información. • El personal encargado le falta capacitación en seguridad de la información.	• Algunos equipos cuentan con software libre como Linux Ubuntu. • Se dispone de control de acceso a computadoras de laboratorios en hoja de registro. • El acceso a red en los equipos es la mayor parte es por cable.

• No existe apoyo en el proceso de TICS. • Falta de comunicación respecto al uso de los recursos tecnológicos. • No se socializa sobre el uso que se debe dar a los equipos tecnológicos.	
AMENAZAS	**OPORTUNIDADES**
• Usar equipos que no se les han asignado para su uso. • No prestar atención a las indicaciones que se muestran durante el uso de los recursos tecnológicos. • Usar equipos sin antivirus, que están caducados o sin licencia. • No cerrar las sesiones en las que se autentifica como correo electrónico, acceso a plataformas, redes sociales, etc. • Utilizar contraseñas comunes y fácil de adivinar. • No hacer copias de seguridad de la información. • Abrir correos electrónicos sospechosos que son intento de robo de información. • Utilizar redes sociales y abrir mensajes o contenido sospechoso de origen desconocido. • Instalar aplicaciones de terceros sin conocer el origen de fabricación. • Usar dispositivos de almacenamiento externo como memorias USB, discos duros, etc. • Conectarse a las redes públicas que se muestran en el dispositivo. • Prestar el recurso tecnológico a terceras personas.	• Aumentar la seguridad de la Unidad Educativa. • Establecer políticas de Seguridad de la Información. • Determinar controles y normas para el manejo de recursos tecnológicos. • Definir procedimientos y políticas para el tratamiento de la información. • Reducir riesgos que afecten a la seguridad, disponibilidad y confidencialidad de la información. • Disponer de un sistema de gestión de seguridad de información.

Nota: Esta matriz muestra un análisis de la situación de la Unidad Educativa Fray Jodoco Ricke.

Actualmente la institución no cuenta con una normativa o algún sistema de gestión de seguridad de la información, una vez realizado el análisis previo del estado actual de la Unidad Educativa, se evidencia que la seguridad de la información en la institución no posee políticas ni normativas, para lo cual las autoridades deben apoyar la propuesta del proyecto.

1.1. Viabilidad de la propuesta

Como se evidencia en hechos anteriores la carencia de seguridades de la información en la Unidad Educativa Fray Jodoco Ricke es necesario esta propuesta de establecer controles y políticas de seguridad para evitar la pérdida de información, las cuales deben estar basadas en la normativa ISO 27001:2013 de acuerdo con las necesidades de aplicación que sean necesarias para la Institución en el ámbito. Se identifica sobre los activos, amenazas, vulnerabilidades. Sin embargo, la implementación de dicha propuesta queda en manos de la Institución, ya que luego de observar la situación, es evidente la necesidad de este caso de estudio, en donde se debe acordar con los involucrados directos acciones presupuestarias y administrativas, para su implementación.

1.2. Desarrollo de la propuesta

En el presente documento se plantea un modelo de sistema de seguridad de la información para la Unidad Educativa Fray Jodoco Ricke, dicho documento proporciona la base fundamental para la protección de la información y su uso queda libre y voluntario para su respectiva implementación, por tal motivo, se presentan a continuación los apartados del modelo de procedimientos que se deben tener para garantizar un funcionamiento adecuado mediante un sistema de gestión de seguridad de la información basado en la normativa ISO 27001:2013 para la Unidad Educativa.

Evaluación de requisitos de la normativa ISO 27001:2013

Para la evaluación de las condiciones iniciales del establecimiento en cuanto a normas y reglamentos de seguridad que son aspectos marcados como obligatorios en la norma 27001:2013, en este sentido, los puntos enumerados en los apartados de la norma ISO utilizada han sido los aspectos que se evalúan en la Institución como el: Contexto, Planificación, Soporte, Operación, Evaluación y Mejora, dicha evaluación se puede ver en el Anexo 2.

1.2.1. Contexto de la organización

La Unidad Educativa Fray Jodoco Ricke es una institución de educación media de bachillerato del sector público, con un tamaño de población conformado por 567, cuenta con 5 directivos 22 docentes y 540 estudiantes. La situación actual de los estudiantes a nivel económico no es la más buena ya que en la mayoría no tiene acceso a internet en sus hogares y también son de escasos recursos económicos. Actualmente el laboratorio cuenta con 15 máquinas las cuales tienen 2 gigas de memoria RAM y sus procesadores son de tercera generación pues estos equipos fueron adquiridos hace más de 10 años y hasta en la actualidad no se han renovado, además tampoco los directivos han hecho alguna gestión para pedir al distrito recursos tecnológicos de nueva generación y el hallazgo más grave es que el sistema operativo de las máquinas es obsoleto ya que están con Windows 7 el cual ya no tiene soporte por parte de Microsoft. En el uso diario también están laptops las cuales se hace cargo cada docente estas tienen 4 Gb de memoria RAM con un sistema operativo de Windows 8, pero tanto su sistema como sus licencias requieren una renovación y actualización.

- **Liderazgo**

Se establece la alta dirección, es decir, autoridades de la institución, se les asigna un rol para desarrollar las actividades del sistema de seguridad de la información en la que participan para determinar los objetivos que se pretenden con la implementación del SGSI, aprobar políticas generales de seguridad de la información, definir los roles y responsabilidades del personal en asuntos de seguridad entre otros, para constancia ver anexo 3 donde se define.

- **Alcance**

De acuerdo con las autoridades de la unidad educativa, un convenio es para la gestión de la seguridad de la información aplicada en las áreas donde se encuentran los recursos tecnológicos, en este caso, es producto en el campo TIC, el cual es a cargo de la infraestructura tecnológica como: telecomunicaciones, instalación, mantenimiento y manejo de recursos informáticos la Unidad Educativa.

- **Objetivos del sistema de seguridad de la información**
  - Mejorar la seguridad de la información de la Institución mediante controles que permitan aumentar la disponibilidad de la información, a través de la modificación de actividades asociadas al área de TIC.
  - Crear políticas de seguridad apropiadas para la institución, que son consideradas por los usuarios de la Institución para mejorar la seguridad de la información.

- Relacionarse con los incidentes y amenazas a la seguridad de la información que puedan darse, para dar una respuesta adecuada a estos inconvenientes.
- Repotenciar la infraestructura de red de la institución con dispositivos y herramientas de seguridad de la información.

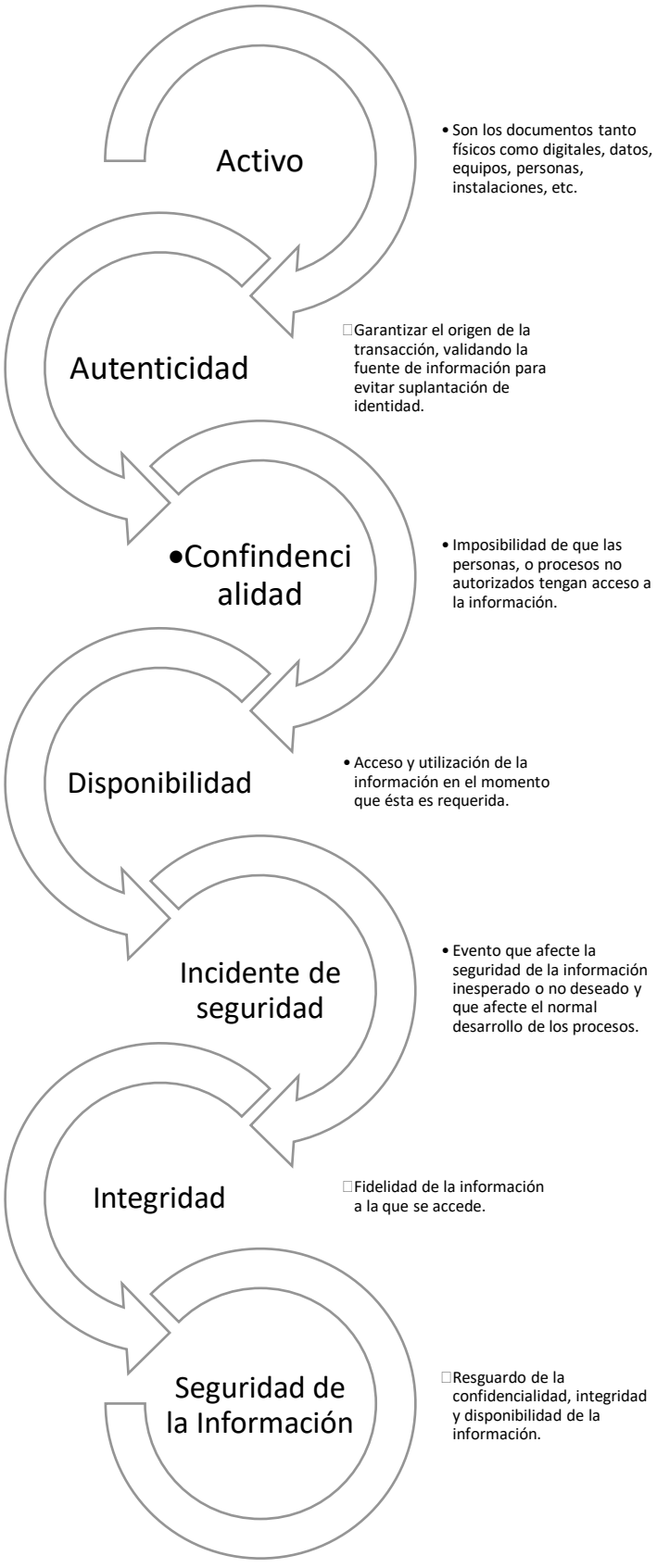
Responsabilidades del sistema de seguridad de la información

Para continuar con la ejecución de la propuesta se requiere una definición de sus responsables, con el objetivo de que todo el personal sea consciente de su papel en el sistema, es fundamental identificar como son: los roles, personal de apoyo y cumplimiento de la política de información, los cuales se describen en el Anexo 4.

Política de seguridad de la información

Se elabora las políticas de Seguridad de la Información las cuales permiten proteger la información de la Unidad Educativa de las diversas amenazas que puedan presentarse, para garantizar la continuidad de su funcionamiento en su estancia, las cuales se basan en los siguientes conceptos, y se determina dichas políticas en el Anexo 5, a demás en la figura 12 se puede ver los conceptos que se consideraron para el desarrollo de las políticas de la seguridad de la información de la Unidad Educativa Fray Jodoco Ricke

Figura 13
Elementos del sistema de seguridad



Elaborado por: Jonathan Cueva, 2022, fuente, propia.

Inventario de activos de información

El inventario de activos de información se elaboró con los responsables de los recursos y usuarios que manejan información en las áreas de TIC, dicho inventario se muestra en Anexo 5.1.

Figura 14
Resumen del inventario de computadoras.

Tipo de computadora	Estado	Sistema Operativo	Marca
15 pc Escritorio	Bueno	Windows 7	XTRATECH
35 laptop	Bueno	Windows 8	HP

Nota. Elaborado por Jonathan Cueva, 2022, Fuente: propia. Resumen del inventario de computadoras que forma parte de los activos de la Unidad educativa Fray Jodoco Ricke.

En lo que respecta el inventario de activos se pudo identificar a los recursos de la Institución en donde se puede notar que están distribuidos en diferentes lugares como es: rectorado, vicerrectorado, audiovisuales y en el laboratorio existen 15 máquinas de escritorio, también se encuentran distribuidos en los Docentes 35 equipos Portátiles, dichos equipos son para uso de labores educativas, a parte de los equipos de computación se incluyó al inventario las impresoras que están distribuidas en el laboratorio y dos en el área de los directivos. Y finalmente se identificó los equipos de telecomunicaciones los cuales se encuentran en el laboratorio de la Institución.

Durante la elaboración del inventario se pudo observar que no disponen de seguridades en los sitios donde se encuentran los recursos tecnológicos y también no hay una persona encargada del control de los equipos y sistemas, por lo tanto, existe un desconocimiento de normas procesos y estándares que aseguran los activos de la información así mismo, la gran parte de los equipos se encuentran desactualizados y sin un software antivirus, estos hallazgos son fundamentales para que se tome en cuenta en el sistema de seguridad de la información.

Identificación de amenazas vulnerabilidades

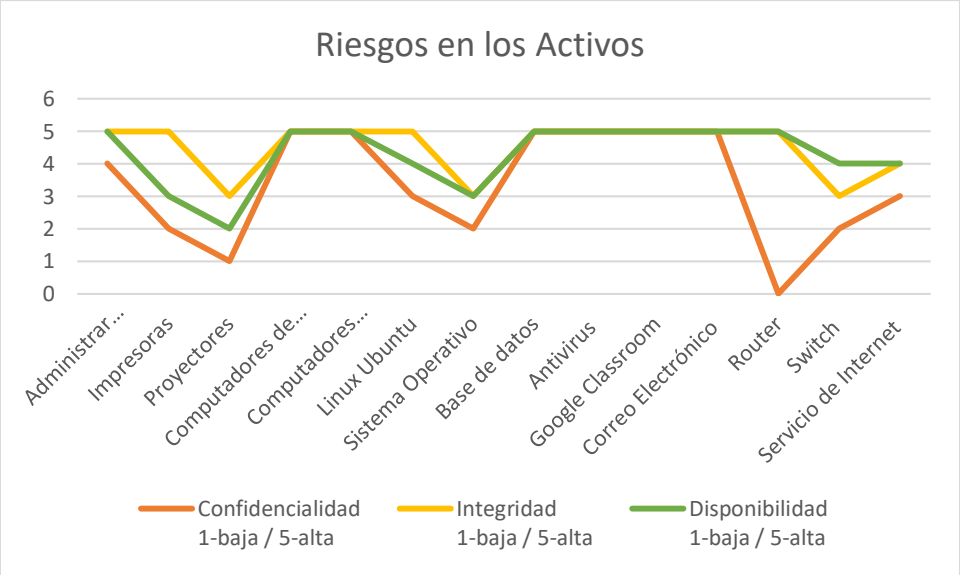
En el Anexo 5.2 se puede observar las detecciones, que se dan en los activos de forma común en la infraestructura, los usuarios, las telecomunicaciones, el hardware y el software. Los cuales están agrupados en las posibles amenazas comunes, por lo que es posible ver que la propuesta del sistema de seguridad de la información es necesaria. En la recolección de las amenazas y vulnerabilidades influye el hecho de que actualmente estos se encuentran comprometidos por los efectos que se puedan dar, en este caso estas brechas de seguridad que se identificó deben ser tratadas para evitar futuras pérdidas de información en los activos de la Institución.

Identificación de riesgos

En el Anexo 5.3 se presenta el nivel de riesgo que tiene la Institución en donde se describe el nombre del activo, el tipo y los criterios de evaluación que corresponden a la confidencialidad, integridad y disponibilidad de los sistemas de información.

Para la identificación de los riesgos en base a las vulnerabilidades y amenazas se procedió con una apreciación con escala de valores y definiendo criterios de evaluación en referencia a las recomendaciones de la norma ISO/IEC 27005, en donde el valor 1 representa muy bajo y el valor 5 representa muy alto, la suma de estos en los criterios de confidencialidad integridad y disponibilidad da el total del riesgo en donde se determina como el valor 1 muy bajo y el valor 15 como muy alto, mostrando el riesgo que tiene los activos que se presentó en la tabla que antecede. En esta evaluación de los riesgos se aprecia que algunos activos que presentan muy alto riesgo son de vulnerabilidades y amenazas evidentes que si no se toma acciones preventivas o correctivas puede generar pérdidas en los activos de la información. Como se muestra en la figura 13 los resultados de la evaluación de riesgos realizada.

Figura 15
Identificación de riesgos en los activos.



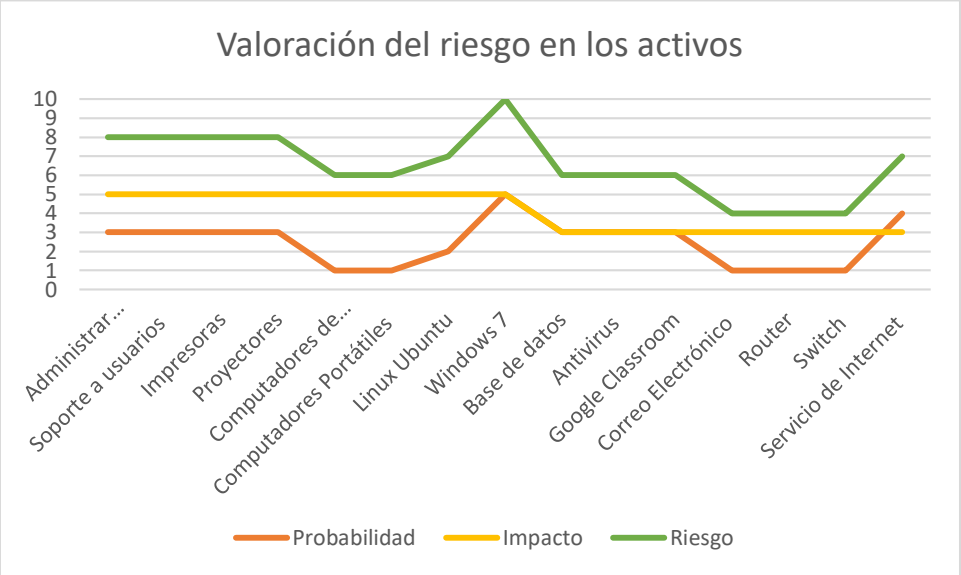
Nota. Elaborado por Jonathan Cueva, 2022, Fuente: propia. Las vulnerabilidades del colegio están totalmente comprometidas tanto en la integridad, confidencialidad y disponibilidad, ya que no se han actualizado y tampoco se han implementado configuraciones adecuadas.

Valoración de riesgos

En la valoración del riesgo para los activos críticos, basado en un listado de amenazas comunes y con la valoración de P= probabilidad, I= impacto, entonces para el cálculo del riesgo se suman los dos R= riesgo el resultado se muestra en el Anexo 5.4.

Figura 16

Valoración del riesgo en los activos.



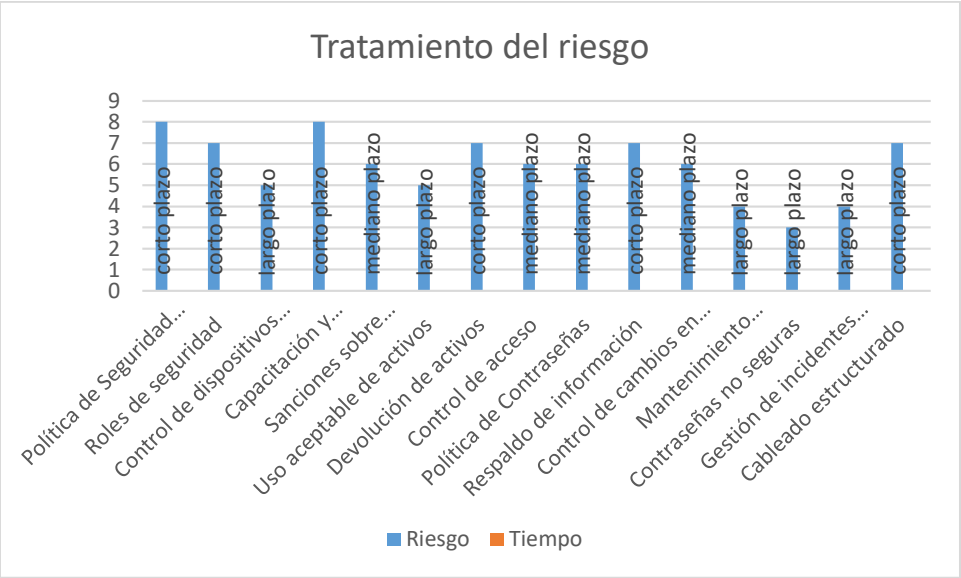
Nota. Elaborado por Jonathan Cueva, 2022, Fuente: propia. Según la escala se aprecia que la valoración del impacto en dichos activos es muy alta, así como también los riesgos que implica esto, sin embargo, no podemos dejar de lado la probabilidad de que suceda a pesar de esta es baja puede pasar.

Tratamiento del riesgo

El tratamiento del riesgo permite tomar decisiones para actuar frente a riesgos analizados, a continuación, se describen los criterios del tratamiento de riesgos:

- Aceptar riesgo: se acepta el riesgo sin realizar ninguna acción, ya que los costos de solución podrían ser mayores al origen del riesgo.
- Reducir riesgo: se toman acciones para minimizar y reducir la probabilidad de que se provoque el riesgo.
- Evitar el riesgo: tratar de eliminar las actividades que tomen riesgo.
- Transferir riesgo: trasladar el riesgo a terceros en este caso se lo hace a: especialistas, empresas, u otras entidades entendidas en el tratamiento de riesgo.

Figura 17
Tratamiento del riesgo



Nota. Elaborado por Jonathan Cueva, 2022, Fuente: propia. Para ver el resultado del tratamiento de riesgo se muestra en el Anexo 5.5, los riesgos identificados que están en un nivel alto o medio se deben realizar acciones a corto o mediano plazo, a diferencia de los riesgos con un nivel bajo pueden tomarse la decisión de asumir el riesgo o realizar acciones en un tiempo más largo y finalmente los riesgos con nivel mínimo serán aceptados por la Unidad Educativa.

Aplicabilidad de los controles de seguridad

La aplicabilidad se puede ver en el Anexo 6, la cual se representa en una matriz que se define criterios de evaluación para confrontarlos con los controles actuales que maneja la Institución, para posteriormente definir controles de aplicabilidad propuestos por el proyecto en prioridad operativa para establecer las bases para eliminar en la medida posible las amenazas y vulnerabilidades detectadas en la Institución.

Propuesta de SGSI

Los sistemas de gestión son muy necesarios y es importante mencionar que estás políticas son complementarias dentro de la Unidad Educativa “Fray Jodoco Ricke”, por la confidencialidad, integridad y disponibilidad que nos brinda, evitando las amenazas y vulnerabilidades de los activos de información esenciales dentro de la comunidad educativa, el cual se encuentra en el Anexo 7.

CONCLUSIONES

Ecuador a pesar de ser un país tercermundista tiene estudiantes que usan computadores, tabletas y teléfonos para su educación, sin embargo, ninguno sabe a qué peligros no más están expuestos, como el acoso a través de redes sociales. Así también el Ecuador en el año 2021 ocupó la sexta posición dentro de los países con más detecciones de malware entre la comparativa con Latinoamérica.

La comunidad educativa se conecta a la red Wi-Fi para hacer documentos legales delicados y transferencias bancarias sin usar ninguna protección, a esto se agrega que muchos de los usuarios desconocen de algún protocolo de seguridad o protección a nivel de la infraestructura que les permita navegar de manera segura a través de la red. Tampoco usan la información en las redes sociales de manera prudente, ya que los ciberdelincuentes se aprovechan de esto para obtener información y a través de esto generar acoso y sobornos.

Las brechas que tiene el laboratorio son muy altas por la limitada capacidad del harware ya que están con sistema operativo obsoleto sin soporte “Windows 7”, además esta mal configurado los protocolos y servicios de seguridad de router de la marca d-link el cual solo tiene configurado como seguridad el protocolo wps en modo desactivado, así también no cuenta con ningún tipo de firewall para el análisis del malware y por último no disponen de ningún antivirus, pues determina que vulnerabilidades por todas partes dentro del laboratorio.

Al revisar las diferentes normativas que existen dentro de la ISO 27000, se puede determinar que esta última fue publicada en mayo de 2022 la misma que tiene algunas autorizaciones que para el caso de este proyecto no se toma en cuenta algunos aspectos de control.

RECOMENDACIONES

En vista que el colegio no tiene estipulada alguna visión y misión dentro de las proyecciones a futuro se recomienda diagnosticar de acuerdo al entorno y definir la proyección a futuro de la institución, además la infraestructura que tiene actualmente el laboratorio esta casi obsoleto ya que los componentes de hardware no son los suficientes, por ende, las autoridades del colegio deben tomar cartas en el asunto para pedir al distrito la Delicia una mejora a nivel de la infraestructura para el laboratorio siendo de una necesidad primordial para el desarrollo de los futuros bachilleres técnicos.

Capacitar a toda la comunidad educativa en Materia de Seguridad de la información ya que el peldaño más débil dentro de la cadena de la seguridad es el factor humano, además de crear una cultura en cuanto a los conocimientos de cómo protegerse ante los ciberdelincuentes, como por ejemplo dar un buen tratamiento a los documentos que son confidenciales.

Se recomienda qué tanto instituciones públicas y privadas deberían contar con el sistema de gestión de seguridad de la información para salvaguardar los activos ya que son la razón de ser de las instituciones, para dar continuidad al funcionamiento de las diferentes actividades que realizan a diario.

BIBLIOGRAFÍA

Acurio, J. A. B. (2019). Propuesta de sistema de gestión de seguridad de la información utilizando la norma ISO 27001 para la Unidad Educativa Nuestra Señora de Fátima (p 2).

Areitio, J. (2018). Seguridad de la información. Redes, informática y sistemas de información. Madrid: Paraninfo.

Cuvi, G. P. A. (2019). Diseño de un sistema de gestión de seguridad de la información mediante a aplicación de la Norma Internacional ISO/IEC 27001: 2013 en la Unidad Educativa Adventista Gedeón, 2, 1–13.

Díaz, F. J., Venosa, P., Macia, N., Lanfranco, E. F., Sabolansky, A. J., Durante, M., ... & Pretto, J. (2021). Investigación en ciberseguridad en un año de pandemia. In XXIII Workshop de Investigadores en Ciencias de la Computación (WICC 2021, Chilecito, La Rioja).

Echeverría, F. R., Márquez-Dominguez, C., Pérez, A. G., & Rodríguez-Clavijo, F. (2020). La importancia de la tecnología en momentos de pandemia. Revista Ibérica de Sistemas e Tecnologias de Informacion, (E32), IX-XI.

Galence, V. P. (2017). El ciber-acoso con intención sexual y el child-grooming. Quadernos de criminología: revista de criminología y ciencias forenses, (15), 22-33.

García Cruz, R. A. (2020). Propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la oficina de Tecnologías de Información del Gobierno Regional Piura; 2020. Universidad Católica Los Ángeles de Chimbote, 9, 102. http://repositorio.uladech.edu.pe/handle/123456789/20291.

ISO 27001. (2015). Paso a paso - Implementación del SGSI. ISO 27001. https://normaiso27001.es/fase-6-implementando-un-sgsi/

Mayorga, T. (2014). Seguridad informática y la relación en la utilización de internet como herramienta de apoyo en la formación de niños, niñas y adolescentes de educación inicial y básica del Centro Educativo la Pradera. Ambato: Universidad técnica de Ambato.

Nieves, A. C. (2017). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma Iso/iec 27001: 2013.

Ortiz, D. (2021, 29 julio). Ecuador está entre los países con más ciberataques en América Latina. El Comercio. https://www.elcomercio.com/tendencias/tecnologia/ecuador-ciberataques-america-latina-hacker.html.

Ormella, C.(2017). SGSI-2700. http://www.criptored.upm.es/ /NuevasVersionesIS027000es.pdf

PAe. (2015). MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Administracionelectronica.gob.es.

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.YwHFBXZBwdU

Patiño Rosado, S. G. (2018). Propuesta metodológica de gestión de riesgos de Tecnología de información y comunicación (TIC) para entidades públicas conforme normativa NTE INEN ISO/IEC 27005.

Puga Jácome, D. S. (2021). Ciberseguridad y la pandemia del coronavirus: phishing y ramsonware, un análisis de ciberinteligencia a las actividades de teletrabajo (Doctoral dissertation, QUITO/UIDE/2021).

Quimíz, E. L. (2021). Modelos de seguridad de la información para el control de los riesgos informáticos en el área administrativa de una empresa de operadores logísticos de comercio exterior en la ciudad de Guayaquil. 1996, 6.

Secaira, J. M., Ocampo, R. D., Mera, E. Z., & Kovalenko, I. E. D. (2020). El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador). (Original). Roca. Revista Cientifico-Educacional de La Provincia Granma, 16, 546–559. https://revistas.udg.co.cu/index.php/roca/article/view/1562/2769.

Seguridad de la información. (2020, July 14). Aspectos a tener en cuenta. Ayuda Ley Protección Datos. https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/

UNIDAD DE EMPRENDIMIENTO VIRTUAL. (2015). Cálculo del Tamaño de la Muestra. Blogspot.com. http://hachepe57.blogspot.com/2010/05/l-calculo-del-tamano-de-la-muestra.html

Vegas, I. (2019). Diseño de un Sistema de Gestión de Seguridad de la Información para los procesos académicos de la Universidad Nacional de Piura Según la NTP ISO/IEC 27001. 181. https://repositorio.unp.edu.pe/handle/UNP/1875.

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. Revista Ibérica de Sistemas e tecnologías de Información, (22), 73.

ANEXOS

ANEXO 1

FORMATO DE ENCUESTA

Universidad Israel

Encuesta

Objetivo: Determinar la seguridad de la información que se esta manejando en el uso de dispositivos y la conexión a internet que utilizan los usuarios de la Unidad Educativa Fray Jodoco Ricke, para identificar las vulnerabilidades o riesgos a los que están expuestos.

Instrucciones: La presente encuesta tiene como finalidad obtener datos para la elaboración de un proyecto de investigación del estudiante de la Universidad Tecnológica Israel. A continuación se presentan preguntas referentes a la seguridad de la información, por favor lea y conteste cada una de las preguntas.

1.- ¿Tiene servicio de internet propio?

- ○ Si
- ○ No

2.-¿Qué tipo de conexión usa para conectarse a internet?

- ☐ Datos móviles
- ☐ Servicio de internet de hogar o trabajo
- ☐ Puntos de internet acceso público

3.- ¿Qué dispositivo usa para conectarse a internet?

- ☐ Smartphone
- ☐ Tablet
- ☐ Computadora de casa o trabajo
- ☐ Computadora de uso público

4.- ¿Al hacer uso de internet que servicios utiliza?

- ☐ Redes sociales
- ☐ Ofimática
- ☐ Correo electrónico
- ☐ Navegación web
- ☐ Entretenimiento
- ☐ Todos

5.- ¿Conoce de algún protocolo de seguridad para la protección de datos?

- ○ Si
- ○ No

6.-¿Alguna vez usted o sus familiares ha sido víctima de estafas a través del uso de un dispositivo?

- ○ Si
- ○ No

7.-¿Cree que la seguridad de la información solo es responsabilidad del departamento de informática o encargado de esta área?

- ○ Si
- ○ No

ANEXO 2

Evaluación de requisitos de la norma ISO 27001

Apartado	Requisitos	Aspectos	Cumple	
4.1	Contexto de	Comprende a la organización y su contexto.	Si	
4.2	la	Comprende las necesidades y expectativas y obligaciones de las partes interesadas.		No
4.3	Organización	Está definido del alcance del SGSI.	Si	
4.4		Existencia de un SGSI.		No
5.1		Esta establecida una línea de Liderazgo y esta, está Comprometida con la implementación del SGSI.	Si	
5.2	Liderazgo	Existen políticas claras y definidas en cuanto al control y manejo de la información.		No
5.3		Se conocen los roles, responsabilidades y autoridades organizacionales con respecto al SGSI.		No
6.1.1		Existen acciones generalidades para tratar los riesgos y oportunidades.		No
6.1.2		Existe un método de valoración de los riesgos de la SI.		No
6.1.3	Planificación	Existe una forma de identificación de los avances en el tratamiento de los riesgos de la SI.		No
6.2		Están definidos y documentados los objetivos de la SI, así como los planes para alcanzar dichos objetivos.		No
7.1		Existen recursos o dispersión para asignar estos para la implementación del SGSI.	Si	
7.2		Esta disponible personal competente que se pueda encargar del SGSI una vez que se implemente.		No
7.3		Se ha realizado alguna campaña institucional para la difusión de importancias y alcances de un SGSI.		No
7.4	Soporte	Se emplean adecuadamente los medios de información institucionales para divulgar lo concerniente al SGSI.		No
7.5.1		Se posee información sobre los SGSI		No
7.5.2		Existen documentos de documentación de un SGSI que se pueda actualizar.		No
7.5.3		Existe controles para los documentos del SGSI		No
8.1		Existen controles de los procesos aplicables a los objetivos del SGSI.		No
8.2	Operación	Existe una valoración de riesgos previa		No
8.3		Existe una planificación o metodología asociada a la corrección de los Riegos de SI		No
9.1	Evaluación del	Existen procesos de SI que puedan ser evaluados		No
9.2	Desempeño	Hay algún plan de auditoría Interna		No
9.3		Existe algún plan de revisión por parte de la dirección del plantel sobre el SGSI		No
10.1	Mejora	Se tiene un plan para tratar las no Conformidades en los procesos relacionados con el SGSI		No
10.2		Existe un plan de mejora continua		No

ANEXO 3

LIDERAZGO

Sujetos Involucrados	Rol
Rector	Máxima autoridad de la Unidad Educativa, quien aprueba las acciones que se toman en la Institución.
Vicerrector	Autoridad que trabaja conjuntamente con el Rector y en caso de ausencia del órgano principal lo reemplaza.
Inspector	Encargado de supervisar actividades de los usuarios de la Unidad Educativa.
Secretaria	Nombrada para gestión de aspectos académicos de la institución.
Departamento de TIC	Encargado de la Gestión de la Tecnología de la Información y Comunicación de la Institución.
Estudiantes	Están sujetos a las indicaciones y normativas quienes asisten y hacen uso de los recursos de la Unidad Educativa bajo jurisdicción de los de las autoridades y Docentes.

ANEXO 4

RESPONSABILIDADES DEL SITEMA DE SEGURIDAD DE LA INFORMACIÓN

Rol	Responsabilidades
Autoridades	Las mismas deberán definir el alcance, definir los objetivos y aprobar la política de seguridad diseñada en la institución. Se conformará una comisión técnica denominada Comité de Seguridad de la Información compuesta por autoridades y director de TIC, esta comisión deberá coordinar la Gestión de la Seguridad de la Información de los usuarios de la Institución.
Oficial de Seguridad de la Información	Se designará como Oficial de Seguridad de la Información al director de TIC, el cual será responsable de velar por las medidas de seguridad de la Institución, identificar temas de capacitación y iniciar acciones adecuadas para el buen funcionamiento.
Responsable de Talento Humano	Se designará al Inspector en coordinación con secretaria como responsables de la Dirección de Talento Humano para comunicar a todos los usuarios de la Institución, las obligaciones respecto a las Políticas de Seguridad de la Información y tendrán a su cargo la suscripción de un acuerdo con términos y condiciones de uso de los recursos tecnológicos.
Responsable de tecnología	Se designará a un responsable ya sea un miembro del departamento de TIC como auxiliar quien instaurará medidas de seguridad para mitigar riesgos.

ANEXO 5: POLÍTICAS DE SEGURIDAD DE LOS ACTIVOS DE LA INFORMACIÓN

Organización de la seguridad de la información

La Gestión de la Seguridad de la Información en la Institución estará a cargo de un comité técnico, que deberá incluir a todo el personal de la Unidad Educativa. Este comité tendrá que reunirse de manera periódica, registrando los encuentros realizados.

El Inspector será responsable de comunicar a los usuarios de la Unidad Educativa, sus obligaciones respecto a las Políticas de Seguridad de la Información.

Las autoridades o el máximo organismo serán los encargados de comunicar a los docentes y estudiantes a su cargo las obligaciones del cumplimiento de estas políticas.

Los propietarios o usuarios de la Información en la Unidad Educativa tendrán la responsabilidad, mantener actualizada la misma y definir los accesos a los usuarios de acuerdo con sus funciones y competencia.

Encargado del departamento de TIC u oficial de seguridad de la información, debe ser elegido por las autoridades y docente, el mismo que será responsable de llevar a cabo medidas de seguridad, capacitación y mantener operativo los recursos tecnológicos.

Activos de información

Los activos deben etiquetarse mediante el procedimiento designado como “Clasificación y etiquetado de Información” de acuerdo a lo siguiente.

El departamento de TIC deberá disponer de herramientas tecnológicas que faciliten el inventario y clasificación de los activos.

Implantar normas y procedimientos para el manejo de la información ya sea en medios, físicos o digitales.

Recurso humano

Las autoridades y el departamento de TIC en sus procedimientos la planificación y administración deberán hacer una previa investigación de los nuevos usuarios que son parte de la Unidad Educativa esto incluye a toda la comunidad educativa para prevenir riesgos de error humano de uso inadecuado de los recursos, robo, fraude, etc.

Se deberá establecer acuerdos y condiciones en los contratos de trabajo estableciendo responsabilidades del personal de la Unidad Educativa.

ANEXO 5.1: INVENTARIO DE ACTIVOS

	DESCRIPCIÓN CARACTERÍSTICA DEL BIEN	CÓDIGO	ESTADO	SERIE	MODELO	MARCA	COLOR	MATERIAL	UBICA
1	C.P.U.	**U.E.F.J.R. 1670**	BUENO	64921	CORE I3	ULTRATECH	NEGRO	METAL/PLASTICO	LABORA
2	C.P.U.	**U.E.F.J.R. 1673**	BUENO	64925	CORE I3	ULTRATECH	NEGRO	METAL/PLASTICO	LABORA
3	C.P.U.	**U.E.F.J.R. 1669**	BUENO	64918	CORE I3	ULTRATECH	NEGRO	METAL/PLASTICO	LABORA
4	C.P.U.	**U.E.F.J.R. 1683**	BUENO	64946	CORE I3	ULTRATECH	NEGRO	METAL/PLASTICO	LABORA
5	C.P.U.	**U.E.F.J.R. 1677**	BUENO	64892	CORE I3	ULTRATECH	NEGRO	METAL/PLASTICO	LABORA
7	C.P.U.	**U.E.F.J.R. 1678**	BUENO	64890	CORE I3	ULTRATECH	NEGRO	METAL/PLASTICO	LABORA
9	C.P.U.	**U.E.F.J.R. 1685**	BUENO	64944	CORE I3	ULTRATECH	NEGRO	METAL/PLASTICO	LABORA
10	C.P.U.	**U.E.F.J.R. 1679**	BUENO	64887	CORE I3	ULTRATECH	NEGRO	METAL/PLASTICO	LABORA
12	C.P.U.	**U.E.F.J.R. 1675**	BUENO	64889	CORE I3	ULTRATECH	NEGRO	METAL/PLASTICO	LABORA
13	C.P.U.	**U.E.F.J.R. 1684**	BUENO	64945	CORE I3	ULTRATECH	NEGRO	METAL/PLASTICO	LABORA
14	C.P.U.	**U.E.F.J.R. 1687**	BUENO	64949	CORE I3	ULTRATECH	NEGRO	METAL/PLASTICO	LABORA
15	C.P.U.	**U.E.F.J.R. 1681**	BUENO	64888	CORE I3	ULTRATECH	NEGRO	METAL/PLASTICO	LABORA
1	**IMPRESORA**	**S/C**	BUENA	L355		EPSON	NEGRO	METAL/PLASTICO	LABORA
1	**LAPTOP**	**S/C**	BUENA	CND4381L1N	CORE I3	HP	NEGRO	PLASTICO	DOCE
2	**LAPTOP**	**S/C**	BUENA	CND4381KC2	CORE I3	HP	NEGRO	PLASTICO	DOCE
3	**LAPTOP**	**S/C**	BUENA	CND4381L5P	CORE I3	HP	NEGRO	PLASTICO	DOCE
4	**LAPTOP**	**S/C**	BUENA	CND4381H79	CORE I3	HP	NEGRO	PLASTICO	DOCE
5	**LAPTOP**	**S/C**	BUENA	CND4381KCB	CORE I3	HP	NEGRO	PLASTICO	DOCE
6	**LAPTOP**	**S/C**	BUENA	CND4381L02	CORE I3	HP	NEGRO	PLASTICO	DOCE
7	**LAPTOP**	**S/C**	BUENA	CND4381HWQ	CORE I3	HP	NEGRO	PLASTICO	DOCE
8	**LAPTOP**	**S/C**	BUENA	CND4378ZR1	CORE I3	HP	NEGRO	PLASTICO	DOCE
9	**LAPTOP**	**S/C**	BUENA	CND4381LHN	CORE I3	HP	NEGRO	PLASTICO	DOCE
10	**LAPTOP**	**S/C**	BUENA	CND4381L2H	CORE I3	HP	NEGRO	PLASTICO	DOCE
11	**LAPTOP**	**S/C**	BUENA	5CG5503L1H	CORE I3	HP	NEGRO	PLASTICO	DOCE
12	**LAPTOP**	**S/C**	BUENA	CND4381HCL	CORE I3	HP	NEGRO	PLASTICO	DOCE
13	**LAPTOP**	**S/C**	BUENA	CND4381KBT	CORE I3	HP	NEGRO	PLASTICO	DOCE
14	**LAPTOP**	**S/C**	BUENA	CND4381HVX	CORE I3	HP	NEGRO	PLASTICO	DOCE
15	**LAPTOP**	**S/C**	BUENA	CND4381FCT	CORE I3	HP	NEGRO	PLASTICO	DOCE
16	**LAPTOP**	**S/C**	BUENA	CND4381KCB	CORE I3	HP	NEGRO	PLASTICO	DOCE
17	**LAPTOP**	**S/C**	BUENA	CND51175B8	CORE I3	HP	NEGRO	PLASTICO	DOCE
18	**LAPTOP**	**S/C**	BUENA	CND4381JQ2	CORE I3	HP	NEGRO	PLASTICO	DOCE
19	**LAPTOP**	**S/C**	BUENA	CND4380R0P	CORE I3	HP	NEGRO	PLASTICO	DOCE

20	**LAPTOP**	**S/C**	**BUENA**	**CND43 81GKY**	**CORE I3**	**HP**	**NEGRO**	**PLASTICO**	**DOCE**
21	**LAPTOP**	**S/C**	BUENA	CND43 81F9V	CORE I3	HP	NEGRO	PLASTICO	DOCE
22	**LAPTOP**	**S/C**	BUENA	CND43 81L2G	CORE I3	HP	NEGRO	PLASTICO	DOCE
23	**LAPTOP**	**S/C**	BUENA	CND43 81JMP	CORE I3	HP	NEGRO	PLASTICO	DOCE
24	**LAPTOP**	**S/C**	BUENA	CND43 81B4R	CORE I3	HP	NEGRO	PLASTICO	DOCE
25	**LAPTOP**	**S/C**	BUENA	CND43 81L31	CORE I3	HP	NEGRO	PLASTICO	DOCE
26	**LAPTOP**	**S/C**	BUENA	CND43 81KBF	CORE I3	HP	NEGRO	PLASTICO	DOCE
27	**LAPTOP**	**S/C**	BUENA	CND43 81L0C	CORE I3	HP	NEGRO	PLASTICO	DOCE
28	**LAPTOP**	**S/C**	BUENA	CND43 81K1B	CORE I3	HP	NEGRO	PLASTICO	DOCE
29	**LAPTOP**	**S/C**	BUENA	5CG638 4LTM	CORE I3	HP	NEGRO	PLASTICO	DOCE
30	**LAPTOP**	**S/C**	BUENA	CND43 8194R	CORE I3	HP	NEGRO	PLASTICO	DOCE
31	**LAPTOP**	**S/C**	BUENA	CND43 819GG	CORE I3	HP	NEGRO	PLASTICO	DOCE
32	**LAPTOP**	**S/C**	BUENA	CND43 81LMT	CORE I3	HP	NEGRO	PLASTICO	DOCE
33	**LAPTOP**	**S/C**	BUENA	CND43 81KTB	CORE I3	HP	NEGRO	PLASTICO	DOCE
34	**LAPTOP**	**S/C**	BUENA	CND43 81KRL	CORE I4	HP	NEGRO	PLASTICO	DOCE
35	**LAPTOP**	**S/C**	BUENA	CND43 81FCG	CORE I5	HP	NEGRO	PLASTICO	DOCE

ANEXO 5.2: IDENTIFICACIÓN DE AMENAZAS, VULNERABILIDADES Y EFECTOS EN LOS ACTIVOS

ACTIVOS	AMENAZAS	VULNERABILIDADES	EFECTO
INFRAESTRUCTURA	Remodelaciones físicas de las instalaciones.	En el sector es común los factores de cambios en la infraestructura, puede generarse pérdida de activos de información	Cambios de autoridades Incendios Terremotos
	Desastres naturales	Edificaciones construidas inadecuadamente	Terremotos
	Interrupción de servicios básicos como sistema eléctrico	Cableado de fácil acceso para robo o daño	Accidentes Físicos
		Mal estado de instalaciones eléctricas produce riesgo en los usuarios de la Institución	Impagos
USUARIOS	Inadecuado manejo de la información	Deficiente controles de acceso a la información	Clonación de información Modificación de información
TELECOMUNICACIONES	Inutilización de equipos en mal estado	Uso de equipos inadecuado, manipulación por cualquier usuario	Daño de equipos factores de conexiones eléctricas
	Interrupción de servicios básicos de telecomunicaciones	Cableado sin normativa o expuestos a intemperie	Interrupción de servicios
		Fácil acceso para robo o daño	
		Mal estado de instalaciones eléctricas produce riesgo en los usuarios de la Institución	
	Acceso a equipos por cualquier usuario	Configuración sin autorización de equipos, o desconfiguración de los equipos	Acceso a los dispositivos de red
	Acceso a equipos de red con claves comunes	Sin controles de acceso a equipos de red no se establece seguridad de autentificación en equipos de red	Acceso a equipos de red que tienen clave de fabrica

ANEXO 5.3

IDENTIFICACIÓN DE RIESGOS EN LOS ACTIVOS

Nombre del activo	Tipo	Confidencialidad 1-baja / 5-alta	Integridad 1-baja / 5-alta	Disponibilidad 1-baja / 5-alta	Total	Riesgo 1- muy bajo 15 - muy alto
Administrar infraestructura tecnológica	TANGIBLE	4	5	5	14	muy alto
Impresoras	TANGIBLE	2	5	3	10	alto
Proyectores	TANGIBLE	1	3	2	6	medio
Computadores de Escritorio	TANGIBLE	5	5	5	15	muy alto
Computadores Portátiles	TANGIBLE	5	5	5	15	muy alto
Linux Ubuntu	INTANGIBLE	3	5	4	12	alto
Sistema Operativo	INTANGIBLE	2	3	3	8	medio alto
Base de datos	INTANGIBLE	5	5	5	15	muy alto
Antivirus	INTANGIBLE	5	5	5	15	muy alto
Google Classroom	INTANGIBLE	5	5	5	15	muy alto
Correo Electrónico	INTANGIBLE	5	5	5	15	muy alto
Router	TANGIBLE	3	4	3	10	alto
Switch	TANGIBLE	2	3	4	9	alto
Servicio de Internet	INTANGIBLE	3	4	4	11	alto

ANEXO 5.4

VALORACIÓN DE RIESGOS EN LOS ACTIVOS

Activo	Amenaza	Responsable	Vulnerabilidad	P	I	R
Administrar infraestructura tecnológica	Interrupción de servicio	TIC	Mantenimiento insuficiente Instalación fallida de los medios de almacenamiento	3	5	8
Soporte a usuarios	Interrupción de servicio	TIC				
Impresoras	Destrucción de equipos o medios.	TIC				
Proyectores	Destrucción de equipos o medios.	TIC	Ausencia de esquemas de reemplazo periódico	3	5	8
Computadores de Escritorio	Robo de equipos	TIC	Mantenimiento insuficiente Ataque de Virus, malware	1	5	6
Computadores Portátiles	Robo de equipos					
Sistemas Operativos	Error en el uso	TIC	Ausencia de un eficiente control de cambios en la configuración	2	5	7
Base de datos	Interrupción de servicio	TIC	Mantenimiento insuficiente Instalación fallida de los medios de almacenamiento	3	3	6
Antivirus	Interrupción de servicio					
Navegación Web	Interrupción de servicio	TIC	Ausencia de esquemas de reemplazo periódico	3	3	6
Correo Electrónico	Interrupción de servicio	TIC	Almacenamiento sin protección Copia no controlada	1	3	4
Router	Robo de equipos					
Switch	Robo de equipos	TIC	Ausencia de un eficiente control de cambios en la configuración	1	3	4
Servicio de Internet	Interrupción de servicio	TIC	Mantenimiento insuficiente Ataque de Virus, malware	4	3	7

ANEXO 5.5

TRATAMIENTO DEL RIESGO

Criterio	Tratamiento de Riesgo	Responsable	Riesgo	Tiempo
Política de Seguridad de la Información	Definición, aprobación y socialización de la Política de Seguridad	Administrativos, Docentes y TIC	8	corto plazo
Roles de seguridad	Definición de roles y responsabilidades	Administrativos y TIC	7	corto plazo
Control de dispositivos móviles	Definir procedimiento para el control y acceso de dispositivos móviles	TIC	5	largo plazo
Capacitación y concienciación del SGSI	Definir e implementar plan de capacitación y concientización de la seguridad de la información	Administrativos y TIC	8	corto plazo
Sanciones sobre incidentes de seguridad	Definir sanciones para empleados que incumplan las políticas de seguridad	Administrativos	6	mediano plazo
Uso aceptable de activos	Definir el procedimiento de uso aceptable de activos	TIC	5	largo plazo
Devolución de activos	Definir el procedimiento para la devolución de activos	Administrativos y TIC	7	corto plazo
Control de acceso	Definir el procedimiento para el control de acceso a los Sistemas de información	TIC	6	mediano plazo

ANEXO 5.6

EVALUACIÓN Y APLICACIÓN DE CONTROLES

Criterio de evaluación	Controles de la Institución	Control a aplicar
Roles y responsabilidad de seguridad de la información	ninguno	Definir y aprobar roles y responsabilidades
Políticas de seguridad de la información	ninguno	Definir, aprobar y socializar políticas de seguridad
Revisión de las políticas de seguridad de la información	ninguno	Revisión anual de las políticas de seguridad
Política de dispositivos móviles	ninguno	Definir procedimiento para el control y acceso de dispositivos móviles
Plataforma virtual	ninguno	Actividades virtuales de la institución supervisado o grabado
Conciencia, educación y entrenamiento de seguridad de la información	ninguno	Capacitación y concientización de la seguridad de la información
Proceso disciplinario	ninguno	Definir sanciones para empleados que incumplan las políticas de seguridad
Termino de responsabilidades o cambio de actividades	ninguno	El área administrativa será responsable de verificar que los activos que se le asigno se los devuelva.
Inventario de activos	al final de año	Reporte periódico del inventario de activos
Responsables de activos	etiquetado solo algunos activos	En el inventario de activos se define el responsable de los activos
Uso específico de los activos	solo en ciertas áreas	Definir el procedimiento de uso específico de activos
Devolución de activos	ninguno	Definir el procedimiento para la devolución de activos
Clasificación de la información	ciertas áreas lo hacen	Clasificación de la información en orden cronológico y por carpetas
Etiquetado de la información	ciertas áreas lo hacen	Etiquetado de la información general
Manejo de activos	ninguno	Definir el procedimiento para el manejo activos

ANEXO 6

ACTIVOS DE LA INSTITUCIÓN

ANEXO 7

DOCUMENTACIÓN DE PROPUESTA SGSI

	Políticas de Seguridad General.	Código: 17H01403
		Fecha: 19/08/22
		Versión: 01
		Nivel de confidencialidad: Alto

Contenido

1. Objetivos

- Mejorar la seguridad de la información en la Institución a través de controles que logren aumentar la disponibilidad de la información, a través de modificación de las actividades asociadas al área de TIC.
- Crear políticas de seguridad apropiadas para la institución, que deberán ser consideradas por los usuarios de la Institución para mejorar la seguridad de la información.
- Relacionarse con los incidentes y amenazas a la seguridad de la información que puedan darse, para dar una respuesta adecuada a estos inconvenientes.
- Repotenciar la infraestructura de red de la institución con dispositivos y herramientas de seguridad de la información.

2. Alcance

El presente documento se aplicará a toda la institución educativa tanto en directivos como docentes y estudiantes; así también hacia los activos que son la información dentro de los equipos y los archivos de forma física. Para evitar el acceso no autorizado en los dispositivos.

3. Documentos de referencia.

- ISO 27001/2013
- Política de uso aceptable

4. Introducción

Con el fin de minimizar los riesgos de seguridad y la confidencialidad de la información para que los docentes y directivos puedan llevarse las computadoras laptops a sus domicilios tienen que firmar un acta de compromiso como el código ingenios para así salvaguardar la integridad con los controles debidos esto aplica tanto en las computadoras

de laboratorio como en dispositivos de almacenamiento como: memorias flas, cd, disco duros y nubes.

5. Controles para minimizar los riesgos.

- Las computadoras y los smartphones no pueden conectarse a redes públicas desconocidas sin usar la "vpn protón" o algún método de protección como cifrado.
- La instalación de cualquier tipo de software sólo debe de ser bajo el petitorio hacia el departamento de TI y este tiene que ser licenciado de forma oficial además que se debe llevar una hoja de control De cada equipo.
- El acceso a las laptops y computadoras del laboratorio deben de ser bajo las credenciales de administrador las mismas que sólo tendrán acceso el departamento de TI.
- La información que es confidencial debe de ser cifrada y tener un respaldo en la nube de office 365 otorgada por el ministerio de educación, además crear un espacio en el vault para guardar información con un nivel de confidencialidad alto.
- En caso de robo presentar el documento de fiscalía oficial y además cambiar las contraseñas de acceso de manera inmediata tanto en cuentas personales como en las cuentas de trabajo en este caso las de office 365 otorgadas por el ministerio de educación.
- Se debe verificar de forma periódica cada 6 meses la actualización del sistema operativo tanto en el laboratorio como en las laptops.
- Se otorgará únicamente el acceso a la red a un dispositivo a la vez por docente.
- En los equipos de laboratorio y docentes se protege con Deep Freeze para impedir la modificación del sistema operativo pero se deja una partición de almacenamiento para la gestión de archivos.

- Instalar el antivirus Panda con licencia en todos los dispositivos como: computadoras de laboratorio, laptops de docentes, tablets y smartphones.

6. Contraseñas.

- Usar contraseñas diferentes para cada plataforma.
- Usar la aplicación key pass para generar contraseñas diferentes de modo aleatorio.
- Cambiar las contraseñas cada 3 meses en las plataformas de uso.
- Guardar las bases de datos de las contraseñas en la nube One drive dentro del vault.
- Guardar la credencial o llaves de acceso en otra nube como Google drive para tener por separado los recursos de acceso a las contraseñas.
- Usar un la aplicación Microsoft Autenticator para generar códigos aleatorios como segundo método de acceso.

7. Reglas de acceso.

Pues bien, la institución es de uso público pero el acceso a diversos recursos como lo que son sistemas como a equipos, instalaciones e información. Para las personas que necesiten el acceso a estos activos, bajo una solicitud podrán acceder a estos la cual debe ser dirigida al departamento de TI y rector. Además de esto a todas las personas que se conecten a la red de la institución van a tener restringido el uso de:

- Mensajería a través de redes sociales
- Llamadas a través de internet
- Correo electrónico personal
- Descarga de archivos de cualquier índole como aplicaciones juegos y programas
- Consumo de streaming no autorizado como: Netflix, Facebook, Disney plus, Amazon prime y etc.

- Acceso a sitios no autorizados como pornografía
- Servicio remoto a través de internet.
- Cualquier otro servicio que degrade la red o vulnere la misma.

8. Formato para guardar archivos

Para guardar los archivos de forma segura en los equipos de laboratorio o laptops y teléfonos se deben comprimir con una contraseña la cual no puede ser compartida de manera pública solo con el receptor del mensaje; además, se guardará una copia de este en el baúl de la nube de office 365. Después de usar los archivos se debe eliminar completamente tanto en él emisor como en el receptor.

9. Pantallas y escritorios seguros.

Para definir la seguridad en los puestos de trabajo se deben cumplir las siguientes reglas.

- Si la persona autorizada abandona su puesto de trabajo debe dejar todos los documentos y dispositivos de almacenamiento como memorias En un escritorio bajo llave para que no pueda ser extraído.
- Cuando la persona deje de usar su equipo de trabajo debe bloquear la misma con el cierre de sesión y también tener configurado el bloqueo automático después de cuatro minutos.
- Cuando manejen documentos delicados, sensibles o confidenciales deben de ser almacenados de forma segura bajo llave.

10. Áreas seguras.

    Las áreas seguras son las aulas en donde el personal autorizado puede hacer sus diligencias sin embargo en todo momento cumplir las políticas de seguridad, A continuación, se enlista las aulas seguras.

    - Laboratorio de computación.

- Aula de audiovisuales.
- Vicerrectorado.
- Rectorado.
- Sala da profesores.
- Inspección.

11. Transferencia de información

Es importante asegurar la información y el software cuando son intercambiados dentro o fuera de la organización ya que es uno de los activos más importantes esta puede ser compartida a través de los siguientes medios nubes correo electrónico dispositivos de almacenamiento mensajes a través de redes sociales foros y aplicaciones de terceros para transferencia de archivos, sin embargo, para cuidar la integridad de los mismos Se deben aplicar las siguientes reglas. En el caso de enviar información confidencial deben encriptar la información y enviar la contraseña por separado esto se lo puede hacer con compresor de archivos.

- Verificar que la dirección del remitente sea la correcta, tanto puntos como números, símbolos especiales y la extensión del correo electrónico.
- No abrir enlaces de dudosa procedencia ante la duda de uno de estos comunicar de forma inmediata al departamento de TI.
- Para el intercambio de información extraoficial usar el correo electrónico de trabajo otorgado por el ministerio de educación (office 365).

12. Recepción clasificación de incidentes y vulnerabilidades

La detección temprana de eventos y debilidades de seguridad es primordial para permitir la continuidad del negocio, así como también la rápida reacción y respuesta ante estos.

Los docentes y directivos que manejan información y sistemas tecnológicos deben reportar de manera inmediata si se llega a comprometer un sistema. Acciones a tomar:

- Reporta los eventos de seguridad al departamento de TI.
- Informar de manera inmediata si existiese un posible potencial evento de seguridad informática que afecte los activos de la información como correos no deseados y un comportamiento inusual en los sistemas tanto del laboratorio como de equipos personales.
- Ejecutar acciones para mitigar el incidente como: desconectar los sistemas del internet o diagnosticar con un antivirus.
- Aprender de los incidentes y dialogar con los docentes y directivos para socializar las nuevas formas de penetración de seguridad y así generar una cultura de seguridad.

13. Sanción por incumplimiento.

- Las dos primeras por incumplimiento será un llamado de atención por la autoridad (Rector).
- Al tercer llamado de atención se presentará un memo en el distrito bajo un informe por parte de la autoridad (Rector).
- Al cuarto llamado de atención se procede a tomar un juicio sumario por parte del distrito.
- En todas estas situaciones del caso de ser comprobado como verídica la infracción se procede a despido inmediato.

14. Formatos

    Los formatos de registros deben llevar el encabezado y la codificación definida para ellos en el documento del procedimiento de control de documentos. A continuación, muestran estructuras de los formatos, cuándo los formatos son

diligenciados, estos se convierten en registros, que permiten evidenciar la ejecución y seguimiento de las actividades propuestas en el sistema de gestión.

12.1.Formato para registro de backups.

Fecha de Backup	Nombre del Archivo	Lugar de almacenamiento	Firma Responsable

12.2.Formato para registro de equipos.

ITEM	DESCRIPCIÓN	OBSERVACIONES
NOMBRE EQUIPO		
SERIAL		
DIRECCIÓN IP		
FECHA COMPRA:		
FECHA INSTALACIÓN:		
USUARIO ADMINISTRADOR:		
CONTRASEÑA ADMINISTRADOR:		
AREA ASIGNADO		
SISTEMA OPERATIVO		
SW OFIMÁTICO		
RAM		
PROCESADOR		
MONITOR		
USUARIO AUTORIZADO		

12.3.Formato para control dispositivos externos.

Fecha Uso	Origen – Propietario	Archivo usado	Responsable Uso

12.4.Formato reporte de incidentes.

Fecha	Incidente	Impacto

13. Glosario de términos.

- Confidencialidad: Característica de la información que indica que esta solo se encuentra disponible solo para personas o sistemas autorizados.
- Seguridad de la información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- SGSI: Parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

- VPN: Es un túnel de conexión en donde todos los datos son encriptados y además primero se conecta a un servidor de un país diferente al de origen para proteger la conectividad a internet.
- Key Pass: Es un administrador de contraseñas el cual permite generar diferentes contraseñas de forma aleatoria para cada servicio, pero también encripta estas en una base de datos y también para acceder a este software se necesita de una llave de acceso, es recomendable tener por separado el almacenamiento de las contraseñas y las llaves de acceso.
- Deep Freezer: es un programa que garantiza la recuperación integral del ordenador, con solo reiniciar el equipo, por ende, se dispone de una protección con seguridad de contraseña para proteger las unidades de almacenamiento.
- Panda Antivirus: Es un antivirus que protege a los equipos de malware, ransomware, troyanos. Es multiplataforma es decir que está disponible para Windows, Mac Os y Android. También dentro de su servicio ofrece conexión de red segura a través de vpn y en el último año agregaron la función de control parental para la seguridad de los menores de edad.

14. Evidencia de monitoreo y evaluación de resultados.

Fecha	Versión	Creado por	Detalles de la modificación.	Resultados
	0.1		Creación del documento	N/A

15. ANEXOS DE CONTROL MEDIANTE NORMATIVA ISO

ANEXO			APLICA	CUMPLIMIENTO
A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**			
A5.1	Orientación de la dirección para la gestión de la seguridad de la información			
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes				

ANEXO			APLICA	CUMPLIMIENTO
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	SI	SI

A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	SI	N/A
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**			
A6.1	Organización interna			
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.				

ANEXO			**APLICA**	**CUMPLIMIENTO**
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	SI	SI
A6.1.2	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 organización	SI	SI
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	NO	N/A

ANEXO	**APLICA**	**CUMPLIMIENTO**

A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	NO	N/A
A6.1.5	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 proyecto.	NO	N/A
A6.2	Dispositivos móviles y teletrabajo			
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles				
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	SI	SI

ANEXO			**APLICA**	**CUMPLIMIENTO**
A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	NO	N/A
A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
A7.1	Antes de asumir el empleo			
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.				

ANEXO			APLICA	CUMPLIMIENTO
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	SI	SI
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	SI	SI
A7.2	Durante la ejecución del empleo			
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.				

ANEXO			APLICA	CUMPLIMIENTO
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	SI	SI

A7.2.2	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, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	SI	SI

ANEXO			APLICA	CUMPLIMIENTO
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	SI	SI
A7.3	Terminación y cambio de empleo			
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo				

A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	NO	N/A
A8	**GESTION DE ACTIVOS**			
A8.1	Responsabilidad por los activos			
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.				

ANEXO			**APLICA**	**CUMPLIMIENTO**
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	SI	SI
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	SI	SI

A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	SI	SI

ANEXO			**APLICA**	**CUMPLIMIENTO**
A8.1.4	Devolución de activos Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.		NO	N/A
A8.2	Clasificación de la información			
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.				
A8.2.1	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 no autorizada.	SI	SI

ANEXO	**APLICA**	**CUMPLIMIENTO**

A8.2.2	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.	NO	N/A
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	SI
A8.3	Manejo de medios			
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios				

ANEXO			**APLICA**	**CUMPLIMIENTO**
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	NO	N/A
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	NO	N/A
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	NO	N/A

A9	**CONTROL DE ACCESO**		
A9.1	Requisitos del negocio para el control de acceso		
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.			

ANEXO			**APLICA**	**CUMPLIMIENTO**
A9.1.1	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 la seguridad de la información.	SI	SI
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	SI	SI
A9.2	Gestión de acceso de usuarios			
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.				
A9.2.1	Registro y cancelación del 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.	SI	SI

ANEXO			**APLICA**	**CUMPLIMIENTO**
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	SI	SI

A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	SI	SI
A9.2.4	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.	SI	SI
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	SI	SI

ANEXO			**APLICA**	**CUMPLIMIENTO**
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	SI	SI
A9.3	Responsabilidades de los usuarios			
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.				
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	SI	SI
A9.4	Control de acceso a sistemas y aplicaciones			
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.				

ANEXO	**APLICA**	**CUMPLIMIENTO**

A9.4.1	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.	SI	SI
A9.4.2	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.	SI	SI
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	SI	SI

ANEXO			**APLICA**	**CUMPLIMIENTO**
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	NO	N/A
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	NO	N/A
A10	**CRIPTOGRAFIA**			
A10.1	Controles criptográficos			
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información				

A10.1.1	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.	SI	N/A

ANEXO			**APLICA**	**CUMPLIMIENTO**
A10.1.2	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.	SI	N/A
A11	**SEGURIDAD FISICA Y DEL ENTORNO**			
A11.1	Áreas seguras			
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	SI	N/A
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	SI	N/A

ANEXO	**APLICA**	**CUMPLIMIENTO**

A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	SI	N/A
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI	N/A
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	SI	N/A
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	SI	N/A
A11.2	Equipos			

ANEXO			**APLICA**	**CUMPLIMIENTO**
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.				
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	SI	N/A
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	SI	N/A

A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	SI	N/A

ANEXO			**APLICA**	**CUMPLIMIENTO**
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	SI	SI
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	SI	SI
A11.2.6	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 dichas instalaciones.	SI	SI

ANEXO			**APLICA**	**CUMPLIMIENTO**
A11.2.7	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	SI	SI

		segura antes de su disposición o reúso.		
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	SI	SI
A11.2.9	Política 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.	SI	SI
A12	**SEGURIDAD DE LAS OPERACIONES**			
A12.1	Procedimientos operacionales y responsabilidades			

ANEXO			**APLICA**	**CUMPLIMIENTO**
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	SI	N/A

A12.1.2	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.	SI	SI
A12.1.3	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 del sistema.	SI	SI

ANEXO		**APLICA**	**CUMPLIMIENTO**
A12.1.4	Separación de los Control: Se deben separar los ambientes de desarrollo, ambientes de desarrollo, pruebas y operación pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	NO	N/A
A12.2	Protección contra códigos maliciosos		
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.			

A12.2.1	Controles 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.	SI	N/A
A12.3	Copias de respaldo			
Objetivo: Proteger contra la perdida de datos				

ANEXO			APLICA	CUMPLIMIENTO
A12.3.1	Respaldo de la Control: Se deben hacer información copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.		SI	SI
A12.4	Registro y seguimiento			
Objetivo: Registrar eventos y generar evidencia				
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	SI	SI
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	SI	SI

ANEXO	APLICA	CUMPLIMIENTO

A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	SI	SI
A12.4.4	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.	NO	N/A
A12.5	Control de software operacional			
Objetivo: Asegurarse de la integridad de los sistemas operacionales				
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI	SI
A12.6	Gestión de la vulnerabilidad técnica			
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas				

ANEXO			**APLICA**	**CUMPLIMIENTO**
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	SI	N/A

A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	SI	N/A
A12.7	Consideraciones sobre auditorias de sistemas de información			
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos				

ANEXO			**APLICA**	**CUMPLIMIENTO**
A12.7.1	Controles de auditorías de Control: Los requisitos y sistemas de información actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.		SI	SI
A13	**SEGURIDAD DE LAS COMUNICACIONES**			
A13.1	Gestión de la seguridad de las redes			
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.				
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	SI	SI

ANEXO			**APLICA**	**CUMPLIMIENTO**
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o	SI	SI

		se contraten externamente.		
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.		
A13.2	Transferencia de información			
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.				

ANEXO			**APLICA**	**CUMPLIMIENTO**
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	SI	N/A
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	NO	N/A
A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	SI	SI

ANEXO			**APLICA**	**CUMPLIMIENTO**
A13.2.4	Acuerdos de	Control: Se deben identificar, revisar regularmente y	SI	SI

	confidencialidad o de no documentar los requisitos para divulgación los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.			
A14	**Adquisición, desarrollo y mantenimiento de sistemas**			
A14.1	Requisitos de seguridad de los sistemas de información			
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.				
A.14. 1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	SI	SI

ANEXO			**APLICA**	**CUMPLIMIENTO**
A.14. 1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	SI	SI

A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben 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.	NO	N/A
A14.2	Seguridad en los procesos de Desarrollo y de Soporte			

ANEXO			**APLICA**	**CUMPLIMIENTO**
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.				
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	SI	SI
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	SI	SI
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 o seguridad de la organización.	SI	SI

ANEXO			APLICA	CUMPLIMIENTO
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	NO	N/A
A.14.2.5	Principio 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.	NO	N/A

ANEXO			APLICA	CUMPLIMIENTO
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.	NO	N/A
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	NO	N/A
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	NO	N/A

ANEXO			APLICA	CUMPLIMIENTO
A.14.2.9	Prueba de aceptación Control: Para los sistemas de sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.		NO	N/A
A14.3	Datos de prueba			
Objetivo: Asegurar la protección de los datos usados para pruebas.				
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	NO	N/A
A15	**RELACIONES CON LOS PROVEEDORES**			
A15.1	Seguridad de la información en las relaciones con los proveedores.			
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.				

ANEXO			APLICA	CUMPLIMIENTO
A15.1.1	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 con estos y se deben documentar.	NO	N/A

A15.1.2	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.	NO	N/A

ANEXO			**APLICA**	**CUMPLIMIENTO**
A15.1.3	Cadena de suministro de Control: Los acuerdos con tecnología de información proveedores deben incluir y comunicación requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.		NO	N/A
A15.2	Gestión de la prestación de servicios de proveedores			
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores				
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	NO	N/A

ANEXO	**APLICA**	**CUMPLIMIENTO**

A15.2.2	Gestión del cambio 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 las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	NO	N/A
A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**			
A16.1	Gestión de incidentes y mejoras en la seguridad de la información			
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				

ANEXO			**APLICA**	**CUMPLIMIENTO**
A16.1.1	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.	SI	SI

A16.1.2	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 apropiados, tan pronto como sea posible.	SI	N/A

ANEXO			APLICA	CUMPLIMIENTO
A16.1.3	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.	SI	N/A
A16.1.4	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.	SI	N/A
A16.1.5	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.	SI	SI

ANEXO	APLICA	CUMPLIMIENTO

A16.1.6	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 impacto de incidentes futuros.	SI	N/A
A16.1.7	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.	NO	N/A
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**			
A17.1	Continuidad de Seguridad de la información			
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.				

ANEXO			**APLICA**	**CUMPLIMIENTO**
A17.1.1	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.	SI	SI

A17.1.2	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.	SI	SI

ANEXO			APLICA	CUMPLIMIENTO
A17.1.3	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.	SI	SI
A17.2	Redundancias			
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.				
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI	N/A
A18	**CUMPLIMIENTO**			
A18.1	Cumplimiento de requisitos legales y contractuales			
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.				

ANEXO			APLICA	CUMPLIMIENTO
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, 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.	NO	N/A
A18.1.2	Derechos propiedad intelectual (DPI)	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.	NO	N/A

ANEXO			APLICA	CUMPLIMIENTO
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación,	SI	SI

		contractuales y de negocio.		
A18.1.4	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 y la legislación y la reglamentación pertinentes, cuando sea aplicable.	SI	SI
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	SI	N/A
A18.2	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.				

ANEXO			**APLICA**	**CUMPLIMIENTO**
A18.2.1	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 la información), se deben revisar independientemente a intervalos planificados o	NO	N/A

		cuando ocurran cambios significativos.		
ANEXO			**APLICA**	**CUMPLIMIENTO**
A18.2.2	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.	SI	SI
A18.2.3	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 la información.	SI	N/A

ANEXO 8

DOCUMENTACIÓN DE APROBACION DEL COLEGIO FRAY JODOCO RICKE

UNIDAD EDUCATIVA "FRAY JODOCO RICKE"
Comité del Pueblo N° 1 Sector La Bota. Av. La Bota E16 - 66 y 28 de Mayo
Correo Electrónico: 17H01403@gmail.com - Telf: 3455-721
Quito Ecuador

APROBACIÓN

PROPUESTA DE UN MODELO DE SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN

DECLARACIÓN

Con el presente documento se hace la constancia para proponer un modelo de gestión para la seguridad de la información en la unidad educativa Fray Jodoco Ricke, el cual permitirá conocer los diferentes tipos de activos para su respectivo inventario análisis y evaluación de los riesgos con la finalidad de proteger la información.

Quito 16 de agosto del 2022

Unidad Educativa
Fray Jodoco Ricke
RECTORADO

Lic. Carlos Benalcázar. MSc

RECTOR

UNIDAD EDUCATIVA "FRAY JODOCO RICKE"
Comité del Pueblo N° 1 Sector La Bota. Av. La Bota E16 - 66 y 28 de Mayo
Correo Electrónico: 17H01403@gmail.com - Telf: 3455-721
Quito Ecuador

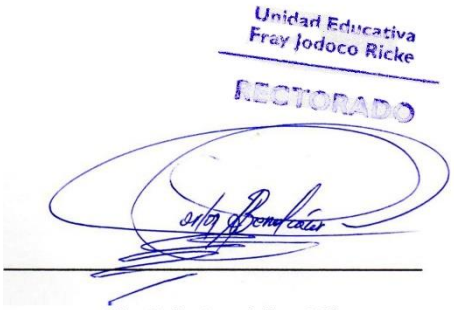
APROBACIÓN

INVENTARIO DE ACTIVOS

DECLARACIÓN

Con el presente documento se hace la constancia de la aprobación sobre la actividad del inventario de activos en la unidad educativa Fray Jodoco Ricke, el mismo que permitirá conocer y clasificar cada uno para mejorar su gestión.

Quito 16 de agosto del 2022



Lic. Carlos Benalcázar. MSc

RECTOR

UNIDAD EDUCATIVA "FRAY JODOCO RICKE"
Comité del Pueblo N° 1 Sector La Bota. Av. La Bota E16 - 66 y 28 de Mayo
Correo Electrónico: 17H01403@gmail.com - Telf: 3455-721
Quito Ecuador

APROBACIÓN

METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE LOS RIESGOS

DECLARACIÓN

Con el presente documento se hace la constancia de la aprobación para la metodología de evaluación y tratamiento de riesgos en la unidad educativa Fray Jodoco Ricke, con el que se puede realizar el análisis sobre las amenazas y las vulnerabilidades a las que está expuesta a la institución y así valorar el impacto que tendrán sobre el sistema de gestión de riesgos de la información.

Quito 17 de agosto del 2022

Unidad Educativa
Fray Jodoco Ricke
RECTORADO

Lic. Carlos Benalcázar. MSc

RECTOR

UNIDAD EDUCATIVA "FRAY JODOCO RICKE"
Comité del Pueblo N° 1 Sector La Bota. Av. La Bota E16 - 66 y 28 de Mayo
Correo Electrónico: 17H01403@gmail.com - Telf: 3455-721
Quito Ecuador

APROBACIÓN

DECLARACION DE APLICABILIDAD

DECLARACIÓN

Con el presente documento se hace la constancia de la aprobación de la declaración de aplicabilidad en la unidad educativa Fray Jodoco Ricke, con el que se pretende sugerir los debidos controles aplicables con base en los resultados de evaluación delriesgo.

Quito 17 de agosto del 2022

Unidad Educativa
Fray Jodoco Ricke
RECTORADO

Lic. Carlos Benalcázar. MSc

RECTOR

UNIDAD EDUCATIVA "FRAY JODOCO RICKE"
Comité del Pueblo N° 1 Sector La Bota. Av. La Bota E16 - 66 y 28 de Mayo
Correo Electrónico: 17H01403@gmail.com - Telf: 3455-721
Quito Ecuador

APROBACIÓN

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

DECLARACIÓN

Con el presente documento se hace la constancia de la aprobación para la elaboración de las políticas de seguridad de la información en la unidad educativa Fray Jodoco Ricke, para documentar, registrar y usar las mismas políticas en las diferentes actividades académicas, las cuales deben tener conocimiento el personal para su respectivo cumplimiento y seguimiento.

Quito 17 de agosto del 2022

Unidad Educativa
Fray Jodoco Ricke
RECTORADO

Lic. Carlos Benalcázar. MSc

RECTOR

APROBACIÓN

FUNCIONES Y RESPONSABILIDADES DE SEGUIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN.

DECLARACIÓN

Con el presente documento se hace la constancia de la aprobación con una definición de responsabilizar las funciones para dar cumplimiento a la seguridad de la información en la unidad educativa Fray Jodoco Ricke, en dónde se declaran las responsabilidades de los actores en cuánto a la protección de la seguridad tanto en los recursos tecnológicos como los datos.

Quito 18 de agosto del 2022

Unidad Educativa
Fray Jodoco Ricke
RECTORADO

Lic. Carlos Benalcázar. MSc

RECTOR