Análisis de la Gestión en la Información, con base en la norma ISO/IEC 27001 para el Colegio Integrado Los Andes, Floridablanca, Santander.

Ruth Fajardo Romero

Universidad Nacional Abierta y a Distancia

Escuela de Ciencias Básicas Tecnologías e Ingeniería

Ingeniería de Sistemas

Bucaramanga

2024

Análisis de la Gestión en la Información, con base en la norma ISO/IEC 27001 para el Colegio Integrado Los Andes, Floridablanca, Santander.

Ruth Fajardo Romero

Monografía para optar por el Título de Ingeniería de Sistemas

Directora de Trabajo de Grado

Liliana Esperanza Bautista Torres

Universidad Nacional Abierta y a Distancia

Escuela de Ciencias Básicas Tecnologías e Ingeniería

Ingeniería de Sistemas

Bucaramanga

2024

Página de Aceptación

Nota de aceptación:

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bucaramanga, Santander, 27/03/2024

Dedicatoria

Dedico este trabajo en primer lugar a Dios, por su amor, bondad, del proveerme, de todas sus bendiciones, para lograr este logro tan importante en mi vida.

Dar gracias a mi familia, mis hijos, quienes estuvieron en el proceso de universidad y en los años más exigentes de la carrera. Así, mismo, dar gracias a mis amados hermanos, Abelardo, Dinita, mi mamá, Paula, Aida, Rubiela, y Yamid, quienes estuvieron a mi lado, cuando llegaron los momentos de desfallecer.

De igual manera, a esas personas hermosas de corazón, que me ayudaron para alcanzar esta meta desde lo económico, quienes fueron esos vasos en las manos de Dios, y participaron para hoy ser parte de momentos así. Agradecida con Dios, porque en cada año trajo a mi vida las personas que serían mi apoyo.

Ruth Fajardo Romero

Agradecimiento

Agradecer, con todo mi corazón, a Dios y cada persona, que ha sido mi apoyo, de manera constante, y que han estado atentos al proceso de avance, con este proyecto de mi vida; el cual, ha sido para mí, una de las tantas razones para luchar, y continuar, en medio de obstáculos y suceso, siempre con el objetivo de adquirir conocimiento, que me permitan, no solo aplicar en mi vida profesional, si no también, en mi vida laboral y social.

Dar gracias, a mis docentes, a los ingenieros, que fueron mi fuente de conocimiento, en el desarrollo de competencias profesionales, y de esta manera permitirme desarrollar, diversas habilidades, para el desarrollo de mi carrera profesional, en la Ingeniera de Sistemas.

De igual manera, poder agradecer, a todos mis compañeros, quienes, mediante equipo, trabajo en conjunto, experiencias de vida, logramos concluir esta etapa, y llegar a alcanzar la meta.

Principal motivo. para concluir la carrera: El deseo de superación.

Resumen

Con el paso del tiempo, los procesos se vuelven más sólidos. Apoyados, automatizados y administrados por sistemas de software. La protección de la información ya no puede ser considerada como el resultado de una respuesta defensiva y reactiva, sino que debe ser abordada como un elemento estratégico que se necesita incorporar. Las organizaciones educativas necesitan considerar estos elementos tecnológicos como colaboradores importantes para la gestión efectiva de los procesos y, en consecuencia, de la información. El objetivo de este estudio es examinar el manejo de la información en el Colegio Integrado los Andes, Floridablanca, Santander, utilizando la Norma ISO/IEC 27001.

Actualmente, el enfoque utilizado genera insatisfacción en todos los niveles de la institución y genera preocupación entre aquellos que reciben servicios educativos, ya que la seguridad de su información está en riesgo. Por eso, se busca una perspectiva adecuada al momento de manejar la seguridad de la información. Por un lado, se busca cumplir con sus responsabilidades y regulaciones, y al mismo tiempo, generar la confianza necesaria en sus clientes.

Palabras claves: Gestión, Información, Proceso, Seguridad.

Abstract

As time goes by, processes become more robust. Supported, automated and managed by software systems. Information protection can no longer be considered the result of a defensive and reactive response, but must be addressed as a strategic element that needs to be incorporated. Educational organizations need to consider these technological elements as important collaborators for the effective management of processes and, consequently, of information. The objective of this study is to examine the management of information at Colegio Integrado los Andes, Floridablanca, Santander, using the ISO/IEC 27001 Standard.

Currently, the approach used generates dissatisfaction at all levels of the institution and generates concern among those who receive educational services, since the security of their information is at risk. Therefore, an adequate perspective is sought when managing information security. On the one hand, it seeks to comply with its responsibilities and regulations, and at the same time, generate the necessary trust in its clients.

Keywords: Management, Information, Process, Security.

Tabla de Contenido

Introducción

La protección de la información es crucial para las organizaciones e instituciones, especialmente en el campo de la educación, ya que se considera un recurso valioso. Por lo tanto, es esencial salvaguardarla con el fin de prevenir cualquier tipo de peligro o amenaza. Es crucial contar con un gran grado de responsabilidad al almacenar y procesar información, con el objetivo de reducir al mínimo las amenazas cibernéticas.

El SGSI administra los riesgos mediante el uso de metodologías basadas en normas y estándares internacionales (ISO/IEC 27000), los cuales contribuyen a reducir las amenazas y revelar los objetivos expuestos de los sistemas de información en las entidades organizativas.

La aplicación de estas estrategias posibilita a los directivos adoptar las decisiones más acertadas. Una vez expresado esto, se comprende que, si una organización no logra administrar adecuadamente la seguridad de la información, su nivel de confianza se verá afectado y, por consiguiente, podría enfrentar consecuencias económicas.

El incremento de las amenazas a la seguridad informática ha llevado a las empresas a adoptar diferentes prácticas de protección en sus sistemas de manejo de datos. La implementación de estas acciones ha sido utilizada como respuesta a los peligros actuales en el manejo de la información en las empresas.

La administración del riesgo de la información juega un papel crucial en la gestión estratégica de las empresas. En algunas ocasiones, puede tener un impacto significativo en la coordinación de las actividades comerciales, la sostenibilidad de las operaciones y la continuidad del negocio.

ISO/IEC 27000 es una colección de normas que posibilitan la incorporación de elementos de seguridad con el fin de salvaguardar los sistemas de información, los cuales son de vital importancia dentro de las empresas. El presente estándar detalla las pautas que las organizaciones deben seguir para asegurar que la información esté disponible, íntegra y auténtica, además de mantener su confidencialidad.

El SGSI es un procedimiento estructurado y normativo que utiliza las pautas de ISO/IEC 27002 para examinar y valorar los peligros a los que se enfrentan los recursos informáticos de una empresa. A través de este sistema, se asegura la disponibilidad, integridad y confiabilidad de la gestión de información de la organización. Un sistema de administración se utiliza para crear y mantener un ambiente seguro en el que se protege la información.

El Sistema de Gestión de la Seguridad de la Información (SGSI) se enfoca en garantizar que los procedimientos y procesos necesarios para mantener la seguridad de las tecnologías de la información estén en constante revisión. Esto implica la identificación de vulnerabilidades, la implementación de estrategias para minimizar los riesgos, la satisfacción de las necesidades de seguridad, la evaluación adecuada de los resultados y la mejora continua de las estrategias de protección, con el objetivo de mitigar los riesgos.

Definición del Problema

Antecedentes del problema

Inicialmente, se tiene en cuenta el estudio realizado por Rivas (2017), con el trabajo de investigación titulado Diagnóstico y plan de acción para la implementación del marco de negocio para el gobierno y gestión de tecnologías de la información (cobit5.0) aplicado a la universidad técnica de Machala, para optar por el título de Magister en Gestión Estratégica de Tecnologías de la información en la ciudad de Cuenca.

El propósito del estudio está orientado en definir un plan de acción de las actividades desarrolladas para la implementación de procesos basados en el diagnóstico inicial en Cobit 5.0 Las dimensiones investigadas lograron establecer planes de acción que conllevaron a la implementación de procesos prioritarios, basada en tipo de estudio descriptivo y de campo, donde el sujeto de estudio fue de 51 trabajadores al cual se aplicó el cuestionario, así mismo, teniendo en cuenta la observación directa, con el cual se recolecto información para dar un diagnóstico basado en seguridad de la información, siendo estos resultados tabulados fundadas en las dimensiones de política de seguridad, confiabilidad, seguridad de la información, acceso y otros aspectos que conllevaron a la validación obteniendo una confiabilidad del 96% en el coeficiente de Alpha Cronbach, el cual dentro del proceso escoge las preocupaciones de las partes interesadas, posteriormente el proceso es aplicado a las actividades prioritarias.

La Universidad Técnica de Machala en la aplicabilidad del proceso se demostró el cumplimiento de la capacidad de los procesos implementados, a su vez, la valoración y el proceso catalizador se encuentran dentro de los márgenes establecidos, logrando analizar las inquietudes generadas en la organización para la toma de acciones que sean ejecutadas a través de actividades que conlleven al mejoramiento continuo de los procesos, por lo cual, la empresa

estima las posibilidades de implementar un sistema acorde a las insuficiencias generadas y de esta manera minimizar las posibilidades de exposición de toda esa información importante.

La investigación sirvió como referencia para la compilación teórica en sistemas de información, a su vez en la revisión de antecedentes se extrajo conceptos relacionados con constructos referenciales en seguridad de la información, donde el desarrollo de los lineamientos giró en torno a la tecnología e información pretendiendo obtener aspectos importantes para suministrar información en futuras investigaciones.

Siguiendo en la misma línea de investigación, se analizó el trabajo de Guamán (2015), titulado Diseño de un sistema de gestión de seguridad de la información para instituciones militares: Escuela Politécnica Nacional, tesis para la obtención del título de Magister en Gestión de las Comunicaciones y Tecnologías de la Información, en la ciudad Quito, Ecuador.

A nivel metodológico se trató de una investigación con enfoque cualitativo, de tipo descriptivo, donde el sujeto de estudio fue de 51 empleados que hacen parte del área de tecnológica de la organización, utilizando como técnica la encuesta recolectando información de manera directa; el instrumento aplicado se encontró relacionado con el cuestionario con 69 preguntas cerradas dirigido al personal de la empresa, el cual fue sometido a validación por 5 expertos, obteniendo una validez del 96 confiabilidad de Alfa de Cronbach.

Los resultados de la investigación conllevaron a la caracterización de los riesgos, amenazas y vulnerabilidades basadas en requerimientos necesarios por parte de la empresa, de igual manera se permitió la caracterización de los activos de la informa, también se determinó la factibilidad a nivel operativo, tecnológico y económico para poder implementar o diseñar el

sistema de gestión de seguridad de la información en las instituciones militares, asignando responsabilidades y compromisos con el SGSI.

Las conclusiones fueron fomentadas en base a los objetivos de la investigación los cuales permiten sustentar que el resultado es la inexistencia de documentos en base a la seguridad de la información y establecer políticas de seguridad inmersas a un sistema de gestión en seguridad de la información, así mismo, requisitos para acuerdos de confidencialidad y el no cumplimiento acceso de usuarios o clientes a información externa a la dirección de tecnologías.

El aporte investigativo, está encaminado a la relación existente entre las variables de estudio, debido al tratamiento aplicado a la misma servirá como base para la realización de la investigación en proceso así mismo, los aportes bibliográficos y la manera adecuada de aplicar la norma ISO 27001, conllevando a establecer puntos de referencia para otro tipo de investigación enmarcada con la variable de estudio.

Así mismo, se tiene el trabajo investigativo de Suarez (2015), llamado Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía.

El estudio está enfocado en la realización del análisis y diseño del sistema de gestión de seguridad informática en la empresa aseguradora. Las dimensiones del estudio están concernidas en la categorización y análisis de riesgos de los activos de información.

Metodológicamente hablando, fue una exploración de tipo descriptiva con enfoque cualitativo, basadas en referencias literarias junto a la elaboración de matrices de riesgos para verificar el estado real de la empresa dentro del factor de seguridad en la información, realizando entrevista de tipo abierta a los trabajadores de la empresa.

En los hallazgos se fundamentaron en los datos aportados por los entrevistados, dando a conocer que la empresa, no dispone de un SGSI, debido a la carencia de personal calificado e idóneo para la asignación de responsabilidades dentro del sistema, donde se demuestra la ausencia de actividades para la protección de los activos u otros aspectos que deben ser cubiertos por la organización.

La investigación permitió evidenciar que los datos conservados por una empresa son de suma importancia, resaltando así mismo, la designación de políticas, roles y responsabilidades son importante en el aseguramiento del éxito dentro de una estructura organizacional bajo los lineamientos que deben ser dirigidos por la alta gerencia, donde todas las personas que hacen parte de la misma, ya sea a nivel interno como externo deben conocer.

El trabajo relaciona con la investigación en curso debido a su aporte extenso en relación a la aplicabilidad de un SGSI junto a la importancia obtenida del mismo; así mismo, los lineamientos y referencias bibliográficas serán tenidas en cuenta para el desarrollo de lineamientos conllevando a una investigación seria y bajo fundamentos reales, las cuales son tenidas en cuenta para el desarrollo de los aportes teóricos de una manera adecuada.

Formulación del problema

¿El Colegio Integrado los Andes mantienen sus procesos adaptados a los requerimientos gubernamentales y técnicos en el manejo y resguardo adecuado de la información?

Descripción del problema

En los últimos tiempos, la protección de la información se ha vuelto un aspecto relevante en las organizaciones de América Latina. Están empezando a notar gradualmente que añadir otro dispositivo de hardware de seguridad, como un firewall, no es adecuado para mejorar la

seguridad de su organización. Según el informe de ISACA de 2008, las organizaciones no podrán obtener la seguridad que esperan de la tecnología de seguridad más actualizada si no tienen en su lugar las personas adecuadas y no se siguen los procesos establecidos.

La utilización de Internet, tanto en países desarrollados como en aquellos en vías de desarrollo, no deja de aumentar. Tanto empresas como individuos utilizan esta herramienta para intercambiar información. Dillard (2006) señala que, de acuerdo con el Informe de investigación de violación de datos de Verizon, se registraron más de 47000 casos de violación de seguridad en el periodo comprendido entre 2012 y 2013. La compañía telefónica Verizon (2013)

Los colegios son instituciones que manejan datos de forma continua en su rutina diaria, considerando que la información completa de los alumnos, profesores y especialmente los datos académicos son esenciales para llevar a cabo los procedimientos de gestión. Comprobar, J. Según Schutt, R.K. (2012), muchas empresas en esta industria no consideran seriamente la importancia de proteger adecuadamente la información frente a posibles ataques cibernéticos perpetrados por individuos sin escrúpulos que buscan sabotear la gestión con el objetivo de obtener beneficios personales a través de las bases de datos.

Desde el punto de vista de la seguridad de la información, esto ha originado inquietudes considerables en relación a la protección de los datos. Es fundamental que las instituciones y las personas involucradas en el campo de la educación comprendan la relevancia de salvaguardar la información y tomen las acciones adecuadas para asegurar su seguridad. Existen diversas guías de referencia disponibles para que las instituciones educativas evalúen los peligros de seguridad y establezcan medidas para cumplir con las normativas gubernamentales.

Según BSI (2012), la identificación de riesgos es una etapa crítica en el proceso de gestión de riesgos. Se deben evaluar tanto los riesgos internos como los externos que pueden afectar a una organización. Además, es necesario identificar las causas subyacentes de los riesgos para poder implementar medidas eficaces de mitigación. Es esencial contar con un enfoque sistemático y estructurado para identificar y evaluar los riesgos, incluyendo la participación de diferentes partes interesadas y la recopilación de datos relevantes.

El colegio CIANDES, también conocido como Colegio Integrado los Andes, es una institución educativa que brinda educación a jóvenes que desean realizar estudios de secundaria y media para poder obtener el título de bachiller en Colombia. Cada semestre, el colegio cuenta con una matrícula de 135 estudiantes. Este grupo posee una estructura organizativa claramente definida, la cual incluye un departamento encargado de supervisar los estudios y mantener registros académicos de los miembros.

El sistema utiliza una plataforma digital en la nube para almacenar la información, aunque también se respalda físicamente. Sin embargo, el sistema presenta un nivel de vulnerabilidad significativo que puede afectar la seguridad de la información.

El propósito de esta investigación, plasmada en esta monografía, es transferir conocimientos con la organización sobre cómo utilizar de manera adecuada procedimientos y herramientas que ayuden a garantizar una gestión de la información segura.

Justificación

La conexión entre la información, los sistemas y las instituciones educativas está experimentando un crecimiento acelerado, lo que ha generado un aumento en la cantidad de amenazas de seguridad que se dirigen a áreas menos comunes. En la actualidad, en un mundo tan tecnológico, si la seguridad de la información de un centro educativo se ve comprometida, sin duda alguna puede generar dificultades para otras personas o entidades involucradas.

Existen escasos retos asociados a esta relación, como la carencia de información. En relación a los criterios, alumnos y miembros de la institución, ausencia de un marco efectivo para emplear durante la ejecución, pautas para garantizar la seguridad de los especialistas, y deficiencia en el acatamiento. En los últimos tiempos, los estudios demuestran que las empresas que no toman precauciones en cuanto a la seguridad de sus sistemas informáticos enfrentan un peligro significativo de ser víctimas de debilidades y riesgos de seguridad. Esto pone en riesgo los tres pilares fundamentales de la seguridad de la información: la privacidad, la exactitud y la accesibilidad.

La salvaguardia de la información, tanto a nivel profesional como personal, se presenta como un aspecto crucial que exige ser abordado en la actualidad. Según AENOR (2004), con el fin de garantizar el cumplimiento de este requisito, los gobiernos establecen leyes que exigen a las organizaciones implementar medidas más sólidas para salvaguardar la confidencialidad de la información hasta cierto grado. Existen diversos estándares, marcos y modelos a nivel internacional que han sido diseñados para brindar a las organizaciones la posibilidad de asegurar la seguridad de su información. Entre ellos se destaca ISO/IEC 27001, un estándar reconocido.

Las organizaciones tienen la opción de alinearse con ISO/IEC 27001 de dos maneras diferentes. Una opción es implementarlo para cumplir con los requisitos básicos de seguridad,

mientras que la otra opción es buscar el registro al finalizar la implementación con el objetivo de obtener un certificado que valide su adhesión y adopción del estándar.

La aplicación de los criterios establecidos en la norma ISO /IEC 27001 podría favorecer una gestión adecuada de los procedimientos para el manejo, protección y conservación de los datos generados dentro de la organización educativa. Esto no solo aseguraría el seguimiento preciso de las actividades realizadas, sino también preservaría la confidencialidad de la información personal de quienes forman parte de la institución. La utilización de conocimientos provenientes de situaciones anteriores en la creación y ejecución de procedimientos de seguridad en la información brinda enfoques renovados que se adapten a las exigencias y necesidades de la empresa, con el fin de mantener el constante mejoramiento en todos los procesos.

La certificación brinda pruebas de la capacidad de la organización para manejar la seguridad de los activos de información confidencial y puede ser utilizada para asegurarlo a cualquier individuo externo, incluyendo los clientes. El texto se puede parafrasear de la siguiente manera: Guan, J., Lei, M., y Zhu, X. son los autores mencionados.

De acuerdo con Liu, J. (2013), la implementación del estándar permite a las empresas detectar y reducir los peligros relacionados con la seguridad de la información. Este enfoque ayuda a mejorar la seguridad de la información en general y generará confianza en las partes involucradas al demostrar que la organización tiene la capacidad para administrar la seguridad de la información mediante un enfoque fundamentado en la gestión de riesgos.

Por último, este estudio brinda la oportunidad de proporcionar bases teóricas y enfoques metodológicos para llevar a cabo investigaciones adicionales sobre este tema, así como también puede ser utilizado como una herramienta para abordar situaciones similares en otras

instituciones. El propósito es comunicar una realidad que posiblemente se manifieste en numerosas organizaciones, por medio de los resultados obtenidos, las conclusiones y las recomendaciones.

Objetivos

Objetivo general

Analizar la gestión en la información, con base en la norma ISO/IEC 27001 para el Colegio Integrado los Andes, Floridablanca, Santander.

Objetivos específicos

Diagnosticar los procesos operacionales para el manejo y uso de la información en el Colegio Integrado los Andes.

Identificar los activos más críticos en la gestión de la información.

Determinar los puntos críticos donde es necesario el uso de nuevas metodologías para el manejo adecuado de la información.

Marco Referencial

Marco teórico

La norma ISO/IEC 27001 ofrece a las empresas un conjunto de directrices para administrar de manera eficiente la seguridad de la información durante su implementación, operación y mantenimiento en curso. Ofrece a las organizaciones la posibilidad de acatar la reglamentación u obtener la certificación correspondiente. No obstante, las compañías necesitan tener en cuenta que el hecho de cumplir o ser certificado en la norma ISO/IEC 27001 no asegura la protección de los activos de información.

Solo indica que la organización posee la capacidad de administrar la seguridad de la información al nivel de seguridad que considere adecuado. y de acuerdo con la normativa. Si existe una deficiencia en la gobernabilidad corporativa y en el respaldo de la alta dirección para proteger los activos de información, hasta la evaluación de riesgos relacionados con la gestión de la seguridad de la información o cómo se evalúa y gestiona el riesgo de la información dentro de una empresa, podría ser plausible que la organización cumpla con los estándares establecidos, pero no esté debidamente protegida.

ISO/IEC 27001 es un estándar que proporciona una descripción completa sobre la gestión de la seguridad de la información. Este estándar establece los requisitos necesarios para implementar un sistema de gestión de seguridad de la información efectivo y mejora la confidencialidad, integridad y disponibilidad de los datos en una organización.

Proporciona una estructura para identificar y evaluar los riesgos de seguridad de la información, implementar controles de seguridad adecuados, establecer procesos de monitorización y revisión, y mejorar continuamente el sistema de gestión de la seguridad de la

información. Conforme a este estándar, las organizaciones pueden demostrar su capacidad para proteger la información de forma adecuada, proporcionando confianza a sus partes interesadas en cuanto a la seguridad de la información que manejan.

Además, la implementación de ISO/IEC 27001 ayuda a cumplir con las leyes y regulaciones de protección de datos y aumenta la resiliencia de una organización frente a incidentes de seguridad. En resumen, el estándar ISO/IEC 27001 es una guía fundamental para establecer y mantener un sistema de gestión de seguridad de la información sólido y eficaz.

Hay diferentes enfoques que las organizaciones pueden utilizar para proteger su información y garantizar que se cumplan los requisitos de gobernanza y regulaciones de privacidad y seguridad. Estos marcos de seguridad de la información permiten a las organizaciones identificar y evaluar los riesgos de seguridad de la información, y también implementar medidas para reducir esos riesgos. Uno de los enfoques más completos para abordar la seguridad de la información es adoptar, implementar y certificar un marco reconocido y utilizado a nivel internacional para la gestión de esta área.

La ISO y la IEC promueven el sistema global de estandarización. La serie ISO 27000 ofrece directrices sobre las mejores formas de administrar la seguridad de la información, los riesgos asociados y los controles necesarios para un Sistema de Gestión de Seguridad de la Información (SGSI). El estándar internacionalmente reconocido ISO/IEC 27001, llamado "Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos", es un estándar que garantiza la protección de la información. La norma establece y define los requisitos necesarios para el desarrollo, así como el funcionamiento y manejo de un SGSI. El propósito de ISO/IEC 27001 es garantizar una implementación,

operación y gestión uniforme y unificada de un Sistema de Gestión de Seguridad de la Información, junto con otros estándares de gestión como ISO 14000, que se enfoca en la Gestión Ambiental (ISO 14000 2004), ISO 9000 que se enfoca en la Gestión de Calidad (ISO 9000 2008), y ISO 31000 que se enfoca en la Gestión de Riesgos (ISO 31000 2009).

La directriz ISO/IEC 27001 ofrece instrucciones a las empresas sobre cómo resguardar su información sensible garantizando su confidencialidad, integridad y disponibilidad a través de un proceso de gestión de riesgos que genera seguridad y confianza en la organización al manejar de manera adecuada los riesgos. La norma ISO/IEC 27001, siguiendo una perspectiva de riesgo empresarial, describe el Sistema de Gestión de Seguridad de la Información (SGSI) como un sistema que permite establecer, implementar, monitorear, gestionar y mejorar de manera constante la seguridad de la información (ISO/IEC 27001 2005).

La adopción del estándar es una elección estratégica para una organización, ya que la creación y ejecución de un Sistema de Gestión de Seguridad de la Información (SGSI) se basa en las necesidades y metas de la organización. La norma ISO/IEC 27001 permite a las empresas establecer un Sistema de Gestión de Seguridad de la Información (SGSI) que atenderá todos los aspectos relacionados con la seguridad de la información de la organización.

Esto involucra desde la estructura organizacional, responsabilidades de los altos directivos, administración de recursos, políticas, procedimientos y procesos (ISO/IEC 27001 2005). Mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) como este, las organizaciones podrán administrar eficientemente la seguridad de sus datos y, al mismo tiempo, disminuir los peligros para sus operaciones empresariales.

Un aspecto clave de la gobernanza en las organizaciones es poder identificar y gestionar los riesgos en consecuencia. Una organización necesita conocer los riesgos que enfrenta para poder crear un enfoque eficaz que, en última instancia, proteja los recursos de información de la organización. Los procesos de evaluación y tratamiento de riesgos ISO/IEC 27001:2013 se alinean con los principios y lineamientos estipulados en la norma ISO 31000 (ISO 31000 2009). El enfoque de gestión de riesgos ISO/IEC 27001 requiere que las organizaciones cumplan con los siguientes procesos (ISO/IEC 27001 2013):

El proceso de evaluación de riesgos de seguridad de la información debe:

• Establecer y documentar un proceso de evaluación de riesgos;

• Garantizar que las evaluaciones se inicien a intervalos planificados o cuando se produzcan cambios importantes, sean coherentes, proporcionen valor y puedan compararse;

• Ser capaz de identificar riesgos de seguridad de la información;

• Ser capaz de analizar los riesgos de seguridad de la información;

• Ser capaz de evaluar los riesgos de seguridad de la información;

• Conservar la información documentada de los resultados de las evaluaciones de riesgos.

El proceso de tratamiento de riesgos de seguridad de la información:

• Define, aplica y documenta un proceso de tratamiento de riesgos;

• Utilizando los resultados de la evaluación de riesgos, selecciona opciones apropiadas de tratamiento de riesgos;

• Determina qué controles se requieren para implementar las opciones de tratamiento de riesgos;

• Formula el plan de tratamiento de riesgos;

• Obtiene la aprobación de los propietarios de riesgos del plan de tratamiento de riesgos, así como la aceptación de los riesgos residuales.

• Conserva la información documentada de los resultados del tratamiento de riesgos.

Una vez que se han identificado los riesgos de seguridad de la información para las organizaciones, los riesgos se registran en un registro de riesgos y se priorizan en orden de tipo y gravedad. Se completan detalles adicionales de los riesgos junto con el impacto estimado que el riesgo podría tener en la organización y detalles que pueden usarse para crear un perfil de riesgo. El siguiente paso es definir las opciones de tratamiento para los riesgos identificados. La versión ISO/IEC 27001:2013 traslada la importancia de la eficacia de los controles a la eficacia del plan de tratamiento de riesgos. ISO/IEC 27001 proporciona cuatro opciones de tratamiento de riesgos de seguridad de la información (ISO/IEC 27001 2013):

• Aceptación del riesgo: aceptar conscientemente el riesgo.

• Evitación de riesgos: evitar la actividad que causó el riesgo.

• Transferencia de riesgo: transferencia al seguro o subcontratación del riesgo.

• Reducción de riesgos: implementar controles para reducir el riesgo.

Es responsabilidad de la dirección, determinar cuál sería la alternativa más adecuada para tratar cada riesgo de seguridad de la información que se haya identificado. Para ello, deben evaluar el impacto, los costos y los beneficios de implementar las medidas de seguridad necesarias para reducir el riesgo, en comparación con la opción de no tomar ninguna medida al respecto. Independientemente de la opción elegida para gestionar los riesgos, siempre habrá una porción de riesgo que no podrá ser completamente eliminada.

Este riesgo residual, como se conoce, permanecerá presente (Humphreys, 2008). Cuando la administración ha elegido y consensuado las medidas para reducir el riesgo de seguridad de la información, es necesario llevar a cabo la implementación y uso efectivo de dichas medidas en la realidad. Para poner en marcha los controles, es necesario asignar roles y responsabilidades a los recursos encargados de llevar a cabo las tareas relacionadas con el control, además de brindarles la formación y el conocimiento adecuados.

La etapa final del proceso de gestión de riesgos implica la evaluación de la efectividad del control implementado y la supervisión y revisión constante de los riesgos de seguridad de la información. Es crucial porque las actividades y modificaciones diarias pueden impactar en el nivel de riesgo de la organización. Es necesario estar atentos a los cambios y evaluar nuevamente los riesgos con el fin de asegurarnos de que los controles sigan siendo eficientes.

Los procedimientos de evaluación, control y revisión del Sistema de Gestión de Seguridad de la Información (SGSI) deben ser llevados a cabo de manera sistemática. Es fundamental que las organizaciones establezcan procesos de medición, seguimiento y revisión para evaluar las medidas de seguridad del sistema de gestión de seguridad de la información

implementadas con el fin de proteger los activos de información de la organización (Humphreys, 2008). Un ejemplo concreto es evaluar la efectividad de una estrategia de sensibilización sobre la importancia de la seguridad de la información, la cual fue implementada con el objetivo de proporcionar conocimiento y educación a los trabajadores respecto a la política de seguridad de datos de la empresa. La medición consiste en evaluar qué tan eficiente ha sido el lanzamiento de la campaña entre todos los empleados de la empresa, así como la receptividad de los miembros del personal hacia la política de seguridad de la información. Se empleará el proceso de seguimiento y revisión para evaluar los resultados obtenidos de las mediciones.

El proceso de supervisión y evaluación también se puede emplear para controlar y revisar actividades como informes de reevaluación de riesgos, reportes de auditoría interna, así como la conformidad y la adherencia de los empleados a los procedimientos establecidos (Humphreys, 2008). Es esencial que las empresas tengan la capacidad de supervisar y evaluar los cambios en el entorno empresarial que puedan afectar la eficiencia de la organización. Esto se debe a que dichos cambios pueden dificultar la capacidad de la empresa para proteger su información y generar inestabilidades en su nivel de riesgo. Es necesario supervisar, analizar y valorar los cambios para determinar su impacto en el nivel de riesgo de la entidad. Esto le brinda a la organización la oportunidad de enfrentar y superar una variedad de amenazas que pueda enfrentar.

Mirando una representación visual del progreso del estándar y explorando su aplicación en organizaciones, resulta revelador analizar las ventajas que las organizaciones perciben en su adopción, así como las discusiones ontológicas en las que se involucra. 2019), es importante destacar que existe poca investigación que se enfoque en la comprensión de la interacción entre el comportamiento humano y la conciencia de los riesgos. Sin embargo, es fundamental tener en

cuenta que existen estudios limitados que abordan esta relación. Las organizaciones pueden obtener varios beneficios al implementar y registrar un SGSI (Sistema de Gestión de Seguridad de la Información) en 2009.

En un análisis de la literatura pertinente a la norma ISO/IEC 27001, se han identificado cuatro aspectos comerciales fundamentales que pueden ser beneficiados por su implementación: el cumplimiento normativo, la generación de ventajas en el ámbito del marketing, la reducción de costos a largo plazo y el control empresarial (ISO/IEC 27001 2005). El mayor beneficio es que brinda a la organización un marco seguro que puede ser utilizado para reducir los riesgos relacionados con la información.

De acuerdo con los beneficios mencionados en el Resumen del informe de investigación de seguridad de la información ISO/IEC 27001 (BSI 2012), se encontró que el 87% de los participantes afirmaron que la adopción del estándar tuvo un impacto positivo en su organización. La implementación del estándar permitió a las empresas cumplir con los requisitos de conformidad y reducir la cantidad de incidentes de seguridad reportados. Las empresas vieron un incremento en la satisfacción de sus clientes externos, lo cual resultó en un aumento en la rentabilidad y las ventas, a pesar de enfrentar mayores costos en la implementación y mejora de la infraestructura tecnológica.

La norma ISO/IEC 27001 asegura la salvaguardia de los recursos informativos en una empresa, no obstante, exige que la empresa promueva un ambiente donde se valore la importancia de la información y su resguardo. Esta meta puede ser alcanzada por medio de:

• El consejo directivo y la alta dirección están comprometidos con la seguridad de la información dentro de la organización, asumiendo la responsabilidad y la obligación de rendir cuentas.

• Asegurar que la seguridad de la información esté ubicada de manera adecuada en la estructura de la organización;

• La cooperación entre la administración corporativa y la de tecnología de la información respecto a la gestión de la seguridad de los datos.

• Garantizar la seguridad de la información mediante una gestión de riesgos eficiente;

• Elección adecuada de estrategias, límites y supervisión de seguridad para la implementación y funcionamiento de un Sistema de Gestión de Seguridad de la Información (SGSI) dentro de la entidad;

• Implementación de medidas, evaluación y supervisión de la seguridad de la información; y

• Una estrategia exitosa de enseñanza y sensibilización acerca de la protección de datos.

Además de las ventajas que la norma proporciona, también se presentan algunos obstáculos. En el artículo de Von Solms y Von Solms (2004) se abordan diversos elementos que generan problemas al momento de llevar a cabo la implementación de la seguridad de la información en una empresa. Varios de estos problemas están vinculados a empresas que no

comprenden que la seguridad de la información es una responsabilidad que deben asumir y un requisito fundamental para el buen gobierno corporativo. Es esencial contar con una estructura de gobierno de la seguridad de la información bien definida para lograr una implementación exitosa del SGSI.

Un estudio de los documentos existentes sobre la norma ISO/IEC 27001, indica que hay seis obstáculos que una empresa podría enfrentar al intentar implementarla de manera exitosa, lo cual podría dificultar la obtención de la certificación. Esto podría dar una pista sobre la razón por la cual las organizaciones tienen una adopción limitada del estándar, ya que los obstáculos percibidos pueden ser mayores que los beneficios evidentes.

Estos retos son reconocidos como (i) la adquisición de información y respaldo; (ii) traducir la jerga técnica de ISO 27001 en instrucciones prácticas; (iii) la integración de ISO 27001 con las normas y procedimientos de control ya existentes; (iv) hacer que ISO 27001 sea "factible" en una empresa de menor tamaño; (v) comprender el proceso de auditoría de ISO; y (vi) promocionar los beneficios percibidos a los clientes (ISO/IEC 27001 2005).

Marco conceptual

Confidencialidad: Una mejor definición del término confidencialidad es proporcionada por National Research Consejo donde se define como el concepto de impedir que se divulgue información por personas no autorizadas o garantizar que la información esté disponible para la persona apropiada solamente. Jason ha dado una definición adicional de confidencialidad. Andress, (2011) quien señaló que el concepto de confidencialidad puede verse comprometido en diferentes maneras, como durante el intercambio de información y los ataques para usar las vulnerabilidades de los sistemas de seguridad para inyectar malwares.

Integridad: La integridad es un grado en el que la capacidad de evitar que los datos o la información sean manipulado o cambiado de manera autorizada Andress, (2011). un resumen de los hallazgos fue identificado por Jason Andress muestra que la falta de implementación de información Los sistemas de seguridad pueden comprometer la integridad no debido al acceso de solo personas no autorizadas, los datos pueden verse comprometidos debido a cambios no deseados, borrado, o partes de datos por parte de una persona autorizada también. Por lo tanto, es extremadamente importante cumplir con la norma ISO 27001, que proporciona una guía precisa hacia la gestión de sistemas de seguridad.

Disponibilidad: La disponibilidad es un factor clave cuando se trata de mantener la capacidad de acceso a los datos cuando requerido y sólo a aquellos que tienen el permiso apropiado. Estaba esbozando que una la pérdida de disponibilidad podría provocar interrupciones de datos en otra parte de la cadena, Honan, (2010). Este tipo de error puede conducir a varios problemas, como cortes de energía, fallas en los sistemas operativos, ataques a la red y otros temas relacionados.

Seguridad de la información: El dominio de seguridad de la información se puede describir como una columna vertebral cuando se trata del concepto de protección de datos en cualquier forma. La investigación muestra que es uno de las crecientes áreas y diversas organizaciones específicamente en el área de la educación están haciendo su mejor esfuerzo adaptar los conceptos de seguridad en sus programas de cursos existentes, así como formular nuevos unos. Michael E va más allá al explicar que la habilitación de los conceptos de TI en varias operaciones comerciales como el almacenamiento de información y el transporte ha puesto de manifiesto muchos desafíos e hizo que las empresas se volvieran vulnerables desde ambos lados, dentro y fuera de la organización Edward, (2018).

Marco: Los marcos pueden describirse como una serie de procesos bien documentados que proporciona un conocimiento profundo sobre la política y los procedimientos mientras gestiona la información controles de seguridad La gestión de la seguridad de la información incorpora varias prácticas tales como protección perimetral, métodos de cifrado de aplicaciones y recuperación ante desastres. La existencia de normativa de cumplimiento como el Reglamento General de Protección de Datos (GDPR), para organizaciones con sede en EE. UU. Portabilidad y responsabilidad del seguro médico (HIPAA) y el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) han obligó a las organizaciones a comenzar a administrar su seguridad de TI siguiendo marcos generales. Los profesionales de la seguridad se benefician de los marcos cuando se trata de prepararse para cumplimiento y muchas más auditorías de TI, definiendo y priorizando las tareas requeridas mientras gestionar la seguridad de la organización Kirvan, (2019).

Marco de estado del arte

En la actualidad una de las principales deficiencias que tienen los centros educativos es la mala gestión de riesgos de seguridad de la información, algunos por desconocimiento y otros porque no le dan importancia, del mismo modo, tener la información requerida clasificada en tiempo real es poder, para las entidades que realizan el intercambio de información en todo momento y tienen ese privilegio de gestionar el conocimiento.

Crespo (2015) describe, la importancia de proteger la integridad, confidencialidad y la disponibilidad de la información es fundamental para evitar la vulnerabilidad de la información y generar confianza en los clientes.

Por consiguiente, otro aspecto a considerar es que los centros educativos deben de ser cautelosos en el tratamiento de su información, tanto interna como externa, para evitar fraudes, robos y pérdidas de información valiosa.

Para que la gestión de riesgos esté empleada en la inteligencia de negocios, se necesita una estrategia que contenga un conjunto de herramientas y servicios, las cuales deben permitir al usuario tener acceso a la información de manera eficiente, para analizar y ayudar en la toma decisiones, tácticas, operativas y estratégicas. Al mismo tiempo, gestionar la seguridad de la información no únicamente protege los activos de los centros educativos.

Por eso, es importante identificar la información más valiosa de los centros educativos, luego analizar la criticidad del riesgo y el impacto que puede ocasionar, en caso sufra un ataque que le afecte.

Por consiguiente, la norma NTC-ISO/IEC 27005 señala que la gestión de riesgo en la seguridad de información debe ser una tarea integral de todas las actividades y continuo para establecer un contexto para evaluar los riesgos, tratar los riesgos utilizando un plan para el tratamiento para analizar lo que puede suceder y cuáles serían las posibles consecuencias en caso sucediera.

En principio, un SGSI implica gestionar los riesgos orientados a la seguridad de la información, la cual ayuda en gran manera a identificar el estado actual de la información. Asimismo, es una estrategia para planificar la gestión de riesgo e implementar controles para establecer la política de seguridad de la información.

La norma NTC-ISO/IEC 27005 (2008) especifica que los controles a implementar estén dentro del alcance, los límites y el contexto deben estar basados en el riesgo. La aplicación del proceso de gestión de riesgo de la información tiene que satisfacer este requisito.

Además, la norma NTC-ISO/IEC 27005 (2008) recomienda, desarrollar criterios para la evaluación del riesgo con el propósito de determinar el nivel de la seguridad de la información, entre ellos: el valor estratégico del proceso de información del negocio, la criticidad de los activos de información implicados y la importancia de disponibilidad, confidencialidad e integridad para la organización.

Para ello, es importante recolectar información acerca de la entidad, tales como los procedimientos, la política de seguridad de la información que posee, las restricciones que afectan a la organización y, lo más importante, los objetivos estratégicos del negocio.

Por un lado, los centros educativos no tienen el área de TI para gestionar su información empresarial. Por eso, tienen mucha deficiencia en la gestión de riesgos de la información, porque no cuentan con especialistas en tecnología que den soporte a la organización. Para realizar la correcta gestión de riesgos es importante llevar a cabo la planificación de gestión que consiste, en identificar, analizar, planificar e implementar la respuesta y monitorear el riesgo, para cumplir los objetivos de la gestión de riesgo que son maximizar los riesgos positivos y minimizar los riesgos negativos; con el fin de garantizar el éxito de los objetivos de la institución.

Por lo tanto, el (SGSI) en una organización puede ayudarle a lograr el éxito y generar valor a su información, porque, los riesgos al estar identificados se pueden gestionar y prevenir para evitar que se materialicen.

Las herramientas y técnicas para identificar el riesgo que están comprendido por los siguientes: juicio de expertos para considerar aspectos de riesgos individuales, recopilación de datos en este nivel es la tormenta de ideas, habilidades interpersonales y de equipo en esta categoría facilitar mejoras efectivas para detectar, lista de ideas rápidas sirven para dar ideas al equipo y reuniones para llevar a cabo la identificación de riesgos.

Por eso, la información para la implementación de gestión de riesgos proviene de diferentes fuentes de las organizaciones, luego es estrictamente analizada para generar definiciones específicas e implementar controles efectivos para otorgar la escala según el impacto y la probabilidad del riesgo.

Asimismo, generar una matriz de riesgo para identificar de forma gráfica el nivel y potencial del riesgo, así poder planificar el tratamiento o respuesta a los riesgos. Por otro lado, la gestión de la seguridad de la información debe ser revisada completamente no solo para cubrir las fallas sino para entender la estructura y los elementos que la componen, tales como herramientas de software que puedan neutralizar el acceso ilegal y los ataques a los sistemas de información que pueden causar consecuencias negativas en los involucrados.

Por otro lado, la gestión de la seguridad de la información debe ser revisada completamente no solo para cubrir las fallas sino para entender la estructura y los elementos que la componen, tales como herramientas de software que puedan neutralizar el acceso ilegal y los ataques a los sistemas de información que pueden causar consecuencias negativas en los objetivos empresariales. Para ello, la norma ISO 27001 (2013) recomienda que es necesario llevar a cabo auditorías internas cada cierto tiempo con el fin de garantizar el óptimo funcionamiento y mantenimiento del SGSI y comprobar que el sistema está en estado correcto.

De igual manera en la siguiente investigación, Andrade (2018) describe que, en estos tiempos, las TICS interrelacionan los procesos de negocio y generan una nueva forma de vida digital para las empresas, a la vez hacen que sea más difícil extraer información relevante debido a que no están organizados. Esto dificulta realizar análisis, determinar y cuantificar los riesgos asociados a ellos.

A causa de ello, la SGSI principalmente se basa en identificar la actividad económica y objetivo de la empresa para ayudar a promover la ejecución de sus procesos administrativos basado en normas internacionales orientados en la protección de la información relevante. y lo más importante buscar la "Innovación" con el objetivo de asegurar los activos informáticos.

La norma ISO 27001 (2013) centra sus objetivos en proteger la confidencialidad, integridad y disponibilidad de la información empresarial, para lo cual, investiga los riesgos potenciales que puedan afectar a la información, y luego define la estrategia para evitar a que estos riesgos sucedan para eso implementa políticas, procedimientos y controles técnicos para mitigar el riesgo.

El SGSI planteado por la ISO 27001:2013 se divide en cuatro pasos. 1) planificar, que se centra en definir la política de seguridad, definir el alcance de SGSI y seleccionar controles. 2) Hacer, se centra el implantar el plan de gestión de riesgos y los controles. 3) Controlar, se centra en revisar internamente el SGSI, realizar auditorías de SGSI. 4) Actuar, este último se centra en realizar acciones correctivas y mejoras. porque, la tecnología cada vez que innova trae nuevos riesgos asociados a ellas que genera mucho peligro para la información.

Además, la norma ISO 27001 (2013) también establece las siguientes fases para la correcta implementación de un SGSI. Análisis y evaluación de riesgo, Implementación de

controles técnicos, definición para de plan para tratamiento de riesgo, definir alcance de gestión de riesgos, establecer el contexto de la organización, definir las partes interesadas, fijar y medir los objetivos de la empresa, documentar los controles establecidos y realizar auditorías internas y externas a la empresa. Para determinar que el uso de la información sea de manera óptima con fines corporativos y que sirva para obtener una mejora continua. Sin embargo, no todos los usuarios utilizan la información de manera eficiente. Hay quienes lo usan para su propio beneficio. Esto pasa en muchos centros educativos que utilizan la tecnología, pero no se enfocan en la seguridad de su información.

El investigador Jara (2018) obtuvo como resultado de su investigación que, existe una evidencia de mejora al aplicar el sistema de gestión de seguridad de información (SGSI) en una empresa. Para ello, en principio descubrió que no contar con una política de gestión de seguridad pone en peligro la confidencialidad, integridad y disponibilidad de la información, además detalla que aplicar la SGSI permite a la empresa estimar ahorros cuando los riesgos no suceden y no afectan a los objetivos de negocio. Esta es la razón para la implementación de (SGSI) en una empresa con aras de proteger el activo más valioso que es la información, ya que cuando no se protege la información de manera óptima se corre el riesgo de sufrir ataques cibernéticos o de otras índoles.

Mirna (2019) sugiere que, es importante diseñar e implementar las buenas prácticas y estándares de calidad. Pero, la mayoría de los centros educativos no las Implementan y a causa de ello falla sus procesos y se producen pérdidas financieras.

Ante lo mencionado, los centros educativos necesitan comprender cómo implementar el SGSI basado en la norma ISO 27001 y aplicarlo a su giro de negocio. Mirna (2019) describe que,

existen herramientas específicas para implementar SGSI y asegurar la información y a la vez conocer sus principales debilidades frente a los riesgos. Para ello, la norma ISO/IEC 27001 recomienda, conocer el origen y la potencialidad de los riesgos para gestionar los controles y verificar si los riesgos se aceptan o se comparten.

Es por ello que esta investigación se centra en el estudio y análisis de las principales debilidades que presentan los centros educativos en gestión de riesgos de la información empresarial. Incluso, es importante conocer las herramientas y software que emplean para gestionar la seguridad de información, para saber cuál es el estado actual de la protección de información que poseen, de acuerdo a ello, planificar la correcta implementación del sistema de gestión de seguridad de información.

En conclusión, después de haber hecho la evaluación comparativa de las investigaciones mencionadas líneas arriba, la gestión de la información con base en la ISO 27001para el Colegio Integrado los Andes se logra de la siguiente manera. Primeramente, la gestión de riesgos es el proceso, donde se debe reconocer qué información debe protegerse frente a las amenazas que lo pueden afectar y cómo actuar frente a ello. También, se descubrió distintas metodologías para gestionar los riesgos de la seguridad de la información, mediante los estándares establecidas por la norma ISO 27005 recomienda gestionar riesgos de la información de un centro educativo frente a las amenazas. Es importante conocer los objetivos y necesidades de la empresa para determinar el alcance y las áreas involucradas y, determinar el tiempo que toma la implementación. Asimismo, mediante la norma ISO 27002 recomienda la implantación de controles óptimos basados en objetivos del negocio y finalmente la medición y monitoreo de controles que establece mediante la norma ISO 27004 ayudan a minimizar las probabilidades de

ocurrencia del riesgo exponencialmente. y la guía del PMBOK (2017) describe, las estrategias para gestionar el riesgo mediante los estándares establecidos.

Resultados o impactos esperados

I Instrumento. Diagnóstico de la organización

1. ¿Existe en su centro educativo una entidad encargada de la seguridad cibernética en el ámbito de las Tecnologías de la Información y las Comunicaciones?

		fa	*fr*	*% Válido*	*% Acumulado*
Válidos	Nunca	10	100	100	100
	Rara vez	0	0	0	0
	Algunas Veces	0	0	0	0
	Muchas Veces	0	0	0	0
	Siempre	0	0	0	0
	Total	10	**100**	**100**	

La primera pregunta de la encuesta dirigida a los empleados del centro educativo indagaba acerca de la existencia de un departamento encargado de la seguridad informática. Los diez individuos dieron una respuesta negativa, lo cual sugiere que no hay una persona encargada en el centro educativo de asegurar y realizar actividades relacionadas con la seguridad informática.

La seguridad de la información en la institución educativa podría estar en peligro debido a esta circunstancia. Si no se cuenta con una protección adecuada en seguridad informática, la

institución educativa estará expuesta a riesgos mayores de ser víctima de ataques cibernéticos, tales como la sustracción de información, el chantaje o la interrupción de los servicios.

2. ¿Tu centro educativo ha experimentado problemas en su sistema de computadoras que hayan afectado su operación de alguna manera?

		fa	*fr*	*% Válido*	*% Acumulado*
Válidos	Nunca	0	0	0	0
	Rara vez	0	0	0	0
	Algunas Veces	0	0	0	0
	Muchas Veces	2	20	20	20
	Siempre	8	80	80	100
	Total	10	**100**	**100**	

En la encuesta llevada a cabo entre los empleados del centro educativo, la segunda interrogante indagaba acerca de la presencia de inconvenientes informáticos que pudieron haber causado un impacto en su desempeño. El 20% de los participantes afirmó que, en varias ocasiones, mientras que el 80% confirmó que en todo momento. El índice es considerablemente elevado y supone una amenaza significativa para la protección de los datos en la institución educativa. Los problemas informáticos tienen la capacidad de generar una interrupción en los servicios, el hurto de datos o la eliminación de información.

3. ¿Su institución educativa tiene políticas de seguridad informática respecto de los activos de información?

		Fa	***fr***	***% Válido***	***% Acumulado***
Válidos	Nunca	10	100	100	100
	Rara vez	0	0	0	0
	Algunas Veces	0	0	0	0
	Muchas Veces	0	0	0	0
	Siempre	0	0	0	0
	Total	10	**100**	**100**	0

La pregunta en la encuesta dirigida al personal del centro educativo indagaba sobre la existencia de políticas de seguridad informática en la institución educativa. Todos los encuestados, sin excepción, afirmaron que nunca se han implementado estas políticas. La seguridad de la información del centro educativo se encuentra amenazada por esta circunstancia, la cual plantea un riesgo significativo. Las políticas de seguridad informática engloban un conjunto de normas y métodos empleados con el fin de salvaguardar los datos del centro educativo.

4. ¿Su institución educativa tiene un inventario de activos de la información?

		fa	*fr*	*% Válido*	*% Acumulado*
Válidos	Nunca	10	100	100	100
	Rara vez	0	0	0	0
	Algunas Veces	0	0	0	0
	Muchas Veces	0	0	0	0
	Siempre	0	0	0	0
	Total	10	**100**	**100**	0

La encuesta dirigida a los empleados del centro educativo incluyó una pregunta adicional sobre si habían realizado un inventario de los activos de información de su organización. Todos los participantes de la encuesta, el 100% exactamente, afirmaron que nunca habían realizado esta acción anteriormente. La seguridad de la información del centro educativo corre un alto riesgo debido a esta situación. La realización de un inventario de activos de información consiste en la identificación, clasificación y documentación de todos los recursos informativos de una empresa.

5. ¿Su institución educativa ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

		fa	*fr*	*% Válido*	*% Acumulado*
Válidos	Nunca	8	80	80	80
	Rara vez	2	20	20	100
	Algunas Veces	0	0	0	0
	Muchas Veces	0	0	0	0
	Siempre	0	0	0	0
	Total	10	**100**	**100**	0

La encuesta dirigida a los empleados del centro educativo incluía un cuestionario que indagaba sobre la existencia de evaluaciones de riesgos previas para evaluar la vulnerabilidad de los individuos y los activos ante cualquier posible amenaza. Según el estudio, el 80% de los encuestados afirmaron que nunca habían llevado a cabo este análisis de riesgos, mientras que el restante 20%, específicamente una de las personas encuestadas, indicó que lo hacía en contadas ocasiones. La seguridad del centro educativo se encuentra en peligro debido a esta situación. El proceso de análisis de riesgos tiene como objetivo identificar, evaluar y gestionar los posibles riesgos a los que se enfrenta una organización.

6. ¿Su institución educativa tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo?

		fa	*fr*	*% Válido*	*% Acumulado*
Válidos	Nunca	10	100	100	100
	Rara vez	0	0	0	0
	Algunas Veces	0	0	0	0
	Muchas Veces	0	0	0	0
	Siempre	0	0	0	0
	Total	10	**100**	**100**	0

En la encuesta dirigida a los empleados del centro educativo, la sexta pregunta indagaba acerca de las medidas preventivas y correctivas adoptadas por la institución para protegerse contra los posibles riesgos asociados a la información. El cien por ciento de los encuestados afirmó que nunca ha llevado a cabo esas acciones. Esta circunstancia implica una amenaza significativa para la protección de la información del centro educativo. Las medidas preventivas y correctivas son estrategias implementadas con el fin de reducir los posibles riesgos.

7. ¿Su institución educativa realiza copias de seguridad de la información de forma periódica?

		fa	*fr*	*% Válido*	*% Acumulado*
Válidos	Nunca	10	100	100	100
	Rara vez	0	0	0	0
	Algunas Veces	0	0	0	0
	Muchas Veces	0	0	0	0
	Siempre	0	0	0	0
	Total	10	**100**	**100**	0

La séptima pregunta de la encuesta realizada a los empleados del centro educativo indagaba sobre la frecuencia con la que hacían respaldos de la información. Cada uno de los participantes, el total del grupo, dio una respuesta negativa. La seguridad de la información del centro educativo se encuentra en peligro debido a esta situación. La realización de copias de seguridad de la información es crucial para salvaguardar los datos en situaciones de pérdida, daño o eliminación de la misma. El centro educativo parece no comprender la relevancia de realizar copias de seguridad, ya que todos los encuestados respondieron negativamente a esta pregunta.

8. ¿El sistema operativo de cada uno de los computadores de la institución educativa está licenciado y es actualizado con regularidad?

		fa	*fr*	*% Válido*	*% Acumulado*
Válidos	Nunca	0	0	0	0
	Rara vez	2	20	20	20
	Algunas Veces	8	8	80	100
	Muchas Veces	0	0	0	0
	Siempre	0	0	0	0
	Total	10	**100**	**100**	0

En el cuestionario aplicado a los empleados del colegio, se indagó sobre si los sistemas operativos (SO) están debidamente licenciados y se mantienen actualizados de forma periódica. El 80% de las personas admitió tener ocasionalmente problemas con sus licencias, mientras que el 20% afirmó que esto ocurre muy poco frecuentemente. La seguridad del centro educativo se ve amenazada por esta circunstancia de alto riesgo. Los sistemas operativos sin licencia o desactualizados pueden presentar vulnerabilidades frente a ataques cibernéticos.

9. ¿Su institución educativa tiene implementados controles físicos y/o lógicos para salvaguardar la información?

		fa	*fr*	*% Válido*	*% Acumulado*
Válidos	Nunca	10	100	100	100
	Rara vez	0	0	0	0
	Algunas Veces	0	0	0	0
	Muchas Veces	0	0	0	0
	Siempre	0	0	0	0
	Total	10	**100**	**100**	0

La encuesta a los empleados del centro educativo incluía la pregunta número nueve acerca de si se habían establecido medidas físicas y/o de seguridad lógica para proteger la información. Todos los encuestados respondieron de forma negativa a esta pregunta. Esta circunstancia conlleva un peligro significativo para la integridad de la información del colegio. Los controles físicos y lógicos son herramientas que se emplean para salvaguardar los datos ante accesos no autorizados, extravíos, manipulaciones o daños.

10. ¿Su institución educativa tiene implementado un sistema de gestión en seguridad informática (SGSI)?

		fa	*fr*	*% Válido*	*% Acumulado*
Válidos	Nunca	10	100	100	100
	Rara vez	0	0	0	0
	Algunas Veces	0	0	0	0
	Muchas Veces	0	0	0	0
	Siempre	0	0	0	0
	Total	10	**100**	**100**	0

En la encuesta realizada a los empleados del centro educativo, se incluyó la pregunta número diez referente a la existencia de un Sistema de Gestión de la Seguridad de la Información (SGSI) en el centro educativo. Todos los encuestados respondieron de manera negativa en su totalidad. La seguridad del centro educativo está en riesgo debido a esta situación. Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de medidas, protocolos y prácticas empleadas para administrar la protección de la información en una empresa u entidad.

II Instrumento. Identificación de activos y puntos críticos

1. ¿Cuáles son los principales activos de información de su organización?

		f a	*f r*	*% Válido*	*% Acumulado*
Válidos	Bases de datos	10	100	100	100
	Documentos electrónicos	0	0	0	0
	Software	0	0	0	0
	Hardware	0	0	0	0
	Otros	0	0	0	0
	Total	10	**100**	**100**	

En la encuesta realizada a los empleados del centro educativo, se incluyó la pregunta número uno referente a Cuáles son los principales activos de información de su organización en el centro educativo. Todos los encuestados respondieron que la base de datos. El hecho de que el 100 % de la población encuestada respondiera que la base de datos es su principal activo de información indica que la organización es consciente del valor de sus datos. Los datos son esenciales para el funcionamiento del centro educativo. Los datos de los estudiantes son el activo de información más importante de una base de datos. Estos datos incluyen información sobre los nombres, direcciones, datos de contacto, historial de estudios, etc.

2. ¿Cuál es la importancia de estos activos para el negocio?

		f a	*f r*	*% Válido*	*% Acumulado*
Válidos	Alta	10	100	100	100
	Media	0	0	0	0
	Baja	0	0	0	0
	Total	10	**100**	**100**	

En el cuestionario aplicado, se indagó sobre la importancia de estos activos para el negocio. El 100% de las personas expreso ser muy alta. La protección de los activos de información del colegio es fundamental para garantizar la seguridad y la continuidad del servicio educativo. El centro educativo debe implementar medidas de seguridad adecuadas para proteger sus datos, como medidas de control de acceso, medidas de cifrado y medidas de detección de intrusiones. Los datos son esenciales para el funcionamiento de la organización, ya que permiten gestionar el aprendizaje de los estudiantes, la administración del colegio y la comunicación con las familias.

3. ¿Cuál es el nivel de sensibilidad de la información contenida en estos activos?

		fa	*fr*	*% Válido*	*% Acumulado*
Válidos	Alta	10	100	100	100
	Media	0	0	0	0
	Baja	0	0	0	0
	Total	10	**100**	**100**	

Para la pregunta número tres donde se consultó cual es el nivel de sensibilidad de la información contenida en estos activos el 100% de la población respondió que es muy alta. Los activos de información más importantes para un colegio son los datos de estudiantes, profesores, personal administrativo y familias. Esta información es sensible por varias razones, incluyendo que puede contener información personal, confidencial o importante para el funcionamiento del colegio. Las consecuencias de la pérdida o la exposición de información sensible pueden ser graves, incluyendo perjuicios económicos, daño a la reputación e interrupción del servicio educativo.

4. ¿Cuál es la necesidad de que estos activos estén disponibles?

		f a	*f r*	*% Válido*	*% Acumulado*
Válidos	Alta	10	100	100	100
	Media	0	0	0	0
	Baja	0	0	0	0
	Total	10	**100**	**100**	

Con respecto a la pregunta número cuatro Cuál es la necesidad de que estos activos estén disponibles el 100% de los encuestados respondió que es muy alta. Por ser una organización que presta servicio educativo la información mantiene un flujo constante dentro de las diferentes áreas del centro educativo y la necesidad de que el personal docente ingrese información de notas, actividades y de cara a la administración tengan los resultados para procesar los datos y determinar resultados que serán entregados a cada representante.

5. ¿Cuáles son los riesgos que pueden afectar a los activos críticos de su organización?

		fa	*fr*	*% Válido*	*% Acumulado*
Válidos	Robo	0	0	0	0
	Pérdida	50	50	500	50
	Alteración	50	50	50	100
	Acceso no autorizado	0	0	0	0
	Otros	0	0	0	0
	Total	100	**100**	**100**	

En la pregunta número cinco los encestados respondieron a cuáles son los riesgos que pueden afectar a los activos críticos de su organización con un 50% los encuestados manifestaron que la perdida de información puede afectar los activos críticos por ser datos sensibles para el usuario, por otra parte el otro 50% manifiesta que las exposición a alteraciones a los datos sería un riesgo inminente a los activos, es por ello la importancia de tomar medidas para mitigar estos niveles de riesgos y así poder garantizar la seguridad y el flujo de la información.

6 ¿Cuáles son las deficiencias en la seguridad de la información que pueden poner en riesgo los activos críticos de su organización?

		fa	*fr*	*% Válido*	*% Acumulado*
Válidos	Falta de control de acceso	10	100	100	100
	Falta de cifrado	0	0	0	0
	Falta de backup	0	0	0	0
	Otros	0	0	0	0
	Total	10	**100**	**100**	

Para la pregunta número seis sobre las deficiencias en la seguridad de la información que pueden poner en riesgo los activos críticos de su organización el 100% de los encuestados manifestaron que la falta de control de acceso es sin duda una de las deficiencias más graves en la organización en el manejo de los procesos operacionales en el colegio. Para proteger los activos críticos de un colegio es importante que la organización adopte medidas de seguridad adecuadas. Estas medidas deben incluir el desarrollo de una política de seguridad de la información, implementación de medidas de control de acceso y uso del cifrado.

7. ¿Qué nuevas metodologías podrían utilizarse para mejorar la seguridad de la información en los puntos críticos?

		f a	*f r*	*% Válido*	*% Acumulado*
Válidos	Cloud computing	10	100	100	100
	Big data	0	0	0	0
	Inteligencia artificial	0	0	0	0
	Otros	0	0	0	0
	Total	10	**100**	**100**	

En la pregunta número siete donde formula qué nuevas metodologías podrían utilizarse para mejorar la seguridad de la información en los puntos críticos el 100% de la población encuestada respondió que la implementación de Cloud computing seria parte de la solución a los desafíos presentes en este centro educativo. La computación en la nube, también conocida como nube computing, es un modelo de entrega de servicios informáticos que permite a las organizaciones acceder a recursos informáticos, como servidores, almacenamiento, bases de datos, redes y software, a través de Internet. Todo esto fortalecido con el desarrollo de procedimientos que estandaricen la forma en cómo se manejan las operaciones para garantizar la seguridad de la información.

Procedimiento para la gestión de incidentes de seguridad de la información

En la era digital, la información se ha convertido en un activo fundamental para las instituciones educativas. El Colegio Integrado Los Andes, consciente de la importancia de proteger su información y los activos de sus estudiantes, personal y comunidad educativa en general, ha desarrollado un Procedimiento para la Gestión de Incidentes de Seguridad de la Información. Este documento establece un marco de acción para detectar, contener, erradicar y recuperar la información en caso de un incidente de seguridad.

El Procedimiento para la Gestión de Incidentes de Seguridad de la Información del Colegio Integrado Los Andes se basa en un enfoque proactivo, con cinco etapas claramente definidas: detección, análisis, contención, erradicación y recuperación.

El éxito del Procedimiento para la Gestión de Incidentes de Seguridad de la Información depende del compromiso de todos los miembros de la comunidad educativa. El Comité de Seguridad de la Información define y supervisa el procedimiento, mientras que el responsable de Seguridad de la Información se encarga de su implementación y coordinación. Los usuarios, por su parte, juegan un papel fundamental al reportar cualquier evento sospechoso.

La comunicación clara y transparente es vital durante todo el proceso de gestión del incidente. Se debe informar a los usuarios y partes interesadas sobre el incidente, las acciones tomadas y el estado de la recuperación.

El Procedimiento para la Gestión de Incidentes de Seguridad de la Información del Colegio Integrado Los Andes es una herramienta fundamental para proteger la información y los activos de la institución. Este documento demuestra el compromiso del colegio con la seguridad de la información y su capacidad para responder de manera efectiva a los incidentes,

minimizando su impacto y previniendo su recurrencia. A continuación, el siguiente documento podrá ser encontrado en el anexo de este documento.

Conclusiones

La investigación se enfocó en examinar cómo se administra la información en el Colegio Integrado los Andes en Floridablanca, Santander, siguiendo las directrices de la norma ISO/IEC 27001. Las conclusiones se derivan de los resultados obtenidos de los Objetivos de la investigación que fueron cuidadosamente planeados y alcanzados.

El propósito de este estudio fue determinar el grado de conocimiento que tiene el Colegio Integrado los Andes sobre la norma ISO/IEC 27001. Se llegó a la conclusión de que la institución educativa carece de conocimientos sobre la norma ISO/IEC 27001. La relevancia de la norma es reconocida, ya que asegura una mayor calidad en el trabajo y proporciona supervisión y confianza en la ejecución de las labores.

El organismo demostró una postura positiva hacia la importancia de tener conocimiento y aplicar la norma ISO/IEC 27001, debido a que ayuda a mejorar la protección de la información en general. Al llevar a cabo esta acción, se logrará una mejora en la forma en que una empresa administra y cumple con las disposiciones de seguridad de los datos, los sistemas de seguridad y los elementos vinculados a la gestión de peligros. Es fundamental que los líderes máximos asuman la responsabilidad y apoyen de forma activa para garantizar una implementación exitosa.

Se puede observar en general que, a pesar de existir una carencia en los métodos y saberes relacionados con la ISO/IEC 27001 en el colegio, su adopción se encuentra restringida. La organización tiene como objetivo principal ofrecer un servicio de calidad, lo cual implica mejorar no solo la educación que brindamos, sino también proteger la privacidad de la información y reducir el riesgo de robo de datos. Cumpliremos con las leyes y regulaciones correspondientes, al mismo tiempo que se satisface las demandas de nuestros clientes.

Adoptar una estrategia de adopción resulta altamente ventajoso para una organización, ya que le brinda una ventaja competitiva en su industria y contribuye a incrementar tanto el valor comercial para sus clientes como para sus proveedores. Sin embargo, implementar la seguridad de la información representa desafíos, siendo el más importante la obligación de cambiar la forma en que la organización ve y aborda este tema. Sin embargo, para las organizaciones, el principal reto consiste en obtener la autorización y apoyo de los altos ejecutivos para llevar a cabo la implementación de la norma ISO/IEC 27001.

Referencias bibliográficas

Aenor, (2004). Asociación Española de Normalización y Certificación (AENOR) UNE 71502:2004. Disponible en: http://www.aenor.es/aenor/normas/normas/fichanorma.asp

Andrés. (2011). Los fundamentos de la comprensión de la seguridad de la información. Disponibleen:https://books.google.fi/books?id=9NI0AwAAQBAJ&pg=PA7&dq=cia+triad&hl=en&sa=X&ved=2ahUKEwjXodG2mtz1AhUklosKHTyXA54Q6AF6BAgGEAI#v=onepage&q=cia%20triad&f=falso

Arnason, ST. Willett, K.D., (2007). Cómo lograr la certificación 27001: un ejemplo de gestión de cumplimiento aplicada, CRC Press.

Bertolín, J. (2008). Seguridad de la Información Redes, informática y sistemas de información. Madrid.

Bsi, (2012). Beneficios de ISO/IEC 27001 Resumen del informe de investigación de seguridad de la información. Disponible en: http://www.bsigroup.ae/upload/CaseStudiesM/Benefits of ISOIEC 27001 Information Security Research Report SummaryResearch_Summary.pdf

Check, J. & Schutt, R.K., (2012). Métodos de investigación en educación, Publicaciones SAGE.

Chew, E., Swanson, M., Stine, K.M., Bartol, N., Brown, A. & Robinson, W., (2018). Publicación especial 800-55 Rev. 1, Guía de medición del rendimiento para la seguridad de la información, Instituto Nacional de Estándares y Tecnología.

Craft, R., Wyss, G., Vandewart, R. y Funkhouser, D., (2018). Un marco abierto para la gestión de riesgos. Instituto Nacional de Normas y Tecnología.

Davis, F.D., (2016). Un modelo de aceptación de tecnología para probar empíricamente nuevos sistemas de información del usuario final: teoría y resultados. Instituto de Tecnología de Massachusetts.

Edward, H. (2018). Estándares de gestión de seguridad de la información. Disponible en: https://doi.org/10.1016/j.istr.2008.10.010

Dillard, K., (2006). La guía de gestión de riesgos de seguridad. Microsoft.

Guamán (2015). Diseño de un sistema de gestión de seguridad de la información para instituciones militares: Tesis de maestría: Quito, Ecuador. Escuela Politécnica Nacional.

Honan (2010). ISO27001 en un entorno Windows: Disponible en: https://books.google.fi/books?id=GMcyZWviyvgC&pg=PA19&dq=conceptos+clave+de+informaciónmation+security+standards&hl=en&sa=X&ved=2ahUKEwiG7v6Z1M_1AhWs-yoKHSmIDQ8Q6AF6BAgIEAI#v=unapágina&q=clave%20conceptos%20de%20información%20seguridad%20estándares&f=false

Isaca, (2008). Alineación de COBIT 4.1, ITIL V3 e ISO/IEC 27002 para Business Benefit. A Informe de gestión de ITGI y OGC, ISACA.

ISO (2013) ISO/IEC 27001 en español. Disponible en: http://www.iso27000.es/iso27000.html

Kirvan, (2019) "Explicación de los marcos y estándares de seguridad". BuscarSeguridad.Disponibleen:https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one.

Logisman. (2011). Familia ISO 27000: Seguridad de la Información. Obtenido deLogisman: http://custodia-documental.com/familia-iso-27000-segur idad-de-lainformacion/

Magerit. (2015). Metodología de Análisis y Gestión de Riesgos de los Sistemas deInformación:http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VBYDL8J5NCY

Poore, R.S., (2016). Manual de gestión de la seguridad de la información, quinta edición, volumen 3, Prensa CRC

Rivas (2017). Diagnóstico y plan de acción para la implementación del marco de negocio para el gobierno y gestión de tecnologías de la información (cobit5.0). Tesis de Maestría: Universidad técnica de Machala

Seguridad de la información (2015) Disponible en: http://www.pmg-ssi.com/2015/07/que-essgsi/

Suarez (2015). Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. Tesis de Maestría: Universidad Nacional Abierta y a Distancia. Bogotá, Colombia.

Verizon, (2013). Informe de investigaciones de violación de datos. Verizon. Disponibleen:http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigationsreport-013.

Anexos 1

Instrumento para el diagnóstico de la organización

A continuación, se presentan algunas preguntas que puede responder marcando con una X en la casilla.

¿Existe en su centro educativo una entidad encargada de la seguridad cibernética en el ámbito de las Tecnologías de la Información y las Comunicaciones?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Tu centro educativo ha experimentado problemas en su sistema de computadoras que hayan afectado su operación de alguna manera?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene políticas de seguridad informática respecto de los activos de información?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene un inventario de activos de la información?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	

Siempre	

¿Su institución educativa tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa realiza copias de seguridad de la información de forma periódica?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿El sistema operativo de cada uno de los computadores de la institución educativa está licenciado y es actualizado con regularidad?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuáles son los principales activos de información de su organización?

Bases de datos	
Documentos electrónicos	
Software	
Hardware	
Otros	

¿Cuál es la importancia de estos activos para el negocio?

Muy alta	
Alta	
Media	
Baja	

¿Cuál es el nivel de sensibilidad de la información contenida en estos activos?

Alta	
Media	
Baja	

¿Cuál es la necesidad de que estos activos estén disponibles?

Muy alta	
Alta	
Media	
Baja	

¿Cuáles son los riesgos que pueden afectar a los activos críticos de su organización?

Robo	
Pérdida	
Alteración	
Acceso no autorizado	
Otros	

¿Cuáles son las deficiencias en la seguridad de la información que pueden poner en riesgo los activos críticos de su organización?

Falta de control de acceso	
Falta de cifrado	
Falta de backup	
Otros	

¿Qué nuevas metodologías podrían utilizarse para mejorar la seguridad de la información en los puntos críticos?

Cloud computing	
Big data	
Inteligencia artificial	
Otros	

Anexos 2

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS

Encuestado N°: 10 Edad: 55 Genero: Masculino Cargo: Docente

Instrumento para el diagnóstico de la organización

A continuación, se presentan algunas preguntas que puede responder marcando con una X en la casilla

¿Existe en su centro educativo una entidad encargada de la seguridad cibernética en el ámbito de las Tecnologías de la Información y las Comunicaciones?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Tu centro educativo ha experimentado problemas en su sistema de computadoras que havan afectado su operación de alguna manera?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	X

¿Su institución educativa tiene políticas de seguridad informática respecto de los activos de información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene un inventario de activos de la información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuáles son los principales activos de información de su organización?

Bases de datos	X
Documentos electrónicos	
Software	
Hardware	
Otros	

¿Cuál es el nivel de sensibilidad de la información contenida en estos

Alta	X
Media	
Baja	

¿Su institución educativa realiza copias de seguridad de la información de forma periódica?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿El sistema operativo de cada uno de los computadores de la institución educativa está licenciado y es actualizado con regularidad?

Nunca	
Rara vez	
Algunas Veces	X
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuál es la importancia de estos activos para el negocio?

Alta	X
Media	
Baja	

¿Cuál es la necesidad de que estos activos estén disponibles?

Alta	X
Media	
Baja	

¿Cuáles son los riesgos que pueden afectar a los activos críticos de su organización?

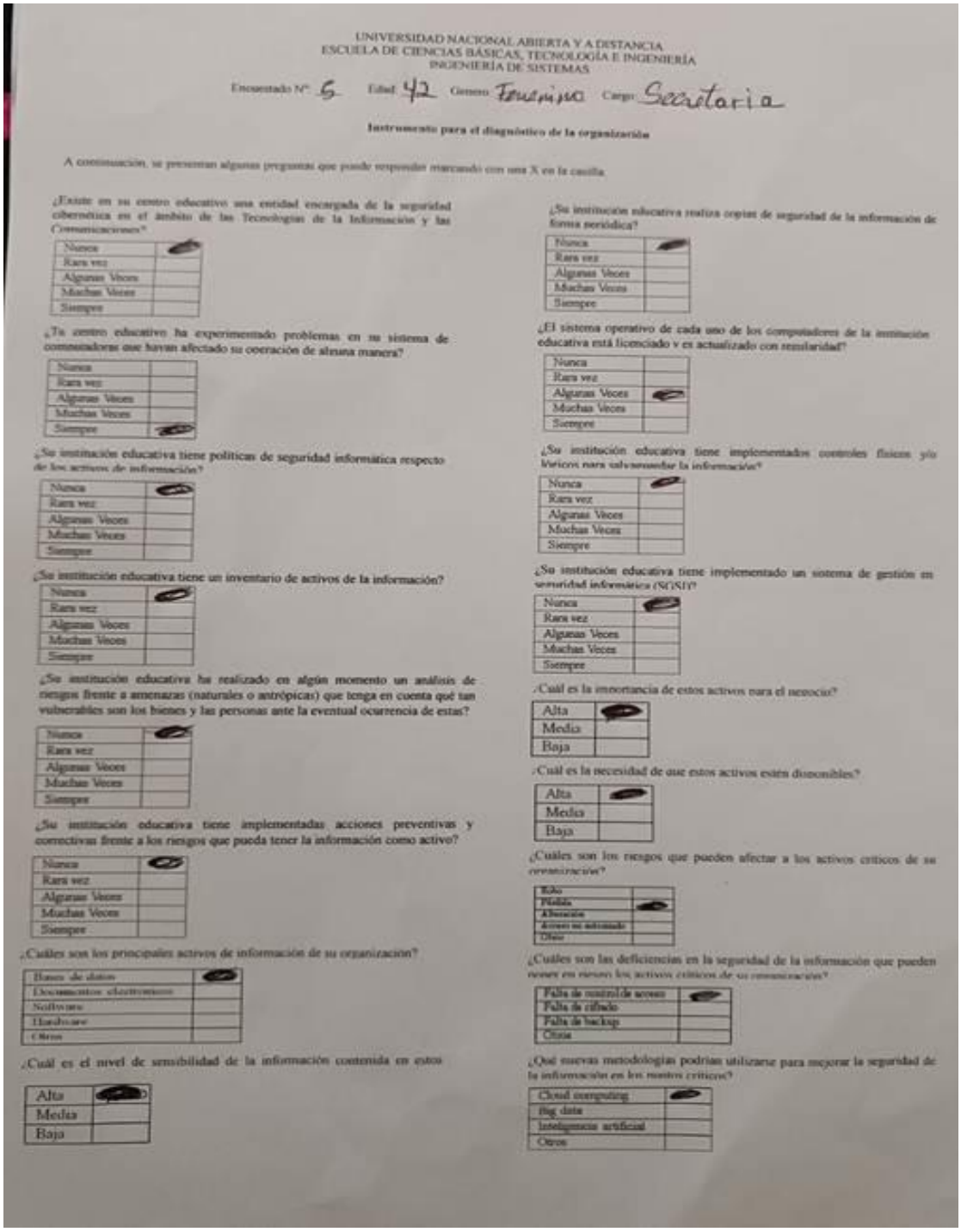
Robo	
Pérdida	
Alteración	X
Acceso no autorizado	
Otros	

¿Cuáles son las deficiencias en la seguridad de la información que pueden poner en riesgo los activos críticos de su organización?

Falta de control de acceso	X
Falta de cifrado	
Falta de backup	
Otros	

¿Qué nuevas metodologías podrían utilizarse para mejorar la seguridad de la información en los puntos críticos?

Cloud computing	X
Big data	
Inteligencia artificial	
Otros	



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS

Encuestado N°: 5 Edad: 42 Genero: Femenino Cargo: Secretaria

Instrumento para el diagnóstico de la organización

A continuación, se presentan algunas preguntas que puede responder marcando con una X en la casilla

¿Existe en su centro educativo una entidad encargada de la seguridad cibernética en el ámbito de las Tecnologías de la Información y las Comunicaciones?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Ha centro educativo ha experimentado problemas en su sistema de computadoras que hayan afectado su operación de alguna manera?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	✓

¿Su institución educativa tiene políticas de seguridad informática respecto de los activos de información?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene un inventario de activos de la información?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuáles son los principales activos de información de su organización?

Bases de datos	✓
Documentos electrónicos	
Software	
Hardware	
Otros	

¿Cuál es el nivel de sensibilidad de la información contenida en estos

Alta	✓
Media	
Baja	

¿Su institución educativa realiza copias de seguridad de la información de forma periódica?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿El sistema operativo de cada uno de los computadores de la institución educativa está licenciado y es actualizado con regularidad?

Nunca	
Rara vez	
Algunas Veces	✓
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuál es la importancia de estos activos para el negocio?

Alta	✓
Media	
Baja	

¿Cuál es la necesidad de que estos activos estén disponibles?

Alta	✓
Media	
Baja	

¿Cuáles son los riesgos que pueden afectar a los activos críticos de su organización?

Robo	
Pérdida	✓
Alteración	
Acceso no autorizado	
Otros	

¿Cuáles son las deficiencias en la seguridad de la información que pueden tener en riesgo los activos críticos de su organización?

Falla de control de acceso	✓
Falla de cifrado	
Falla de backup	
Otras	

¿Qué nuevas metodologías podrían utilizarse para mejorar la seguridad de la información en los nuevos críticos?

Cloud computing	✓
Big data	
Inteligencia artificial	
Otros	

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS

Encuestado N°: 6 Edad: 51 Genero: Femenino Cargo: Coordinadora

Instrumento para el diagnóstico de la organización

A continuación, se presentan algunas preguntas que puede responder marcando con una X en la casilla.

¿Existe en su centro educativo una entidad encargada de la seguridad cibernética en el ámbito de las Tecnologías de la Información y las Comunicaciones?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Tu centro educativo ha experimentado problemas en su sistema de computadoras que havan afectado su operación de alguna manera?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	X

¿Su institución educativa tiene políticas de seguridad informática respecto de los activos de información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene un inventario de activos de la información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuáles son los principales activos de información de su organización?

Bases de datos	X
Documentos electrónicos	
Software	
Hardware	
Otros	

¿Cuál es el nivel de sensibilidad de la información contenida en estos

Alta	X
Media	
Baja	

¿Su institución educativa realiza copias de seguridad de la información de forma periódica?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿El sistema operativo de cada uno de los computadores de la institución educativa está licenciado y es actualizado con regularidad?

Nunca	
Rara vez	
Algunas Veces	X
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuál es la importancia de estos activos para el negocio?

Alta	X
Media	
Baja	

¿Cuál es la necesidad de que estos activos estén disponibles?

Alta	X
Media	
Baja	

¿Cuáles son los riesgos que pueden afectar a los activos críticos de su organización?

Robo	
Pérdida	
Alteración	X
Acceso no autorizado	
Otros	

¿Cuáles son las deficiencias en la seguridad de la información que pueden poner en riesgo los activos críticos de su organización?

Falta de control de acceso	X
Falta de cifrado	
Falta de backup	
Otros	

¿Qué nuevas metodologías podrían utilizarse para mejorar la seguridad de la información en los puntos críticos?

Cloud computing	X
Big data	
Inteligencia artificial	
Otros	

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS

Encuestado N°: 7 Edad: 36 Genero: Masculino Cargo: Control de Estudios

Instrumento para el diagnóstico de la organización

A continuación, se presentan algunas preguntas que puede responder marcando con una X en la casilla.

¿Existe en su centro educativo una entidad encargada de la seguridad cibernética en el ámbito de las Tecnologías de la Información y las Comunicaciones?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Tu centro educativo ha experimentado problemas en su sistema de computadoras que hayan afectado su operación de alguna manera?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	X

¿Su institución educativa tiene políticas de seguridad informática respecto de los activos de información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene un inventario de activos de la información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Nunca	
Rara vez	X
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuáles son los principales activos de información de su organización?

Bases de datos	X
Documentos electrónicos	
Software	
Hardware	
Otros	

¿Cuál es el nivel de sensibilidad de la información contenida en estos

Alta	X
Media	
Baja	

¿Su institución educativa realiza copias de seguridad de la información de forma periódica?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿El sistema operativo de cada uno de los computadores de la institución educativa está licenciado y es actualizado con regularidad?

Nunca	
Rara vez	
Algunas Veces	X
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuál es la importancia de estos activos para el negocio?

Alta	X
Media	
Baja	

¿Cuál es la necesidad de que estos activos estén disponibles?

Alta	X
Media	
Baja	

¿Cuáles son los riesgos que pueden afectar a los activos críticos de su organización?

Robo	
Pérdida	X
Alteración	
Acceso no autorizado	
Otros	

¿Cuáles son las deficiencias en la seguridad de la información que pueden poner en riesgo los activos críticos de su organización?

Falta de control de acceso	X
Falta de cifrado	
Falta de backup	
Otros	

¿Qué nuevas metodologías podrían utilizarse para mejorar la seguridad de la información en los puntos críticos?

Cloud computing	X
Big data	
Inteligencia artificial	
Otros	

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS

Encuestado Nº 9 Edad 47 Genero Femenino Cargo Administrativo

Instrumento para el diagnóstico de la organización

A continuación, se presentan algunas preguntas que puede responder marcando con una X en la casilla

¿Existe en su centro educativo una entidad encargada de la seguridad cibernética en el ámbito de las Tecnologías de la Información y las Comunicaciones?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Tu centro educativo ha experimentado problemas en su sistema de computadoras que hayan afectado su operación de alguna manera?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	✓

¿Su institución educativa tiene políticas de seguridad informática respecto de los activos de información?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene un inventario de activos de la información?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuáles son los principales activos de información de su organización?

Bases de datos	✓
Documentos electrónicos	
Software	
Hardware	
Otros	

¿Cuál es el nivel de sensibilidad de la información contenida en estos

Alta	✓
Media	
Baja	

¿Su institución educativa realiza copias de seguridad de la información de forma periódica?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿El sistema operativo de cada uno de los computadores de la institución educativa está licenciado y es actualizado con regularidad?

Nunca	
Rara vez	
Algunas Veces	✓
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuál es la importancia de estos activos para el negocio?

Alta	✓
Media	
Baja	

¿Cuál es la necesidad de que estos activos estén disponibles?

Alta	✓
Media	
Baja	

¿Cuáles son los riesgos que pueden afectar a los activos críticos de su organización?

Robo	
Pérdida	✓
Alteración	
Acceso no autorizado	
Otros	

¿Cuáles son las deficiencias en la seguridad de la información que pueden poner en riesgo los activos críticos de su organización?

Falta de control de acceso	✓
Falta de cifrado	
Falta de backup	
Otros	

¿Qué nuevas metodologías podrían utilizarse para mejorar la seguridad de la información en los puntos críticos?

Cloud computing	✓
Big data	
Inteligencia artificial	
Otros	

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS

Encuestado N°: 3 Edad: 45 Genero: Masculino Cargo: Rector

Instrumento para el diagnóstico de la organización

A continuación, se presentan algunas preguntas que puede responder marcando con una X en la casilla

¿Existe en su centro educativo una entidad encargada de la seguridad cibernética en el ámbito de las Tecnologías de la Información y las Comunicaciones?

Nunca	—
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Tu centro educativo ha experimentado problemas en su sistema de computadoras que hayan afectado su operación de alguna manera?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	—
Siempre	

¿Su institución educativa tiene políticas de seguridad informática respecto de los activos de información?

Nunca	—
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene un inventario de activos de la información?

Nunca	—
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Nunca	—
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo?

Nunca	—
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuáles son los principales activos de información de su organización?

Bases de datos	—
Documentos electrónicos	
Software	
Hardware	
Otros	

¿Cuál es el nivel de sensibilidad de la información contenida en estos

Alta	—
Media	
Baja	

¿Su institución educativa realiza copias de seguridad de la información de forma periódica?

Nunca	—
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿El sistema operativo de cada uno de los computadores de la institución educativa está licenciado y es actualizado con regularidad?

Nunca	
Rara vez	
Algunas Veces	—
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Nunca	—
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Nunca	—
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuál es la importancia de estos activos para el negocio?

Alta	—
Media	
Baja	

¿Cuál es la necesidad de que estos activos estén disponibles?

Alta	—
Media	
Baja	

¿Cuáles son los riesgos que pueden afectar a los activos críticos de su organización?

Robo	
Pérdida	✓
Alteración	
Acceso no autorizado	
Otros	

¿Cuáles son las deficiencias en la seguridad de la información que pueden poner en riesgo los activos críticos de su organización?

Falta de control de acceso	—
Falta de cifrado	
Falta de backup	
Otros	

¿Qué nuevas metodologías podrían utilizarse para mejorar la seguridad de la información en los puntos críticos?

Cloud computing	—
Big data	
Inteligencia artificial	
Otros	

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS

Encuestado N°: 4 Edad: 39 Genero: Femenino Cargo: Docente

Instrumento para el diagnóstico de la organización

A continuación, se presentan algunas preguntas que puede responder marcando con una X en la casilla.

¿Existe en su centro educativo una entidad encargada de la seguridad cibernética en el ámbito de las Tecnologías de la Información y las Comunicaciones?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	X

¿Tu centro educativo ha experimentado problemas en su sistema de computadoras que hayan afectado su operación de alguna manera?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	X

¿Su institución educativa tiene políticas de seguridad informática respecto de los activos de información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene un inventario de activos de la información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Nunca	
Rara vez	X
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuáles son los principales activos de información de su organización?

Bases de datos	X
Documentos electrónicos	
Software	
Hardware	
Otros	

¿Cuál es el nivel de sensibilidad de la información contenida en estos

Alta	X
Media	
Baja	

¿Su institución educativa realiza copias de seguridad de la información de forma periódica?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿El sistema operativo de cada uno de los computadores de la institución educativa está licenciado y es actualizado con regularidad?

Nunca	
Rara vez	
Algunas Veces	X
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuál es la importancia de estos activos para el negocio?

Alta	X
Media	
Baja	

¿Cuál es la necesidad de que estos activos estén disponibles?

Alta	X
Media	
Baja	

¿Cuáles son los riesgos que pueden afectar a los activos críticos de su organización?

Robo	
Perdida	
Alteración	X
Acceso no autorizado	
Otros	

¿Cuáles son las deficiencias en la seguridad de la información que pueden poner en riesgo los activos críticos de su organización?

Falta de control de acceso	X
Falta de cifrado	
Falta de backup	
Otros	

¿Qué nuevas metodologías podrían utilizarse para mejorar la seguridad de la información en los puntos críticos?

Cloud computing	X
Big data	
Inteligencia artificial	
Otros	

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS

Encuestado N°: 2 Edad: 42 Genero: Femenino Cargo: Controladora de documentos

Instrumento para el diagnóstico de la organización

A continuación, se presentan algunas preguntas que puede responder marcando con una X en la casilla.

¿Existe en su centro educativo una entidad encargada de la seguridad cibernética en el ámbito de las Tecnologías de la Información y las Comunicaciones?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Tu centro educativo ha experimentado problemas en su sistema de computadoras que havan afectado su operación de alguna manera?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	X

¿Su institución educativa tiene políticas de seguridad informática respecto de los activos de información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene un inventario de activos de la información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuáles son los principales activos de información de su organización?

Bases de datos	X
Documentos electronicos	
Software	
Hardware	
Otros	

¿Cuál es el nivel de sensibilidad de la información contenida en estos

Alta	X
Media	
Baja	

¿Su institución educativa realiza copias de seguridad de la información de forma periódica?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿El sistema operativo de cada uno de los computadores de la institución educativa está licenciado y es actualizado con regularidad?

Nunca	
Rara vez	X
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuál es la importancia de estos activos para el negocio?

Alta	X
Media	
Baja	

¿Cuál es la necesidad de que estos activos estén disponibles?

Alta	X
Media	
Baja	

¿Cuáles son los riesgos que pueden afectar a los activos críticos de su organización?

Robo	
Pérdida	
Alteración	X
Acceso no autorizado	
Otros	

¿Cuáles son las deficiencias en la seguridad de la información que pueden poner en riesgo los activos críticos de su organización?

Falta de control de acceso	X
Falta de cifrado	
Falta de backup	
Otros	

¿Qué nuevas metodologías podrían utilizarse para mejorar la seguridad de la información en los puntos críticos?

Cloud computing	X
Big data	
Inteligencia artificial	
Otros	

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS

Encuestado N°: 1 Edad: 30 Genero: Femenino Cargo: Asistente

Instrumento para el diagnóstico de la organización

A continuación, se presentan algunas preguntas que puede responder marcando con una X en la casilla.

¿Existe en su centro educativo una entidad encargada de la seguridad cibernética en el ámbito de las Tecnologías de la Información y las Comunicaciones?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su centro educativo ha experimentado problemas en su sistema de computadoras que hayan afectado su operación de alguna manera?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	X
Siempre	

¿Su institución educativa tiene políticas de seguridad informática respecto de los activos de información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene un inventario de activos de la información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

Cuáles son los principales activos de información de su organización?

Bases de datos	X
Documentos electrónicos	
Software	
Hardware	
Otros	

¿Cuál es el nivel de sensibilidad de la información contenida en estos

Alta	X
Media	
Baja	

¿Su institución educativa realiza copias de seguridad de la información de forma periódica?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿El sistema operativo de cada uno de los computadores de la institución educativa está licenciado y es actualizado con regularidad?

Nunca	
Rara vez	X
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Nunca	X
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuál es la importancia de estos activos para el negocio?

Alta	X
Media	
Baja	

¿Cuál es la necesidad de que estos activos estén disponibles?

Alta	X
Media	
Baja	

¿Cuáles son los riesgos que pueden afectar a los activos críticos de su organización?

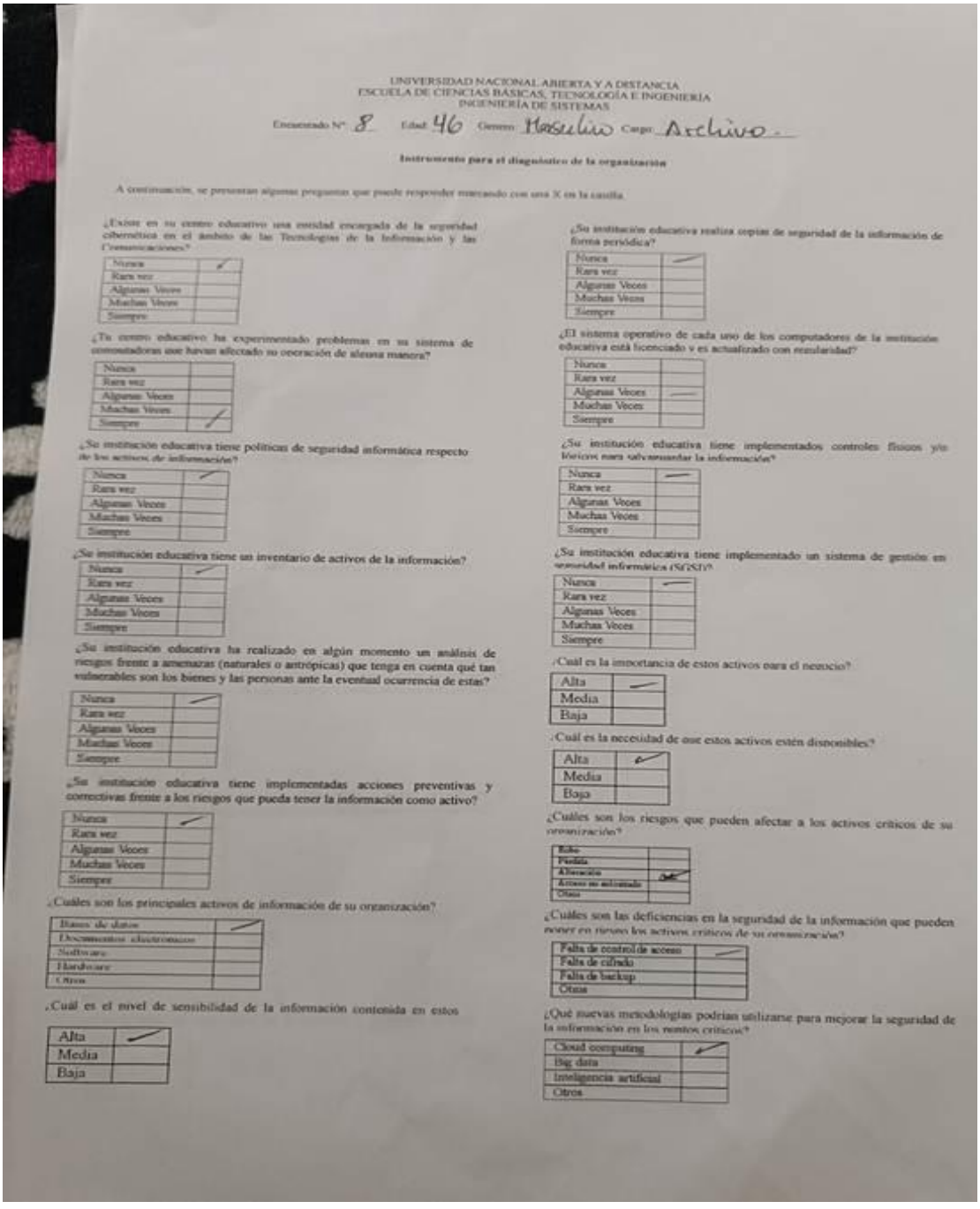
Robo	
Perdida	X
Alteración	
Acceso no autorizado	
Otros	

¿Cuáles son las deficiencias en la seguridad de la información que pueden tener en riesgo los activos críticos de su organización?

Falta de control de acceso	X
Falta de cifrado	
Falta de backup	
Otros	

¿Qué nuevas metodologías podrían utilizarse para mejorar la seguridad de la información en los puntos críticos?

Cloud computing	X
Big data	
Inteligencia artificial	
Otros	



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS

Encuestado Nº: 8 Edad: 46 Genero: Masculino Cargo: Archivo.

Instrumento para el diagnóstico de la organización

A continuación, se presentan algunas preguntas que puede responder marcando con una X en la casilla

¿Existe en su centro educativo una entidad encargada de la seguridad cibernética en el ámbito de las Tecnologías de la Información y las Comunicaciones?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su centro educativo ha experimentado problemas en su sistema de computadoras que hayan afectado su operación de alguna manera?

Nunca	
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	✓

¿Su institución educativa tiene políticas de seguridad informática respecto de los activos de información?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene un inventario de activos de la información?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuáles son los principales activos de información de su organización?

Bases de datos	✓
Documentos electrónicos	
Software	
Hardware	
Otros	

¿Cuál es el nivel de sensibilidad de la información contenida en estos

Alta	✓
Media	
Baja	

¿Su institución educativa realiza copias de seguridad de la información de forma periódica?

Nunca	✓
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿El sistema operativo de cada uno de los computadores de la institución educativa está licenciado y es actualizado con regularidad?

Nunca	
Rara vez	
Algunas Veces	—
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Nunca	—
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Su institución educativa tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Nunca	—
Rara vez	
Algunas Veces	
Muchas Veces	
Siempre	

¿Cuál es la importancia de estos activos para el negocio?

Alta	✓
Media	
Baja	

¿Cuál es la necesidad de que estos activos estén disponibles?

Alta	✓
Media	
Baja	

¿Cuáles son los riesgos que pueden afectar a los activos críticos de su organización?

Robo	
Perdida	
Alteración	✓
Acceso no autorizado	
Otros	

¿Cuáles son las deficiencias en la seguridad de la información que pueden poner en riesgo los activos críticos de su organización?

Falta de control de acceso	✓
Falta de cifrado	
Falta de backup	
Otros	

¿Qué nuevas metodologías podrían utilizarse para mejorar la seguridad de la información en los puntos críticos?

Cloud computing	✓
Big data	
Inteligencia artificial	
Otros	

	Procedimiento para la Gestión de Incidentes de Seguridad de la Información	**CODIGO** CIA-PR-001
		REVISIÓN / **FECHA** DIC 2023
		PÁGINA 1 de 9

Procedimiento para la Gestión de Incidentes de Seguridad de la Información

Hoja de Revisión

EV. NO.	FECHA	BREVE DESCRIPCIÓN DEL CAMBIO	ELABORADO	REVISADO	APROBADO

Índice

1 **OBJETIVO**

	Procedimiento para la Gestión de Incidentes de Seguridad de la Información	CODIGO CIA-PR-001	
		REVISIÓN	FECHA DIC 2023
		PÁGINA	1 de 9

Asegurar un enfoque estructurado y planificado que permita la detección, análisis, evaluación y tratamiento a los eventos e incidentes de Seguridad de la Información de manera eficiente, por medio de la documentación y divulgación de las actividades necesarias para mitigar o reducir la probabilidad de impacto de la materialización de un incidente, presentado a nivel organizacional. en el Colegio Integrado los Andes

1. Alcance

El presente procedimiento aplica para todos los procesos, servicios, recursos e infraestructura tecnológica del Colegio Integrado los Andes, iniciando con la notificación de un evento o incidente de Seguridad de la Información y finalizando con la recopilación de evidencias y la documentación de la resolución del incidente.

2. Responsables

Calidad

Seguridad Informática

3. Definiciones

Evento de Seguridad de la Información: Ocurrencia o cambio de circunstancias identificadas en un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información, falla de los controles o una situación desconocida.

Evidencia: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.

Gestión de Incidentes de Seguridad de la Información: Procesos o fases para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Incidente o Violación de Seguridad de la Información: Uno o varios eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer la confidencialidad, integridad y/o disponibilidad de la información.

Informática Forense: Aplicación de la ciencia para la identificación, recolección, examen y análisis de los datos, preservando correctamente su integridad, llevando a cabo a su vez una estricta cadena de custodia de la información.

Csirt: Cyber Security Incident Response Team (Equipo de Respuesta a Incidentes de Seguridad de la Información), el cual se encarga de gestionar de forma eficiente el daño resultante de incidentes, así como también proveer de respuesta y recuperación efectiva, ante estos.

Siem: Security Information and Event Manager (Gestión de Eventos e Información de Seguridad), es una tecnología compatible con la detección de amenazas y la respuesta a incidentes de seguridad a través de la recopilación en tiempo real y el análisis histórico de eventos de seguridad de varias fuentes de datos contextuales y de eventos con la capacidad de correlacionarlos.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguridad Informática: Medidas de prevención que impiden la ejecución de operaciones no autorizadas sobre sistemas de información o redes informáticas.

4. Procedimiento

Política de Gestión de Activos de Información

	Procedimiento para la Gestión de Incidentes de Seguridad de la Información	**CODIGO** CIA-PR-001
		REVISIÓN / **FECHA** DIC 2023
		PÁGINA 1 de 9

Colegio Integrado los Andes entendiendo la importancia de proteger sus activos de información, es consiente que cada uno de estos se encuentra expuesto a la materialización de un evento de seguridad no deseado, que tiene una probabilidad de comprometer la confidencialidad, integridad y/o disponibilidad de la información, por lo tanto, se hace necesario contar con un procedimiento que gestione de forma adecuada los incidentes de seguridad de la información. Por lo tanto, el Sistema de Gestión de Seguridad de la Información-SGSI, da a conocer los lineamientos establecidos en el presente procedimiento, tomando como referente lo especificado en el anexo A.16 de la norma ISO 27001:2013, los cuales se describen a continuación:

- Se deben asignar roles y responsabilidades durante todo el procedimiento de gestión de incidentes de seguridad de la Información, teniendo en cuenta lo documentado en el procedimiento Roles y responsabilidades en seguridad y privacidad de la información.

- Se dinamizará una estrategia, mediante un gestor de eventos para Seguridad de la Información y/o Seguridad Informática, que atenderá de manera general a la organización y de manera particular a sus partes interesadas incluyendo los diferentes canales de comunicación autorizados.

- El CSIRT o quien haga sus veces, deberá hacer la identificación y/o evaluación del incidente, en donde se logre identificar si hace referencia a un incidente de seguridad de la información, seguridad informática y/o a un incidente en relación a la protección de datos personales, además deberá identificar si este se trata de un evento, incidente o una falsa alarma, por ende, deberá hacer la clasificación del incidente estableciendo prioridades para atender los incidentes que se presenten a nivel organizacional.

- Es responsabilidad de los funcionarios administrativos, docentes y demás partes interesadas, reportar al área competente en temas de seguridad de la información y/o seguridad informática, cualquier irregularidad que se considere como un evento que atente contra los principios de seguridad de la información, por los canales dispuestos para tal fin.

- Una vez el CSIRT o quien haga sus veces, sea notificado de un evento o incidente en seguridad de la información, darán desarrollo a los procedimientos, que se encuentran documentados y aprobados a nivel organizacional para atender y dar respuesta ante la posible materialización del incidente de seguridad.

- Como parte de las medidas de prevención ante los eventos y/o incidentes de seguridad, se podrá incluir en el procedimiento de sensibilización y entrenamiento en seguridad y privacidad de la información, las estrategias para la sensibilización a las partes interesadas, acerca de los incidentes de seguridad de la información, divulgando a quien se debe reportar, los tipos de incidentes, niveles de categorización y mejores prácticas para la mitigación de tipo de eventos.

- Como parte de las medidas de monitoreo ante los eventos y/o incidentes de seguridad, el rol de vigía de seguridad de la información podrá verificar el cumplimiento de los lineamientos enfocados en la mitigación de incidentes de seguridad, con el propósito de identificar y documentar las fortalezas y debilidades encontradas. De ser necesario podrá reportar el o los eventos de seguridad de la información que tienen una alta probabilidad de comprometer la confidencialidad, integridad y/o disponibilidad de la información.

- La alta dirección o su representante, en articulación con el equipo de respuesta inmediata a incidentes de Seguridad de la Información y/o quien haga sus veces, establecerán las estrategias para el diseño y realización de análisis de vulnerabilidad y pruebas de penetración a los sistemas de información, con el objetivo de evaluar el estado real de la seguridad en la infraestructura tecnológica y de aplicaciones informáticas de la Institución.

	Procedimiento para la Gestión de Incidentes de Seguridad de la Información	CODIGO CIA-PR-001	
		REVISIÓN	FECHA DIC 2023
		PÁGINA	1 de 9

- De presentarse un incidente que sobre pase las capacidades técnicas y tecnológicas de la institución, el CSIRT o quien haga sus veces, podrá contactar a los grupos de apoyo como autoridades, grupos de interés externos que manejen asuntos relacionados a incidentes de seguridad de información para dar solución al mismo.

Este procedimiento se realiza en cumplimiento de la Norma ISO 27001:2013 y del ítem 16 de la Tabla 1 de los controles del Anexo A del estándar ISO/IEC 27001 y del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones.

ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA
1. Monitoreo de eventos e incidentes de Seguridad de la Información. Nota: En caso de identificarse un incidente en las herramientas de auditoría a los servicios TI, se deberá	Equipo de respuesta inmediata a incidentes de Seguridad de la Información	Implementación de herramientas de monitoreo. (Herramientas tecnológicas de TI, mesa de servicios). Visita del rol de vigía de seguridad de la	Manual de uso de las herramientas TI.

	Procedimiento para la Gestión de Incidentes de Seguridad de la Información	CODIGO CIA-PR-001	
		REVISIÓN	FECHA DIC 2023
		PÁGINA	1 de 9

registrar en la herramienta que se disponga para tal fin.		información.	
2. Notificar cualquier situación o evento que atente contra la confidencialidad, integridad y disponibilidad de la información.	coordinadores, analista y cualquier colaborador	Implementación de medios de comunicación (mesa de servicio, formularios web, correo electrónico, línea telefónica, etc.) mediante los cuales se pueda informar cualquier evento de seguridad de la información.	Guía para el reporte de eventos y/o eventos de seguridad de la información.
3. Clasificar los eventos y/o incidentes de seguridad de la información.	Equipo de respuesta inmediata a incidentes de Seguridad de la Información.	Categorización del evento o incidente de seguridad de la Información y realizar las indagaciones, investigaciones y pruebas necesarias para determinar si se trata de un ejercicio de	Manual – Política de Gestión de Incidentes de seguridad de la información

	Procedimiento para la Gestión de Incidentes de Seguridad de la Información	CODIGO CIA-PR-001	
		REVISIÓN	FECHA DIC 2023
		PÁGINA	1 de 9

		ingeniería social, un evento o un incidente de seguridad de la información.	
Si el evento reportado no es considerado un incidente de seguridad de la información o hace parte de un pentesting avalado por la alta dirección, continuar con la actividad No.9, de lo contrario seguir en la actividad No.4.			
4. Analizar y evaluar el evento o incidente de seguridad de la información.	Equipo de respuesta inmediata a incidentes de Seguridad de la Información.	Evaluación del impacto del evento de seguridad de la información con el fin de identificar posibles causas. Dar respuesta en el tiempo previsto para esta actividad.	Manual – Política de Gestión de Incidentes de seguridad de la información
Si el evento reportado afecta los datos personales de un trabajador o trabajadora de la organización, continuar con la actividad No. 5, de lo contrario seguir en la actividad No.6			

ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA

	Procedimiento para la Gestión de Incidentes de Seguridad de la Información	CODIGO CIA-PR-001	
		REVISIÓN	FECHA DIC 2023
		PÁGINA	1 de 9

5. Ejecutar el procedimiento Reporte de Incidente de Protección de Datos Personales. Nota: Finaliza este procedimiento.	Oficial de tratamiento de datos personales. Sistema de Gestión de Seguridad de la Información	Esta actividad solo se realiza si el incidente ha sido efectuado sobre una base de datos personales el Colegio Integrado los Andes acude como responsable del tratamiento.	Manual – Política de Gestión de Incidentes de seguridad de la información
6. Ejecutar acciones correctivas para detener el incidente de seguridad.	Equipo de respuesta inmediata a incidentes de Seguridad de la Información.	Realizar todas aquellas tareas necesarias, con el fin de contener el incidente de seguridad y así minimizar su impacto.	No aplica
Si en el evento reportado, se hace necesario la recopilación, preservación y análisis de información para determinarla causa del incidente, continuar con la actividad No. 7, de lo contrario seguir con la actividad No. 8			
7. Realizar investigación informática forense sobre el incidente.	Equipo de respuesta inmediata a incidentes de Seguridad de la Información	Es indispensable contar con los recursos suficientes para llevar a cabo este procedimiento, en caso de materializarse el incidente se escalará a las instancias pertinentes para documentar las posibles causas y material	Manual – Política de Gestión de Incidentes de seguridad de la información

	Procedimiento para la Gestión de Incidentes de Seguridad de la Información	CODIGO CIA-PR-001	
		REVISIÓN	FECHA DIC 2023
		PÁGINA 1 de 9	

		probatorio del mismo.	
8. Tratar y solucionar las vulnerabilidades relacionadas con el incidente.	Equipo de respuesta inmediata a incidentes de Seguridad de la Información	Definir e implementar la solución definitiva al incidente, permitiendo la mitigación al máximo de la probabilidad de ocurrencia y el impacto causado.	Manual – Política de Gestión de Incidentes de seguridad de la información
9.. Registrar y hacer cierre formal del incidente.	Equipo de respuesta inmediata a incidentes de Seguridad de la Información	El incidente de seguridad de la información debe haberse tratado satisfactoriamente. Así mismo se debe identificar las lecciones aprendidas.	No Aplica

ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA
10. Comunicar el desarrollo del manejo del incidente a las partes interesadas.	Equipo de respuesta inmediata a incidentes de Seguridad de la	Notificar la solución del incidente involucrando el impacto y las buenas prácticas para su prevención.	Manual – Política de Gestión de Incidentes de seguridad de la información

	Procedimiento para la Gestión de Incidentes de Seguridad de la Información	CODIGO CIA-PR-001	
		REVISIÓN	FECHA DIC 2023
		PÁGINA	1 de 9

	Información	Así mismo se debe comunicar las lecciones aprendidas.	
11. Documentar el análisis y la resolución del incidente.	Equipo de respuesta inmediata a incidentes de Seguridad de la Información	Es necesario contar con una herramienta que actúe como base de conocimiento para registrar el desarrollo de cada incidente presentado. Establecer contacto con las autoridades.	Manual – Política de Gestión de Incidentes de seguridad de la información

	Reporte de Evento Y/O Incidentes de Seguridad de la Información	**CODIGO** CIA-FO-001
		REVISIÓN / **FECHA** DIC 2023
		PÁGINA 1 de 2

INFORMACIÓN GENERAL	
Código:	
Fecha de reporte del evento y/o incidente:	
Hora de reporte del evento y/o incidente:	
DATOS DE LA PERSONA QUE NOTIFICA EL EVENTO Y/O INCIDENTE	
Nombre completo:	
Documento de identificación:	
Correo electrónico empresarial:	
Área u Oficina:	
Teléfono:	
Ubicación física de la persona:	
INFORMACIÓN SOBRE EL EVENTO Y/O INCIDENTE	
Fecha de ocurrencia del evento y/oincidente:	
Hora de ocurrencia del evento y/o incidente:	
Tipos de evento y/o incidente de seguridad (Marque una o más de las opciones de respuesta)	☐Accesos no autorizados. ☐Ingeniería Social (Phishing) ☐Presencia de código malicioso (Malware) ☐Abuso y/o uso inadecuado de los servicios de información. ☐Borrado de información (compromiso) ☐Denegación de servicio

	Reporte de Evento Y/O Incidentes de Seguridad de la Información	**CODIGO** CIA-FO-001
		REVISIÓN | **FECHA** DIC 2023
		PÁGINA 1 de 2

	☐Intrusiones ☐Multicomponente ☐Otro ¿Cuál? _____
Ubicación sitio física o lógica del eventoy/o incidente: (Marque una o más de las opciones de respuesta)	☐Plataforma organizacional ☐Página web Colegio Integrado los Andes ☐Servicio de Office 365 ☐Servicios institucionales tercerizados ☐Otro ¿Cuál? _____
Describa el evento y/o incidente:	

	Reporte de Evento Y/O Incidentes de Seguridad de la Información	**CODIGO** CIA-FO-001
		REVISIÓN / **FECHA** DIC 2023
		PÁGINA 1 de 2

Información Comprometida: - Describa brevemente la información contenida en el sistema (Computador/archivador/repositorio de información)	
Observaciones o comentarios adicionales:	
¿El evento y/o incidente aún está enprogreso? (Marque una de las opciones de respuesta)	SÍ NO
GESTIÓN DEL EVENTO Y/O INCIDENTE (Sólo se diligencia por parte del área encargada de dar respuesta)	
Nombre del responsable de recibir el evento y/o incidente:	
Categorización del evento y/o incidente (Marque una o más de las opciones derespuesta)	☐Incidente de seguridad ☐Evento tecnológico ☐Falla tecnológica ☐Desastre natural ☐Conflicto social ☐Otro ¿cuál? _____

	Reporte de Evento Y/O Incidentes de Seguridad de la Información	**CODIGO** CIA-FO-001
		REVISIÓN / **FECHA** DIC 2023
		PÁGINA 1 de 2

Impacto de evento y/o incidente:	☐Afecta Confidencialidad e Integridad ☐Afecta Confidencialidad y disponibilidad ☐Afecta Disponibilidad e Integridad ☐Afecta la Confidencialidad ☐Afecta la Disponibilidad ☐Afecta la Integridad ☐Afecta la Confidencialidad, Disponibilidade integridad
Priorización del evento y/o incidente	☐Muy Alta ☐Alta ☐Media ☐Baja ☐Muy Baja
Nombre del área o responsable de tratar el evento y/o incidente:	

	Reporte de Evento Y/O Incidentes de Seguridad de la Información	**CODIGO** CIA-FO-001
		REVISIÓN / **FECHA** DIC 2023
		PÁGINA 1 de 2

Describa las acciones para detener el evento y/o incidente:	
Describa las acciones para resolver el evento y/o incidente:	
Fecha de finalización del evento y/o incidente:	
Describa las acciones pendientes a resolver el evento y/o incidente:	

	Reporte de Evento Y/O Incidentes de Seguridad de la Información	**CODIGO** CIA-FO-001
		REVISIÓN / **FECHA** DIC 2023
		PÁGINA 1 de 2

Grupo de interés contactados:	☐Lideres ☐Coordinaciones ☐Control Interno ☐Control de operaciones ☐Profesores ☐Administrativos ☐ ¿Otro cuál?