ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"USO DE LA ISO 27001 PARA LA APLICACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN EN EL DEPARTAMENTO INFORMÁTICO DE LA UNIVERSIDAD SAN GREGORIO DE PORTOVIEJO"

EXAMEN DE GRADO (COMPLEXIVO)

Previo la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

MARCOS RAMON GALLEGOS MACIAS

GUAYAQUIL – ECUADOR

2016

AGRADECIMIENTO

A Dios por brindarme la paz espiritual lo que conlleva a dar serenidad y predisposición para alcanzar asertivamente la culminación de mis metas, a mi esposa Cecilia Valdiviezo Pinargote por su compañía, comprensión y motivación para lograr mis objetivos, a mi madre por convencerme de que una formación profesional me permitirá alcanzar un mejor porvenir.

DEDICATORIA

Dedico este éxito profesional a Dios, a mi esposa y a mi madre por formar parte de mi vida, y ser la motivación para buscar con firmeza y humildad el logro de mis metas.

TRIBUNAL DE SUSTENTACIÓN

_____

Mgs. Lenin Eduardo Freire Cobo

DIRECTOR DEL MSIA

_____

Mgs Lenin Eduardo Freire Cobo

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

_____

Mgs. Juan Carlos García Plúa

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

En la actualidad no es ajeno escuchar lo relevante que es proteger la información y los sistemas informáticos de una organización u empresa, a medida que la tecnología avanza en todas las áreas, de manera paralela también los delincuentes informáticos adquieren nuevas estrategias y métodos para apoderarse de una red o sistema informático. Afortunadamente existen normas estándares para implementar controles de seguridad de la información, una de ellas es la Norma ISO 27001, que plantea las directrices para la Implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información), mismo que requiere de un alto compromiso por parte de las autoridades de la institución.

El presente trabajo de investigación se basa en la aplicación de controles de seguridad de la información mismos que fueron seleccionados de acuerdo a los procesos relevantes del Departamento de Informática de la Universidad San Gregorio de Portoviejo.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

CEAACES. : Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior.

ISO :Organización Internacional de Normalización

PDCA : Plan, Do, Check, Act, Planificar, Ejecutar, Monitorear, Actualizar.

SGSI : Sistema de Gestión de Seguridad de Información.

UPS : Uninterruptible Power Supply, Sistema de alimentación interrumpida.

USGP :Universidad San Gregorio de Portoviejo

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Es innegable que los activos de información que se manejan en las empresas son importantes para el desempeño estratégico y, por ende los medios en donde es almacenada dicha información, las personas encargadas de su custodia también juegan un papel relevante para garantizar la integridad, confidencialidad y la disponibilidad de la información.

Innegable también los riesgos que enfrenta la información día a día, ya que en la actualidad es común que las empresas ofrezcan servicios de transacciones económicas a través de cualquier dispositivo con acceso a internet; agreguemos también el hecho de que las amenazas no solo se encuentran fuera de las empresas, sino que en la mayoría de ocasiones los ataques informáticos provienen del interior.

Ante lo expuesto anteriormente, las empresas deben concientizar en la aplicación de políticas, normativas, procedimiento que permitan controlar los diferentes entornos donde se mueven la información, sean estos físicos o lógicos; lo expuesto anteriormente adquiere relevancia cuando sabemos que las universidades ecuatorianas son evaluadas constantemente con modelos rigurosos que exigen la calidad.

La norma ISO 27001 plantea un enfoque completo a la seguridad de la información, mediante procesos sistemáticos, debidamente documentados y socializados a toda la organización, implica por tanto un compromiso de la máxima autoridad y todo el organigrama institucional.

CAPÍTULO 1

GENERALIDADES

1.1. Descripción del Problema

La Universidad San Gregorio de Portoviejo, fue creada el 14 de diciembre del año 2000, ubicada en la avenida Metropolitana y Olímpica, es una institución autofinanciada y su desarrollo institucional se ha basado únicamente en las colegiaturas de las diferentes carreras que oferta. La Universidad está ubicada en la categoría “C” y en la actualidad se encuentra frente al proceso de Recategorización, donde aspira posicionarse en la categoría “B”.

La Universidad cuenta con un Departamento de Informática conformado por un equipo de tres personas y existen cerca de 320 terminales en la institución, en su campus universitario existen 4 edificios, cada uno cuenta con Bunker ubicado en la planta baja.

La entidad no cuenta con políticas formales de Seguridad de la Información lo que conlleva a un riesgo eminente de los equipos físicos y de la información, algunos de los procesos que no disponen de una normativa son: gestión de cuentas de usuarios, asignación de privilegios, administración de usuarios en la red, control de acceso, registro al área de servidores, entre otras.

La institución cuenta con un Data Center equipado con un servidor de datos, servidor de aplicaciones, servidor de archivos, equipos de almacenamiento, algunos no presentan las características de hardware óptimas para brindar un mejor servicio, además el lugar físico donde se encuentra no presenta las condiciones recomendables para un data center.

Los Modelos de Evaluación Institucional de Universidades aplicados por el CEAACES cada vez son más exigentes y tienen gran énfasis en la tecnología, sin duda porque la tecnología es el soporte de almacenamiento de información y de automatización de todos los

procesos académicos y administrativos de la institución y apoyo incondicional para ejes como la Organización, Academia, Investigación y Vinculación con la Sociedad.

Todas las Universidades del Ecuador entraran a un nuevo proceso de evaluación en el año 2017, por tal razón es importante que la Universidad San Gregorio de Portoviejo cuente con controles implementados que garanticen la confidencialidad, integridad y disponibilidad de la información, sin duda el Modelo que utilizará el CEAACES no estará centrado solo en evaluar la existencia de Infraestructura Tecnológica y Software que evidencien la automatización de procesos, sino que la institución cuenten con políticas que garanticen los pilares de la seguridad de la información.

1.2. Solución propuesta

La calidad es dinámica, porque debe ajustarse necesariamente a las exigencia del mercado, y el mercado cualquiera que sea, nunca es estable; esta reflexión es aplicable también a las Instituciones de Educación Superior y más aún cuando en nuestro país todas las universidades se encuentra en constante evaluación, mismas que buscan sin temor a equivocarme la calidad académica.

El presente trabajo consiste en aplicar controles de seguridad a aquellos procesos que comprometan la seguridad de la información y se evidencie la aplicación de políticas como decisión estratégica para brindar servicios de calidad, basados en información confiable e integra.

Los bunker y data center deben disponer de mecanismos de acceso seguro, restringir al acceso solo a personal autorizado, además de un control óptimo de visita.

Administrar de manera segura las cuentas de usuarios al sistema informático de la institución, correo electrónico, cuentas de sesión de docentes y estudiantes.

Las autoridades deben estar comprometidas con la gestión de la seguridad de la información, de tal manera que se asigne el recurso necesario para garantizar la seguridad física y del entorno para el data center.

En la actualidad las instituciones dependen cada día más de la tecnología, redes de datos, aplicaciones informáticas y de la información digital, para lograr sus objetivos y acercarse más a su visión institucional. La aplicación de controles de seguridad de información beneficiara la Universidad San Gregorio de Portoviejo en lo siguiente:

- Tomar decisiones estratégicas por parte de las autoridades en beneficio a la Universidad.

- Normalizar procesos entorno a la seguridad física y lógica de la información, esto conlleva a garantizar la confidencialidad, integridad y disponibilidad de los datos.

- Establecer en los integrantes del departamento informático de la Universidad San Gregorio de Portoviejo precedentes sobre la importancia de evidenciar la aplicación de procesos orientados a garantizar la seguridad de la información.

- Estar preparados para la próxima Evaluación Institucional por parte del CEAACES en cuanto a los indicadores relacionados a la seguridad de la información.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1. Análisis del estado actual de la Universidad San Gregorio de Portoviejo entorno a la seguridad de la información.

La Universidad San Gregorio de Portoviejo cuenta con un Departamento de Informática, encargado de mantener las redes de datos e internet en funcionamiento; el desarrollo de software institucional y procesos que necesitan automatizarse son realizados por una entidad externa. El Departamento no cuenta con políticas de Seguridad de la Información, ni con la aplicación de controles que permitan evidenciar procedimientos para custodiar la información, a lo expuesto anteriormente se le suma la falta de atención e interés de las

autoridades para garantizar la integridad, disponibilidad y confidencialidad de la información.

Es urgente que la Universidad aplique controles de seguridad de información, con el propósito de brindar un servicio de calidad a la comunidad y estar preparados para las futuras evaluación por parte del CEAACES.

2.1.1. Antecedentes Históricos de la Universidad.

La Universidad San Gregorio de Portoviejo, fue creada el 14 de diciembre del año 2000, ubicada en la avenida Metropolitana y Olímpica, en la actualidad cuenta con aproximadamente 3200 estudiantes, 210 docentes y cerca de 200 empleados. La Universidad está ubicada en la categoría “C” y en la actualidad se encuentra frente al proceso de Recategorización, donde aspira posicionarse en la categoría “B”.

Desde el año 2010 las universidades del Ecuador han sido evaluadas por instancia del Gobierno con el único propósito de garantizar la calidad académica y entregar profesionales competentes a la sociedad. La Universidad San Gregorio ha

enfrentado todos los procesos evaluación obteniendo resultados satisfactorios, sin embargo se realizaron recomendaciones por parte del CEAACES, en indicadores relacionados a los sistemas de información y al Departamento Informático.

2.1.2. Orgánico funcional de la Universidad San Gregorio de Portoviejo.

La Universidad San Gregorio de Portoviejo obedece a una Estructura Organizacional, misma que se muestra en la figura (2.1):

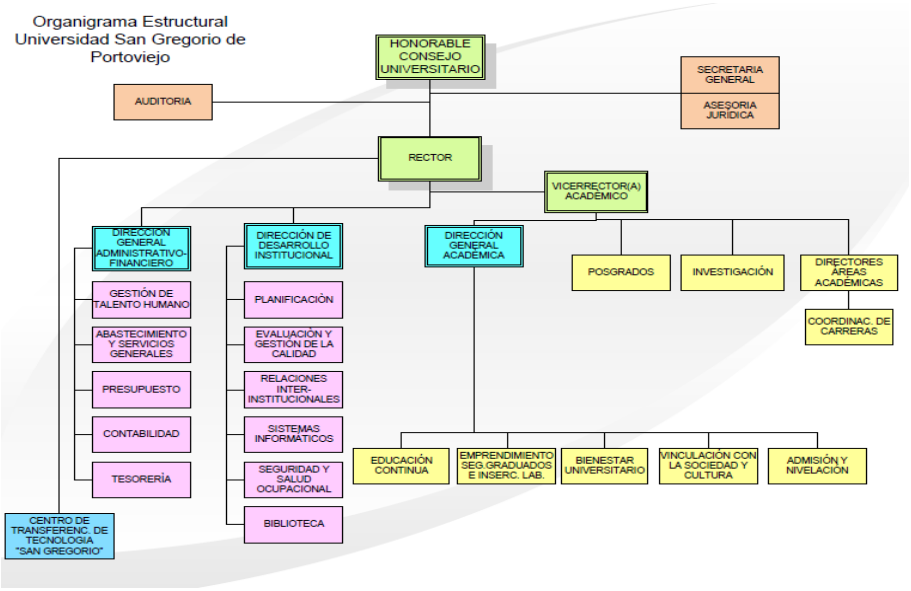

Figura 2. 1. Orgánico Funcional

A continuación se expone una breve descripción funcional de las jefaturas y direcciones donde está inmersa la seguridad de la información:

Secretaría General.- está a cargo una persona quien es responsable de actividades relacionadas a la gestión de trámites para la gradación de estudiantes, matrículas y notas. Esta secretaría dispone de un módulo informático como apoyo para su gestión.

Dirección General Administrativo Financiero.- se encarga de la gestión del recurso económico, para lo cual cuenta con diferentes módulos informáticos como: presupuesto, contabilidad, proveeduría. Bajo esta dirección se encuentra también el departamento de Talento Humano responsable entre otras actividades de mantener actualizada la información de docentes, administrativos y empleados de la universidad, para lo cual cuenta con un software.

Dirección de Desarrollo Institucional.- esta dirección es responsable de crear proyectos y planes de mejoras que permitan mantener a la universidad en constante crecimiento ya sea de infraestructura, aulas y tecnología con el fin de estar siempre listos a brindar un mejor servicio a docentes y

estudiantes. A su cargo están diferentes departamentos que aportan significativamente al logro de los objetivos planteados en los proyectos y planes operativos.

Dirección General Académica.- esta dirección juega un papel muy importante en la universidad ya que se encarga de monitorear los procesos de enseñanza aprendizaje, monitorear el desempeño de docentes y coordinadores, mallas curriculares, rediseños curriculares. Por otro lado la Dirección General Académica está muy involucrada en los procesos de evaluación por parte del CEAACES justamente por el rol relevante en la institución y la academia. Para su apoyo cuenta con módulos informáticos para su correcta gestión y toma de decisiones.

De manera General todas las instancias que conforman el organigrama disponen de módulos informáticos donde reposa la información que permite monitorear y tomar decisiones entorno a sus funciones.

2.2. Establecer los controles de seguridad de la información basado en la norma ISO 27001 en la Universidad San Gregorio de Portoviejo.

Para establecer el alcance del presente trabajo se realizó una entrevista al Jefe del Departamento de Informática quien desempeña esta función desde la creación de la universidad en el año 2001. Esta información fue consolidada con los indicadores del último modelo de evaluación y recategorización de universidades por parte del CEAACES, lo que permitió puntualizar los controles de la Norma ISO 27001:2013 para la aplicación. [1]

A continuación se exponen los controles a utilizar:

Tabla 1 Control, Propósito y fundamento.

Control	Propósito	Fundamento
Gestión de Activos (A8)	Minimizar que las amenazas se materialicen mediante la asignación de activos de información a responsables.	La mayoría de amenazas identificadas en la recolección de información están relacionadas con la manipulación errónea del equipo de tecnologías de la información, tales como: errores de configuración, y ausencia de normativas que garanticen un uso correcto de la información y de los activos.

Control de Acceso (A9)	Minimizar la posibilidad de que usuarios no autorizados tengan acceso a información privilegiada; así mismo equipos como router y switch cuya alteración en su configuración podría causar daños graves a la institución.	Amenazas como: acceso no autorizado, usurpación de identidad, robo de contraseñas, alteración de la información, destrucción de bases de datos, pueden materializarse debido a la ausencia de mecanismos que garanticen que solo los usuarios autorizados tengan acceso a los programas asignados; esto va de la mano con una gestión estricta de normativas debidamente aprobadas.
Seguridad Física y Medio Ambiente (A11)	Evitar el acceso físico no autorizado al área de servidores, así mismo evitar su perdida, daño o robo; además asegurar que existan mecanismos que garanticen un ambiente físico y seguro para los	Otras amenazas que atentan contra los activos y en particular a los ubicados en el área de servidores son: incendios, ingreso físico no autorizado, fallas eléctricas, falta de detectores de humo, ausencia de un biométrico u otro dispositivo para restringir el acceso; todos identificados en el análisis del riesgo. Por tanto se hace necesario referenciar a este control.

	equipos del área de servidores.	
Políticas de Seguridad (A5)	Comprometer a la máxima autoridad en garantizar la seguridad de la información, aprobando y monitoreando políticas, procedimientos y normativas que minimicen a que los riesgos informáticos se consoliden.	De manera implícita para que exista una gestión idónea, estricta y legal en cuanto a la seguridad informática, se debe contar con políticas debidamente documentadas y aprobadas por la máxima autoridad de la institución. A este control se puede asociar la amenaza de falta socialización de políticas de seguridad a todo el personal de la institución, para garantizar la confidencialidad, integridad y disponibilidad de la información.

En este punto es importante puntualizar conceptos que están estrictamente relacionadas con la seguridad de la Información:

2.2.1. Objetivos de la Seguridad de la información.

La información de las instituciones siempre está expuesta a amenazas que pueden poner en riesgos a la información y perjudicar a la entidad, riesgos que puede llevar a pérdidas

económicas o intangibles como la credibilidad e imagen corporativa. Por esta razón hay que tomar medidas para minimizar la probabilidad de pérdida de información, modificación o falsificación, es así que la seguridad informática tiene como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información. [3].

Confidencialidad: “Consiste en la capacidad de garantizar que la información almacenada en el sistema informático o transmitida por la red, solo va estar disponible para aquellas personas autorizadas.”. [2]

Integridad: “Garantizar que los datos no han sido modificados desde su creación sin autorización”. [2]

Disponibilidad: “La capacidad de garantizar que tanto el sistema como los datos van estar disponible al usuario en todo momento”. [2]

2.3. Aplicar los controles de seguridad de la información basados en la norma ISO 27001 en la Universidad San Gregorio de Portoviejo.

2.3.1. Política de seguridad

“Las políticas de seguridad es un documento en donde se plasman los objetivos, procedimiento y responsables para la

aplicación de controles que permitirán minimizar los riesgos a los que está expuesta la información”. [4]

Se levanta la documentación necesaria para establecer las Políticas de Seguridad de la Información, en este se establece el nivel de responsabilidad y compromiso de la máxima autoridad, así mismo se definen los controles que se aplicaran: Seguridad Física y del Entorno, control de Acceso y gestión de activos.

Las políticas deben ser socializadas con todos y cada uno de los docentes y empleados de la universidad, el compromiso de garantizar la calidad de información y su integridad es responsabilidad de todos.

2.3.2. Control de acceso a recursos informáticos.

Cuando hablamos de recursos informáticos nos referimos a todos los recursos físicos y lógicos (hardware y software) necesarios para el manejo de la información y, como sabemos la información es el motor de todas las empresas, y considerada también un activo muy importante para su correcto funcionamiento.

Estos recursos de hardware y software pueden sufrir daños provenientes de fuentes externas e internas de la organización, por ejemplo robo, uso no autorizado, desastres naturales. Por lo tanto deben existir controles, normas o políticas que permitan realizar actividades de prevención, detección y corrección de cualquier problema con los recursos informáticos. Las estadísticas sobre ataque informáticos siempre indican que el mayor porcentaje está asociado con ex empleados y empleados actuales, ya que estos tienen conocimiento de las vulnerabilidades informáticas de la organización.

En este apartado se exponen todos los lineamientos que se deben adoptar para la correcta ejecución de los diferentes procesos donde está involucrada la información, mismos que deben ser socializados con los empleados de la universidad.

2.3.2.1. Gestión de registros de usuarios

Objetivo: establecer procesos claros y aprobados por la autoridad pertinente para que se realice un seguro registro de usuarios a los sistemas

informáticos y correo corporativo para todos los empleados de la universidad.

Política: El departamento informático de la universidad es el responsable de la creación de cuentas de usuarios al sistema informático institucional y correo corporativo.

Lineamientos:

- Garantizar que el responsable de registro de usuario no proceda hasta que el empleado cumpla con los procedimientos de autorización.

- Entregar a los usuarios un documento donde se detalle los derechos de acceso y confidencialidad de la clave, mismo que debe ser firmado y aceptado, indicando que comprenden y aceptan las condiciones de uso.

Responsable: Departamento Informático y Departamento de Talento Humano.

2.3.2.2. Administración de los Privilegios de cuentas de usuarios.

Objetivo.- Establecer límites y controlar la asignación de privilegios de usuarios.

Política: el Departamento Informático es responsable de crear, monitorear y actualizar el inventario de privilegios y categorías de usuarios que tendrán acceso al sistema informático institucional.

Lineamientos:

- Crear perfiles de privilegios de los recursos informáticos e identificar las categorías de empleados para la asignación correspondientes de acceso.
- Asignar los privilegios en base a las funciones del puesto que desempeña el empleado y de acuerdo a un análisis de los recursos que necesita para su rol.
- Los privilegios deben ser asignados hasta que el empleado cumpla con los procesos de autorización.

- Mantener registro de los privilegios asignados a los usuarios.
- Establecer periodos de vigencia de los privilegios.

Responsable.- Jefe del departamento de Informática.

2.3.2.3. Administración de claves de usuarios

Objetivo: Establecer requisitos obligatorios para garantizar contraseñas seguras para el inicio de sesiones.

Política: El departamento Informático debe establecer requisitos para la creación de contraseñas seguras, incluyendo periodos de vigencias.

Lineamientos:

- Garantizar que los usuarios cambien sus claves en el primer ingreso, asi mismo que estas claves provisionales tengan un periodo de vigencia.
- Almacenar las contraseñas en sistemas informáticos protegidos.

- Disponer de un inventario de usuarios registrado.
- Inhabilitar cuentas inactivas por 30 días.
- Establecer requisitos de creación de contraseñas:
    - Las claves deben tener 8 o más caracteres
    - Las claves deben contener por lo menos una mayúscula, número y un carácter especial.
    - Solicitar el cambio de contraseña cada cierto tiempo, por ejemplo 30 días.
    - Impedir que las 12 últimas contraseñas de los usuarios sean reutilizadas.
    - Suspender la cuenta de usuarios después de tres intentos fallidos.

Responsable.- Jefe del departamento de Informática.

2.3.2.4. Cancelación de accesos a los sistemas informáticos.

Objetivo: Desactivar las cuentas de usuarios a aquellos que se separan de la institución.

Política: El departamento informático de la universidad es el responsable de la cancelación de cuentas de usuarios al sistema informático institucional y correo corporativo con autorización del Departamento de Talento Humano.

Lineamiento:

- El Jefe de Talento Humano debe informar al Rector y al Departamento Informático sobre los empleados cuyos contratos finalizaron o en tal caso de aquellos que han renunciado a la universidad, para que se proceda con la cancelación de registro y la anulación de privilegios.

- Si un empleado cambia de rol, el Departamento de Talento Humano debe realizar la respectiva comunicación para que el departamento de Informática proceda a la cancelación de las cuentas, y la creación de otro perfil de usuario y sus privilegios según sea el caso.

- Llevar un control documentado sobre la información relevante de los empleados que entran

en este proceso de desactivación de cuentas, con el propósito de realizar mantenimientos.

Responsable: Departamento Informático Y Departamento de Talento Humano.

2.3.3. Control para la gestión de los activos

La universidad debe disponer de un inventarios de la activos, identificando sus características y usabilidad y valorados de acuerdo a los criterios requeridos por la seguridad de la información. A partir de esta inventario se deben definir los responsable de cada activo, asi como también los niveles de acceso y procedimientos debidamente establecidos para su manipulación; es importante que el inventario y asignación de responsables sea revisado periódicamente.

2.3.3.1. Inventario de Activos

Objetivos.- Disponer de un inventario identificando el activo, con la información pertinente, así como su propietario y ubicación.

Política: El Jefe del Departamento Informático debe crear y mantener actualizado el inventario de activos de información.

Lineamientos:

- Crear el inventario de activos, con su respectiva catalogación
- Realizar revisiones periódicas del inventario.
- Mantener actualizado el inventario de activos.

Responsable: Jefe del Departamento Informático.

2.3.3.2. Clasificación de la información.

Objetivo.- Clasificar a los activos de acuerdo a criterios de la Seguridad de la Información.

Política: La jefatura del Departamento Informático debe disponer de un inventarios de activos de la información y clasificarlos por los criterios de confidencialidad, disponibilidad e integridad.

Lineamientos:

- **Confidencialidad**
    - Información que puede ser conocida por personas dentro de la universidad o fuera. Tipo: Publica

- Información que puede ser conocida solo por los empleados de la universidad y cuya difusión no represente ningún tipo de riesgo para la universidad Tipo: Interna
- Información que puede ser conocida por un grupo de empleados que laboran en la universidad y cuya difusión podría ocasionas pérdidas para la universidad Tipo: Reservada.
- Información que puede ser conocida por un grupo específico de empleados que laboran en la universidad, Tipo: Secreta

- **Integridad**
  - Información que al ser modificada sin autorización puede repararse con facilidad.
  - Información que al ser modificada sin autorización puede repararse, pero sin embargo podría ocasionar pérdidas menores para la institución.
  - Información que al ser modificada sin autorización, resulta compleja su

reparación y podría ocasionar pérdidas significativas para la universidad.

- Información que al ser modificada sin autorización no podría repararse, lo cual ocasionaría graves pérdidas para la universidad.

- **Disponibilidad.**
  - Información que al no ser accesible por ningún empleado de la universidad no afectaría en su función.
  - Información que si durante una semana es inaccesible causaría pérdidas significativas para la universidad.
  - Información que si durante un día es inaccesible causaría pérdidas significativas para la universidad.
  - Información que si durante una hora es inaccesible causaría pérdidas significativas para la universidad.

- Compréndase por perdidas aquellas materiales y lógicas (obligaciones

contractuales, imagen corporativa, valor estratégico, credibilidad)

Responsable: Jefe del Departamento Informático.

2.3.4. Control para la seguridad física de los equipos y su entorno.

La universidad mediante la gestión del Departamento de Informática debe asegurar la integridad de los equipos informáticos, estableciendo normativas el control oportuno para evitar, daños, robos y minimizar las eventualidades suscitadas en caso de desastres naturales.

2.3.4.1. Perímetro de la seguridad de la información.

Objetivo.- Determinar perímetros que deben ser considerados como áreas restringidas ante amenazas externas.

Política: Las autoridades de la universidad deben declarar mediante documento a las consideradas como restringida de personal no autorizada. Además equipar estas áreas con dispositivos para registrar el acceso y proteger el área contra incendios.

Lineamientos

- Establecer áreas de servidores como acceso solo a personal autorizado.
- El personal autorizado debe estar capacitado para manipular los equipos informáticos que reposan en este espacio.
- Instalar cámaras de video dentro de los bunker de la universidad.
- Instalar detectores de humo en los bunker de la universidad
- Instalar extintores de fuego en los bunker de la universidad.
- Proteger los equipos del bunker con UPS.

Responsable: Jefe del Departamento Informático y Jefe Financiero y Administrativo.

2.3.4.2. Gestión del control de visitas a áreas restringidas

Objetivos.- Llevar un control ordenado de visitas a las declaradas como restringidas.

Política: El departamento informático debe crear un formulario con los datos pertinentes para llevar un registro de visitas ordenado.

Lineamientos

- Crear un registro de visitas al área de servidores con los datos pertinentes para su control.
- Las visitar deben ser supervisadas por lo menos por integrante del Departamento de Informático.
- Por ninguna razón los visitantes pueden estar solos en el área de servidores.
- Restringir con firmeza el acceso a personal no autoriza al área de servidores y/o bunkers.

Responsable: Integrantes del Departamento Informático.

CAPÍTULO 3

ANALISIS DE RESULTADOS

3.1. Criterios de evaluación de los controles de seguridad de la información.

Para la evaluación de los controles se establecen los siguientes valores y criterios:

Tabla 2 Registro de usuarios.

VALOR	CRITERIO
0	Se realiza el registro de usuarios sin comunicación del

	departamento de talento humano.
1	Se realiza el registro de usuario con comunicación del departamento de talento humano pero no existe documento firmado por el usuario donde acepta conocer y entender los derechos de acceso.
2	Se realiza el registro de usuario con comunicación del departamento de talento humano y existe documento firmado por el usuario donde acepta conocer y entender los derechos de acceso.

Tabla 3 Lista de usuarios y privilegios

VALOR	CRITERIO
0	No existe un documento o lista donde se identifican a los usuarios con sus privilegios de accesos.
1	Existe una lista donde se identifican a los usuarios con sus privilegios de accesos, pero no corresponden a los asignados en el sistema informático.
2	Existe una lista donde se identifican a los usuarios con sus privilegios de accesos y coinciden a los asignados en el sistema informático.

Tabla 4 Administración para la asignación de privilegios.

VALOR	CRITERIO
0	Los privilegios de acceso son asignados sin disposición del Departamento de talento humano.
1	Los privilegios de acceso son asignados mediante disposición de talento humano, pero no se actualiza el

	documento de confidencialidad del usuario.
2	Los privilegios de acceso son asignados mediante disposición de talento humano y se actualiza el documento de confidencialidad del usuario.

Tabla 5 Administración de claves de usuarios.

VALOR	CRITERIO
0	La creación de contraseñas no exige ningún criterio de claves seguras.
1	La creación de contraseñas solo exige una longitud mayor de 8 caracteres.
2	La creación de contraseñas exige criterios de longitud (8 o más caracteres) y contenido (mayúsculas, minúsculas, números, carácter especial)

Tabla 6 Cancelación de cuentas de usuario.

VALOR	CRITERIO
0	Se cancela el registro de usuarios sin comunicación del departamento de talento humano.
1	Se cancela el registro de usuario con comunicación del departamento de talento humano, pero no se la realizó en la fecha pertinente.
2	Se cancela el registro de usuario con comunicación del departamento de talento humano en la fecha pertinente.

Tabla 7 Inventario de activos.

VALOR	CRITERIO
0	El departamento informático no cuenta con un inventario de activos de información.
1	El departamento informático cuenta con un inventario de activos de información, pero su clasificación no responde a los criterios de confidencialidad, disponibilidad e integridad.
2	El departamento informático cuenta con un inventario de activos de información, debidamente clasificados por los criterios de confidencialidad, disponibilidad e integridad.

Tabla 8 Control de acceso a data center.

VALOR	CRITERIO
0	No existen restricciones para el acceso al data center
1	Solo personal autorizado ingresa al data center, pero no existe un documento o dispositivo físico para llevar un control de los que ingresan al área.
2	Solo personal autorizado ingresa al data center y existen registros de ingresos.

3.2. Resultados de la Evaluación de controles de Seguridad de la Información.

A continuación se muestra una tabla con los valores puntuados de acuerdo a los criterios establecidos para la evaluación de los controles:

Tabla 9 Resultados de evaluación de controles

CONTROLES	VALOR	OBSERVACIÓN
Registro de Usuarios	2	El Departamento informático no procede a la creación de usuarios hasta que tenga la autorización escrita del Departamento de Talento Humano y el usuario firma el documento de confidencialidad.
Lista de Usuarios y Privilegios	1	Existe una lista de usuarios y privilegios, pero al comprobarlos en el sistema no correspondieron a los detallado en el documento.
Asignación de privilegios	1	Los privilegios se actualizan con autorización de talento humano, pero se comprueba que un usuario no cuenta con el documento de confidencialidad actualizado.
Administración de claves de usuarios	2	Las claves de usuarios exigen criterios de claves seguras.
Cancelación de claves de	2	El proceso de cancelación de usuarios se realiza previa autorización escrita por

usuarios		parte del Departamento de Talento Humano.
Inventario de Activos	1	En el inventario de activos no está completo, no se consideran criterios de integridad, confidencialidad y disponibilidad.
Control de ingreso al data center.	1	El acceso al data center es inseguro, todos los integrantes del Departamento tienen llaves; el guardia y proveeduría también tiene copias.

3.3. Análisis de los resultados:

- La aplicación de los controles ha permitido mejorar la gestión de accesos, sin embargo es necesario que se fortalezcan mediante auditoria periódicas y compromiso del jefe del Departamento Informático.

- No se comprobó mejoras en el acceso físico, debido a la falta de inversión económica de la institución, sin embargo es necesario tomar la decisión de fortalecer esta área, ya que los equipos se exponen a diario a amenazas que se pueden materializar y causas perdidas graves a la institución.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. En la actualidad las empresas u organización deben aplicar controles que permitan asegurar la calidad de la información y los medios donde es transmitida y almacenada, afortunadamente existen normativas que contienen directrices que facilitan la implementación de controles de seguridad de la información.

2. La Universidad San Gregorio ha dado un paso importante, brindando la importancia y compromiso para mantener y mejorar los controles de seguridad de la información.

3. La aplicación de los controles planteados ha permitido evidenciar una organización y aplicación de procedimientos para asegurar la confidencialidad, integridad y disponibilidad de la información.

4. La aplicación de estos controles permitirá demostrar ante evaluaciones por parte del CEAACES, que se dispone de controles de seguridad y que son aplicados en la institución con fines de garantizar la seguridad de la información, lo cual aporta sin lugar a dudad la calidad de servicios brindados a los estudiantes y docentes.

RECOMENDACIONES

1. Realizar auditorías internas de la seguridad de la información al departamento informático con el objetivo de incorporar mejoras en los procedimientos y controles implementados.

2. Las autoridades de la universidad deben brindar el apoyo incondicional a la implementación de un Sistema de Gestión de la Seguridad de la Información con el fin de que en el futuro pueda aspirar a una certificación ISO.

3. El Jefe del Departamento Informático, debe mantener comunicada a las autoridades sobre avancen alcanzados y debilidades encontradas, en materia de seguridad de la información.

4. Capacitar periódicamente a los integrantes del Departamento Informático en temas de seguridad de la información especialmente en normas como la ISO 27001.

BIBLIOGRAFÍA

[1] I. S. Organization, Information tecnology - Security Techniques - Information security managment systems, Segunda ed., ISO/IEC 27001:2013, 2013.

[2] S. R. Cesar, Seguridad Informática, Mc Graw Hill/Interamericana., 2010.

[3] C. Álvarez, "La ley y la seguridad de la información una perspectiva regional, " *Sistemas Rastreando la Inseguridad,* vol. 1, no. 101, pp. 12-20, Abril 2007.

[4] G. Alfonso,Seguridad Informática, España, Ediciones Paraninfo, 2011.

[5] K. Astudillo, Hacking Ético 101, Segunda ed., Guayaquil, Guayas: Lexington, 2013, pp. 268-269.