ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE CIENCIAS NATURALES Y MATEMATICAS

DEPARTAMENTO DE MATEMATICAS

"PLANEACIÓN Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 EN UNA UNIDAD ADSCRITA A LA PRESTACIÓN DE SERVICIOS BIBLIOTECARIOS EN UNA UNIVERSIDAD PÚBLICA"

PROYECTO DE GRADUACIÓN
(Dentro de una materia de la malla)

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
"INGENIERO EN AUDITORÍA Y CONTADURÍA PÚBLICA AUTORIZADA"

PRESENTADO POR

VIESHA SOLANGE FRANCO AGUILAR
ALAN STEFANO LUGMANIA MEDINA

GUAYAQUIL - ECUADOR

2014

AGRADECIMIENTO

El presente trabajo es producto del esfuerzo realizado en los últimos meses, le quiero agradecer de manera especial a mi padre y hermanos por su invaluable e incondicional apoyo durante este tiempo.

Así mismo a personas que participaron directa o indirectamente en el desarrollo de este trabajo, gracias por su invaluable ayuda

Finalmente quisiera compartir una frase que me motivó durante la elaboración del presente trabajo: “El barco está más seguro cuando está en el puerto, pero no fue para esto que se construyeron los barcos”

Viesha Solange Franco Aguilar

AGRADECIMIENTO

Mi eterna gratitud a Dios por toda su bondad y misericordia, sin la cual no hubiese sido posible lograr todo lo que he alcanzado, todo cuanto tengo y he hecho es gracias a Dios.

Mi agradecimiento a mis padres, que siempre han sido ejemplo para mí, de quienes he aprendido que ante todo está el amor y la entrega.

Finalmente hago extenso mi agradecimiento a todos los docentes de mi carrera que día a día me guiaron en el camino del saber y que con sus enseñanzas son artífices de este gran logro

Alan Lugmania Medina

DEDICATORIA

A mi papá y hermanos.

A mi mamá, siempre presente.

Viesha Solange Franco Aguilar

DEDICATORIA

Este trabajo lo dedico ante todo a mis padres, que han sido mi inspiración a cada instante de mi vida, con su anegación y entrega han hecho posible que yo pueda seguir en este camino.

Le dedico este trabajo al Ingeniero PR cuya colaboración fue determinante en el desarrollo de este proyecto, a la Ing. SS que día a día me ha arengado para lograr la consecución de esta meta

Especialmente le dedico este trabajo a AG quien siempre ha estado allí y en muchas ocasiones ha sido una pequeña lucecita en medio de la obscuridad

Alan Lugmania Medina

TRIBUNAL DE GRADUACIÓN

MBA Antonio Márquez Bermeo
DIRECTOR DE PROYECTO DE GRADUACIÓN

Ing. Jorge Ugarte Fajardo
DELEGADO

DECLARACION EXPRESA

La responsabilidad del contenido de este proyecto de graduación nos corresponde exclusivamente, y el patrimonio intelectual de la misma a la **“ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL”**.

(Reglamento de graduación de la ESPOL)

Viesha Solange Franco Aguilar

Alan Stéfano Lugmania Medina

RESUMEN

El presente proyecto tiene como objetivo establecer las bases para el diseño de un sistema de gestión de seguridad de la información basado en la ISO/IEC 27001:2008.

El objeto de estudio será un centro de información bibliotecario de una universidad pública en el que se buscará mejorar la eficiencia y seguridad de los servicios que brinda

La información recopilada será analizada según el marco de referencia especificada en la ISO/IEC 27001 y a las impuestas por Alberto Lardent en su libro “Sistemas de Información para la Gestión Empresarial” como herramienta de apoyo. El diseño del sistema de gestión se hará acorde a las directrices especificadas en la ISO/IEC 27001; de esta manera la empresa, en caso de requerirlo, podrá certificarse en la norma.

En este trabajo se hará énfasis en la primera etapa del ciclo de Deming o ciclo PHVA, en la primera etapa “Planear” se detallará la política de seguridad, el alcance del sistema de gestión de seguridad de la información, se analizarán los riesgos y establecerán controles que preserven y aseguren la seguridad de la información proporcionada.

El proyecto se divide en cuatro capítulos, el primero comprende el planteamiento y justificación del estudio, así como los objetivos que se pretenden alcanzar al realizarlo. En el segundo capítulo se encontrará el marco teórico, que incluirá definiciones básicas de los métodos a utilizar para una mejor comprensión del desarrollo del estudio que se pretende realizar. En el tercer capítulo detallaremos la situación actual de la empresa, describiremos los procesos del área de sistemas, el análisis de riesgos y los hallazgos encontrados. El cuarto capítulo incluirá la política de seguridad de la información, esta política comprenderá el alcance y controles a aplicar según los detalla la ISO/IEC 27001.

ÍNDICE GENERAL

RESUMEN ..... **VII**

ÍNDICE GENERAL ..... **IX**

ÍNDICE DE TABLAS ..... **XIII**

ÍNDICE DE FIGURAS ..... **XIV**

CAPÍTULO I **1**

1 PLANTEAMIENTO DEL PROBLEMA **1**

1.1 INTRODUCCIÓN 1

1.2 DEFINICIÓN DEL PROBLEMA 4

1.3 OBJETIVO GENERAL 5

1.4 OBJETIVOS ESPECÍFICOS 5

1.5 JUSTIFICACIÓN DEL PROYECTO 6

1.6 HIPÓTESIS 8

1.7 INFORMACIÓN DE LA EMPRESA 9

1.7.1 Misión *9*

1.7.2 Visión *9*

1.7.3 Objetivos *10*

1.7.4 Valores *10*

1.7.5 Estructura *10*

1.7.6 Organigrama *16*

CAPÍTULO II **17**

2 MARCO TEÓRICO **17**

2.1 SERIE ISO 27000 20

2.2 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001 21

2.3 ISO/IEC 27002 22

2.4 APORTE DE LA ISO 27001 A LA SEGURIDAD DE LA INFORMACIÓN 23

2.4.1 ¿Qué incluye un SGSI? *24*

2.4.2 Ciclo PHVA (Planear-Hacer-Verificar-Actuar) *25*

2.4.3 Etapas para el diseño e implantación de un SGSI (4) *26*

2.4.4 Beneficios de la implantación *29*

2.5 SISTEMAS DE INFORMACIÓN PARA LA GESTIÓN EMPRESARIAL (5) 30

2.5.1 Planificación de la auditoría *30*

2.5.2 Desarrollo de un programa de auditoría: *31*

2.5.3 Preparación de informe de auditoría y de informe a la alta gerencia. *33*

2.5.4 Seguimiento de acciones correctivas *34*

CAPÍTULO III **35**

3 SITUACIÓN ACTUAL DE LA EMPRESA **35**

3.1 IDENTIFICACIÓN DE PROCESOS, ANÁLISIS DE IMPACTO 35

3.2 DESCRIPCIÓN DE LOS PROCESOS DEL ÁREA DE SISTEMAS 38

3.2.1 Desarrollo de sistemas de información *38*

3.2.2 Organización de recursos informáticos *39*

3.2.3 Implementación de sistemas y recursos de información *41*

3.2.4 Control y evaluación de sistemas de información 42

3.3 SITUACIÓN ACTUAL DEL CENTRO DE INFORMACIÓN BIBLIOTECARIO 43

3.3.1 EVALUACIÓN DE LOS OBJETIVOS DE CONTROL 46

A.5 Política de seguridad de la información 46

A.6 Organización de la Seguridad de la Información 47

A.7 Gestión de activos de información 50

A.8 Seguridad de los recursos humanos 55

A.9 Seguridad física y medioambiental 58

A.10 Gestión de operaciones y comunicaciones 61

A.11 Control de acceso 66

A.12 Adquisición, desarrollo y mantenimiento de sistemas de información 69

A.13 Gestión de incidentes de seguridad de información 73

A.14 Gestión de continuidad de operaciones 75

A.15 Cumplimiento regulatorio 76

3.3.2 ANÁLISIS DE RIESGOS 78

CAPÍTULO IV 86

4 DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 86

4.1 PLAN DE IMPLEMENTACIÓN 87

4.2 ALCANCE DEL SGSI 89

4.3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 90

4.3.1 INTRODUCCIÓN 90

4.3.2 OBJETIVOS DE LA POLÍTICA DE SEGURIDAD 91

4.3.3 ALCANCE *93*

4.3.4 RESPONSABILIDAD *93*

4.3.5 SANCIONES POR INCUMPLIMIENTO *94*

4.3.6 CONTROLES A APLICAR SEGÚN ISO 27001 ..... *95*

A.6 Organización de la seguridad de la información 95

A.7 Gestión de activos 104

A.8 Seguridad de los recursos humanos 113

A.9 Seguridad física y ambiental 121

A.10 Gestión de las comunicaciones y operaciones 135

A.11 Control de acceso 152

A.12 Adquisición, desarrollo y mantenimiento de sistemas de información 160

A.13 Gestión de incidentes de seguridad de información 171

A.14 Gestión de continuidad de operaciones 173

A.15 Cumplimiento regulatorio 177

***CAPÍTULO V* 180**

***5 CONCLUSIONES Y RECOMENDACIONES* 180**

5.1 CONCLUSIONES 180

5.2 RECOMENDACIONES 181

***6 ANEXOS* 184**

ÍNDICE DE TABLAS

TABLA 3.1 TABLA DE ESCALA PARA ISO 27001 E ISO 27002 45

TABLA 3.2 CUMPLIMIENTO DE OBJETIVOS DE CONTROL 79

TABLA 3.3 RIESGOS ASOCIADOS A ÁREAS CRÍTICAS 84

ÍNDICE DE FIGURAS

FIGURA 1.1 ESTRUCTURA ORGANIZACIONAL DEL CENTRO DE INFORMACIÓN BIBLIOTECARIO 16

FIGURA 2.1 CICLO DE DEMING ASOCIADO A CLÁUSULAS DE NORMA ISO/IEC 27001 (3) 26

FIGURA 2.2 ETAPAS DEL DISEÑO E IMPLANTACIÓN DEL SGSI 29

FIGURA 3.1 GRÁFICO DE CUMPLIMIENTO DE OBJETIVOS DE CONTROL RESPECTO A CUMPLIMIENTO IDEAL 79

CAPÍTULO I

1 PLANTEAMIENTO DEL PROBLEMA

1.1 Introducción

En la actualidad la información ocupa un papel muy crucial en el desarrollo de todas las organizaciones, sean estas grandes o pequeñas, bien se podría afirmar que actualmente la información que manejan las empresas constituye uno de los activos más importantes dentro de las mismas.

El auge tecnológico, y la constante evolución que se ha dado en el campo de la tecnología, permiten que en la actualidad se maneje de forma ilimitada la información dentro de las organizaciones, por pequeñas que estas sean, logrando compartir estos datos incluso a través de grandes redes. Todo esto ha logrado, en algunos casos, la optimización de gran parte de las operaciones que realizan las empresas.

La trascendencia y la dependencia de la información en las empresas, hace que las organizaciones necesariamente deban caminar de la mano junto al constante desarrollo tecnológico, puesto que éste facilita la disponibilidad, integridad y confidencialidad de la información que manejan.

No obstante; se debe considerar que paralelo al desarrollo de la tecnología y al manejo de la información, la empresa se vuelve vulnerable a los distintos ataques a la información, por eso es necesario que toda empresa considere los riesgos a los que se expone como consecuencia del uso de la información, y busque mitigarlos, tomando medidas preventivas, detectivas y correctivas.

Se ha vuelto una necesidad imperante, para las empresas, buscar los medios necesarios que garanticen la seguridad de la información, sea cual sea el sector económico en que se desenvuelvan las organizaciones. Sin embargo las estrategias para garantizar la seguridad de la información serán distintas de acuerdo a la situación particular de cada empresa.

Estudios internacionales[1] en materia de seguridad de la información señalan que el mayor riesgo asociado a la seguridad de la información es el factor humano, ya sea por errores, o prácticas fraudulentas o negligencia; el desafío es diseñar un sistema de gestión de la seguridad, que sea más efectivo que la adquisición de recursos tecnológicos.

---

[1] Encuesta RSA. División de seguridad de la empresa EMC

El éxito de un sistema de gestión no viene dado por la rigurosidad de controles que se establezcan o las medidas que se tomen para mitigar riesgos, es el control del recurso humano el que garantizará una efectiva gestión de la seguridad de la información.

Las empresas en la actualidad dependen de los sistemas de información, y al ser estos vulnerables es necesario que se diseñe un sistema de gestión de seguridad de la información, razón por la cual se va a proporcionar a la organización un sistema que le permita garantizar la integridad, disponibilidad y confiabilidad de la información, lo cual acarreará a la empresa avanzar hacia la mejora continua en su desarrollo como ente económico.

Se han establecido estándares que ayudan a gestionar la seguridad de la información, siendo de los más conocidos los de la serie ISO/IEC 27000; sin embargo el éxito de todo sistema de gestión lo dicta la adaptación del mismo a la realidad de la empresa. Este estudio lejos de ser impositivo, propondrá una serie de estrategias, que la organización pudiera implementar para gestionar eficientemente la información que se genera.

1.2 Definición del problema

Se puede afirmar que la información de una empresa constituye un punto neurálgico, lo cual hace que sea vulnerable a distintos tipos de ataques; ya sea la alteración, la substracción, o el uso fraudulento de la misma. Las empresas deben estar pendientes, incluso de su ambiente interno, dado que los ataques pueden venir desde el interior de la organización. Un ataque a la información dentro de una empresa puede ser catastrófico; es por esto que se vuelve muy necesario diseñar procedimientos de control, y de no existir, la probabilidad de ocurrencia de un ataque informático se vuelve alta.

La seguridad de la información se debe gestionar es decir, establecer metas medibles y cuantificables, diseñar estrategias, y establecer controles que disminuyan el riesgo residual inherente al manejo de la información. Cabe aclarar que la seguridad de la información no es una propiedad que la empresa adquiere, ni tampoco es un estado que alcanzar, se deben medir los diferentes escenarios en los cuales la organización se desenvuelve.

El presente estudio consiste en diseñar un sistema de gestión de seguridad de la Información en una entidad adscrita dedicada a la prestación de servicios bibliotecarios en una Universidad pública, puesto que el constante desarrollo de

esta entidad ha hecho que los controles y procedimientos que allí se han aplicado no sean suficientes para mitigar el riesgo asociado al manejo de la información.

Cabe recalcar que no tomar medidas de control, puede hacer a la entidad vulnerable a ataques informáticos, o a situaciones que pongan en peligro la integridad de la información que el centro maneja. El presente estudio buscará ser una solución a esta problemática.

1.3 Objetivo general

Diseñar un sistema de gestión de seguridad de la información que permita eliminar y aminorar los riesgos asociados al uso de la información de forma documentada, sistemática, estructurada y eficiente para su posterior implementación.

1.4 Objetivos específicos

- Evaluar los procesos de planificación, organización, administración y control del área de sistemas de la unidad dedicada a la prestación de servicios bibliotecarios.

- Evaluar los recursos informáticos (Hardware, software, firmware, datos) para determinar un uso eficiente de los mismos.

- Revisar los controles preventivos, detectivos y correctivos dentro de cada proceso para identificar su efectividad en el mitigamiento de riesgos.

- Verificar el control interno de todos los procesos existentes en el área de sistemas, para establecer potenciales riesgos y aminorarlos.

1.5 Justificación del proyecto

Con todos los riesgos asociados a la seguridad de la información rondando el entorno del centro bibliotecario objeto del presente estudio, se vuelve necesario el diseño de un Sistema de Gestión de Seguridad de la Información, ya que éste permitirá disminuir las eventualidades que comprometan la integridad y la disponibilidad y eventualidades que vayan contra la confidencialidad de la información que este centro maneja.

Identificar vulnerabilidades en los sistemas de información que actualmente maneja el centro Bibliotecario, permitirá tomar medidas tanto preventivas para

evitar la ocurrencia de eventualidades riesgosas; y medidas correctivas que permitan mitigar el riesgo por eventualidades ya ocurridas.

Un sistema de gestión de seguridad de la información será capaz de mostrar si las necesidades de acceso a la información; disponibilidad, confiabilidad y seguridad de la información; tanto de sus usuarios internos como externos son actualmente satisfechas; y en caso de no serlo se proporcionarán directrices que permitan manejar de forma más eficiente y eficaz la información que aquí se procesa. De ser necesario se propondrá la adquisición de un sistema que se adapte a las necesidades de la empresa, o se evaluará si es necesario desarrollar sistemas que cumplan con las necesidades de la empresa.

Se debe evaluar si los objetivos planteados por la institución se ven satisfechos con el uso del sistema de información que actualmente se maneja. Se destaca que la no disponibilidad de uno de estos sistemas podría generar disconformidad en los procesos del centro bibliotecario y/o se podría comprometer la disponibilidad de la información a la que los usuarios necesitasen acceder.

El auge tecnológico ha generado, de cierta manera, dependencia de las empresas respecto a sus sistemas de información. Las telecomunicaciones y redes han hecho también que el riesgo de las empresas aumente, bien se podría decir que

la información es de los activos más delicados de la empresa y perderla podría generar problemas muy grandes para ésta.

Dada la importancia de la información en las empresas, éstas están tomando los recaudos necesarios para cuidar uno de sus activos más valiosos y delicados a la vez, por lo que diseñar un Sistema de Gestión de Seguridad de la Información, apegado a estándares internacionales será de gran utilidad para el centro bibliotecario, permitiéndole en un futuro acceder a una certificación internacional en seguridad de la información.

Si bien el Estándar ISO/IEC 27001, es base de todos los sistemas de gestión de la seguridad de la información, no es un estándar dogmático e impositivo, pues el éxito de un sistema de gestión viene dado por la capacidad de éste de adaptarse a la realidad de la empresa, a su actividad económica, a su magnitud, al volumen de datos que maneje.

1.6 Hipótesis

El diseño del sistema de gestión de seguridad de la información garantizará la detección de riesgos a la organización y planteará posibles soluciones para la

minimización de éstos, estableciendo controles en los procesos de planificación, organización, administración y control del área de sistemas.

1.7 Información de la empresa

1.7.1 Misión

Ofrecer servicios de accesibilidad y transmisión de información con tecnología de punta, científica e investigativa que satisfaga las necesidades de la comunidad politécnica y del país, como apoyo al desarrollo de la formación integral y liderazgo a la educación.

1.7.2 Visión

Un Sistema Bibliotecario con tecnología moderna de la era digital cuyas colecciones bibliográficas electrónicas - hemerográficas, audio-videográficas y otros servicios de soportes sean un pilar académico en el que se asegure accesibilidad libre e ilimitada a redes internacionales. Planes y programas de intercambio de información entre universidades locales y extranjeras. Recursos de información modernos, que correspondan a la diligencia y a la producción de nuevos conocimientos académicos.

1.7.3 Objetivos

- Desarrollar un ambiente para el aprendizaje y la investigación con alcance internacional, interdisciplinario en la orientación y basado en la información y el conocimiento.
- Contribuir a la formación integral y liderazgo de los estudiantes.

1.7.4 Valores

- Espíritu de Servicio.
- Ética.
- Respeto.
- Calidad.

1.7.5 Estructura

En cuanto a la estructura operativa, el CIB, dispone de un Director General y, bajo su ámbito, tres áreas fundamentales de funcionamiento:

- Área de Recursos Bibliotecarios.
- Área de Recursos Tecnológicos – Informáticos.
- Área de Servicios.

El Director General del CIB es el responsable de su correcto funcionamiento, coordina las labores del personal y el funcionamiento de las áreas que forman este centro y que se describen a continuación.

Área de Recursos Bibliotecarios

Esta área ejerce las siguientes funciones:

- Control de adquisiciones de los recursos bibliotecarios, canje de documentos, donaciones, catalogación, clasificación, indización, resumen y alimentación de las bases de datos del CIB.
- Determinación de los perfiles de usuarios en cooperación con las unidades académicas y con el área de servicios para establecer la demanda de recursos.
- Selección, presupuesto, adquisición e inventariado de todo el material bibliográfico disponible en cualquier formato (libro, revista, multimedia, audiovisuales, etc.).

- Coordinación de la seguridad y custodia de los bienes bibliográficos.
- Gestión global de la Información del CIB.
- Coordinación en la elaboración de catálogos y promoción de servicios de información y difusión.
- Implementación de metodologías informativas y temáticas para los usuarios de la información.
- Contribuir a la búsqueda de relaciones económicas para el desarrollo de la biblioteca.
- Coordinación de la promoción de los servicios de información del CIB.
- Planificar la estrategia global de marketing para ofrecer los servicios de la biblioteca a sus usuarios: asesoría para servicios bibliotecarios, cursos, conferencias, seminarios y talleres.
- Reservación de auditorio para conferencias, laboratorios de Informática para cursos o talleres y salas multifuncionales.
- Llevará a cabo campañas de promoción de los servicios de la biblioteca dentro de la ESPOL.
- Coordinación en la elaboración de catálogos, *brochures* y promoción de servicios de información y difusión.

- Promover las actividades culturales dentro de las unidades bibliotecarias.

Área de Recursos Tecnológicos e Informáticos

Esta área tiene un coordinador y es la base del cambio tecnológico e informático. Comprende las siguientes funciones:

- Establecimiento de la demanda de servicios tecnológicos e informáticos del CIB y las Bibliotecas Seccionales de la universidad pública.
- Coordinación de disponibilidad y confiabilidad de las redes de comunicación, internet, redes locales de equipos de computación, base de datos de gestión administrativa, y sistemas de información bibliotecaria del CIB y Bibliotecas Seccionales de la universidad pública.
- Administración del acceso a las fuentes de información especializadas para la comunidad de la universidad pública. Como es Bibliotecas Virtuales Internacionales, y Base de Datos del Material Bibliográfico Digital.
- Gestionar la implementación de Sistemas de Información y recursos tecnológicos en el CIB y Bibliotecas Seccionales.
- Elaboración y control de la ejecución del plan de mantenimiento preventivo de los equipos tecnológicos del CIB.

- Integración del sistema de información bibliotecario de la universidad pública con otras bibliotecas locales, nacionales e internacionales.
- Evaluar la calidad de los servicios tecnológicos e informáticos para el mejoramiento continuo del CIB y sus Laboratorios. Así mismo para cumplir con los estándares bibliotecarios internacionales.
- Coordinar y planificar los préstamos de los laboratorios de computación del CIB, para los cursos, talleres y demás actividades que realizan las diferentes facultades de la universidad pública.
- Coordinar y controlar los préstamos de equipos informáticos para la comunidad de la universidad pública. (Laptops y Computadores Personales en el Laboratorio).
- Coordinar y ejecutar la digitalización de documentos bibliográficos de edición universidad pública, para incrementar la base de datos digital y repositorio de la institución.

Área de Servicios

Esta área tiene un coordinador y comprende las siguientes funciones:

- Manejo de los procedimientos de circulación, préstamos y devoluciones a través de mecanismos automatizados.

- Provisión de servicios de préstamos interbibliotecarios, reservas y notificación de disponibilidad de recursos.
- Conservación y mantenimiento del patrimonio documental.
- Coordinación de la disponibilidad de salas de consulta, cubículos de trabajo y salas libres de estudio.
- Operar los mecanismos de consulta y de referencia adecuada y automatizada utilizando tecnología de punta.
- Explotación de los recursos tecnológicos mediante la innovación de servicios bibliotecarios utilizando los recursos tecnológicos de punta.
- Elaboración de estadísticas y determinación de tendencias de servicios automatizados orientados al usuario.
- Reservaciones de auditorio, salas multifuncionales, cubículos de estudios y laboratorios de informática para cursos y/o talleres.
- Apoyo al área de recursos Tecnológicos – Informáticos en la implantación de los sistemas de control y seguridad de recursos.
- Suministro de servicios complementarios al usuario como fotocopiado, acceso a redes internacionales de consulta como Internet y uso local de recursos de computación, multimedia y audiovisuales.

1.7.6 Organigrama

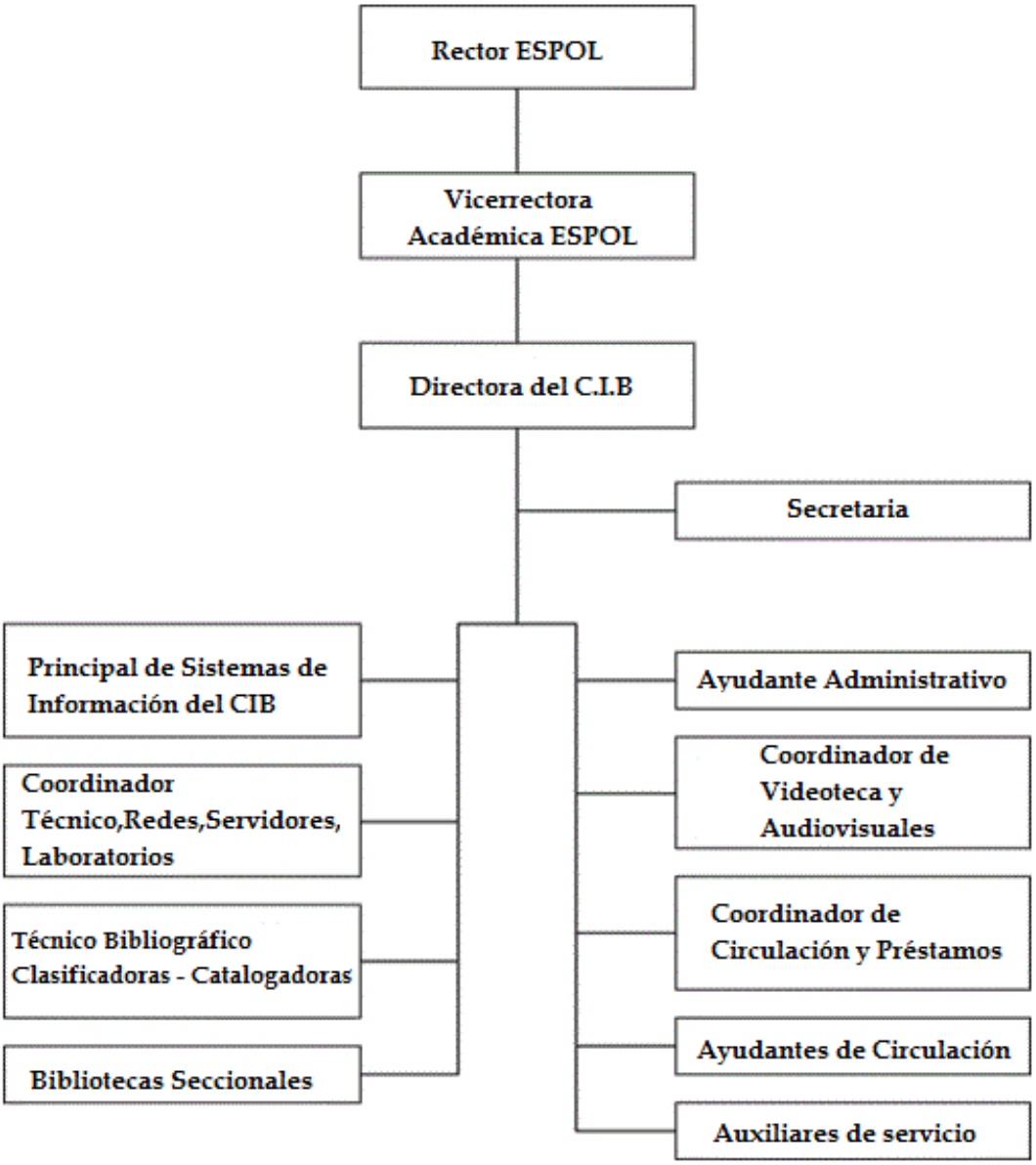

Figura 1.1 Estructura Organizacional del Centro de Información Bibliotecario

CAPÍTULO II

2 MARCO TEÓRICO

Como se mencionó en el capítulo anterior, la información actualmente es el activo más importante de una organización puesto que ayudará en la toma de decisiones para el crecimiento de la empresa; los recursos informáticos de la empresa actúan en conjunto y la seguridad de estos recursos incluidos la información debe ser garantizada, para lograr una toma de decisiones más efectiva.

Para analizar y estudiar los sistemas de información de las empresas existen varios métodos, en este estudio se realizará el enfoque basado en la ISO 27001 como herramienta de apoyo al igual que al método descrito por Alberto Lardent en su libro “Sistemas de Información para la Gestión Empresarial”

Se procederá a ejecutar procedimientos de auditoría basados en Lardent. Y el diseño del sistema de gestión de seguridad de la información se elaborará con el marco de referencia de la normativa ISO/IEC 27001, lo cual le permitirá al centro bibliotecario en un futuro certificarse en esta normativa internacional.

Para hacer este estudio se utilizarán dos tipos de investigación:

Investigación de campo: Se obtendrá información a través de la observación y reuniones con los usuarios de la información aplicando cuestionarios y entrevistas. (6)

Investigación explicativa: Se intentará establecer las causas del objeto de estudio. (6)

Para efectos de comprensión de este trabajo, se deben mencionar y revisar algunos conceptos:

Información: Conjunto de datos organizados para ser procesados con el objetivo de brindar un mensaje para su interpretación.

Seguridad de la Información: Asegura la utilización eficiente de los recursos del sistema y su disponibilidad, integridad y confidencialidad.

Seguridad Informática: Protección de la infraestructura de tecnologías de la información que soporta al negocio

Sistema de Gestión: Proceso continuo definido por etapas con el objetivo de ayudar a la consecución de metas y objetivos establecidos en una organización.

Integridad: Involucra la certeza que la información no ha sido alterada ni manipulada por terceros. La información es completa, clara y precisa.

Disponibilidad: Especifica que el sistema de información es accesible por y para los usuarios cuando estos lo requieran.

Confidencialidad: Establece que la información sólo puede ser leída y manipulada por el usuario autorizado.

Control interno: Medidas adoptadas dentro de una empresa con el fin de salvaguardar sus activos promoviendo la eficiencia operativa.

Control preventivo: Diseñados para evitar que se produzca un error, omisión o acto doloso.

Control correctivo: Corrige errores, omisiones o actos dolosos.

Control detectivo: Detectan errores, omisiones o actos dolosos.

Pruebas de cumplimiento: Determina si un control está funcionando correctamente y eficientemente y se clasifican en pruebas de detalle –revisión de documentos- y en pruebas de indagación y observación –verifica acciones de los usuarios en la gestión de los sistemas de información-.

Pruebas sustantivas: Verifican la adecuación de controles, se encargan de comprobar la integridad de la información.

Riesgo inherente: Es el riesgo propio de la organización que está fuera del control de los auditores y son independientes a los sistemas de control interno que se estén implementando en la organización.

Riesgo de control: Es el riesgo que se genera por fallas en el control interno de la entidad.

Riesgo de detección: Riesgo que se ocasiona por la no detección de la existencia de errores en el proceso realizado.

Riesgo de auditoría: Posibilidad que la información financiera pueda contener errores materiales o que estos errores no hayan sido detectados por los controles de la organización.

La norma ISO/IEC 27001 se enmarcar dentro de una serie de estándares conocidos como la familia ISO 27000

2.1 Serie ISO 27000

La serie ISO 27000 la conforma una serie estándares; entre los cuales están los siguientes:

- ISO 27000 = Gestión de la Seguridad de la Información: Fundamentos y Vocabulario.
- ISO 27001 = Especificaciones para un SGSI.
- ISO 27002 = Código de Buenas Prácticas.

- ISO 27003 = Guía de implantación de un SGSI
- ISO 27004 = Sistema de Métricas e Indicadores
- ISO 27005 = Guía para el Análisis y Gestión del Riesgo
- ISO 27006 = Especificaciones para Organismos Certificadores SGSI
- ISO 27007 = Guía para auditar un SGSI

2.2 Sistema de Gestión de Seguridad de la Información ISO/IEC 27001

La norma ISO/IEC 27001 especifica cómo establecer, implementar, operar, monitorear, revisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información. En este capítulo se expondrá el aporte, los beneficios y los métodos utilizados planear y diseñar este estándar. Al ser esta norma certificable puede ayudar a la organización que desee implantarla alcanzar un sistema de gestión integral basado en normas ISO.

La norma ISO 27001 en su Anexo nos especifica 11 controles que servirán como guía porque no es mandatorio que se cumplan. La ISO 27002 nos da un mayor detalle de los controles que se utilizan.

2.3 ISO/IEC 27002

La ISO 27002 se estructura en 11 secciones o dominios de los que emanan 39 objetivos de control:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos de la Información.
4. Seguridad de los Recursos Humanos.
5. Seguridad Física y Ambiental.
6. Gestión de las Comunicaciones y Operaciones.
7. Control de accesos.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

9. Gestión de Incidentes en la Seguridad de la Información.

10. Gestión de Continuidad del Negocio.

11. Cumplimiento.

Figura 2.1 Dominios de la norma ISO 27001
Fuente: TCP Corp.

Los controles serán analizados con mayor detalle en el capítulo 3 y 4 del presente documento**.**

2.4 Aporte de la ISO 27001 a la Seguridad de la Información

La norma ISO/IEC 27001 proporcionará un modelo que ayudará a la organización a garantizar que los riesgos de la seguridad de la información sean conocidos,

asumidos, gestionados y minimizados de una forma sistemática, documentada, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, entorno y tecnologías (1).

2.4.1 ¿Qué incluye un SGSI?

Según la ISO 27001, un Sistema de Gestión de Seguridad de la Información debe incluir los siguientes documentos (2):

- Alcance del SGSI.
- Política y Objetivos de Seguridad.
- Procedimientos y Mecanismos de Control que soportan al SGSI.
- Enfoque de Evaluación de Riesgos.
- Informe de Evaluación de Riesgos.
- Plan de Tratamiento de Riesgos.
- Procedimientos Documentados.
- Registros.

- Declaración de Aplicabilidad.

2.4.2 Ciclo PHVA (Planear-Hacer-Verificar-Actuar)

En la ISO/IEC 27001 así como en todos los sistemas de gestión calidad el método utilizado como herramienta de análisis y gestión de riesgos es el ciclo de Deming o ciclo PHVA (Planear-Hacer-Verificar-Actuar) de mejora continua, cada una de estas etapas del ciclo está relacionada a cláusulas de la norma.

Planear: Establecimiento del Sistema de Gestión de Seguridad de la Información.

Hacer: Implementación y operación del Sistema de Gestión de Seguridad de la Información.

Verificar: Monitoreo o seguimiento y revisión del Sistema de Gestión de Seguridad de la Información.

Actuar: Mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información.

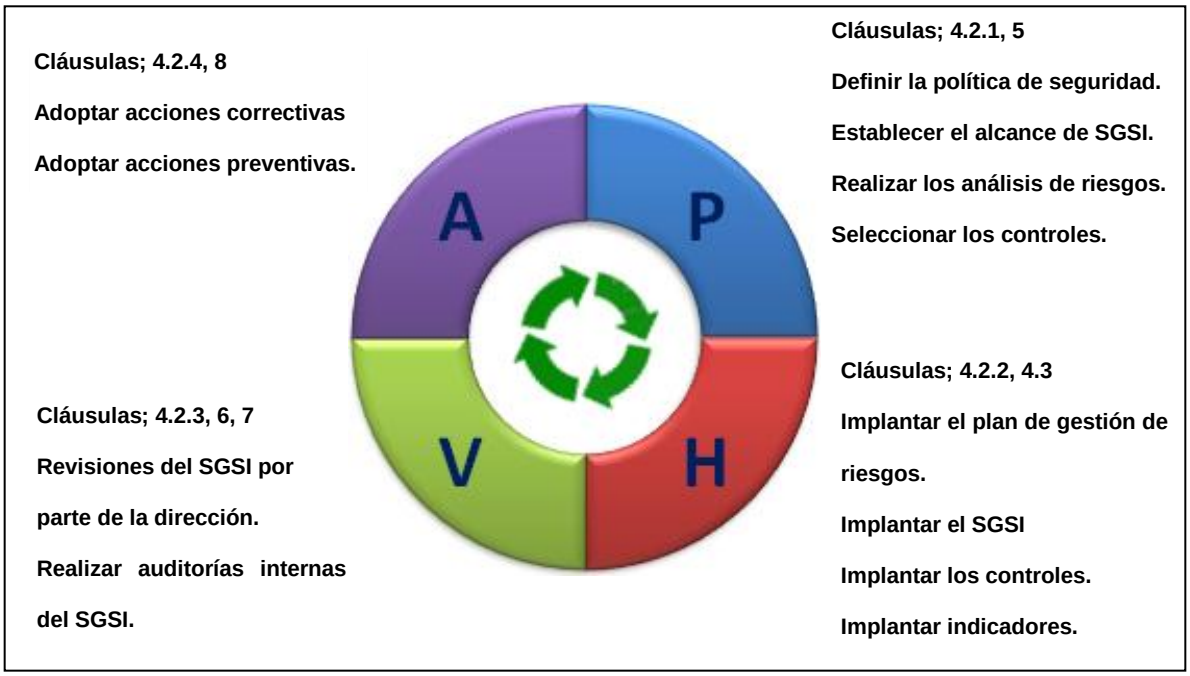

Figura 2.1 Ciclo de Deming asociado a cláusulas de norma ISO/IEC 27001 (3)
Fuente: ISO 27001, adaptación modelo PDCA

2.4.3 Etapas para el diseño e implantación de un SGSI (4)

Para diseñar e implantar un Sistema de Gestión de Seguridad de la Información basado en la ISO/IEC 27001, se deben cumplir etapas (ver figura 2.2) que se explican a continuación:

Política de seguridad: Deberá reflejar lo que la organización busca conseguir con la implementación de esta norma, los objetivos que pretende alcanzar y el compromiso de la dirección junto con los requisitos legales y reglamentarios.

Alcance del SGSI: Para definir el alcance que tendrá el SGSI será necesario definir los servicios o departamentos a los que se pretende auditar, tomando en cuenta que la confiabilidad de la información dará seguridad a nuestros clientes y usuarios.

Análisis de riesgos: Para lograr la eficiencia operativa del SGSI es necesario evaluar los riesgos a los que los sistemas de información estarían expuestos, estableciendo criterios de aceptación del riesgo. La norma no especifica cuál metodología usar, simplemente nos dice que debe permitir abordar un plan de gestión de riesgos ayudando a verificar que los resultados obtenidos sean comparables y repetibles.

Para el análisis de riesgos se debe primero identificar los riesgos, evaluarlos y proponer opciones para el tratamiento de estos.

Gestión de riesgos: Después del análisis de riesgos, la organización debe decidir qué hacer con estos, midiendo el impacto que tienen en la organización. Cada riesgo puede adoptar varias posturas:

1.- Aceptarlo y no tomar acciones

2.- Eliminar la causa

3.- Transferirlo

4.- Reducirlo

Selección de controles: Definido el tratamiento de los riesgos se seleccionan controles para cubrir los requisitos de seguridad. Estos controles se pueden elegir del Anexo A de la norma ISO 27001 que contiene 133 controles de seguridad y de otros que complementen los controles ya seleccionados.

Declaración de aplicabilidad e implantación: La selección de controles se plasma en un documento llamado “Declaración de Aplicabilidad”, este documento reúne las justificaciones del por qué la selección o exclusión de cada control. Este documento deberá siempre estar disponible para los auditores externos certificadores del sistema.

Revisión y Mejora continua: La revisión del SGSI debe realizarse de manera regular buscando siempre el cumplimiento de la política de seguridad y la mejora continua de este.

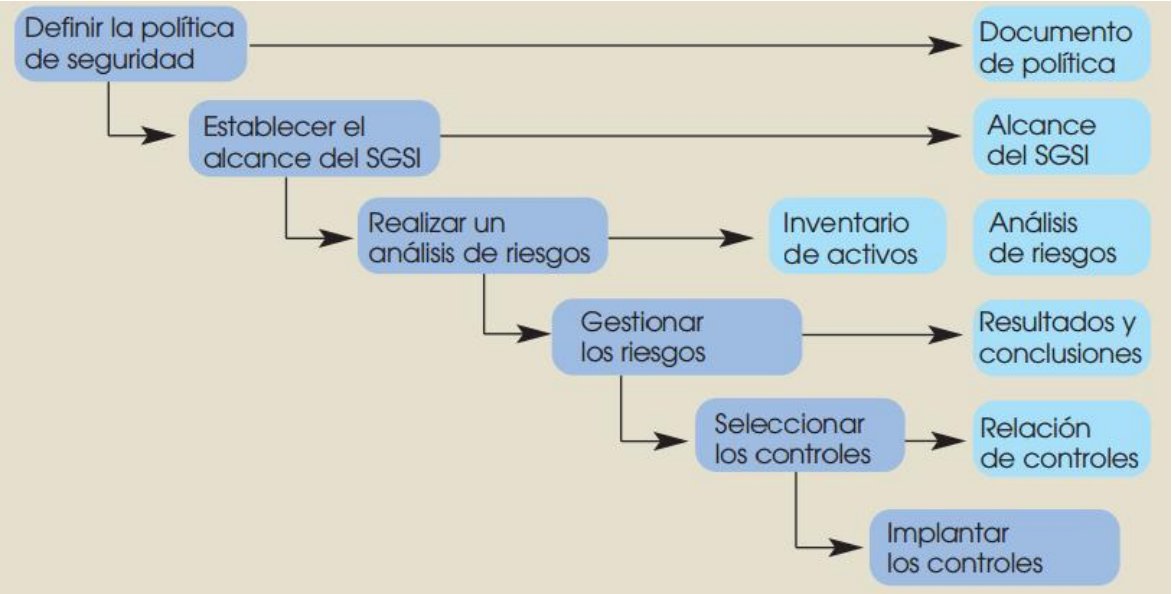

Figura 2.2 Etapas del diseño e implantación del SGSI
Fuente: Asociación Española para la Calidad

2.4.4 Beneficios de la implantación

- Disminuye los riesgos que impiden asegurar la integridad, confiabilidad y disponibilidad de la información.

- Mejora la imagen corporativa incrementando los niveles de confianza con usuarios de la información.

- Minimiza el riesgo de las vulnerabilidades a las que está expuesta la información.

- Ayuda a la gestión de la información en las empresas para una correcta toma de decisiones.

2.5 Sistemas de Información para la Gestión Empresarial (5)

Para la ejecución de una auditoría de sistemas de información Alberto Lardent establece los siguientes pasos[2]:

2.5.1 Planificación de la auditoría

Uno de los pilares para la planificación de una auditoría es conocer los objetivos de la auditoría a realizarse. El marco dentro del cual se debe planificar la auditoría debe abarcar controles operativos y administrativos del área a auditar.

Entre los aspectos que se deben considerar en la planificación constan:

- *Conocimiento del negocio:* Se debe saber qué se va a revisar, el entorno y antecedentes de la organización, el ambiente normativo y toda la información relacionada con el procesamiento electrónico de datos.

---

[2] Alberto Lardent. Sistemas de Información para la Gestión Empresarial. Prentice Hall 2001

- *Evidencia de auditoría y auditabilidad:* Es importante contar con fuentes verificables y auditables para poder determinar si los sistemas de información están operando correctamente.

- *Evaluación de riesgos globales:* El riesgo global de auditoría es el riesgo incluido en todo proceso de auditoría que involucra tres tipos de riesgos: riesgo inherente, riesgo de control y riesgo de detección. El objetivo de la auditoría es minimizar este riesgo.

2.5.2 Desarrollo de un programa de auditoría:

Previo a la ejecución de la auditoría se deberá desarrollar el programa que nos indicará los pasos a realizar hasta la presentación del informe, se deberá tener en cuenta el enfoque, las áreas a auditar, la metodología a utilizar, etc.

- *Objetivos de control:* Una vez desarrollado el programa se deberán establecer los objetivos del control que es el resultado que planeado a alcanzar implementando procedimientos de control específico.

- *Procedimientos de auditoría:* Simultáneamente con la definición de los objetivos de control se debe establecer cuáles son los procedimientos de

auditoría a seguir. Por ejemplo, procedimientos para acceso lógico y físico a datos y programas, aplicación de metodologías para el desarrollo del sistema, control de calidad para procesamiento de datos.

- *Revisión de evidencias:* Evidencia es el conjunto de información reunida que servirá al auditor para la determinación del cumplimiento de los objetivos de la auditoría, la evidencia debe reunir condiciones de calidad -competente, válida y relevante- y cantidad -suficiente-.

Cuando la evidencia viene de fuentes externas se la considera más confiable que la suministrada por la organización; la evidencia objetiva será preferible a la que exige un juicio de valor; la calidad de la evidencia dependerá de la confiabilidad de quien provee la información.

Se puede recopilar evidencia revisando estructuras organizacionales -segregación de funciones-, revisando documentos de los sistemas de información y aplicando técnicas de muestreo.

- *Evaluación de fortalezas y debilidades de control:* Una vez reunida la evidencia necesaria se evaluará el control definiendo sus fortalezas y debilidades para determinar soluciones a los problemas de la organización.

Para la determinación de las debilidades puede utilizarse una planilla que constituya una matriz de control, en la que se registre, sobre el eje vertical, los errores que puedan presentarse y, sobre el horizontal, los controles a través de los cuales se pueden detectar o corregir esos errores.

2.5.3 Preparación de informe de auditoría y de informe a la alta gerencia.

El informe de auditoría constituye el producto final del trabajo del auditor; luego de la revisión, el auditor debe decidir cuáles de las evidencias detectadas incorporará en su informe de auditoría evaluando el grado de materialidad.

El informe de auditoría podrá ser sin salvedades, con salvedades, con opinión adversa y sin opinión.

a. *Informe sin salvedades:* No se encontraron problemas materiales.

b. *Informe con salvedades:* Se encuentran problemas con importancia relativa que significan un riesgo para el resguardo patrimonial de la empresa.

c. *Informe con opinión adversa:* Se detecta debilidades significativas en los procedimientos de control.

d. Informe sin opinión: Se emite en los casos que la auditoría es limitada.

El informe de auditoría debe incluir los siguientes conceptos:

- Introducción.
- Descripción de hallazgos y formulación de recomendaciones.
- Detalle de acciones correctivas a desarrollar.
- Expresión de la opinión del auditor sobre la situación encontrada.
- .Anexos

2.5.4 Seguimiento de acciones correctivas

Evaluado el riesgo y presentado el informe, se buscará establecer acciones correctivas y se hará el respectivo seguimiento en busca de la mejora continua en la organización.

CAPÍTULO III

3 SITUACIÓN ACTUAL DE LA EMPRESA

3.1 Identificación de procesos, análisis de impacto

Una vez analizada la problemática y de comprobar la necesidad de diseñar un sistema de gestión de seguridad de la información en un centro de información Bibliotecario en una Universidad pública, se debe proceder a evaluar la situación actual del centro objeto de estudio.

El marco de referencia es la normativa internacional ISO/IEC 27001:2008, esta normativa, como previamente se puntualizó, no ofrece una metodología de revisión, por lo cual para poder evaluar la situación de la organización se procederá a evaluar el control interno de cada uno de los procesos dentro del área de sistemas del centro Bibliotecario.

Se procederá a evaluar los procesos, los recursos informáticos, las políticas y procedimientos establecidos, con lo cual se podrá determinar los factores de riesgo y las posibles vulnerabilidades del centro, también se evaluarán los controles detectivos, preventivos y correctivos que se aplican.

La normativa ISO/IEC ofrece un grupo de 133 objetivos y grupos de control que se deben aplicar para garantizar la seguridad de la información, estos 133 controles están establecidos de manera muy general y no obligatoriamente los 133 controles serán aplicables a la realidad del centro Bibliotecario, se realizará una evaluación de los controles aplicables al área de sistemas y en base a esto se determinará en la actualidad si dichos controles garantizan los principios de integridad, confidencialidad y disponibilidad.

Los objetivos de control y controles están divididos en los siguientes aspectos, los cuales deberán ser tomados en cuenta para poder garantizar la seguridad de la información:

- Política de Seguridad de la Información.
- Organización de la Seguridad de la Información.
- Gestión de activos de información.
- Seguridad de los recursos humanos.
- Seguridad física y medioambiental.
- Gestión de operaciones y comunicaciones.

- Control de acceso.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Gestión de incidentes de seguridad de la información.
- Gestión de continuidad de operaciones.
- Cumplimiento regulatorio.

Los procesos objeto de la evaluación, es decir los procesos del área de sistemas del centro Bibliotecario son los siguientes:

- Desarrollo de sistemas de Información.
- Organización de Recursos informáticos.
- Implementación de sistemas de Información.
- Control y evaluación de los sistemas de Información.

3.2 Descripción de los procesos del área de Sistemas

3.2.1 Desarrollo de sistemas de información

Este proceso del área de sistemas del centro Bibliotecario se encarga, en base a las necesidades de los usuarios tanto internos como externos, de determinar cuáles son las necesidades de activos de la información que tiene la organización; sean estas necesidades de software o de hardware, este proceso determina si es necesario adquirir software o si éste puede ser desarrollado para suplir con las necesidades de gestión de la seguridad de la información. Estas necesidades se evalúan en base al establecimiento de metas y objetivos que el centro ha establecido

Las tareas que se cumplen dentro de este proceso son:

- Establecimiento de la demanda de servicios tecnológicos e informáticos del CIB y las Bibliotecas Seccionales de la Universidad.

- Gestionar la implementación de Sistemas de Información y recursos tecnológicos en el CIB y Bibliotecas Seccionales.

- Coordinar y ejecutar la digitalización de documentos bibliográficos de edición ESPOL, para incrementar la base de datos digital y repositorio de la institución.

- Gestionar las necesidades de adquisición tanto de hardware como de software del centro de Información.

Actualmente el centro de información bibliotecario se encuentra en una fase de desarrollo de sistemas de información, se está desarrollando un módulo en línea que permitirá la gestión de préstamos interbibliotecarios con otras instituciones de educación superior del país, este desarrollo se está llevando a cabo con normalidad, aunque la rotación de personas que desarrollan el sistema no permite un avance acelerado del proceso.

3.2.2 Organización de recursos informáticos

Este proceso se encarga de gestionar de manera correcta todos los recursos de los que dispone el centro, este proceso toma vital importancia debido a que en la medida que el manejo de recursos esté debidamente organizado se garantizará a mediano y largo plazo un cumplimiento de las metas y de los objetivos establecidos, además que se logrará la satisfacción de todos los usuarios dentro del centro bibliotecario.

Aquí se deben destacar que los recursos del centro lo constituyen:

- Software para desarrollo.
- Software utilitarios laboratorios.
- Sistema de información bibliotecario.
- Hardware laboratorios.
- Hardware área de desarrollo.
- Servidores.
- Terminales de consulta.

Las principales funciones que este proceso desarrolla son:

- Administración del acceso a las fuentes de información especializadas para la comunidad universitaria, como son las Bibliotecas Virtuales Internacionales, y Base de Datos del Material Bibliográfico Digital.
- Coordinar y planificar los préstamos de los laboratorios de computación del CIB, para los cursos, talleres y demás actividades que realizan las diferentes facultades de la institución.

- Coordinar y controlar los préstamos de equipos informáticos para la comunidad universitaria.

3.2.3 Implementación de sistemas y recursos de información

Una vez que se ha planeado y se ha gestionado un correcto uso de los recursos en el área de sistemas del centro bibliotecarios, la implementación se encarga de ejecutar todo lo planificado previamente, se encarga de que los sistemas que se requerían sean aplicados correctamente y que a su vez garantice satisfacción de parte de todos los usuarios tanto internos como externos.

Las funciones que se llevan a cabo dentro de este proceso son:

- Coordinación de disponibilidad y confiabilidad de las redes de comunicación, internet, redes locales de equipos de computación, base de datos de gestión administrativa, y sistemas de información bibliotecaria del CIB y Bibliotecas Seccionales.

- Integración del sistema de información bibliotecario de la ESPOL con otras bibliotecas locales, nacionales e internacionales.

- Manejo de los procedimientos de circulación, préstamos y devoluciones a través de mecanismos automatizados.

- Provisión de servicios de préstamo interbibliotecarios, reservas y notificación de disponibilidad de recursos.

3.2.4 Control y evaluación de sistemas de información

Este proceso se encarga de evaluar que los sistemas funcionen correctamente y los recursos estén siendo utilizados correctamente, para este proceso es imprescindible la presentación de procesos de controles preventivos y detectivos que van a permitir saber cuáles son los potenciales riesgos asociados a la información.

Las tareas que se llevan a cabo dentro de este proceso son:

- Provisión de servicios de préstamo interbibliotecarios, reservas y notificación de disponibilidad de recursos.

- Evaluar la calidad de los servicios tecnológicos e informáticos para el mejoramiento continuo del CIB y sus Laboratorios. Así mismo para cumplir con los estándares bibliotecarios internacionales.

- Implantación de sistemas de control y de seguridad de los recursos informáticos.

3.3 Situación actual del centro de información Bibliotecario

Una vez definidos los procesos y las tareas dentro del área de sistemas del centro de información Bibliotecario, se procede a evaluar los objetivos de control y los controles que la normativa ISO 27001 establece, como se indicó anteriormente el estándar Internacional contempla la aplicación de 133 controles divididos en 11 grupos acorde a la realidad de la organización que se somete a estudio.

Se detallará a continuación cuales fueron los hallazgos para cada área en base a la aplicación de cuestionarios, entrevistas, levantamientos de información, interacción con cada uno de los sistemas de información del centro y de controles sobre las funciones de cada uno de los objetivos de control. Primero se señalará cuáles de los controles que la normativa establece, no son aplicables a la realidad de la entidad adscrita objeto del presente estudio.

La escala con la que se ha procedido a evaluar el cumplimiento de cada uno de los objetivos de control es la siguiente:

Tabla de Escala para ISO27001 e ISO27002		
Escala	**%**	**Descripción**
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Definido	60	Los procesos y los controles se documentan y se comunican. Es poco probable la detección de desviaciones.

Tabla de Escala para ISO27001 e ISO27002		
Escala	**%**	**Descripción**
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Tabla 3.1 Tabla de Escala para ISO 27001 e ISO 27002

Para realizar una correcta evaluación de controles se han aplicado cuestionarios de auditoría que abarcan los procesos del centro de cómputo, basados en estos cuestionarios y en pruebas de control se elaborará el diagnóstico de cuál es el porcentaje de seguridad del centro de cómputo del Centro bibliotecario. Se estudiará si el control se cumple, y su ocurrencia e impacto dentro de los procesos, una vez aplicados estos cuestionarios, se procederá a evaluar los controles que la normativa propone en la escala previamente señalada y esto va a permitir determinar el porcentaje de cumplimiento de cada objetivo de control, y se podrá identificar los respectivos riesgos y proponer mejoras que garanticen una eficiente gestión de la seguridad de la información.

3.3.1 EVALUACIÓN DE LOS OBJETIVOS DE CONTROL

A.5 Política de seguridad de la información

El objetivo de esta serie de controles es dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requisitos institucionales, leyes y reglamentos pertinentes.

Este objetivo contempla la existencia de manuales, políticas y de que todos los usuarios afines tengan conocimiento del mismo, se evalúan dos controles que se mencionan con sus respectivos hallazgos.

1. Que la entidad disponga de una política de seguridad aprobada por la dirección, publicada y comunicada a todos los empleados y partes externas pertinentes

   No hay evidencia que muestre que la entidad posee una política de seguridad de la información propia. La biblioteca cuenta con políticas de manejos de los recursos, de uso y gestión de activos; sin embargo, no tiene establecida una política de seguridad de la información, la política con la que actualmente se rige es la política de la institución pública de educación superior, se diseñará la respectiva política de seguridad de la información

2. La política se revisa a intervalos planificados, y si ocurren cambios significativos se asegura su conveniencia, adecuación y eficacia continua

   Actualmente, el departamento de calidad del centro de información bibliotecario se encuentra en la elaboración de políticas de seguridad de la información y de manuales de procedimientos, pero dado que no se registran revisiones previas no se puede establecer conveniencia y analizar si esto contribuye a la mejora continua.

Se concluye que el objetivo de política de la seguridad de la información no se cumple; sin embargo, el centro de información bibliotecario es consciente de la necesidad de adoptar una política de seguridad de la información.

A.6 Organización de la Seguridad de la Información

Con este grupo de 11 controles se busca gestionar la organización de la seguridad de información a continuación se detallan estos controles y los respectivos hallazgos en base a los levantamientos de información y cuestionarios aplicados al personal del área de sistemas, este objetivo de control divide la organización interna de la organización externa.

- La alta dirección apoya activamente la seguridad de la información en la Institución.

- En las actividades de Seguridad de la Información participan representantes de todas las unidades. Tienen roles y funciones.

- Los roles y responsabilidades en seguridad de la información están bien definidos.

- Está establecido el proceso de autorización para nuevos activos de información.

- Están definidos acuerdos de confidencialidad y se revisa con regularidad.

- Se mantiene contacto apropiado con las autoridades pertinentes

- Se mantiene contactos apropiados con entidades especializadas en seguridad de la Información.

- El enfoque de la organización para gestionar la seguridad de la Información se revisa de manera independiente y periódica.

Todos estos controles van encaminados a lograr una adecuada organización del centro Bibliotecario, se ha evidenciado que la alta dirección si apoya los procesos de seguridad de la Información; más, sin embargo, no hay una dirección orientada a la mejora continua y no se muestra evidencia de que se hayan establecido metas a mediano plazo respecto a la seguridad de la información.

Si bien el centro Bibliotecario dispone de manuales de procedimientos y de descripción de funciones lo que se pudo notar es que éstas funciones no se llevan a cabo conforme lo indicado en el manual, se destaca que el área de desarrollo y sus tareas si se encuentra debidamente segregadas.

Las funciones están correctamente definidas, pero dado que en el último período ha habido necesidades de personal en otras áreas del centro no se ha podido segregar correctamente las funciones en el centro, cabe recalcar que el área de calidad se encuentra también en la elaboración de nuevos manuales de procedimientos y descripción de funciones.

Los controles de organización de seguridad de la información respecto a las entidades externas no aplican a la realidad del centro de Información Bibliotecario, dado que este centro solo maneja relaciones con entidades dentro de la misma universidad y con estudiantes de la misma. Todo lo

referente a compras, proveeduría, pagaduría se gestiona por medio de otras entidades adscritas con lo cual, el centro de momento no tiene relaciones con entidades externas, por lo cual los controles de este objetivo no aplican para la evaluación de los objetivos de control.

De manera general existe una organización de la seguridad de la información, la entidad ha reconocido la necesidad de segregar funciones y de describir cada función; pero esta segregación no se lleva a cabo completamente, además no se encontró evidencia de que previamente la organización de la seguridad de la información haya sido objeto de auditorías independientes que verifiquen su correcta gestión.

A.7 Gestión de activos de información

Este grupo de controles pretende lograr y mantener la protección apropiada de los activos de información, y se aplican 5 controles que buscan determinar el grado de responsabilidad por los activos y la manera en que la entidad clasifica la información que maneja, para así poder garantizar los principios de seguridad de la información, así como la correcta gestión de los activos.

Como activos de la información se entiende no sólo computadoras sino también software, redes, firmwares, y demás recursos que tomen acción en la gestión de la seguridad de la información. Se procede a detallar los 5 controles objeto de evaluación y las respectivas observaciones respecto a la implementación de cada uno de ellos:

1. Se mantiene un inventario de activos de la información

   El centro ha identificado correctamente un inventario de activos informáticos, se puede conocer a que área están asociados, el tiempo de cada uno de éstos y se han tomado ciertas características de cada uno de estos activos de la información, es decir hay una intención por parte de la organización de gestionar adecuadamente cada uno de estos activos.

   Las especificaciones que el inventario proporciona permite conocer el estado actual, la ubicación, la marca del activo. Este inventario se lo maneja en una hoja electrónica y está bajo la custodia de la directora del centro de información, nadie más tiene acceso a este.

Uno de los problemas con el detalle que se maneja es que los datos no incluyen el custodio del activo y datos como: marca, memoria RAM, procesador, etc.

2. Todo activo de la información tiene asignado un responsable

Se halló que todos los activos de la información tienen asignado un responsable, que es la directora del centro de información bibliotecario, es decir ella está a cargo de todos los activos de la información.

Esto no resulta del todo conveniente ya que la directora del centro tiene otras funciones establecidas y hacerse cargo de los activos es una tarea que requiere mucho tiempo, el que se asigne como responsable de los activos debería preocuparse que todos los activos informáticos están en un correcto funcionamiento, y de no estarlo advertir cuáles serían los procedimientos de mantenimiento o reemplazo de los mismos.

Esto evidencia que hay una centralización de funciones, lo cual no es conveniente para una correcta gestión de los recursos informáticos y humanos del centro, la directora del centro no debería ser la custodio de todos los activos, éstos deberían ser asignados a cada persona que

directamente opere con éstos activos, o el inmediato funcionario que los tenga a cargo.

3. Se dispone de una normativa de uso de los activos de la Información

   La entidad sí cuenta con una normativa que regula el uso de cada uno de los activos de la información, tanto para los usuarios internos como los externos, esta normativa abarca el uso de los laboratorios, de las videotecas, el préstamo de computadoras portátiles, incluso se regula el acceso a determinados sitios web que la entidad ha marcado como prohibidos.

   Se establecen procesos que controlan el uso indebido de los activos; sin embargo no existe evidencia del monitoreo y seguimiento que se le dan a estos controles.

4. La información está clasificada según su valor, requisitos legales, sensibilidad y criticidad

   La información no se encuentra clasificada bajo ninguno de estos parámetros.

5. Se dispone del procedimiento de rotulado y manejo de la información

Se encontró evidencia que para la accesibilidad de la información la entidad cuenta con tres niveles de acceso de la información: acceso para estudiantes, acceso para docentes y acceso para el personal de sistemas. Dependiendo de los permisos que se den a cada usuario éstos estarán facultados para crear, modificar y actualizar, es necesario destacar por ejemplo que un estudiante no debería tener accesos a actualizar una base de datos, o a modificar registros ya existentes y pudimos verificar que estos accesos a funciones de alteración, eliminación y actualización si se cumplen debidamente existen controles de autentificación bien definidos para restringir los accesos; no obstante no se han actualizado estos controles, y la estructura del centro sí ha sufrido cambios.

La gestión de los activos de la información se lleva a cabo dentro de la entidad objeto de estudio; muchos de estos procedimientos de control no se llevan a cabo orientados a la mejora continua sino solo al cumplimiento. Además muchos de estos controles no se encuentran actualizados a la funcionalidad del centro de información bibliotecario, si bien se pudo

identificar niveles de acceso de información, esto no brinda seguridad razonable de una correcta gestión de la información.

A.8 Seguridad de los recursos humanos

El objetivo de éste grupo de controles es asegurar que todo el personal involucrado entienda sus responsabilidades, sean apropiados para sus roles y así reducir el riesgo de robo, fraude o mal uso de los activos de información, para ello se han establecido 9 controles que permitirán evaluar cómo se gestiona el recurso humano para la consecución de una buena gestión de la seguridad de la información.

La mayoría de riesgos asociados a la información vienen dados por factores humanos ya sean de omisión, negligencia o errores que derivan en fraudes, a continuación se detallan los controles a evaluar y su repercusión en la gestión de la seguridad de la información

- Se tiene documentado los roles y responsabilidades de seguridad de la información de todo el personal.

- Se verifica antecedentes de todo candidato a empleado.

- Se firman contratos donde se incluye las responsabilidades de seguridad de la información.

El centro lleva un somero proceso de selección de personal basado principalmente en convocatorias abiertas a los estudiantes, se presentan una serie de requisitos para las funciones del área de cómputo, y se lleva a cabo un proceso de selección basándose en el cumplimiento de los requisitos que el puesto en concurso exige. No hay evidencia de que estos controles se monitorean constantemente.

Al momento de firmar contratos se resumen cada una de las funciones que la persona desempeñará y se le realiza la respectiva inducción para cada una de sus funciones.

- Se procura que todos los empleados apliquen la seguridad de la información.

- Se sensibiliza, capacita y educa en seguridad de la información pertinente a su función de trabajo.

- Se tiene establecido un proceso disciplinario ante el incumplimiento de seguridad de la información.

Durante el empleo la entidad tiene establecidos controles que garantizan la seguridad del personal, se busca que todos los empleados conozcan la política; sin embargo no todos la manejan, constantemente se busca la capacitación del personal en los aspectos inherentes a seguridad de la información; no obstante estas capacitaciones se tramitan a través de otra entidad adscrita de la Universidad, como centro Bibliotecario la unidad no maneja el tema de capacitaciones.

Como unidad adscrita a una institución educativa las políticas disciplinarias del centro de información bibliotecario son las mismas que de manera general maneja la universidad; no obstante se considera necesario que el centro debe administrar sus propias políticas disciplinarias para garantizar que tanto los recursos y como tal la información sean gestionados de manera segura y adecuada.

- Están definidas las responsabilidades para el término o cambio de empleo.

- Se procura la entrega de activos al término del contrato.

- Se retira los derechos de acceso al término del contrato.

En caso de una eventual terminación de contrato o cese de funciones la entidad tiene establecidos procedimientos para salvaguardar su información; los acceso son denegados por ende usuarios sin autorización no podrían acceder al sistema de información, paralelo a esto todos los activos a los que el usuario tenía acceso son devueltos; sin embargo no existe evidencia que éstas entregas sean debidamente documentadas.

La gestión de los recursos humanos está contemplada en los procedimientos del centro bibliotecario, mas no se encontró evidencia de que estos controles estén correctamente documentados o que den seguridad razonable de la correcta gestión del recurso humano, son controles que claramente pueden ser optimizados y en algunos casos rediseñados para garantizar que el recurso humano dentro del centro contribuya a la adecuada gestión de la seguridad.

A.9 Seguridad física y medioambiental

Prevenir el acceso físico no autorizado, daño e interferencia en las instalaciones y activos de la información es el objetivo de este grupo de 13 controles, de manera general se controlan las instalaciones, la infraestructura y la seguridad de todos

los activos informáticos, desde las ubicaciones de los mismos se llega incluso a medir la preparación del centro frente a eventualidades externas que pueden generar riesgos en la seguridad de la información.

Los controles que se enuncian a continuación contemplan la seguridad en cada una de las áreas además de la seguridad de los equipos dentro del centro de cómputo.

- Se utilizan mecanismos de protección perimétrica, a las áreas que contienen información e instalaciones que procesan información.
- Se utiliza mecanismos de control de acceso en áreas críticas.
- Se utiliza mecanismos de seguridad en oficinas, habitaciones e instalaciones.
- Se aplica medidas de seguridad física y directrices para trabajar en áreas seguras.
- Se aplica medidas de seguridad en áreas de acceso público.

El centro tiene bien definidas las áreas seguras, y existen medidas de seguridad establecidas; se considera que los mecanismos de seguridad pueden ser mejorados, y que es necesario proveerse de un plan de acción contra amenazas externas y ambientales. Los servidores principales de bases de datos se

encuentran aislados y con acceso restringido al personal no autorizado por el área de sistemas del centro bibliotecario.

- Los equipos están ubicados en salas con protección física ante un posible acceso no autorizado.
- Los equipos están protegidos frente a fallas de servicios públicos.
- El cableado eléctrico y de comunicaciones está protegido frente a intercepción o daños.
- Los equipos son mantenidos en forma periódica.
- Se aplica seguridad a los equipos fuera del local.
- Antes de dar de baja un equipo se elimina la información.
- Todo equipo requiere autorización para ser retirado de la institución.

De manera general los equipos están debidamente protegidos y se realiza mantenimiento periódico; pero existe evidencia que este mantenimiento es más correctivo que preventivo, por lo que se cree conveniente que se deben planificar procedimientos de mantenimiento preventivos, para así evitar eventualidades que pongan en riesgo la seguridad de la información. Respecto a los activos que deben ser dados de baja, esto no se realiza sin una previa autorización de la encargada de sistemas.

Dentro del centro la seguridad física y ambiental si está siendo tomada en cuenta, es decir se han tomado medidas para garantizar un reconocimiento de áreas seguras y la seguridad de todos los equipos dentro del centro de manera general; más se vuelve necesario establecer procedimientos de control preventivos que permitirán gestionar de mejor manera la seguridad física dentro del centro Bibliotecario.

Se considera necesario el diseño y la mejora de muchas políticas de seguridad física, se cree que éstas políticas deben ser más específicas y deben estar acorde a cada área segura del centro, evidentemente la seguridad entre áreas será diferente, dependiendo de los recursos, la criticidad de la información. Además de un constante monitoreo de las áreas seguras, en aras de lograr que las vulnerabilidades no sean de orden físico, es decir que las áreas estén debidamente resguardadas ante cualquier acceso no autorizado o eventualidad externa.

A.10 Gestión de operaciones y comunicaciones

Este grupo de 32 controles tiene como objetivo asegurar la operación correcta y segura de los activos de información, y abarca procedimientos y

responsabilidades operacionales y la verificación de una adecuada gestión de redes dentro del centro.

- La entidad posee un mapa de redes que identifica los servidores, las ubicaciones de los equipos y a que redes están asociadas

- Procedimientos de operación documentados.

- Gestión del control de cambios en los recursos de procesamiento de información.

- Segregación de responsabilidades para reducir el mal uso de los activos.

- Separación de los recursos de desarrollo, prueba y producción.

- Monitorear, afinar y realizar proyecciones de uso de recursos para asegurar su buen desempeño.

- Establecer los criterios de aceptación de sistemas y realizar las pruebas antes de la aceptación.

- Implementar controles de prevención, detección y recuperación ante software malicioso.

- Asegurar que el código móvil autorizado opere de acuerdo a las políticas de seguridad.

- Se realiza copias de respaldo de información y software.

- Manejar y controlar adecuadamente las redes para proteger la información e infraestructura.

Se evidenció que todos los procedimientos se encuentran documentados y en su gran mayoría los usuarios del centro bibliotecario tienen acceso a éstos; sin embargo se considera que la descripción de las funciones y políticas que actualmente se manejan en el centro son muy generales y no ofrecen una visión completa de la realidad del centro por lo que se vuelve necesario que estas políticas sean rediseñadas para adaptarse exclusivamente a la realidad del centro de cómputo.

Actualmente el centro de cómputo se encuentra en fase de desarrollo de nuevas aplicaciones, éste proyecto de desarrollo se encuentra debidamente documentado, y se verifica que exista el cumplimiento de cada uno de los requisitos y necesidades de los usuarios del centro.

Cabe destacar que el centro periódicamente realiza copias de respaldo; sin embargo este requerimiento no está debidamente documentado y por ende no hay requerimientos mínimos para realizar estos respaldos. Se piensa que es necesario establecer directrices para realizar las copias de éstos respaldos de manera que éstos sean efectivos

La entidad dispone de una lista de todas las máquinas y a que redes están conectadas, con su respectiva máscara de red y dirección IP; se cree conveniente para mejorar la seguridad en redes que se diseñe el respectivo mapa de redes que permita identificar más fácilmente a que red está asociada cada equipo.

- Se dispone de procedimientos para la gestión de medios removibles.
- Se dispone de procedimientos formales para la eliminación de medios.
- Se dispone de procedimientos para el manejo de información de manera confidencial.
- La documentación de los sistemas es protegida del acceso no autorizado.
- Se dispone de normativa para proteger la información durante su intercambio.

- Se firma acuerdos para el intercambio de información.

- Se protege los medios en tránsito contra acceso no autorizado.

- Se protege adecuadamente la información involucrada en los mensajes electrónicos.

- Monitoreo de actividades no autorizadas.

La transferencia de información y la gestión de medios están debidamente establecidas, hay procedimientos que aunque no están documentados se aplican para controlar los medios removibles, además en cuanto al intercambio de información está disponible la política general de la institución superior.

No se ha registrado auditorías independientes previas, por lo que no se documentan pistas de auditoría, si se detectan deficiencias; sin embargo se ha notado que la entidad tiene más capacidad de corregir errores que de prevenirlos, por lo que se sugiere se implanten procedimientos de control que permitan detectar y prevenir vulnerabilidades en la gestión de información y comunicaciones.

A.11 Control de acceso

Este objetivo se cumple aplicando 25 controles que buscan controlar el acceso lógico a los activos de la información, es una parte fundamental de la gestión de la seguridad de la información ver los controles de acceso, para esta verificación se ha procedido a realizar pruebas directamente con los distintos módulos del sistema, se procedió a verificar cada módulo, a generar reportes a ver pruebas de redundancia.

Todas estas pruebas ofrecieron un marco de referencia de cuál es la situación actual en cuanto a los controles lógicos, se pretende lograr que la interacción entre la aplicación y el usuario sea lo más segura y efectiva posible, y dado el volumen de información que el centro maneja constituye como un punto neurálgico dentro de la seguridad de la información.

Estos controles no solo se encaminan a la interacción de la aplicación sino también al cuidado y adecuado funcionamiento que debe tener cada componente que interviene en el centro bibliotecario.

- Se dispone de una política de control de acceso con base en requerimientos del negocio.

- Se dispone de procedimientos de registro y baja de concesión de acceso a los sistemas y servicios de información.

- Se dispone de procedimientos para la gestión de privilegios.

- Se dispone de procedimientos para la gestión de contraseñas.

- Se audita los derechos de acceso de manera regular.

- Se promueve las buenas prácticas de seguridad para selección de contraseñas seguras.

- Se promueve la práctica del uso de escritorio limpio.

- Los usuarios solo tienen acceso a los servicios a que están autorizados.

- Se controla el acceso para el diagnóstico y configuración de puertos.

- Se restringe la capacidad de conexión de usuarios a redes compartidas.

- Se controla el acceso al SO en las estaciones o terminales.

- Las sesiones inactivas se cierran luego de un tiempo de inactividad.

- Se restringe el acceso a los usuarios y a las personas.

- Los sistemas sensibles están en un ambiente aislado.

- Se segrega en la red los usuarios y sistemas de información.

- Todo usuario dispone de una cuenta de acceso única.

- Se dispone de política de protección de equipos móviles.

Se identificó que existen 3 niveles de acceso a la información que van acorde a la necesidad que el centro tiene, estos accesos son debidamente controlados y cada usuario tienen una cuenta única y dependiendo de sus funciones tendrá acceso a distintos niveles de la aplicación, estos accesos difícilmente se pueden ver vulnerados; sin embargo no existen pruebas que aumenten el nivel de seguridad, es decir con un usuario y contraseña se puede acceder al sistema, se deberían implementar más pruebas de seguridad y se debería documentar un procedimiento para la gestión de los usuarios.

Las terminales ubicadas dentro del centro bibliotecario están controladas con los mismos requerimientos de acceso, en el caso de los estudiantes, estos pueden tener acceso a los módulos que como tal les servirán para consultas y demás gestiones.

En el caso del uso de los laboratorios cuando una sesión se inactiva ésta se cierra y para poder acceder se deberá volver a validar los datos del usuario, en caso de que el usuario no esté autorizado, no podrá acceder a los módulos que pretende.

De manera general el sistema cuenta con controles lógicos definidos, algunos no se encuentran documentados pero si se aplican, el sistema presenta errores de entrada es decir no se han establecido parámetros de los datos que se busca ingresar, por lo que esta aplicación debe ser revisada para establecer los criterios de posibles mejoras.

Los módulos están siendo actualizados, más existe evidencia de que estos cambios no han llegado aún a todos los usuarios del sistema, lo cual podría generar dificultades a la hora de realizar operaciones con la información de la entidad.

A.12 Adquisición, desarrollo y mantenimiento de sistemas de información

Este grupo de 16 controles busca procurar que la seguridad sea una parte integral de los sistemas de información.

Para garantizar esto en un centro de cómputo es muy necesario medir los requerimientos de sistema que tiene la entidad, y así mismo ver cuál es la seguridad que esta aplicación puede aportar a los procedimientos del centro y la capacidad que estos sistemas tienen de actuar ante alguna eventualidad.

En el caso particular del objeto de estudio cabe señalar que actualmente se encuentra desarrollando una serie de aplicaciones que le permitirá al centro trabajar con bibliotecas de otras instituciones de educación superior, y actualmente este proyecto se está llevando a cabo cumpliendo con una serie de directrices previamente establecidas.

En el caso de presentarse una necesidad de software, ésta se gestiona a través del área de compras de la institución.

- Se especifican los requerimientos para nuevos sistemas o mejoras, incluyendo los controles de seguridad.

- Se validan los datos de entrada a las aplicaciones para detectar corrupción de la información.

- Se valida la data de salida de las aplicaciones.

- Se dispone de una política de uso de controles criptográficos para proteger la información.

- Se realiza gestión de claves para dar soporte al uso de las técnicas criptográficas.

- Se dispone de procedimientos para la instalación de software de los sistemas.

- Se selecciona, protege y controla los datos de prueba del sistema.

- Se controla el acceso al código fuente del sistema.

- Los cambios se controlan mediante el uso de procedimientos de control de cambios.

- Las aplicaciones se revisan después de haber hecho cambios en el sistema operativo.

- Se procura evitar las fugas o filtraciones de información.

- Se supervisa y monitorea el desarrollo tercerizado de software.

- Se procura minimizar la explotación de vulnerabilidades de los sistemas.

Como se ha indicado previamente el centro actualmente se encuentra en fase de desarrollo, todos los requerimientos se encuentran debidamente documentados y el proyecto avanza con un poco de retraso por temas imprevistos que no se han podido solucionar.

Al estar en fase de desarrollo no se ha realizado ningún plan de implementación. Cabe mencionar que constantemente se modifican módulos del sistema y existe evidencia que hay una capacitación constante al personal respecto a estas modificaciones.

Debido a la ausencia de un plan de implementación, no es posible establecer si el sistema en desarrollo cumple con los criterios de seguridad necesarios para una adecuada gestión de la información dentro de la biblioteca.

Se recomienda que esta fase de desarrollo sea evaluada por una entidad externa, para poder lograr el principio de independencia en las revisiones, no debe ser sólo misión de la directora de la entidad evaluar el progreso en esta etapa de desarrollo.

A.13 Gestión de incidentes de seguridad de información

Este objetivo es evaluado por 5 controles que buscan asegurar que los eventos y debilidades de seguridad de información sean comunicados de manera tal que permita una acción correctiva oportuna. Primero se contempla el reporte de incidentes que puedan ocurrir en las funciones cotidianas del centro bibliotecario.

Además de esto, una vez identificados los incidentes, estos deben ser gestionados y se debe proponer el respectivo plan de mejora. Se vuelve necesario un plan de controles correctivos que permitan dar seguimiento a las acciones que se tomen para corregir los incidentes, y así garantizar la confidencialidad, integridad y disponibilidad de la información.

Los incidentes asociados a la información son muy comunes, muchos de éstos se producen por eventualidades ajenas al centro como eventos naturales, pero la gran mayoría de incidentes vienen asociados a la intervención del ser humano, ya sea por error, o por omisión intencionada la mayoría de incidentes asociados a la información son producidas por el mismo recurso humano del centro de cómputo.

- Los incidentes de seguridad de la información se reportan por los canales apropiados tan rápido como sea posible.

- Se promueve que todo el personal reporte las debilidades que observe o se sospeche

Los incidentes asociados a la información son muy comunes, especialmente en un centro de cómputo que maneja los niveles de información que una biblioteca maneja. No existe un proceso documentado de gestión de incidentes, pero existe evidencia que indica que los incidentes son tratados oportunamente; sería recomendable que los canales de comunicación se mejoren y que los incidentes sean debidamente registrados, para en lo posterior poder realizar los respectivos seguimientos de las acciones que se han tomado.

Cabe destacar que el centro tiene a su cargo bibliotecas seccionales, si bien cada una de ellas cuenta con sus ayudantes, existen incidentes que necesariamente se deben tratar por personal de sistemas del área de cómputo, lo cual podría retrasar la gestión oportuna de éstos.

- Se dispone de procedimiento para respuesta rápida, eficaz y ordenada ante incidentes de seguridad de información.

- Se dispone de mecanismos para aprender a resolver incidentes, que permitan cuantificar y realizar el seguimiento de los tipos, volúmenes y costo de los incidentes.

- Se recolecta y mantiene evidencias.

Los ayudantes de cada área, incluyendo las bibliotecas seccionales, son debidamente capacitados para poder dar una respuesta rápida ante incidentes menores; más en el caso de presentarse incidentes mayores de la naturaleza de perder información o perder alguna funcionalidad del sistema son casi siempre resueltas por el personal del área de sistemas, lo cual retrasa la acción correctiva, se recomienda capacitar más al personal, que pueda dar respuesta pronta y eficaz ante las eventualidades.

Así mismo se sugiere que se documente con un formato prestablecido cada uno de los incidentes que afecte la seguridad informática del centro bibliotecario, para así poder tener un historial de incidentes y cuando sea necesario realizar el respectivo seguimiento, además documentar los incidentes y sus respectivas medidas de acción en un futuro servirá como pistas de auditoría.

A.14 Gestión de continuidad de operaciones

Siempre una entidad debe estar preparada ante cualquier eventualidad que pueda poner en riesgo, sus funciones, cuando se habla de información y de

activos de información como tal se vuelve imperante tener un plan de continuidad ante cualquier eventualidad dañosa, este grupo de controles buscan contrarrestar las interrupciones de las actividades del negocio y proteger los procesos críticos, de los efectos de fallas significativos o desastres y asegurar su reanudación oportuna.

El centro de cómputo como tal no tiene documentado un plan de continuidad de operaciones, más si maneja las directrices que debe seguir en caso de que las operaciones se vean interrumpidas. Se tienen identificados riesgos asociados a la seguridad de la información.

La institución de educación superior si cuenta con un plan de continuidad, y el centro de cómputo se rige a éste plan, pero se ha considerado necesario para mejorar la seguridad del centro que se diseñe un plan de continuidad propio que abarque toda la realidad de un centro de información bibliotecario y la magnitud de información que día a día se suele procesar.

A.15 Cumplimiento regulatorio

Este objetivo de control busca evitar el incumplimiento de cualquier ley, estatuto, obligación, reglamentos contractuales y de cualquier requisito de seguridad, se

debe proceder a analizar primeramente el cumplimiento con los requerimientos legales, después se debe cerciorar que se está en cumplimiento con las políticas y estándares de seguridad de la información, y se debe evaluar la integridad de la información que se genere producto de auditorías previas a los sistemas de información.

La universidad cuenta con una serie de requisitos legales que debe cumplir, particularmente el centro de cómputo de la biblioteca conoce la normativa legal a la que está sujeta; sin embargo se sugiere el diseño de una matriz de requisitos legales para tener de forma detallada y ordenada cada requisito de ley que la biblioteca tenga.

Para que se cumpla con la política de seguridad de la información es preciso que el personal tenga un claro conocimiento de la política en mención, de no conocerla es muy difícil que se pueda garantizar el cumplimiento de la misma.

En cuanto a las auditorías internas no hay evidencia de auditorías internas recientes por lo que no se puede garantizar un adecuado procedimiento de protección de dicha información, o cumplimiento de los requisitos legales.

Si bien se puede decir que todos los controles están establecidos y que el centro ha intentado garantizar la seguridad de la información, se han encontrado

falencias que evidentemente deberán ser corregidas; y es que, a pesar de la presencia de controles, éstos no son del todo eficientes para gestionar la seguridad informática y disminuir el riesgo informático.

3.3.2 ANÁLISIS DE RIESGOS

Una vez que se ha analizado específicamente cada grupo de objetivos de control sugerido por la normativa ISO se puede determinar cuál es el porcentaje de seguridad de la información dentro del área de sistemas de la universidad pública, en base a este estudio se podrá determinar las posibles mejoras las cuales serán incluidas en la política de seguridad que se debe diseñar conforme al marco referencial de la ISO 27001.

Como se puede evidenciar a continuación existen áreas críticas donde urgentemente de deberán proponer mejoras para ayudar a mejorar la gestión de la seguridad del centro.

Objetivo de control	Promedio	Promedio Ideal
Política de seguridad de la información	20,00	100,00
Gestión de activos de información (AI)	44,00	100,00
Seguridad de los recursos humanos	33,33	100,00
Seguridad física y medioambiental	43,08	100,00
Gestión de operaciones y comunicaciones	36,00	100,00
Control de acceso (lógico)	41,60	100,00
Adquisición, desarrollo y mantenimiento de sistemas de información	38,75	100,00
Gestión de incidentes de seguridad de información	40,00	100,00
Gestión de continuidad de operaciones	28,00	100,00
Cumplimiento regulatorio	42,50	100,00
Promedio Total	37,42	100,00

Tabla 3.2 Cumplimiento de objetivos de control

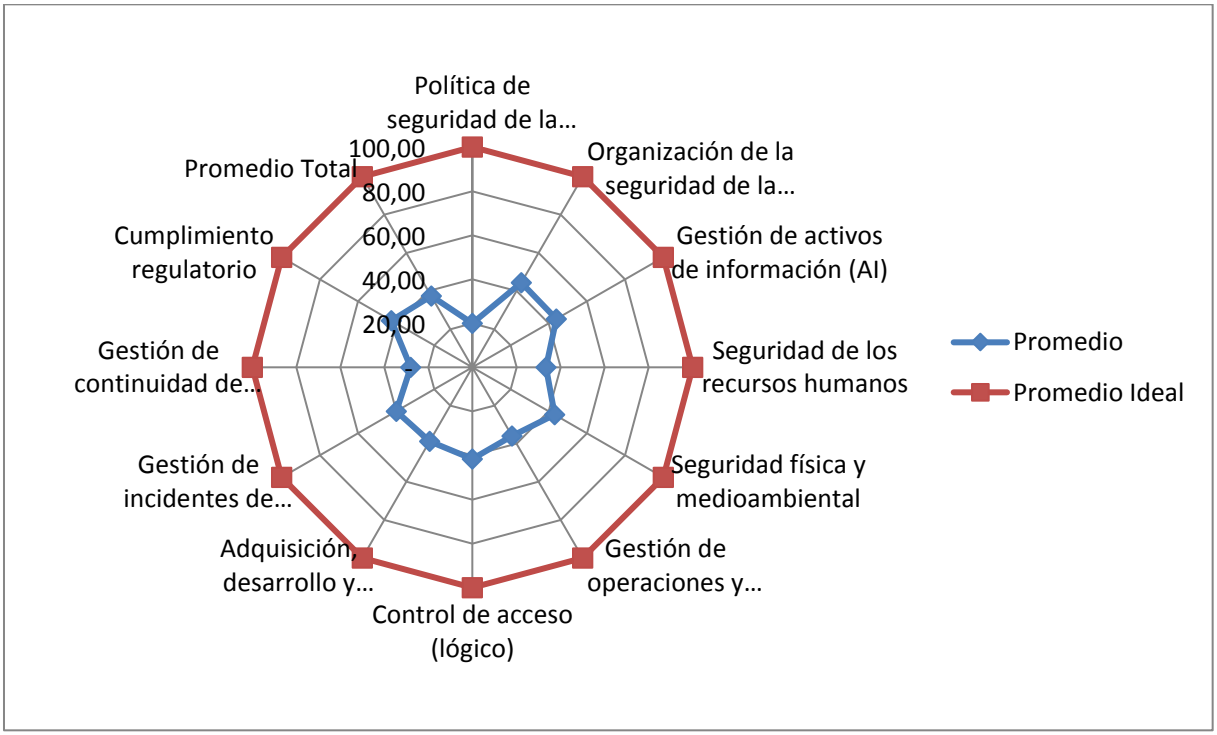

Figura 3.1 Gráfico de cumplimiento de objetivos de control respecto a cumplimiento ideal

Se ha llegado a detectar que de manera general el porcentaje de seguridad de la información dentro del centro de cómputo de la biblioteca central es del 37,42 %, una alarmante cifra si se considera los volúmenes de información que día a día el centro maneja, y lo importante de esta información ya que el centro maneja información histórica de inventarios, de multas, de deudas, de transiciones, de bajas de libros de inventario, por lo que se vuelve imperante el diseño de procedimientos que permitan que la realidad del centro mejore y se garantice una adecuada gestión de la seguridad del mismo.

Claramente se evidencia que la política de seguridad de la información constituye el punto más bajo en cuanto a seguridad de la información, esto se debe a que el centro no tiene establecida una política de seguridad en el marco que la norma ofrece. El centro dispone de varias políticas de manejo de procesos, y de gestión de eventualidades; sin embargo no se ha documentado una política que abarque los 10 grupos de controles que la norma nos refiere.

Se ha mencionado que la universidad posee políticas propias y que el centro bibliotecario se rige en su gran mayoría por estas políticas, pero esto no es del todo recomendable porque estas políticas resultan muy generales y no abarcan como tal la realidad del centro bibliotecario.

Además, se vuelve también muy necesario realizar un plan de continuidad de operaciones el cual permita tener un marco de acción establecido ante cualquier eventualidad que se pudiere presentar y pudiere atentar contra la disponibilidad, integridad y confidencialidad de la información.

De manera general se puede decir claramente que si bien el centro tiene en su gran mayoría procedimientos de control estos no están debidamente establecidos y en algunos casos no se han documentado; no obstante la evidencia muestra que si se han aplicado controles, se podría concluir que estos controles pueden claramente ser mejorados, y al ser mejorados e implementados pueden mejorar la realidad del área de sistemas de la biblioteca central.

El diseño de la política de seguridad con marco de referencia de la ISO incluirá procedimientos de mejoras, rediseño de controles y en algunos casos creación de controles para cada uno de los objetivos de control, éstas mejoras de ser implementadas mejorarán la seguridad de la información, dependerá mucho de el compromiso del centro bibliotecario en implementar estas acciones para lograr una mejora constante de sus procedimientos.

Se procederá de manera inmediata a diseñar el sistema de gestión de seguridad de la información, la cual incluye una política de seguridad de la información cuyo alcance es el área de sistemas del centro de información bibliotecario.

Parte de la normativa ISO señala la gestión de riesgos, es por eso que previo al diseño del SGSI se detallará en la matriz de riesgos cuales constituyen los riesgos asociados a cada función que se desarrolla en el área de sistemas de la entidad objeto de estudio, para esto se considerará:

Probabilidad de ocurrencia donde:

1. Se entiende que es poco probable que ocurra el riesgo.
2. Se entiende que es medianamente probable la ocurrencia de incidentes.
3. Se entiende que es alta la probabilidad de la ocurrencia de eventualidades.

Magnitud de impacto donde:

1. Se entiende que el impacto del incidente es bajo.
2. Se entiende que el impacto es medio.
3. Se entiende que el impacto en la entidad sería muy alto.

Control, donde se evaluará la eficiencia, la ineficiencia o la inexistencia del control siendo:

1. Eficiente.

2. Ineficiente.

3. Inexistente.

A continuación se detallará los principales riesgos asociados a las áreas más críticas que se hallaron en el estudio y se podrá determinar los impactos de ocurrencia de incidentes asociados a estos controles:

PROCESO	RIESGO	O	I	C
Dar a conocer la política de seguridad de la información	Si el personal no conoce la política de seguridad de la información se puede vulnerar la seguridad del centro	3	2	2
Revisión frecuente de la política de seguridad de información	La política no se revisa con frecuencia	2	2	2
Segregación de funciones	Ocurren centralización de las funciones	3	2	1
Asignación de responsabilidades de loa activos de información	En caso de falla de algún activo no existe quien controle la situación oportunamente	2	2	2

PROCESO	RIESGO	O	I	C
Gestión amenazas externas	El centro no tengas respuesta ante eventualidades externas	1	2	2
Gestión de la seguridad de los equipos	Los equipos se exponen a eventualidades dañosas	2	3	2
Accesibilidad al sistema	Se pueden vulnerar los filtros de acceso	3	3	2
Generación de datos y reportes	Se pueden alterar datos de reportes por usuarios no autorizados	2	3	2
Generación eficaz de datos para usuarios externos	Que los datos revelados al usuario no sean veraces	2	2	2
Gestión de incidentes y continuidad de operaciones	No se sigan procedimientos ante incidentes	2	3	3
Cumplimiento requerimientos legales	El personal no respete la normativa vigente por falta de conocimiento	2	2	3

Tabla 3.3 Riesgos asociados a áreas críticas

O: Ocurrencia I: Impacto C: Control

Se identificaron los riesgos más importantes; el sistema de gestión de seguridad que se va a diseñar en lo posterior abarcará todos los hallazgos que se hicieron del área de sistemas, se advierte que si el centro implementare este sistema, el centro bibliotecario quedaría listo para una posterior certificación internacional en seguridad de la información.

CAPÍTULO IV

4 DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El centro de información bibliotecario es una organización que no tiene definidos sus procesos, procedimientos y políticas aplicables a ISO 27001. Según lo analizado en el capítulo 3, el centro de información bibliotecario presenta deficiencias en los controles de la política de seguridad, se encontró que no hay una política de continuidad de operaciones, y que la entidad carece de procedimientos de uso de recursos tecnológicos

Sin embargo para efectos de este estudio se diseñarán todos los controles evaluados en el capítulo 3 y se los incluirá como parte de la política de seguridad de la información.

Con el diseño del SGSI la entidad va a estar en capacidad de controlar, evaluar, reconocer e implementar mejoras que mitiguen los riesgos asociados a la información.

4.1 Plan de Implementación

Para establecer el SGSI, la organización debe realizar los siguientes pasos establecidos en la ISO/IEC 27001[3]:

1. El alcance y límites del SGSI deben estar en términos de las características del negocio, la organización, su ubicación, sus activos y tecnología.

2. Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, sus activos y tecnología que incluya:

    a. Política de seguridad.

    b. Organización de la seguridad de la información.

    c. Gestión de activos.

    d. Seguridad de los recursos humanos.

    e. Seguridad física y ambiental.

---

3 ISO/IEC 27001:2008, cláusula 4.2.1

f. Gestión de las comunicaciones y operaciones.

g. Control de accesos.

h. Adquisición, desarrollo y mantenimiento de los sistemas de información.

i. Gestión de un incidente en la seguridad de la información.

j. Gestión de la continuidad del negocio.

k. Cumplimiento.

3. Definir el enfoque de valuación del riesgo de la organización.

4. Identificar, analizar y evaluar el riesgo y las opciones para el tratamiento de estos.

5. Seleccionar objetivos de control y controles para el tratamiento de riesgos

6. Obtener la aprobación de la gerencia para los riesgos residuales propuestos.

7. Preparar un enunciado de aplicabilidad.

El presente estudio se enfocará exclusivamente al diseño de la política de seguridad de la información debido a que los demás literales están enmarcados en la fase de implementación del sistema

4.2 Alcance del SGSI

El SGSI incluirá las actividades y procesos del departamento de sistemas, al igual que a los laboratorios de cómputo, sus activos y tecnología destinados a preservar la disponibilidad, integridad y confidencialidad de la información que brinda el centro de información bibliotecario, así mismo también se incluirá el análisis de los módulos incluidos en el sistema.

La información que se maneja en este centro, es de vital importancia para los usuarios de la información debido a que en este podrán ver las deudas que tengan pendiente con la institución por préstamos de libros, así como la ubicación física de éstos. Estos servicios deberán garantizar que la información sea completa, segura y libre de modificaciones por usuarios no autorizados.

El centro de información bibliotecario está ubicado dentro de una institución de educación superior pública en la ciudad de Guayaquil.

4.3 Política de seguridad de la información

4.3.1 INTRODUCCIÓN

Como se expresó anteriormente el centro de información bibliotecario no tiene una política de seguridad definida, tampoco tienen planes de contingencia o continuidad de las operaciones en casos de fuerza mayor.

Debido a la importancia que tiene la información que proporciona el centro de información bibliotecario, se buscará protegerla frente a amenazas o ataques para poder asegurar el cumplimiento de la disponibilidad, confidencialidad e integridad de ésta, implementando medidas de seguridad que aseguren la eficiencia de recursos y eficacia en el cumplimiento de los objetivos de la organización en concordancia con los requerimientos comerciales, leyes y regulaciones relevantes.

Las amenazas o ataques a los que puede estar sometida la información son muchos y el riesgo nunca va a dejar de existir, siempre va a existir una cantidad, aunque sea mínima, de riesgo, que la organización no pueda mitigar. El objetivo de esta política es minimizar al máximo posible los riesgos existentes en la información y la única forma de lograrlo es alineando la política de seguridad con la política de la organización.

El departamento de sistemas del centro de información bibliotecario es el encargado de toda la parte informática de la Biblioteca Central de la institución de educación superior, de atender los requerimientos de laptops y de laboratorios de estudiantes y profesores, y de realizar el debido mantenimiento y brindar soporte a todos los equipos que están bajo responsabilidad de la Biblioteca Central.

El presente modelo podrá sufrir modificaciones, cambios o actualizaciones futuras, acorde a las necesidades del centro de información bibliotecario, estas modificaciones deberán ser debidamente aprobadas por el director del centro de información bibliotecario y por el responsable del sistema de gestión de seguridad de la información.

Para poder lograr una adecuada de reducción de riesgos asociados al manejo de la información es necesario el compromiso de todos los niveles de la organización.

4.3.2 OBJETIVOS DE LA POLÍTICA DE SEGURIDAD

- Asegurar que la información entregada a los usuarios sea confiable y libre de errores.

- Analizar los riesgos de la organización regularmente y formular los planes de contingencia y continuidad del negocio, sujetos a revisión periódica.

- Proteger la información de ataques o modificaciones que puedan sufrir por terceros.

- Garantizar que la información esté siempre disponible para los usuarios cuando estos lo requieran.

- Mantener la confidencialidad de la información.

- Asegurar que el personal y usuarios administrativos del centro sean capacitados y sean conscientes del cumplimiento de la política de seguridad de la información.

- Buscar la mejora continua en los procesos del departamento de sistemas del centro de información bibliotecario.

4.3.3 ALCANCE

Esta política es aplicable a todos los usuarios internos y externos de la información, sea cual fuere su nivel jerárquico y de manera primordial al Departamento de Sistemas del centro de información bibliotecario.

4.3.4 RESPONSABILIDAD

Son responsables de observar y cumplir la política de seguridad de la información todas las personas que pertenecen al centro de información bibliotecario, especialmente al departamento de sistemas, incluyendo a los estudiantes y al personal administrativo responsable del manejo de la información que será entregada a los usuarios.

Los encargados de la administración de la información serán los encargados de mantenerla actualizada y de velar por el cumplimiento de la confidencialidad, disponibilidad e integridad de la información manteniéndola documentada y definiendo restricciones en caso de ser necesario.

Los usuarios de la información serán los encargados de cumplir con la política de seguridad de la información en todos los niveles que tengan acceso y de mantenerla libre de manipulaciones, modificaciones y mal uso.

Así mismo la dirección deberá gestionar con el departamento de Talento Humano la difusión de esta política de manera obligatoria para el personal nuevo, en pro de buscar el mitigamiento de riesgos a su manejo que podría ocasionar el desconocimiento de la política.

Esta política deberá ser revisada como mínimo de manera anual o antes si las necesidades lo ameritan, en busca de la mejora continua y mantenimiento del Sistema de Gestión de Seguridad de la Información. La revisión deberá ser efectuada por los auditores internos, garantizando siempre el fiel cumplimiento de los lineamientos incluidos en este documento, actualizándola y modificándola en caso de ser necesario por cambios en procedimientos internos o inclusión de nuevos siempre bajo aprobación de la dirección de la institución, adicionalmente deberán hacer llegar la política al departamento de Talento Humano para su difusión.

4.3.5 SANCIONES POR INCUMPLIMIENTO

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y características de los aspectos no cumplidos.

4.3.6 CONTROLES A APLICAR SEGÚN ISO 27001

A.6 Organización de la seguridad de la información

El centro de información bibliotecario tiene un convenio con otras bibliotecas nacionales e internacionales, debido a eso es necesario proteger la información de accesos o modificaciones indebidas; la información debe llegar íntegra a estos clientes.

Para poder llegar a un punto óptimo que logre que la información esté debidamente gestionada y administrada se debe organizar el entorno de los usuarios que interactúan con la información, por ello es necesario definir un responsable de la gestión de la seguridad de la información, esta persona deberá encargarse de la modificación o creación de nuevas políticas según sean las necesidades del centro de información.

La presente política establecerá y definirá los puestos que considere necesarios para el fiel cumplimiento de la política de seguridad; así mismo en caso de requerir servicios de entidades externas se deberá organizar la información de manera que las entidades reciban la información necesaria para su servicio, se vuelve

necesario asegurarse que estas entidades no tengan acceso a activos de la información a los que no están autorizados.

Las funciones de los usuarios que interactúan con el sistema deben ser establecidas con claridad para evitar confusiones al momento de ejecutar las actividades, es necesario evaluar los puestos de trabajo y hacer una correcta asignación de responsabilidades y accesos en el sistema.

El control que se va a diseñar será aplicable a todos los usuarios o activos que interactúan directa o indirectamente con los activos de la información, incluyendo a las entidades externas que tengan acceso a información interna de servicios o sistemas informáticos.

El responsable de la gestión de la seguridad de la información será el encargado de realizar modificaciones o actualizaciones de la política de seguridad de la información, debidamente aprobadas por la dirección; así mismo se encargará de la designación de responsabilidades en busca del cumplimiento estricto de las políticas, de la contratación de personal a su cargo para la realización de pruebas de control, análisis de riesgos e implementación de controles, o de ser necesario de analizar la contratación de una entidad externa experta en seguridad de la información, para minimizar el riesgo al máximo posible y de la difusión e implantación de esta política.

En caso de la contratación de servicios externos se debe incluir una cláusula de confidencialidad y del cumplimiento estricto de las políticas de seguridad de la información vigentes en la institución.

A.6.1 Organización interna

A.6.1.1 Compromiso de la gerencia con la seguridad de la información

La gerencia del centro de información bibliotecario deberá velar por el cumplimiento de la política de seguridad de la información y apoyará las actividades que se realicen en busca del fiel cumplimiento de la política para lograr minimizar al mínimo los riesgos asociados al uso de la información.

A.6.1.2 Coordinación de la seguridad de la información

Debido a que en el centro de información bibliotecario se está gestionando la implementación de un departamento de calidad, que controlará y vigilará el cumplimiento de los procesos del centro de información bibliotecario; es necesario que sea el director de este departamento el encargado de:

- Fomentar la cultura de seguridad en todos los niveles de la organización.

- Modificar y actualizar la política de seguridad de la información, fomentar su aprobación por la dirección y delegar su difusión para que sea conocida por todos los usuarios internos y externos de la información.

- Documentar los controles y riesgos a los que está expuesta la información y los métodos y acciones implementadas para su minimización.

- Establecer y velar por la ejecución de los planes de contingencia y continuidad del negocio.

- Velar por el cumplimiento de la política de seguridad de la información en los contratos que se realizan o en caso de adquisición de nuevos activos.

Es el director del departamento de calidad el encargado de asignar un coordinador de seguridad de la información, esta asignación deberá quedar documentada y será firmada por ambas partes.

El coordinador de la seguridad de la información podrá pedir a los departamentos de la organización la información y ayuda necesaria que lo ayuden a gestionar la seguridad de la información de una forma más eficiente y eficaz.

A.6.1.3 Asignación de responsabilidades

Control de accesos – Vanessa Llongo - Asistente de sistemas

Gestión de incidentes de seguridad – MSc. Victoria Plaza - Directora Centro Bibliotecario

Desarrollo y mantenimiento de los sistemas de información – Vanessa Llongo - Asistente de sistemas

Adquisición de los sistemas de información – MSc. Victoria Plaza - Directora Centro Bibliotecario

A.6.1.4 Proceso de autorización para los medios de procesamiento de información

Los medios y usuarios empleados en el procesamiento de la información, sean estos nuevos o existentes, deberán contar con la debida aprobación del director del Departamento de Calidad y de la dirección; de tal manera que se busque el fiel cumplimiento de la política de seguridad de la información.

A.6.1.5 Acuerdos de confidencialidad

La actividad principal del centro de información bibliotecario es brindar información sobre los libros que posee, por lo que no es necesario establecer un acuerdo de confidencialidad entre los usuarios de internos y externos de la organización, exceptuando a las entidades externas que nos brindan servicios.

Las entidades externas si deberán firmar un acuerdo de confidencialidad de la información y la información a la que ellos acceden deberá ser la necesaria para el eficiente desempeño de las actividades por las que fueron contratados.

A.6.1.6 Contacto con autoridades

En busca de la optimización de los controles que van a ser implementados, el responsable del sistema de gestión de seguridad de la información deberá mantener acercamientos frecuentes e informar a las autoridades de todas las áreas de la organización sobre las buenas prácticas en temas de seguridad de la información.

A.6.1.7 Contacto con grupos de interés especial

Se deberá mantener contacto con grupos de interés común en materias de seguridad de la información, de manera que sirvan de asesoría y auditoría para el correcto desempeño de la política de seguridad de la información.

A.6.1.8 Revisión independiente de la seguridad de la información

El centro de información bibliotecario deberá buscar asesoría externa para la revisión del cumplimiento del sistema de gestión; esta revisión deberá ser periódica, de manera anual o cuando la entidad lo considere necesario, para poder asegurar que los riesgos a los que está sujeta la información están siendo gestionados y controlados.

La entidad y sus empleados deberán estar a entera disposición de los auditores independientes en busca del fiel cumplimiento de la política de seguridad de la información y de su mejora continua.

A.6.2 Entidades externas

A.6.2.1 Identificación de riesgos relacionados con entidades externas

El centro de información bibliotecario, al momento de recibir servicios por parte de entidades externas debe evaluar los riesgos vinculados al uso y manipulación de la información por la ejecución del servicio respectivo.

Estos riesgos deberán ser analizados y evaluados para verificar el impacto que tienen en la organización y en base a estos tomar medidas que los minimicen. El análisis de riesgos, así como sus acciones preventivas y correctivas deberán ser debidamente documentados y estarán firmados por el responsable del sistema de gestión de seguridad de la información y del director del departamento de sistemas. Este análisis deberá ser efectuado previo a la firma del contrato entre las partes.

A.6.2.3 Tratamiento de la seguridad en contratos con terceras personas

Los contratos con entidades externas deberán observar el conocimiento y cumplimiento de políticas, los controles que se aplicarán para obtener certeza de la seguridad de la información serán:

- Cualquier requerimiento de información deberá ser analizado para su posterior aprobación por el director del centro de información bibliotecario velando siempre por el cumplimiento de las políticas de seguridad.

- Las entidades externas que vayan a prestar servicios deberán firmar un acuerdo de confidencialidad por la información y datos que vayan a manejar.

- En el contrato a firmar se deberán establecer los niveles de servicio y las limitaciones en accesos físicos y lógicos que tendrán; así como los planes de contingencia y continuidad en casos premeditados o de fuerza mayor.

- Se deberá establecer un acuerdo de protección de activos, sean estos hardware, software, información; en caso de inconsistencias con cualquiera de estos activos, y si se afirma que el activo estaba a cargo de la entidad externa, y el daño fue de responsabilidad exclusiva de ésta, la entidad externa se comprometerá a la reposición del activo.

- Las revisiones al trabajo efectuado por las entidades externas estarán a cargo del director del centro de información bibliotecario, se recomienda llevar un control semanal documentado de las actividades realizadas.

- Una vez finalizada la realización del trabajo se quitarán todos los accesos, sean lógicos o físicos a la entidad externa.

A.7 Gestión de activos

INTRODUCCION

El manejo de los activos de información en una empresa es parte fundamental para la consecución de objetivos, y más cuando nos referimos a un centro de información bibliotecario, cuya actividad principal es brindar información a los usuarios sobre ubicación y disponibilidad de libros.

La entidad debe optar por mantener una adecuada gestión o manejo de los activos que posee con el propósito de que sean íntegros, confidenciales y disponibles. Estos activos deben ser protegidos contra cualquier intento de intrusión, amenaza o robo que puedan sufrir porque como se conoce, la información es el activo más importante de cualquier organización; para lograr esto se deben implementar los debidos controles.

El centro de información bibliotecario deberá tener conocimiento de estos activos para poder efectuar un análisis de riesgos y evaluar e implementar mejoras contra

los riesgos. Para tener un buen control de activos, es necesario que la compañía opte por mantener un inventario de estos, este inventario deberá incluir cosas elementales que indiquen la ubicación del activo, su custodio y características.

En el caso de activos de información que no sean físicos, tal es el caso de la información que se maneja en el departamento, el centro de información bibliotecario también mantendrá un riguroso control en pro de alcanzar las tres características de la información mencionadas arriba (integridad, disponibilidad y confidencialidad).

ALCANCE

Este control es aplicable a todos los niveles de la organización, incluyendo a los receptores de la información que interactúan con los activos, físicos o intangibles del centro de información bibliotecario.

RESPONSABILIDAD

Serán responsables del correcto manejo de los activos, todos los usuarios que interactúen con estos. Es responsabilidad del director del centro de información bibliotecario mantener un adecuado inventario que sirva para identificar las características principales de los activos.

A.7.1 Responsabilidad por los activos

A.7.1.1 Inventarios de Activos

Los activos deben mantenerse correctamente identificados, para lograr esto se llevará un listado que indique la ubicación del activo, su custodio y características principales.

Los activos físicos deberán ser plaqueados con un número de identificación que deberá estar en un lugar visible del equipo; además del número de identificación, se incluirán las características más relevantes del activo (Marca, modelo, departamento en el que lo van a utilizar, especificaciones técnicas)

El director del departamento de sistemas designará a un responsable para el control de estos activos; cada departamento del centro de información bibliotecario está en la responsabilidad de informar al responsable del control de activos sobre cualquier modificación o cambio de los activos.

Se recomienda inventariar los activos dos veces al año, a finales del primer y segundo término académico en la universidad.

A.7.1.2 Propiedad de los activos

Los activos son de propiedad exclusiva de la universidad pública pero estarán bajo responsabilidad de los departamentos para los que se destine su uso.

Cuando un empleado deje su cargo por traslado, renuncia, cierre de operación o por algún otro motivo que lo desvincule del departamento de sistemas, se deberá realizar un inventario de los activos que tenía a su cargo y deberán ser recibidos formalmente por reemplazo o por la persona que el director del departamento de sistemas considere pertinente.

A.7.1.3 Uso aceptable de los activos

Debido a la naturaleza de la organización, los activos son de uso público en algunos casos; por ello, se definirán ciertos lineamientos que se deben cumplir para establecer un mejor control del uso de los activos y en busca del cumplimiento de la política de seguridad de la información.

Computadores de escritorio

Para trabajadores:

- Los computadores de escritorio serán de uso personal y sólo se utilizarán para fines laborales.

- Está prohibida la extracción de información confidencial sin la debida autorización del jefe del departamento al que pertenece el empleado.

- Modificaciones, actualizaciones e instalaciones de programas, cableado o redes sólo podrán ser efectuadas por miembros del departamento de sistemas del Centro de Información Bibliotecario y deberán contar con la aprobación del jefe departamental y del director del centro de información bibliotecario.

- Está prohibido dejar los equipos encendidos de un día para otro.

Para estudiantes:

- Los computadores de escritorio serán utilizados exclusivamente para fines académicos, se prohíbe el acceso a páginas de apuestas, sociales, etc.

- Se prohíbe la extracción o copia de programas, códigos fuente o de activación de programas instalados en los computadores personales.

- No se permitirá más de un estudiante por computadora.

- El estudiante se deberá hacer responsable de los inconvenientes que se presenten en hardware, software, cableado; si se comprueba que el daño fue hecho a sabiendas, se lo sancionará según el reglamento de disciplina de la universidad.

Computadores portátiles

Además de los lineamientos para computadores personales, los trabajadores y estudiantes deberán cumplir los siguientes lineamientos para el correcto uso de los computadores portátiles:

Para trabajadores:

- Está terminantemente prohibida la salida del recinto académico de los computadores portátiles.

- Trabajador deberá firmar un documento en el que acepte las condiciones en las que se le entrega el computador.

- Préstamos de computadores portátiles se deberán hacer luego de haber efectuado un compromiso de cuidado y devolución de laptops firmado por el trabajador y el encargado de los préstamos de portátiles.

- Los inconvenientes o accidentes que se presenten por el mal uso de los computadores portátiles serán de entera responsabilidad del trabajador de la institución y deberán ser sancionados según lo dispongan las políticas de la institución educativa.

Para estudiantes:

- Está terminantemente prohibida la salida de los computadores portátiles del recinto universitario.

- El estudiante deberá firmar un documento de aceptación del conocimiento de la política de seguridad de la información; también firmará un documento que indique el estado en el que se le está entregando el equipo.

- No se permitirá más de un estudiante por computadora.

- El estudiante se deberá hacer responsable de los inconvenientes que se presenten en hardware, software, cableado; si se comprueba que el daño fue hecho a sabiendas, se lo sancionará según el reglamento de disciplina de la universidad.

Sistemas de información

Es responsabilidad del departamento de sistemas del centro de información bibliotecario tomar las debidas medidas en busca del cumplimiento de la política de seguridad de la información y de velar por el correcto funcionamiento de los programas y sistemas destinados para uso de los usuarios.

Las licencias o autorizaciones de uso de programas deberán ser originales y en ningún caso podrán ser extraídas de los computadores del centro de información bibliotecario para uso personal de los usuarios de la información o de terceros.

El departamento de sistemas es el encargado del monitoreo de las actividades de los usuarios de los sistemas de información y son ellos los que establecerán los permisos en el sistema siempre que estos vengan con aprobación del director del departamento de sistemas.

A.7.2 Clasificación de la información

A.7.2.1. Lineamientos de clasificación

El centro de información bibliotecario, a pesar de ser parte de una universidad pública con el objetivo de brindar información acerca de libros a usuarios externos, no puede dar el libre acceso a los datos que proporciona. La información deberá ser clasificada por niveles siempre buscando el cumplimiento de los principios de integridad, confidencialidad y disponibilidad.

Este procedimiento establecerá un esquema de clasificación, a fin de tipificar, manejar y proteger toda la información generada, almacenada, transmitida o procesada en cualquier medio físico y medio de transmisión.

La información deberá ser clasificada de la siguiente manera:

Información pública: Puede ser accedida por todos los niveles internos de la organización y también por los externos.

Información privada: Puede ser accedida sólo por el personal que conforma el centro de información bibliotecario.

Información confidencial: Sólo podrán acceder a este tipo de información personal autorizado por los directores departamentales.

A.7.2.2 Etiquetado y manejo de información

Se etiquetará la información de acuerdo a los lineamientos definidos arriba aumentándoles el origen y destino del documento.

Se utilizarán las palabras: copia, original, borrador.

A.8 Seguridad de los recursos humanos

INTRODUCCIÓN

Para lograr el fiel cumplimiento de la política de seguridad de la información, se debe capacitar a los usuarios o clientes internos de la información. Es necesario

que todos los empleados nuevos o existentes estén conscientes que existe una política y que deben cumplirla; caso contrario, se los sancionará según el reglamento de disciplina de la universidad.

Los controles que se mencionarán aquí se deberán aplicar para garantizar la reducción de riesgos asociados al manejo de información, estos riesgos derivarán exclusivamente de aspectos humanos, como errores, omisiones, fraude.

Los empleados nuevos deberán estar en conocimiento de la política de seguridad de la información al momento de suscribir el contrato de prestación de servicios con la institución, y deberá mantenerse actualizado en este tema en caso de reformas a la política vigente.

ALCANCE

Es aplicable a todo el personal que labore en el centro de información bibliotecario, incluyendo específicamente al área de sistemas. También será aplicable a todos los usuarios internos y externos que brinden soporte a las actividades que realiza el centro de información bibliotecario.

RESPONSABILIDAD

La responsabilidad por la difusión de la política de seguridad de la información por parte del capital humano de la institución será compartida. Para el personal existente, será responsabilidad del encargado del sistema de gestión dar a conocer la existencia de la política; sin embargo, será responsabilidad del departamento de talento humano dar a conocer la política de seguridad al personal nuevo que vaya a ingresar a la institución

Será responsabilidad de los empleados cumplir con las disposiciones especificadas en la política de seguridad de la información.

A.8.1 Antes del empleo

A.8.1.1 Roles y responsabilidades

Será responsabilidad del departamento de talento humano la difusión de la política de seguridad de la información a los aspirantes del cargo a contratar; luego de la difusión, los aspirantes asumirán entera responsabilidad de haber leído y estar de acuerdo con los términos especificados en la política de seguridad para su cumplimiento en caso de aceptar el cargo.

El departamento de talento humano será el encargado de informar al director del departamento de sistemas sobre la contratación de nuevo personal para que le sean dados los debidos accesos.

A.8.1.2 Selección

El departamento de talento humano será el encargado de la selección del personal bajo los requerimientos del director del departamento que solicita el personal y del director del centro de información bibliotecario.

El analista encargado de la selección de dicho cargo deberá informar al director del departamento solicitante de personal, el estado del proceso de selección cuando este lo requiera. Se deberán aplicar pruebas, realizar investigaciones y pedir documentos que acrediten que el aspirante no presente y no haya tenido problemas legales, también se podrán pedir referencias laborales, entre otros documentos.

En el caso de ayudantes de laboratorio se cumplirá con los lineamientos establecidos por la ESPOL para la contratación de estos, adicionando los requerimientos según el cargo que se solicita; por ejemplo, para un analista de redes se necesitará un estudiante de redes, para un desarrollador o programador se necesitará un estudiante de sistemas, etc.

Todas estas evaluaciones y requerimientos específicos del cargo serán realizadas por el director del departamento que solicita el personal.

A.8.1.3 Términos y condiciones de empleo

Todos los empleados y contratistas de la entidad deberán firmar el contrato acordando velar por el cumplimiento de las características de la información (integridad, disponibilidad y confidencialidad).

Al firmar el contrato establecen que están de acuerdo con los términos y condiciones de empleo que además de los requeridos por la institución, serán:

- Firmar un acuerdo de confidencialidad de la información, donde se establezca que no se podrá utilizar información privada de la institución para fines personales o para su divulgación sin autorización expresa del director del centro de información bibliotecario.

- Respetar las condiciones en materia de seguridad de los equipos físicos.

- Aceptar las responsabilidades que tiene con los activos de la información, cuidándolos y protegiéndolos de accesos indebidos.

- Velar por el cumplimiento de la política de seguridad de la información.

A.8.2 Durante el empleo

A.8.2.1 Gestión de responsabilidades

El director del centro de información bibliotecario junto con el responsable del sistema de gestión de seguridad de la información, deberán garantizar que los usuarios internos y externos, incluyendo a las entidades externas que presten servicios, apliquen la política de seguridad de la información en concordancia con los objetivos y políticas organizacionales.

A.8.2.2 Capacitación y educación en seguridad de la información

El responsable del sistema de gestión será el encargado de crear conciencia de los beneficios de las buenas prácticas de seguridad en los usuarios de la información.

Los usuarios internos y externos recibirán adecuada capacitación y actualización periódica en términos de políticas y procedimientos a seguir en busca de la

minimización de riesgos y el mantenimiento de la seguridad de la información. Las capacitaciones por este concepto serán organizadas por el responsable del sistema de gestión junto con el departamento de talento humano de la entidad.

A.8.2.3 Proceso disciplinario

En caso de violaciones a la política de seguridad de la información se impondrán sanciones acorde al reglamento de disciplina de la entidad, siempre que se compruebe la responsabilidad del implicado. Las sanciones las impondrá el tribunal de disciplina de la universidad pública.

A.8.3 Terminación o cambio de empleo

A.8.3.1 Responsabilidades de terminación

Es responsabilidad del departamento de talento la notificación al departamento de sistemas cuando un empleado o contratista termina la relación laboral con la entidad.

Es responsabilidad del departamento de sistemas quitar los accesos físicos y lógicos que haya tenido el empleado o contratista siempre que existe un comunicado formal del departamento de talento humano.

Es responsabilidad del empleado identificar e informar sobre todos los activos de información que estaban a su cargo para su posterior entrega.

A.8.3.2 Devolución de activos

En caso de que el empleado haya terminado la relación laboral con la entidad o viceversa, se deberá gestionar la entrega formal de todos los activos de información (hardware, software, cableado) que estuvieron a su cargo; esta entrega formal se realizará entre el empleado, una persona designada por el responsable del sistema de gestión y el delegado del departamento al que pertenece.

A.8.3.3 Eliminación de derechos de acceso

El departamento de talento humano será el responsable de comunicar al director del departamento de sistemas la salida del empleado, de esta forma se quitarán

los accesos que haya tenido; la inhabilitación de accesos no podrá ocurrir en un lapso superior a 48 horas luego de la salida del empleado.

En caso de compartir información con otros usuarios se procederá al cambio de contraseñas, claves o tarjetas y se notificará a los otros usuarios los nuevos accesos.

El retiro de derecho de accesos deberá gestionarse con la debida anticipación para evitar inconvenientes futuros de fuerza mayor que puedan presentarse.

A.9 Seguridad física y ambiental

INTRODUCCION

La seguridad física es de gran importancia en cualquier institución, por ello se deben establecer ciertos lineamientos para evitar los riesgos que derivan del uso físico y ambiental de los equipos.

Más adelante se observará con mayor detalle las medidas que se tomarán para proteger la seguridad física de los equipos, por ejemplo en los cuartos de servidores se deberán restringir los accesos a personas no autorizadas, así mismo para minimizar el riesgo se deberán resguardar los equipos en áreas

protegidas que eviten que cualquier factor ambiental afecte el funcionamiento de estos.

ALCANCE

Este control será aplicable a todos los equipos físicos que se utilicen en las actividades de procesamiento de información, servidores de base de datos, cuartos de computación, programación, desarrollo, y las actividades destinadas a las operaciones del negocio.

RESPONSABILIDAD

Es responsabilidad del responsable del sistema de gestión de seguridad de la información delimitar el área o perímetro sobre el que se van a tomar las medidas preventivas.

El director del centro de información bibliotecario deberá trabajar en conjunto con el responsable del sistema de gestión en busca de la reducción de riesgos, acatando todas las instrucciones que este requiera y proporcionando facilidades para el desenvolvimiento de sus actividades.

Los empleados serán responsables de acatar las medidas de seguridad establecidas por el responsable del sistema de gestión.

A.9.1 Áreas seguras

A.9.1.1 Perímetro de seguridad física

Se deberá evitar el acceso no autorizado a los recursos tecnológicos que posea la entidad, por lo que se crearán diversas barreras o medidas de control físicas alrededor de los centros de cómputo, departamentos de sistemas, cuartos de servidores y cuartos de procesamiento de datos.

El centro de información bibliotecario establecerá perímetros de seguridad para proteger las áreas, consideradas críticas, que alterarán el correcto funcionamiento de los sistemas de información.

En el caso de los cuartos de servidores y de procesamiento se recomienda que para establecer los perímetros de seguridad se instalen puertas de acceso con lectores biométricos y cámaras de seguridad, sin olvidarse de poner alarmas automáticas y manuales en caso de incidentes (detectores de humo en caso de incendio).

Los lectores biométricos proporcionarán un listado que servirá como registro de ingreso y egreso al área restringida.

Se deberán cumplir normas básicas de higiene para optimizar el desempeño de los recursos tecnológicos y evitar la pérdida de información, se deberán establecer medidas que aseguren la protección de los equipos contra la contaminación ambiental, incendios, inundaciones, etc.

El perímetro de seguridad deberá estar documentado y será aprobado por el responsable del sistema de gestión de seguridad de la información y por el director del centro de información bibliotecario.

Las construcciones deberán ser sólidas, se recomienda que sólo exista una puerta de acceso y una puerta de emergencia al departamento o cuartos de servidores y de procesamiento; no deberán existir brechas que permitan el acceso no autorizado.

Todo cambio en infraestructura deberá ser aprobado por el responsable del sistema de gestión de seguridad de la información y se deberán tomar las medidas preventivas y correctivas de ser el caso.

El responsable del sistema de gestión de seguridad de la información mantendrá un registro actualizado de los sitios protegidos, indicando:

a) Identificación del Edificio y Área.

b) Principales elementos a proteger.

c) Medidas de protección física.

A.9.1.2 Controles de entrada físicos

Para proteger las áreas de seguridad se deberán implementar controles físicos de entrada a estas áreas denominadas como áreas de alto riesgo. El responsable del sistema de gestión de seguridad de la información será el encargado de establecer, mantener y actualizar estos lineamientos en busca del cumplimiento de la política de seguridad de la información.

Se recomienda poner una recepción o un *counter* en el que registren las visitas a las áreas restringidas con fecha de entrada y salida, e identificación del visitante. Los trabajadores podrán sólo a las áreas a las que estén autorizados según las responsabilidades de su cargo y sólo después de validar su huella digital en los lectores biométricos.

Los visitantes deberán tener conocimiento de las normas de seguridad física y de la política de seguridad de la información al momento de ingresar a las áreas.

Los ascensores podrán ser utilizados sólo por personal que labore en el centro de información bibliotecario, bajo ningún motivo, personas no autorizadas podrán utilizarlo.

Se pondrán carteles que indicarán cuáles son las áreas en las que sólo puede ingresar el personal autorizado, estos carteles deberán estar a vista de todas las personas.

Los registros de acceso de áreas protegidos serán revisados por el departamento de calidad de la entidad y quedarán debidamente documentado para auditorías futuras.

A.9.1.3 Seguridad de oficinas, habitaciones y medios

En busca de la protección de los activos de información se deberán seguir las siguientes recomendaciones:

- Prohibir el acceso a las áreas restringidas a las personas no cuenten con la debida autorización firmada por el director del centro de información bibliotecario y por el responsable del sistema de gestión de seguridad de la información.

- Instalar cámaras de seguridad que vigilen las puertas de entrada y salida de oficinas y habitaciones.

- Las llaves de las oficinas sólo las tendrá el personal que trabaje en el espacio destinado, los duplicados o llaves maestro las tendrá el director del centro de información bibliotecario.

- Cuando el personal que labore en determinada área no se encuentre, deberán asegurarse que las ventanas o brechas queden debidamente cerradas.

A.9.1.4 Protección contra amenazas externas y ambientales

Se deberán planificar planes de contingencia y continuidad del negocio en caso de emergencias por amenazas externas y ambientales.

Los cuartos de procesamiento de información y de cómputo no deberán estar en la planta baja del edificio; los cuartos de servidores deberán estar en el piso más alto del edificio, preferiblemente deben estar aislados de otros departamentos, cuartos o accesos.

Se deberá dar mantenimiento constante a los aires acondicionados para evitar que el goteo de estos provoque un cortocircuito o daños en los equipos de cómputo.

Los materiales inflamables o de fácil combustión deberán mantenerse alejados de los cuartos de servidores, de procesamiento de información y de cómputo.

Se deberá contar con extintores y gabinetes contra incendios en todos los departamentos del centro de información bibliotecario, y se tendrán al menos dos de estos en los cuartos de servidores.

A.9.1.5 Trabajo en áreas seguras

En busca del fortalecimiento de la protección en las áreas seguras de la empresa, se establecerán controles que serán aplicables por todas las personas que ejecuten actividades en el centro de información bibliotecario.

- Se prohíbe ingresar con alimentos, bebidas o artículos de fácil combustión a las áreas protegidas de la entidad.

- No se puede conectar o desconectar artefactos eléctricos de uso personal en las áreas protegidas, tampoco se podrá efectuar modificaciones de redes o cableado sin la autorización del director del centro de información bibliotecario, director del departamento de sistemas y del responsable del sistema de gestión de seguridad de la información.

- Está terminantemente prohibido fumar dentro de las áreas seguras.

- A menos que se requiera por temas estrictamente laborales se prohíbe la divulgación de la ubicación de los cuartos de servidores de datos, de procesamiento de información y centros de cómputo.

A.9.1.6 Áreas de acceso público, entrega y carga

Las áreas de procesamiento de información, cuartos de servidores y centro de cómputo, deberán estar alejadas de las áreas de acceso público en busca de la protección de la confidencialidad de la información.

A.9.2 Seguridad del equipo

A.9.2.1 Ubicación y protección del equipo

Los equipos utilizados para el procesamiento y almacenamiento de la información deberán estar debidamente identificados y deberán estar ubicados en los cuartos restringidos destinados exclusivamente para su operación.

Sólo se podrán acceder a los equipos mediante el ingreso de contraseñas de acceso, teniendo en cuenta que a cada empleado se le asignará una contraseña personal que deberá ser cambiada inmediatamente, al momento del primer acceso al equipo o sistema.

A.9.2.2 Servicios públicos

Los equipos deberán estar protegidos de cualquier fallo en servicios públicos que intente interrumpir las actividades normales de estos y la disponibilidad de los sistemas de información. Se deberán implementar controles que ayuden a minimizar el riesgo de estos fallos.

Todas las computadoras del centro de cómputo, cuartos de servidores y de procesamiento de información deberán contar con un sistema de alimentación

ininterrumpida (SAI) en caso de interrupción de la energía eléctrica. El SAI deberá proporcionar a los usuarios el tiempo necesario para que realicen el respaldo y guardado de la información en la que trabajaban.

Los equipos SAI deberán someterse a evaluaciones periódicas para asegurar el correcto funcionamiento por parte de los encargados del mantenimiento de los equipos del centro de información bibliotecario.

A.9.2.3 Seguridad en el cableado

La seguridad de las redes y el cableado son de vital importancia para el logro de los objetivos del centro de información bibliotecario y para el cumplimiento de las políticas de seguridad, es por eso que se deberán cumplir ciertos controles para mitigar los riesgos por intercepción o daños que puedan sufrir:

- El cableado no podrá estar en áreas acceso público.

- Se deberán usar canaletas o tuberías para proteger el cableado. Se debe utilizar de preferencia cableado subterráneo o de techo.

- Establecer un mapa de redes ya actualizarlo según las necesidades o cambios que se den el cableado.

- Utilizar marcadores numéricos para identificar los cables.

- Para evitar interferencias, separar los cables de energía de los cables de procesamiento de información.

- Instalar cajas con cerraduras en los puntos terminales o de inspección.

A.9.2.4 Mantenimiento de equipo

En busca del correcto funcionamiento de los equipos se deberá realizar el mantenimiento de estos para asegurar su disponibilidad e integridad. Para lograr esto se considerará:

- Efectuar mantenimiento a los equipos que integran el centro de información bibliotecario, según los lineamientos establecidos por los proveedores.

- De preferencia efectuar mantenimientos preventivos anuales con técnicos asignados por el departamento de sistemas y en caso que estos no estén en capacidad de realizar los mantenimientos, contratar técnicos especializados en materia de seguridad.

- Llevar un listado que indique los datos de los mantenimientos que se han realizado a los equipos, este listado deberá incluir el nombre del técnico encargado, la fecha del mantenimiento, las actividades realizadas y la firma del supervisor encargado de revisar el cumplimiento del mantenimiento.

- Darle seguimiento a los mantenimientos realizados, verificando el correcto funcionamiento de los equipos.

- Efectuar respaldos de información en el momento previo al mantenimiento del equipo.

A.9.2.5 Seguridad del equipo fuera del local

El centro de información bibliotecario es una institución que brinda servicios a estudiantes y entre estos servicios está el préstamo de laptops. Al referirnos a equipos, nos referimos al hardware e incluye las computadoras portátiles, de escritorio, teclado, mouse, parlantes, etc. Para proteger los intereses y para logar el cumplimiento a cabalidad de la política de seguridad de la información, se deben implementar los siguientes controles:

- Limitar el acceso a computadoras portátiles cuando estas salgan del recinto académico.

- A los empleados les está terminantemente prohibido llevarse los equipos de trabajo fuera de la oficina en la que trabajan.

- En caso de algún incidente con algún equipo cuando este se encuentre fuera del lugar establecido para ejecutar sus funciones, el responsable será la persona que se haya destinado como custodio del activo.

- Se deberán cumplir las instrucciones del fabricante respecto al cuidado de los equipos y sistemas de información.

A.9.2.6 Eliminación seguro o re-uso del equipo

Se deberá asegurar que a los equipos que vayan a ser re-utilizados o desechados se les realice el respectivo respaldo de información para posteriormente formatearlos, esto en busca del cumplimiento de las características de la información (integridad, disponibilidad y confidencialidad)

A.9.2.7 Traslado de propiedad

Equipos, software e información no podrán ser sacados del recinto académico sin la autorización previa del jefe departamental, del director del departamento de sistemas y del responsable del sistema de gestión de seguridad de la información.

A.10 Gestión de las comunicaciones y operaciones

INTRODUCCION

Parte fundamental del desarrollo de las actividades del centro de información bibliotecario es el buen manejo que se tenga en las comunicaciones y operaciones para evitar la propagación de amenazas.

La única manera de garantizar que la manipulación de la información cumpla con las características de integridad, confidencialidad y confiabilidad, es implementando controles que ayudarán en el mitigamiento de estos riesgos. Es fundamental separar las actividades de desarrollo, las de prueba y las operativas para minimizar los riesgos asociados a la manipulación de las comunicaciones y operaciones.

ALCANCE

Es aplicable a toda la organización encargada de la manipulación de información.

RESPONSABILIDAD

Es responsabilidad del responsable del sistema de gestión velar por el cumplimiento de la presente política de seguridad, incluyendo las modificaciones o actualización que se realicen.

Es responsabilidad del departamento de sistemas establecer los lineamientos necesarios en ámbitos de programación e implementación en busca del fiel cumplimiento de la política de seguridad.

A.10.1 Procedimientos y responsabilidades operacionales

A.10.1.1 Procedimientos de operación documentados

Es necesario documentar los procedimientos ejecutados en el centro de información bibliotecario en busca de la constancia y cumplimiento de los lineamientos de seguridad establecidos.

Se deberán documentar los procedimientos y manuales de usuarios en todas las áreas de servicio. Así mismo se documentarán todas las actividades efectuadas en el cargo y los procedimientos de instalación y monitoreo de sistemas de información.

A.10.1.2 Gestión de cambio

Los cambios en el ambiente operativo deberán ser notificados por el responsable de la seguridad de la información

Cualquier cambio en la base de datos de la entidad deberá ser debidamente aprobada por el director del departamento que pidió el cambio y por el director del departamento de sistemas que a su vez asignará a la persona que está a cargo de las actividades de manipulación de activos.

A.10.1.3 Segregación de deberes

Las funciones de los usuarios internos y externos deberán estar segregadas en la organización, teniendo en cuenta que no existan funciones incompatibles que tiendan a dañar los intereses del negocio.

La correcta segregación de funciones las realizará el departamento de desarrollo organizacional junto con el departamento de calidad de la empresa y los directores departamentales; esto para alinear las necesidades organizacionales y departamentales.

A.10.1.4 Separación de los medios de desarrollo y operacionales

Se considera necesario separar los ambientes de desarrollo y de procesamiento de información. Es obligatorio que el área de desarrollo tenga ambientes de prueba para evitar el acceso a datos operativos.

Se deberá evitar bajo toda circunstancia el acceso a códigos fuente a las personas que no tengan que ver con el desarrollo del sistema; los códigos fuente no podrán divulgarse.

Las pruebas realizadas en el departamento de desarrollo serán documentadas y contarán con la aprobación del encargado del área de desarrollo y del director del área de sistemas del centro de información bibliotecario.

A.10.2 Gestión de la entrega del servicio de terceros

A.10.2.1 Entrega del servicio

El centro de información bibliotecario cuenta con alianzas estratégicas con otras bibliotecas nacionales e internacionales para brindar servicios de acceso a libros a estudiantes. En estos casos se deberá contar con parámetros para la entrega del servicio que busquen el logro de los objetivos de la institución y el cumplimiento de la política de seguridad.

La entrega del servicio deberá ser acorde a lo pactado en el contrato, el contrato deberá definir los niveles de servicio. El personal de sistemas será responsable de cumplir con las disposiciones contractuales y de ayudar en todo lo que necesiten las entidades externas.

A.10.2.2 Monitoreo y revisión de los servicios de terceros

Es responsabilidad del departamento de sistemas y del responsable de los sistemas de gestión de seguridad de la información el monitoreo y revisión de los servicios que se mantengan con entidades externas y que estos cumplan con las cláusulas especificadas en los contratos.

A.10.2.3 Manejar los cambios en los servicios de terceros

La universidad, al ser una institución pública, todas sus compras y contrataciones de servicios se harán mediante el portal de compras públicas.

En caso de cambios en los contratos por servicios, estos deberán realizarse según las especificaciones que la legislación vigente establezca para ello.

A.10.3 Planeación y aceptación del sistema

A.10.3.1 Gestión de capacidad

El director del departamento de sistemas y el responsable del área de desarrollo serán los encargados de establecer la capacidad de los nuevos proyectos o sistemas.

En caso de proyectos o sistemas ya existentes deberán hacer un análisis de riesgos y de las nuevas necesidades del centro de información bibliotecario periódicamente en busca del correcto desempeño de los activos de información.

A.10.3.2 Aceptación del sistema

Antes de aprobar el sistema y que esté entre a módulos de producción se deberán evaluar los riesgos y probar la efectividad en busca de posibles errores que puedan existir.

Se deberá efectuar planes de contingencia y continuidad del negocio en casos de fallos del sistema y su capacidad de recuperación.

El responsable del sistema de gestión deberá asegurar haber realizado todos los controles que considere necesario e indicar las posibles fallas que pueda tener, asegurando que este sistema no va a ir en contra de los objetivos organizacionales y de la política de seguridad de la información.

Se deberán efectuar capacitaciones al personal que va a interactuar con el sistema antes de implementarlo en ambiente de producción.

A.10.4 Protección contra software malicioso y código móvil

A.10.4.1 Controles contra software malicioso

En busca de la protección de la integridad, confidencialidad y disponibilidad de la información se deberán seguir los siguientes lineamientos:

- Prohibir el uso de dispositivos de almacenamiento externo en todos los equipos que pertenezcan al centro de información bibliotecario.

- Toda adquisición de equipos deberá ser por medio del portal de compras públicas.

- Se realizarán controles diarios de análisis de virus y de respaldo de información, cualquier software ilegal encontrado deberá ser desinstalado.

- Todos los equipos del centro de información deberán tener activados programas antivirus.

- Se restringirá el acceso a páginas con alto contenido malicioso.

- Los programas utilizados deberán ser licencias oficiales, se deberá poner una barrera (ingreso de usuarios y contraseñas de administrador) para la

instalación de programas en los equipos del centro de información bibliotecario.

A.10.5 Respaldo (back-up)

A.10.5.1 Back-up o respaldo de la información

Es responsabilidad del director del departamento de sistemas designar a responsables para el respaldo de la información.

Los responsables del respaldo de la información deberán estar capacitados en cuanto al uso correcto, manejo y soporte de los sistemas, incluyendo la capacitación y conocimiento de la política de seguridad de la información y los objetivos organizacionales.

Se realizarán respaldos automáticos de la información todos los días a las 02h00, esta información deberá ser encriptada y se deberá realizar y cumplir el plan de pruebas de restauración.

A.10.6 Gestión de seguridad de redes

A.10.6.1 Controles de red

Las tareas de administración de red deberán delegarse a personal que no esté relacionado con actividades de procesamiento de información.

El director del departamento de sistemas será el encargado de administrar y coordinar el mantenimiento, implementación y ubicación de las redes y personal a cargo de ellas, velando por la seguridad de estas y de la información que trasmiten.

Los empleados deberán seguir con las normas dispuestas por el director del departamento de sistemas en busca del cumplimiento de la política de seguridad de la información.

A.10.7 Gestión de medios

A.10.7.1 Gestión de los medios removibles

Sólo se permitirá el uso de equipos removibles al personal que por sus funciones necesite el uso de estos. Este personal será establecido en un documento firmado

por el director del departamento de sistemas y el responsable del sistema de gestión de seguridad de la información, ellos serán los encargados de analizar si el puesto por las funciones necesita el uso de medios removibles.

En caso de uso de medios removibles, el personal deberá cumplir con las normas de seguridad establecidas en el anexo A.7 en busca del cumplimiento de las políticas de seguridad de la información.

A.10.7.2 Eliminación de medios de información

La información que maneja el centro de información bibliotecario debe ser íntegra, por tal motivo se debe tener cuidado en que la información que se proporcione sea real y no sufra de modificaciones; esta información también puede ser eliminada en busca del cumplimiento de este control establecido en la política de seguridad de la información.

En caso que se necesite la eliminación de los datos que ofrece el centro de información bibliotecario se deberá seguir un procedimiento formal establecido por el responsable del sistema de gestión de seguridad de la información y aprobado por el director del departamento de sistemas de la entidad. El procedimiento deberá incluir:

- Autorización escrita de la dirección del departamento afectado indicando la eliminación de los datos.

- Lineamientos a seguir en el proceso de eliminación de la información.

- Confirmación por parte del departamento de sistemas de haber procedido con la eliminación de la información.

A.10.7.3 Procedimientos de manejo de la información

Para garantizar un adecuado manejo de la información, la organización evaluará los posibles riesgos asociados a esta e implementará los debidos controles para mitigar estos riesgos; esto estará a cargo del responsable del sistema de gestión.

Algunos de los procedimientos que se deberán seguir son:

- Los medios de almacenamiento de la información deberán estar en un lugar y ambiente seguro, libre de fuego y humedad. El ambiente concordará con las especificaciones del fabricante del equipo.

- El ingreso de información en la base de datos deberá realizarse de forma manual y segura, pidiendo un usuario y contraseña.

- Los datos deberán no podrán tener accesos que permitan modificarlos cuando los usuarios externos interactúen con el sistema.

- El área de procesamiento de información deberá estar alejada del área de acceso público.

A.10.7.4 Seguridad de documentación del sistema

Se deberá proteger la documentación del sistema de accesos no autorizados, debido a que esta información es confidencial, sólo podrá tener acceso a ella el director del departamento de sistemas y el encargado del área de desarrollo. Las excepciones por la distribución de esta documentación deberán quedar documentada y será aprobada por el director del departamento de sistemas de la entidad.

A.10.8 Intercambio de información

A.10.8.1 Procedimientos y políticas de información y software

El responsable del sistema de gestión de seguridad de la información será el encargado de establecer los procedimientos y políticas asociados al intercambio de información y software con entidades externas.

A.10.8.2 Acuerdos de intercambio

Se deberá establecer de manera contractual los acuerdos y requerimientos que se tengan al intercambiar la información, así como las responsabilidades y obligaciones en caso de pérdida de datos y los términos de licencia o versiones de los equipos a utilizar para este efecto.

A.10.8.3 Medios físicos en tránsito

La entidad externa asumirá entera responsabilidad en caso de mal uso o corrupción de los medios de intercambio de información y se responsabilizarán también de cumplir con las buenas prácticas de los medios que servirán para difundir la información.

Se deberá vigilar por la integridad, confidencialidad y disponibilidad de la información impidiendo el acceso no autorizado a esta, la información se transmitirá de manera encriptada y con niveles de seguridad que dificulten cualquier intrusión que busque modificar la información atentado contra la veracidad.

A.10.8.4 Mensajes electrónicos

Los medios empleados en el uso del correo electrónico para el envío y recepción de mensajes serán administrados por el centro de tecnologías de la información de la universidad pública.

A.10.10 Monitoreo

A.10.10.1 Registro de auditoría

Los accesos a los sistemas de información servirán como prueba en caso de auditorías que se realicen en la institución; el objetivo de las auditorías es asegurar que la información está siendo bien gestionada y que está cumpliendo con las características de confidencialidad, disponibilidad e integridad.

Se deberán realizar monitoreos que indiquen las direcciones IP desde donde se ha accedido al sistema, fecha y hora de acceso y los intentos fallidos para acceder al sistema.

Estos datos se almacenarán en forma encriptada velando por el cumplimiento de la política de seguridad de la información.

A.10.10.2 Uso del sistema de monitoreo

Los monitoreos serán realizados permanentemente, estos se encargarán de verificar que la integridad de los activos de información no está siendo vulnerada, en caso de amenazas a los activos de información se procederá a tomar medidas que boqueen estos intentos de vulnerabilidad.

Los sistemas de monitoreo serán empleados por las personas que el director del departamento de sistemas del centro de información bibliotecario considere necesarios; entre las medidas de seguridad a tomar está la expulsión forzada del sistema del usuario que está cometiendo la infracción.

A.10.10.3 Protección de la información del registro

Se deberá proteger la información de alteraciones y accesos no autorizados estableciendo barreras en el desarrollo y programación del sistema.

Se hará un análisis de riesgos que establecerá las barreras que deberán implementarse, el análisis de riesgos será efectuado por el director del departamento de sistemas en coordinación con el responsable del sistema de gestión de seguridad de la información.

A.10.10.4 Registros del operador y administrador

Las actividades y accesos del administrador, los encargados del procesamiento de información y de los usuarios del sistema deberán ser registradas automáticamente por los medios de respaldo de la entidad.

A.10.10.5 Registro de fallas

Todas las fallas ocasionadas en el sistema deberán mantenerse documentadas, este registro servirá para controlar las fallas y verificar si se les ha dado el mantenimiento respectivo. Las acciones correctivas serán documentadas para su posterior uso.

A.10.10.6 Sincronización de relojes

Los relojes que se utilizarán en todos los equipos pertenecientes al centro de información bibliotecario deberán estar sincronizados con el horario internacional asignado a la zona regional continental de Ecuador (GMT -5)

A.11 Control de acceso

INTRODUCCION

Los sistemas de información deberán contar con un mecanismo que regule los accesos al sistema. Un sistema con restricciones asegurará y brindará la confiabilidad necesaria a los usuarios de la información; para mantener la información protegida se deberán implementar ciertos controles que velen por el cumplimiento de la política de seguridad de la información.

En esta política se incluirán los procesos desde la autorización del acceso a personal nuevo o existente, hasta la finalización o exclusión de los permisos del sistema.

ALCANCE

La presente política será aplicable a toda la organización y a los procesos que interactúen y requieran acceso del sistema, también será aplicable a los administradores, programadores y personal a cargo de la seguridad lógica del centro de información bibliotecario.

RESPONSABILIDAD

El responsable del sistema de gestión de seguridad de la información, será el encargado de la elaboración de las políticas y procedimientos que contribuyan al mejoramiento de la seguridad de la información.

Son responsables los jefes departamentales de solicitar los accesos debidos y necesarios para sus empleados, esta petición deberá ser revisada y aprobada por el responsable del sistema de gestión de seguridad de la información y por el director del departamento de sistemas del centro de información bibliotecario.

El director del departamento de sistemas será responsable de asignar un empelado para que efectúe los requerimientos de acceso lógico del responsable del sistema de gestión.

Es responsabilidad de los usuarios de la información velar por el cumplimiento de la política de seguridad de la información.

A.11.1 Requerimiento comercial para el control de acceso

A.11.1.1 Política de control de acceso

El correcto manejo y desenvolvimiento de los sistemas de información es una de las partes más importantes del centro de información bibliotecario, estas ayudarán a la consecución de objetivos de la organización y de la política de seguridad de la información.

Los accesos a los sistemas de información deberán estar definidos en la presente política que puede estar sujeta a modificaciones y actualizaciones por parte del responsable del sistema de gestión.

Es parte fundamental la difusión de la presenta política y el cumplimiento fiel de los establecido aquí.

A.11.2 Gestión del acceso del usuario

A.11.2.1 Inscripción del usuario

Para poder registrar usuarios en el sistema existirá un procedimiento formal que contendrá en el caso de inscripciones de empleados, el envío de la solicitud de

inscripción del usuario por el director del departamento que esté haciendo la requisición. Esta solicitud deberá enviarse al departamento de sistemas y luego de hacer las validaciones de firma y confirmaciones por mail se procederá a la inscripción del usuario para el acceso a los sistemas de información.

En el caso de estudiantes que requieran acceso en los laboratorios destinados para su uso, la inscripción se realizará una sola vez y será necesario que el estudiante presente su carnet estudiantil, posterior a esto se ingresarán los datos al sistema para validarlos y se habilitará el acceso a los sistemas de información que contenga e laboratorio. Si el estudiante en ocasiones posteriores llegase a utilizar los servicios del laboratorio, ya no va a ser necesaria la inscripción, bastaría sólo la activación de los servicios.

En el caso de des-inscripción de usuarios se ejecutará el mismo procedimiento empleado para la inscripción.

A.11.2.2 Gestión de privilegios

Los empleados podrán contar con privilegios siempre que éstos hayan sido debidamente autorizados por su jefe inmediato y por el director del centro de información bibliotecario.

Al otorgar privilegios, se deberá asegurar que estos no vayan contra las políticas de seguridad de la información establecidas. Estos privilegios se controlarán semanalmente, verificando que los accesos o privilegios otorgados sean los correctos.

A.11.2.3 Gestión de la clave del usuario

La asignación de claves se realizará por medio de un comunicado vía correo electrónico en la que se le dará al usuario una clave temporal que deberá ser cambiada en el primer inicio de sesión.

El listado de claves de los usuarios deberá ser almacenado de forma encriptada para evitar la difusión de la información privada y asegurar la confidencialidad de la información administrada.

A.11.2.4 Revisión de los derechos de acceso del usuario

Los accesos que tienen los usuarios deberán ser revisados de manera que estén conforme a las necesidades de estos y a las funciones de su trabajo para evitar manipulaciones no autorizadas de la información.

A.11.3 Responsabilidades del usuario

A.11.3.1 Uso de clave

Es responsabilidad del usuario el correcto uso y confidencialidad de su clave. Se prohibirá cualquier tipo de divulgación de contraseñas y se obligará al usuario al cambio de su contraseña en un periodo no mayor a 3 meses continuos.

En caso de robo o pérdida de la contraseña el usuario deberá notificar inmediatamente al departamento de sistemas.

A.11.3.2 Equipo de usuario desatendido

Los equipos desatendidos deberán contar con la debida protección por parte del usuario custodio del equipo. Esto incluirá las claves de acceso a equipos que los usuarios posean.

Como método de protección, las pantallas de bloqueo deberán utilizar contraseñas para su desbloqueo, éstas se bloquearan automáticamente luego de que el equipo esté inactivo o desatendido por un periodo no mayor a 20 minutos.

A.11.3.3 Política de pantalla y escritorio limpio

Se deberá proteger la información confidencial de la entidad cumpliendo con lineamientos que aseguren la protección de la información.

La información confidencial deberá guardarse bajo llave y no podrá estar a la vista del público en general; así mismo con los archivos que representen datos importantes del negocio, estos no podrán estar en la pantalla de escritorio de los equipos de cómputo sino que debe estar bien resguardada en carpetas de acceso privado.

A.11.4 Control de acceso a redes

A.11.4.1 Política sobre el uso de servicios en red

Se deberá asegurar que los usuarios no comprometan la seguridad de los servicios en red manteniendo vigiladas las operaciones que realizan.

Las direcciones IP o servicios de red deberán ser estrictamente confidenciales y solo podrán ser conocidas por los usuarios que laboren en el departamento de sistemas de la entidad.

A.11.4.2 Autenticación del usuario para conexiones externas

Una de los principales métodos de intrusión en los sistemas de información son las conexiones externas. Están intrusiones deberán ser gestionadas para minimizar los riesgos asociados a ellas.

Los métodos de autenticación a utilizar podrían ser: Filtrado de paquetes, IDS/IPS, Redes privadas virtuales.

Es el director del departamento de sistemas, en conjunto con el responsable del sistema de gestión de seguridad de la información el encargado de definir el método de autenticación a implementar en la organización según sus necesidades.

Cualquiera que sea la elección del método, deberá contar con un protocolo de autenticación y la verificación del origen de la conexión.

A.11.4.3 Identificación del equipo en red

Es importante que los métodos de autenticación que tiene la entidad aseguren que los equipos conectados en red sean los autorizados. Para lo cual se deben establecer lineamientos que regulen el uso de los equipos de red.

A.11.5 Control de acceso al sistema de operación

A.11.5.5 Sesión inactiva

Se considerará una sesión como inactiva cuando está no haya tenido ningún tipo de manipulación por un lapso no mayor a 20 minutos continuos.

A.12 Adquisición, desarrollo y mantenimiento de sistemas de información

INTRODUCCIÓN

Parte fundamental del avance del centro bibliotecario de la universidad será el desarrollo y la adquisición de sistemas de información, una organización no es una entidad estática sino que está en constante movimiento y avance, se desarrolla constantemente, y los sistemas de información deberán responder a esta nueva realidad, por esto la adquisición debe ser debidamente regulada de manera que se cumplan los requerimientos reales del centro de cómputo

No obstante no siempre bastará con adquirir un sistema de información muy probablemente se requiera el desarrollo de sistemas, en respuesta a la realidad que la institución objeto de estudio muestre, ya que no todos los sistemas disponibles en el mercado son necesariamente los mejores para la realidad y entorno del centro

Se deberá documentar debidamente cuales son los requerimientos tanto de seguridad como de sistemas, además se deberán implementar los respectivos controles para verificar que el sistema desarrollado o adquirido cumple con los requerimientos previamente señalados.

Los desarrolladores y analistas del centro de cómputo también deben regirse por una serie de directrices que garanticen que sus labores se estén llevando a cabo dentro del marco y las exigencias que el centro establezca, se buscará con esto evitar los riesgos asociados a una inadecuada gestión de los sistemas y recursos del centro.

También se deberá definir los métodos para proteger la información crítica y sensible durante la fase de desarrollo de los sistemas de información, y establecer procedimientos para cada ciclo sea de adquisición o de desarrollo.

ALCANCE

Las directrices que se establezcan en esta política se aplicarán a todas las aplicaciones del centro de información bibliotecario sean éstas adquiridas o desarrolladas, se extenderá también a las aplicaciones que tanto usuarios internos y externos y terceros usen para cumplir con las operaciones del centro de cómputo

RESPONSABILIDADES

La responsabilidad de establecer los controles que se implementarán en los sistemas que se desarrollen o en su defecto se adquieran estará a cargo del supervisor de sistemas, quien realizará estas gestiones enmarcado en una gestión adecuada de los riesgos.

Será función de la directora de sistemas del centro bibliotecario el establecer cuáles son las necesidades de sistemas y aplicativos que tiene el centro, y ella en conjunto con el supervisor de sistemas será quién se encargue de establecer y gestionar como suplir estas necesidades.

Adicionalmente el supervisor de sistemas del centro deberá documentar todo lo inherente a las licencias y a la calidad del software que se adquiera, también gestionarán todo lo inherente al desarrollo de sistemas, sea esto contratos con terceros, lo cual deberá ser verificado por el responsable legal del centro bibliotecario.

En caso de que el desarrollo del sistema de información sea interno, es decir que se gestione el desarrollo de los sistemas de información por los mismos empleados del centro de cómputo se deberá establecer un mecanismo de evaluación para verificar los lineamientos, requerimientos y que éstos estén siendo respetados por los desarrolladores del sistema.

A.12.1 Análisis y especificaciones de los requerimientos de seguridad

Para un correcto análisis de los requerimientos de seguridad se deberán tener en cuenta las siguientes directrices:

1.- Realizar el establecimiento de requerimientos, y que se gestione adecuadamente los riesgos asociados a la adquisición o desarrollo de un sistema, esto deberá servir para identificar adecuadamente los controles que se debe implementar

2.- Hacer un análisis tanto cuantitativo y cualitativo que incluya análisis de cualidades, análisis de costos y beneficios previa aplicación de un sistema de información

3.- Hacer un somero análisis de implementación del sistema y de los controles que se deriven posterior a la implementación de los sistemas.

A.12.2 Seguridad en los sistemas de información

Se deberán verificar los datos de entrada, los procedimientos internos y las autenticaciones de mensajes y la validación de datos de salida, para todas estas cosas se deberán establecer procedimientos que adecuadamente permitan gestionar la seguridad de los sistemas de información

En lo referente a la validación de datos de entrada se debe establecer un procedimiento que regule la validación de los datos de entrada en la fase de diseño se deberán evaluar controles de secuencia, controles de redundancia, controlar que valores se cargan, se deberá controlar la parametrización correcta tanto de los datos como de los campos donde se ingresan los mismos.

Se deben establecer procedimientos para revisar periódicamente los archivos de datos y los campos de ingreso, con el fin de resguardar la integridad y veracidad de la información que se ingresa.

Adicionalmente se deberá definir procesos y asignación de responsabilidades de todo el personal que esté involucrado en la entrada de datos.

También se diseñarán procesos que permitan verificar el orden correcto de ejecución de los aplicativos, y además cuales serían los procesos a seguir en caso que una o más aplicaciones fallen.

Para garantizar la confidencialidad de la información se deberán seguir controles criptográficos que validen los mensajes que son enviados por el sistema y la transmisión de datos considerados críticos.

A.12.3 Controles criptográficos

A.12.3.1 Política de controles criptográficos

Se vuelve necesario el uso de sistemas de encriptación. El uso de estos sistemas garantiza la protección de información así como permite velar por la integridad y confidencialidad de los datos que el centro de cómputo maneja

Se establecerá el uso de controles criptográficos en estas situaciones:

- Protección de claves de acceso.
- Resguardo de información sensible que se maneje dentro del centro bibliotecario.
- Información que se transmita de una entidad adscrita al centro bibliotecario y viceversa.

La administración de las claves estará a cargo de del departamento de Sistemas, no de una sola persona sino de todos quienes integren el área de sistemas.

Se busca de manera especial que los controles criptográficos cumplan con los principios de seguridad de la información, mediante el uso de codificación y de firmas digitales.

A.12.3.2 Gestión de claves

La gestión y protección de claves deberá cubrir los siguientes lineamientos:

- Generar claves para diferentes aplicaciones.

- Obtención de certificaciones de clave pública.

- Desarrollo de mecanismos de transmisión de claves a los usuarios del centro.

- Cambio y actualización regular de claves.

- Recuperación de claves perdidas.

- Auditoría del uso de claves por parte de los usuarios tanto internos como externos.

A.12.4 Seguridad de los archivos del sistema

Se deberá designar un responsable para cada sistema o aplicativos que el área de sistemas del centro bibliotecario desarrolle, y se restringirán los accesos al sistema por parte de los desarrolladores, es decir el encargado de desarrollo no necesariamente tiene que tener acceso a funciones del sistema que no le competen.

Se debe controlar estrictamente la instalación de modificaciones que se hagan en los sistemas de información de la organización, para realizar estas instalaciones

se deberá contar con la aprobación de la directora de sistemas así como haber realizado los *testings* necesarios para verificar el cumplimiento de todos los requerimientos.

Importante también es mantener actualizada la actividad y las actualizaciones que el sistema sufre, es importante que el implementador no tenga nada que ver con el desarrollo previo del sistema, se deberá restringir su acceso a la codificación de la aplicación.

Se deberá garantizar una segregación de funciones correcta; es decir el responsable de desarrollo no deberá intervenir en la implementación de la aplicación.

Se deberá adicionalmente designar un funcionario que administre todos los códigos fuente de la organización, el cual deberás mantener documentado que programas tiene a su cargo, que versión de programa posee, y quién es el analista responsable de dicha aplicación.

A.12.5 Seguridad en los procesos de desarrollo y soporte

Se deberá implementar una política de control de cambios que contemple lo siguiente:

- Se deberá documentar debidamente cualquier solicitud de cambios en el sistema que se quiera realizar

- Que se documente de manera correcta cuales son los niveles de acceso para efectos de modificaciones

- Se deberá identificar que elementos requieres modificación

- La única manera de avalar un proceso de cambios será la autorización de la directora del área de sistemas

- Los usuarios de las aplicaciones sometidas a cambios deberán ser notificados oportunamente de los mismos.

Para evitar filtraciones de información o presencias de códigos maliciosos se deberá calificar debidamente a los proveedores de los sistemas de información, además permanentemente se deberá verificar el acceso al código fuente de los sistemas adquiridos para garantizar que no se presenten modificaciones.

A.12.6 Gestión de vulnerabilidades técnicas

Se deberá establecer una normativa para gestionar vulnerabilidades que contemple los siguientes aspectos:

- Se deben establecer responsables de monitorear, evaluar y corregir las vulnerabilidades que se pudieren presentar en el centro

- Inmediatamente a la detección de una vulnerabilidad se deberá realizar le respectiva gestión de riesgos y establecer los mecanismos de acción que se tomarán

- De ser necesario se deberán aplicar actualizaciones para mitigar las vulnerabilidades detectadas

- Para garantizar la eficiencia y eficacia de la gestión de vulnerabilidades éste deberá ser monitoreado frecuentemente

- Las vulnerabilidades presentes en sistemas críticos deberán ser tratados primero

A.13 Gestión de incidentes de seguridad de información

INTRODUCCIÓN

El centro bibliotecario a pesar de sus esfuerzos por mitigar riesgos asociados a la información siempre va a tener incidentes que vulneren la seguridad informática, esta sección buscará asegurar una correcta gestión y establecerá planes de acción adecuados para poder tratar oportunamente, y eficientemente los incidentes asociados a la información que se presenten.

Se buscará establecer los mecanismos necesarios para reportar oportunamente y correctamente los incidentes que se presenten, se buscará además documentar las acciones correctivas que se tomen para así lograr más experiencia dentro del centro y en lo posterior tener una respuesta más ágil ante cualquier eventualidad dañosa que se presente.

ALCANCE

Se aplicará esta política al tratamiento de eventualidades dañosas, incidentes y vulnerabilidades de todos los sistemas de información y aplicaciones que se utilizan dentro del centro de información bibliotecario, así como las vulnerabilidades presentadas en bibliotecas seccionales, se buscará que el

personal del área de sistemas esté en la capacidad de atender oportunamente éstas vulnerabilidades.

RESPONSABILIDAD

En el caso de existir incidentes asociados a la seguridad de la información será responsabilidad del analista principal de sistemas atenderlas, y gestionar acciones para cada incidente que se presente, además todo el personal del área de sistemas estará inmerso en la gestión de los incidentes que se pudieren presentar.

A.13.1 Reporte de eventos y debilidades de la seguridad de la información

Se vuelve necesario que todos los eventos relacionados a incidentes de seguridad deberán estar regulados y debidamente documentados, con miras a lograr una correcta toma de decisiones respecto a las vulnerabilidades tratadas.

Todos los usuarios tanto internos como externos del centro bibliotecario deben hacer conciencia de sus responsabilidades, de manera especial la responsabilidad de notificar oportunamente cualquier incidente que vulnere la seguridad.

Este procedimiento debe seguir con una serie de lineamientos:

- Se deberá establecer un formato adecuado para reportar los eventos de seguridad para tener un sustento que en lo posterior justifique las acciones correctivas que se seguirán.

- No se deberá gestionar un incidente de manera personal éste deberá ser gestionado al analista principal de sistemas, para esto el desarrollo de un *help desk* sería una buena opción.

- Se debe gestionar un manual de sanciones para los usuarios que cometan violaciones contra los procedimientos de seguridad.

- La evidencia que se recabe deber ser correctamente documentada y sustentada de manera que ésta fuere admitida incluso en situaciones de orden legal.

A.14 Gestión de continuidad de operaciones

INTRODUCCIÓN

Ante cualquier eventualidad dañosa que ponga en peligro la continuidad de las operaciones dentro del centro de cómputo de la biblioteca central se deberá

establecer un plan detallado que contemple las acciones a seguir y los caminos a tomar para lograr una continuidad de las operaciones, se deberán establecer planes de contingencia para poder gestionar la seguridad de información ante un incidente que detenga las operaciones del centro, en estos casos se deberá tomar medidas que permitan que el impacto de estas paralizaciones no sea tan alto para la organización.

Esta política buscará minimizar al máximo las pérdidas que se pudieren derivar de paralizaciones de las actividades, buscando resguardar los activos, los recursos informáticos y principalmente la información, sean estos incidentes accidentales o sea causado por factores naturales.

ALCANCE

Se aplicará esta política en todo el centro bibliotecario que tiene una interacción con los sistemas de información, así como todos los recursos informáticos y bases de datos que se utilizan dentro del centro bibliotecario.

RESPONSABILIDAD

La directora del área de sistemas de la biblioteca será parte fundamental en la documentación y diseño de una política de continuidad de las operaciones.

Los analistas de sistemas también tomarán responsabilidad en este desarrollo, y serán responsables de identificar las amenazas que pudieren derivar en interrupciones, se deberá también evaluar los riesgos e identificar sus respectivos impactos.

Se deberá también proceder a la evaluación de los controles preventivos que se están aplicando actualmente en el centro. Las soluciones propuestas son de responsabilidad del personal de sistemas del centro.

A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio

Se deberá comprender los riesgos analizando su impacto y su probabilidad de ocurrencia en el entorno del negocio, y en base a este análisis se deberá identificar los riesgos más críticos que requerirán de atención urgente, hasta los de menos prioridad, sin descuidarles completamente.

Se debe de diseñar los planes de contingencias y continuidad necesarios para evitar interrupciones en los servicios y funcionalidades del centro de cómputo y minimizar el impacto que dichas paralizaciones pudieren causar.

Es vital que el plan de continuidad de las operaciones identifique, procesos, recursos y la información que se considere crítica, además se vuelve necesario que esta política se acople correctamente a las demás políticas organizacionales de la universidad.

Se vuelve imperante que se evalúen los riesgos asociados a la continuidad de las operaciones, se debe estimar los impactos de ocurrencia y diseñar procedimientos que hagan que el impacto sea menos y no se interrumpan las operaciones.

Preferentemente esta revisión no debe ser solo realizada por el área de sistemas, sino que deben intervenir todas las áreas de la entidad adscrita que son parte de la interacción de los sistemas de información, se deben considerar los servicios de devolución y préstamos de libros, los asociados a laboratorios, los préstamos de computadoras de escritorio y portátiles, que son las funciones que el sistema de información ha desarrollado.

Parte fundamental de esta política también es capacitar al personal sobre el plan de continuidad de operaciones, las directrices que se seguirán y las técnicas y procedimientos a aplicar, para que así este plan en caso de ser requerido sea conocido y aplicado por todos los miembros del área de sistemas.

Orientados a la mejora continua esta política y estos procedimientos de continuidad deberán ser periódicamente sometidos a evaluaciones técnicas para garantizar un mejoramiento continuo de los procesos.

A.15 Cumplimiento regulatorio

INTRODUCCIÓN

Esta política de seguridad de la información será aplicada a todos los procedimientos del centro de información bibliotecario de una entidad de educación superior y es deber de ésta entidad cumplir muy someramente esta política.

Cada disposición aquí mencionada deberá ser debidamente cumplida para evitar sanciones disciplinarias por el incumplimiento de las mismas, se deberá también garantizar que cada proceso, y sistema cumpla con la política que aquí se ha establecido.

Es prioritario garantizar mediante evaluaciones periódicas que el sistema y todos los recursos informáticos cumplen a cabalidad con la política de seguridad de la información.

ALCANCE

Se aplicará a todo el personal del centro bibliotecario sean usuarios internos o externos, sean miembros del área de sistemas o de otras áreas de la biblioteca, además se aplicará esta política a todos los sistemas de información que el centro maneja así como sus recursos informáticos.

RESPONSABILIDADES

Es responsabilidad de todo el área de sistemas y de todo el personal del centro de información bibliotecario el conocimiento de la política de seguridad así como su correcta aplicación y su adecuada difusión a los usuarios interesados, además velar constantemente por el cumplimiento de la política es responsabilidad de la encargada del centro bibliotecario, por lo que de ser necesario se deberá establecer evaluaciones que muestren si se está o no cumpliendo con la política de seguridad.

A.15.1 Cumplimiento de las políticas y estándares de seguridad y cumplimiento técnico

Periódicamente se debe verificar el cumplimiento de la política y ante cualquier incumplimiento se debería determinar que motivó el incumplimiento, cual fue el impacto derivado de esa falta y cuál fue la corrección que se tomó al respecto.

Cabe destacar que toda acción de incumplimiento debe ser documentada para analizar futuros incidentes y factores de reincidencia y poder facilitar una mejor toma de decisiones.

Los análisis técnicos deberán ser realizados por el analista principal de sistemas buscando siempre que los chequeos no comprometan la seguridad de la información, en caso de detectar vulnerabilidades, éstas deberán ser tratadas inmediatamente.

CAPÍTULO V

5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Una vez que se realizó el estudio en el centro bibliotecario pudimos evidenciar una serie de debilidades, las cuáles de no ser debidamente gestionadas podrían traer consigo eventualidades dañosas que pongan en peligro al centro bibliotecario.

La seguridad de la información en el centro Bibliotecario es del 37,42% una cifra alarmante considerando los volúmenes de información que la biblioteca tiene a su cargo

No se ha gestionado correctamente la seguridad de los recursos humanos, debido especialmente a la falta de segregación de funciones, y a la falta de existencia de controles al personal que ahí labora

No se encontró una política de seguridad informática adecuadamente definida, si bien hay lineamientos establecidos de seguridad, no existe una política integrada que abarque todos los objetivos de control, es necesario la creación de una política de seguridad en el marco de la normativa ISO.

Uno de los problemas de mayor dificultad en el centro es que por varias dificultades no se realiza una segregación de funciones en el centro, a pesar de que tienen documentadas las funciones y los procedimientos en la realidad esto no se cumple.

Se diseñó una política de seguridad informática acorde a la realidad del centro informático, de seguir esta política como se indica se garantiza que el 37% de seguridad de la información podrá mejorar, disminuyendo vulnerabilidades del centro.

No se encontró evidencia de que exista un plan de continuidad en las operaciones del centro, lo cual constituye un riesgo informático alto, ya que si no se posee un plan de contingencias no habrá respuestas ante una suspensión de las operaciones, para lo cual se sugirió el diseño de una política de continuidad de operaciones.

5.2 Recomendaciones

Se recomienda un rediseño de la estructura organizacional, en función de las necesidades actuales del centro de información bibliotecario, esto logrará una adecuada segregación de las funciones y se logrará mejorar la eficiencia en las

operaciones del centro Bibliotecario, si bien definir funciones y puestos puede resultar costoso esto garantizaría una correcta gestión de la seguridad de los recursos informáticos

Es recomendable que el centro gestione un plan de continuidad de operaciones que pueda disminuir el riesgo asociado a la seguridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

(1) Sistema de Gestión de Seguridad de la Información. (Disponible en http://www.iso27000.es/sgsi.html. Consultado el: 20 de Junio del 2013).

(2) ¿Qué incluye un Sistema de Gestión de Seguridad de la Información? (Disponible en http://www.iso27000.es/sgsi.html#section2c. Consultado el: 20 de Junio del 2013).

(3) ISO/IEC 27001:2008. 2008.

(4) DIAZ, A. 2010. Gestión de Riesgos/ Sistema de Gestión de Seguridad de la Información UNE-ISO/IEC 27001. (Disponible en http://www.aec.es/c/document_library/get_file?p_l_id=32315&folderId=195657&name=DLFE-7132.pdf Consultado el: 23 de Junio del 2013).

(5) LARDENT, A.R. 2001. Sistemas de Información para la Gestión Empresarial. Argentina. Prentice Hall. 443 p.

(6) BUENAÑO Q, J.L. 2009. Planeación y diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001-27002. Tesis Ing. Guayaquil, Univ. Politécnica Salesiana, Fac. Ing. 205 p.

6 ANEXOS

POLITICA DE CONTROL

DE CAMBIOS

CENTRO DE INFORMACIÓN

BIBLIOTECARIO CIB - ESPOL

INDICE GENERAL

1 PROPÓSITO 187

2 ALCANCE 187

3 OBJETIVO 187

4 AMBIENTES DE CONTROL 188

5 CAMBIOS EN APLICACIONES 188

6 ACTUALIZACIÓN DE VERSIONES 189

7 CAMBIOS EN INFRAESTRUCTURA 189

8 PROCEDIMIENTOS DE REGRESION (BACKOUT) 190

1. PROPÓSITO

El propósito de esta política es administrar y controlar los cambios realizados durante las etapas de desarrollo y soporte de los procesos para brindar seguridad a la unidad minimizando el riesgo asociado a éstos.

2. ALCANCE

Esta política es aplicable a toda la unidad, específicamente al departamento de desarrollo y soporte en caso de actualización o modificación de los procesos.

Todos los empleados deberán cumplir con la presente política, las violaciones serán sanciones de acuerdo al código de ética de la institución educativa.

3. OBJETIVO

El cumplimiento de esta política tiene como objetivo proporcionar estabilidad a los usuarios internos y externos respecto al uso del sistema y de los procesos vinculados, gestionando y controlando los cambios producidos en los diferentes procesos de desarrollo de la entidad.

Los usuarios deben ser informados de los cambios, los cambios deberán ser analizados, documentados, aprobados y programados.

4. AMBIENTES DE CONTROL

Todo cambio en las aplicaciones deberá pasar por tres ambientes:

Ambiente de Desarrollo: En este ambiente se desarrollaran y programaran las aplicaciones.

Ambiente de Prueba: Ambiente donde los cambios podrán ser probados en el que existe una base de datos ficticia para estos efectos.

Ambiente de Producción: Ambiente final, listo para el público; utilizado cuando la aplicación ya ha sido desarrollada y ha pasado por pruebas verificando su correcta funcionalidad.

5. CAMBIOS EN APLICACIONES

El Desarrollador Senior será el encargado de revisar y aprobar todos los cambios que se efectúen en las aplicaciones siempre que éstas estén en etapa de desarrollo y no se las haya implementado.

Todos los cambios ocurridos desde la etapa de implementación, sean planificados (programados por anticipado) o no planificados (emergencia)

deberán cumplir con la revisión y aprobación del Director del CIB o a quien éste haya delegado, adicional a la aprobación del Desarrollador Senior.

Cualquier modificación realizada posterior a la etapa de implementación deberá quedar documentada y contará con las firmas respectivas de los encargados de las aprobaciones.

Todo cambio deberá ser evaluado en el ambiente de prueba para buscar concordancia con los requerimientos por los que se pidió el cambio.

6. ACTUALIZACIÓN DE VERSIONES

Las actualizaciones de versiones realizadas en la etapa de desarrollo se las manejará a través de GITHUB; todos los desarrolladores previo a la subida de versiones, están obligados a descargar la versión anterior, trabajar en esta, y subir los nuevos datos al sistema para generar una nueva versión.

7. CAMBIOS EN INFRAESTRUCTURA

Todos los cambios en infraestructura (hardware, redes, estaciones de trabajo) deberán ser controlados por el Analista Senior de sistemas y deberán ser aprobados por el Director del CIB.

8. PROCEDIMIENTOS DE REGRESION

El Desarrollador Senior, y sólo él, tiene la potestad de degradar (asignar un grado más bajo) la versión del desarrollo del sistema.

	Centro de Información Bibliotecario	**Fecha de Creación:** Octubre 01/2013	
Política de Control de Cambios		**Creado por:** Alan Lugmania Medina	
Versión: 1.1		**Reemplaza:** N/A	

MANUAL Y POLITICA DE USO

DE RECURSOS INFORMATICOS

CENTRO DE INFORMACIÓN

BIBLIOTECARIO CIB - ESPOL

INDICE GENERAL

1 SEGURIDAD DE LA INFORMACIÓN - PRINCIPIOS 193

1.1 PRINCIPIO DE PROPIEDAD DE LA INFORMACIÓN 193

1.2 PRINCIPIO DE PROTECCIÓN DE LA INFORMACIÓN 194

1.3 PRINCIPIO DE PROTECCIÓN DE LA RECURSOS TECNOLÓGICOS 194

1.4 PRINCIPIO DE ORIENTACIÓN AL CUMPLIMIENTO DE LA MISIÓN DE ENTIDAD .. 194

1.5 PRINCIPIO DE AUTORIZACIÓN DE USUARIOS 195

1.6 PRINCIPIO DE RESPONSABILIDAD 195

1.7 PRINCIPIO DE DISPONIBILIDAD 196

1.8 PRINCIPIO DE INTEGRIDAD 196

1.9 PRINCIPIO DE CONFIANZA 196

2 NORMATIVA 197

3 FRENTE AL CUMPLIMIENTO 198

1. SEGURIDAD DE LA INFORMACIÓN - PRINCIPIOS

Los siguientes principios básicos fundamentan las Políticas de Seguridad de los Activos de Información y toda la arquitectura informática electrónica del centro bibliotecario.

1.1. PRINCIPIO DE PROPIEDAD DE LA INFORMACIÓN

Los activos de información que son propiedad de la Biblioteca Central son entregados para su uso, operación o custodia al personal a quien se aplica esta reglamentación, de acuerdo a las funciones específicas y necesidades derivadas de las actividades que deban realizar, sin que esto altere en ningún momento la propiedad de los mismos que seguirá estando a nombre del centro bibliotecario, aunque dentro de las funciones específicas se nombre dentro de la cadena de custodia u operación un propietario de cada activo de información. Este nombramiento como propietario, se hará únicamente, con el fin de asignar las responsabilidades operativas y de custodia sobre los diferentes activos.

1.2. PRINCIPIO DE PROTECCIÓN DE LA INFORMACIÓN

Los activos de información serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida de la Biblioteca. La protección debe acentuar la confidencialidad, integridad y disponibilidad de los activos de información.

1.3. PRINCIPIO DE PROTECCIÓN DE LOS RECURSOS TECNOLÓGICOS

Los recursos tecnológicos serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida de la biblioteca. Dichos recursos deben ser utilizados exclusivamente para desarrollar actividades relacionadas con los procesos misionales de docencia, investigación, extensión y de desarrollo humano y bienestar y los laborales y de apoyo que de ellos se deriven. Así mismo su utilización se hará en forma adecuada, con el máximo de eficiencia y Responsabilidad.

1.4. PRINCIPO DE ORIENTACIÓN AL CUMPLIMIENTO DE LA MISIÓN DE LA ENTIDAD

El espíritu de estas políticas es el de mejorar la operación y seguridad de la información del centro Bibliotecario, por lo que se debe evaluar las necesidades

de la Institución y vigilar el cumplimiento de dichas políticas, por lo que se admite que al evaluar de manera adecuada una solicitud, se puedan tomar acciones documentadas, que sin estar en total cumplimiento de la política, pueden tipificar necesidades reales de la entidad adscrita, sin romper los procesos de evaluación de alternativas y plantear modificaciones o excepciones documentadas a la misma.

1.5. PRINCIPIO DE AUTORIZACIÓN DE USUARIOS

Todos los usuarios deben ser identificados independientemente con permisos de acceso específicos e individualmente autorizados por razones básicas de la biblioteca. Los métodos de acceso de usuarios deben exigir un proceso robusto de autenticación, autorización apropiada y auditoria confiable.

1.6. PRINCIPIO DE RESPONSABILIDAD

Los usuarios, depositarios y custodios de los activos de información de la unidad bibliotecaria son responsables por el uso apropiado, protección y privacidad de estos activos. Los sistemas de la biblioteca generarán y mantendrán unas apropiadas pistas de auditoria para identificar usuarios y documentar acciones relacionadas con situaciones violatorias de la seguridad.

1.7. PRINCIPIO DE DISPONIBILIDAD

El centro de información bibliotecario debe tener a entera disposición de los usuarios los recursos informáticos lo cual puede ayudar e resolver eventualidades dañosas, y permitirá que se recupere correctamente la información.

1.8. PRINCIPIO DE INTEGRIDAD

Los activos de información deben estar adecuadamente protegidos para asegurar su integridad y precisión. Las medidas de validación definidas permitirán detectar la modificación inapropiada, eliminación o adulteración de los activos de información.

1.9. PRINCIPIO DE CONFIANZA

Los usuarios, internos y externos deben demostrar capacidad para reunir o exceder los requerimientos de seguridad de la biblioteca y justificar la confianza en sus capacidades para asegurar los activos de información de la unidad.

2. NORMATIVA

Se considera uso adecuado de los recursos tecnológicos del centro bibliotecario los siguientes ítems:

- El Almacenamiento de la información requerida para el desarrollo de las actividades laborales en los equipos y sistemas de información que son suministrados por la biblioteca para este fin, evitando tener dicha información en otros equipos o dispositivos.

- Solo se debe tener información o sistemas de información cuando se tenga la certeza de que no se está violando los derechos de propiedad, lo que implica evitar utilizar, recibir, mantener o copiar información o sistemas de información, que estén protegidos por leyes de derechos de autor, así como la distribución y/o instalación de software “pirata” u otros productos que no estén licenciados por la entidad bibliotecaria, incluidos fotografías de revistas, libros, música u otras fuentes.

- No hacer uso de los recursos informáticos para ver material pornográfico y obsceno, además de acceder a sitios web maliciosos.

- El escaneo de puertos o el análisis de tráfico y vulnerabilidades de la red con el propósito de evaluar vulnerabilidades de seguridad, sólo se considera adecuado cuando se lleve a cabo por parte de los encargados de la seguridad de la información en el centro bibliotecario.

- No permitir el acceso a la red de equipos que no han sido previamente autorizados por el centro bibliotecario.

- El uso de los servicios de telefonía debe ser orientado al cumplimiento de los objetivos misionales y del cargo para el cual fue contratado y evitar otros usos sin las debidas autorizaciones.

3. FRENTE AL INCUMPLIMIENTO

El incumplimiento de estas normas, podría acarrear de parte del centro bibliotecario: Suspensión del servicio inmediato a infractores, restricciones o suspensiones temporales para utilizar servicios y demás acciones pertinentes.