ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

DESARROLLO DE UN PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL CENTRO DE EDUCACIÓN CONTINUA DE LA ESCUELA POLITÉCNICA NACIONAL

PROYECTO PREVIO A LA OBTENCIÓN DE TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

UCHUPANTA MOLINA JORGE ANDRÉS

jaum7790@gmail.com

DIRECTOR: MSc. Ing. CESÁR GUSTAVO SAMANIEGO BURBANO

gustavo.samaniego@epn.edu.ec

Quito, Enero 2015

DECLARACIÓN

Yo, Jorge Andrés Uchupanta Molina, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondiente a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Jorge Andrés Uchupanta Molina

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Jorge Andrés Uchupanta Molina, bajo mi supervisión.

_____

MSc. GUSTAVO SAMANIEGO

DIRECTOR DEL PROYECTO

DEDICATORIA

Les dedico este proyecto de titulación a mis padres Jorge y Carlota por siempre haber estado ahí para mí, brindarme su apoyo siempre que lo necesite, y que gracias a sus enseñanzas soy la persona que soy.

A mis hermanas Ximena y Norma por siempre darme un consejo cuando lo necesite y más que ser mis hermanas ser mis amigas.

A mis amigos de la FIS que fueron mi segunda familia y estuvieron en el malo y bueno momento mientras avanzaba en mis estudios, gracias por ser los mejores amigos que alguien podría tener.

A mi director de Tesis quien nunca dudo en dar su guía durante la realización del proyecto dando las directrices necesarias para cumplir de la mejor manera con el mismo.

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

El presente proyecto formula un Plan de Gestión de Seguridad Informática para el Centro de Educación Continua de la Escuela Politécnica Nacional (CEC-EPN).

El Plan constituirá la propuesta del Sistema de Gestión de Seguridades de la información con el fin de manejar el riesgo y mejorar la seguridad de la Información para entregar resultados que se ajusten a las políticas y objetivos generales del Centro de Educación Continua de la Escuela Politécnica Nacional (CEC - EPN), mediante la utilización de los estándares ISO/IEC 27001 e ISO/IEC 27002, de los cuales seleccionaremos los objetivos de control y controles que puedan ser implantados dentro del Centro de Educación Continua (CEC).

RESUMEN

Actualmente, el Centro de Educación Continua de la Escuela Politécnica Nacional no cuenta con un plan de Gestión de la Seguridad de la Información. Por ello los procesos de este no se encuentran formalizados e integrados a un Sistema de Gestión de la Seguridad de la Información, lo cual ha provocado que no se lleve un manejo seguro de la información interna del mismo lo que expone a la institución a un grave riesgo de seguridad de su información. Por ello se plantea un plan de Gestión de Seguridad de la Información que permita asegurar la protección de la información e incrementar la confianza del personal administrativo y de los estudiantes en el CEC-EPN.

Capítulo 1: Este capítulo se enfocará en la realización de un estudio de vulnerabilidades y análisis de riesgos con la herramienta MSAT y la aplicación de la Guía NIST 800-30, con el fin de conocer los niveles actuales de seguridad de la información e identificar los requerimientos de seguridad del CEC-EPN.

Capítulo 2: Este capítulo se enfocará en la selección de objetivos de control y controles de la ISO/IEC 27002, con el fin de cubrir los requerimientos de seguridad encontrados.

Capítulo 3: Este capítulo contiene las directrices necesarias para la implantación de los controles seleccionados.

Capítulo 4: Este capítulo contempla las conclusiones y recomendaciones obtenidas por el autor del proyecto una vez realizado el mismo.

CAPÍTULO 1: DIAGNOSTICO DE VULNERABILIDADES Y RIESGOS DEL CENTRO DE EDUCACIÓN CONTINUA.

1.1. RECONOCIMIENTO DEL CENTRO DE EDUCACIÓN CONTINUA.

En el año 1989 la Escuela Politécnica Nacional firma un convenio con el Ministerio de Educación, para capacitar a profesores secundarios.

Desde el año 1991 hasta el año 1995, el Centro prestó servicios de capacitación y actualización a diferentes empresas e instituciones, sin embargo en mayo de 1995 fue creado como Centro de Educación Continua, mediante normativa de la Escuela Politécnica Nacional, con la finalidad de impartir conocimientos y desarrollar actividades académicas que propendan a la actualización permanente de conocimientos de los miembros de la comunidad de la Escuela Politécnica, de los egresados de la institución, de las empresas públicas y privadas y de la comunidad en general.

En agosto del 2000 el Consejo Politécnico crea el CEC-EPN con autonomía económica, administrativa y financiera, como Centro de Transferencia y Desarrollo de Tecnologías de Estudios para la Comunidad de la Escuela Politécnica Nacional, con la finalidad de capacitar y emprender actividades en pro de la comunidad.

El 11 de octubre de 2005, el Consejo Politécnico resuelve suprimir el Centro de Transferencia y Desarrollo de Tecnologías de Estudios para la Comunidad y dispone que todas las actividades continuarán ejecutándose ininterrumpidamente a través del Centro de Educación Continua reactivado el 4 de enero de 2005 por el mismo Consejo Politécnico.[1]

1.1.1. MISION VISION

Misión

El Centro de Educación Continua de la Escuela Politécnica Nacional ofrece a la comunidad servicios de capacitación y consultoría, con profesionales altamente calificados y tecnología avanzada para aportar al desarrollo y a la competitividad de la sociedad.

Visión

Ser el Centro de Educación Continua referente en el Ecuador, con estándares internacionales, en servicios de capacitación y consultoría, mediante una gestión efectiva y con responsabilidad social.

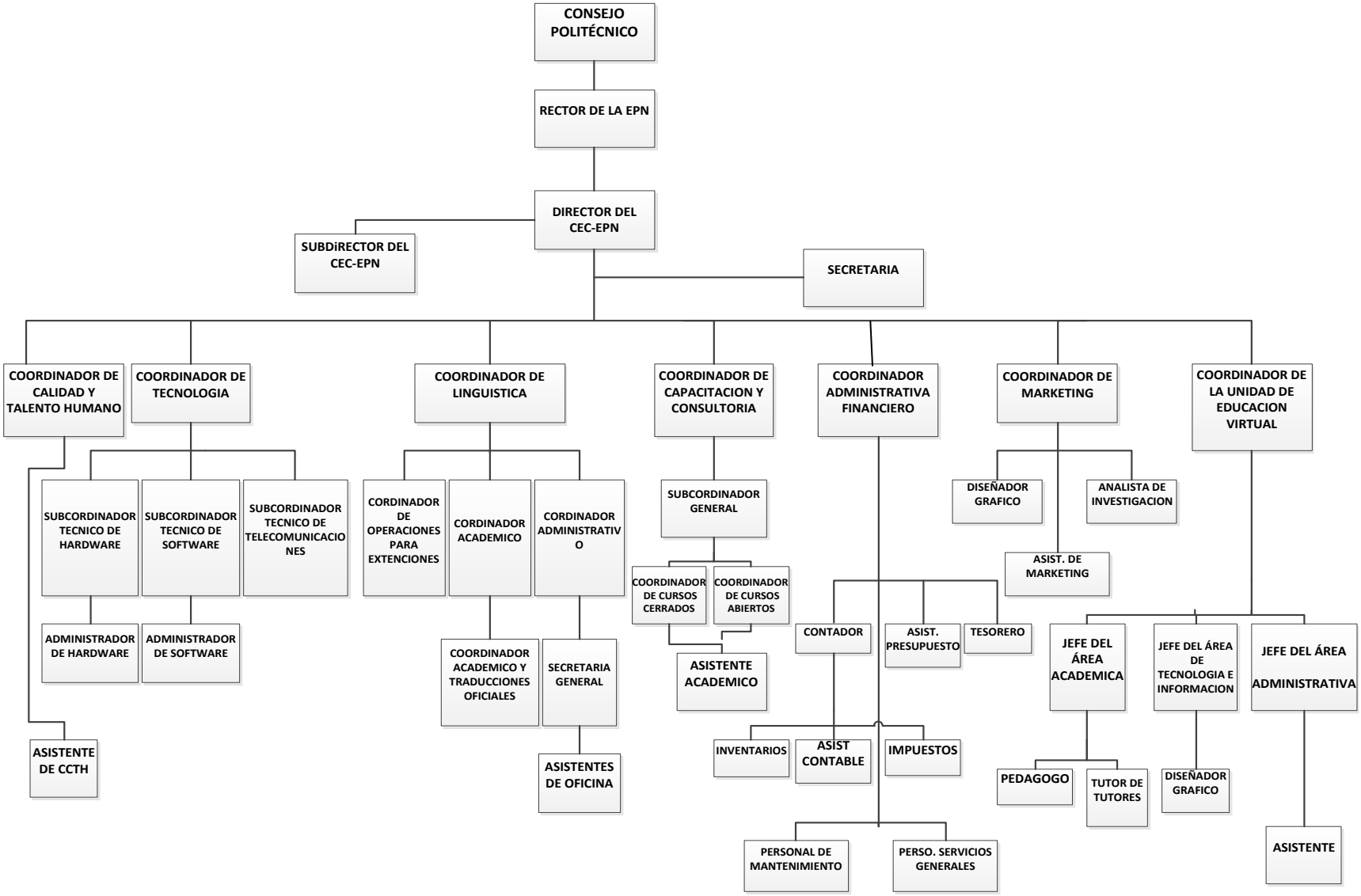
1.1.2. OBJETIVOS ESTRATEGICOS.

- Asegurar la satisfacción de los clientes y partes interesadas.
- Implementar las mejores prácticas de gestión académica y administrativa en los procesos del CEC-EPN.
- Fortalecer el posicionamiento en el mercado.
- Fomentar una cultura organizacional en base a nuestros valores.
- Promover proyectos de responsabilidad social.

1.1.3. ORGANIGRAMA

A continuación en la Figura 1-1 se presenta el organigrama CEC-EPN así como los jefes de cada área y sub área. [2]

Figura 1-1: Organigrama del CEC-EPN



1.2. ESTUDIO DE VULNERABILIDADES Y RIESGOS DEL CENTRO DE EDUCACIÓN CONTINUA.

Para realizar el Estudio de Vulnerabilidades y Riesgos del Centro de Educación Continua (CEC – EPN), se utilizó la Herramienta de Microsoft "Microsoft Security Assessment Tool" (MSAT), con la cual se pudo tener una noción del nivel actual de seguridad que posee el negocio. [3]

La herramienta MSAT tiene como propósito principal identificar y evaluar las debilidades del entorno de TI del negocio ayudando de esta forma a minimizar los riesgos dentro del mismo.

Utilizando una serie de preguntas, la herramienta analiza las siguientes Áreas: infraestructura, aplicaciones, operaciones y usuarios. MSAT creará el Perfil de Riesgos del Negocio (BRP) con el fin de calcular el riesgo al que está expuesta el área del negocio seleccionado al realizar sus actividades.

La siguiente serie de preguntas nos permitirá obtener un listado de las medidas de seguridad existentes en el negocio, al juntar todas estas medidas de seguridad se forman capas de defensa las mismas que proporcionan una mayor protección al negocio contra riesgos de seguridad y vulnerabilidades específicas.

Al sumar estas capas obtendremos el índice de defensa a Profundidad (Defense-in-Depth Index (DiDI)), luego compararemos este índice con nuestro Perfil de Riesgos del Negocio para medir la distribución del riesgo a través de las áreas de análisis antes mencionadas.

Una vez finalizado el banco de preguntas obtendremos los puntajes tanto del Perfil de Riesgos del Negocio (BRP) como del índice de defensa a Profundidad

(DiDI), los mismos que los podremos ver representados mediante una gráfica la misma que nos servirá para observar la disparidad entre ellos.

Finalizado esto la herramienta pasará a la evaluación del nivel de madurez de la seguridad del negocio, la cual nos servirá para realizar una comparación entre las prácticas de seguridad que posee el negocio contra las mejores prácticas de la industria con el fin que esta pueda alinear sus prácticas de seguridad con las que en realidad necesita su actividad comercial.

"La madurez de la seguridad incluye los controles (tanto físicos como técnicos), la competencia técnica de los recursos informáticos, las directivas, los procesos y las prácticas sostenibles. La madurez de la seguridad se puede medir únicamente a través de la capacidad de la empresa para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de muchas disciplinas.

Todas las empresas deben esforzarse en alinear su nivel de madurez y estrategia de seguridad asociada, en relación a los riesgos que conlleva su actividad comercial:

Básica: Algunas medidas eficaces de seguridad utilizadas como primer escudo protector; respuesta de operaciones e incidentes aún muy reactiva

Estándar: Capas múltiples de defensa utilizadas para respaldar una estrategia definida

Optimizada: Protección efectiva de los asuntos de forma correcta y garantía de la utilización del mantenimiento de las mejores prácticas recomendadas"

1.2.1. ANÁLISIS DE RESULTADOS

Una vez implantando la herramienta MSAT en el área de TI del Centro de Educación Continua (CEC-EPN) se obtuvo los siguientes resultados como se muestra en la figura a continuación.

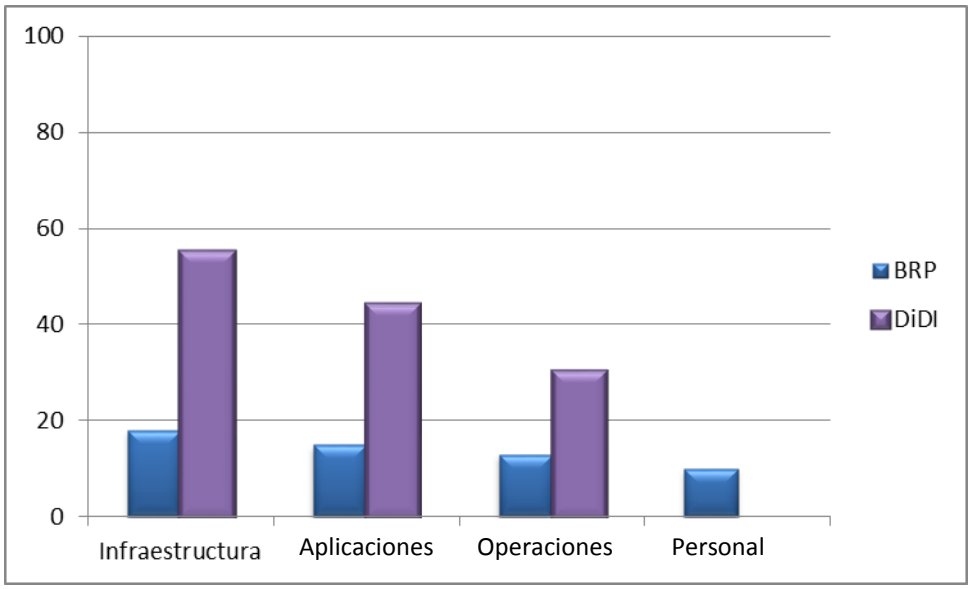


Figura 1-2: Resultados Riesgo-Defensa
Fuente: Informe de la herramienta MSAT

Para interpretar la figura mostrada anteriormente debemos tener en cuenta la relación que existe entre los puntajes del Perfil de Riesgos del Negocio (BRP) como del índice de defensa a Profundidad (DiDI), de esta manera al evaluar los puntajes que tiene cada uno podremos observar posibles disparidades entre ellos, estas disparidades en caso de ser significativas en alguna de las Áreas de Análisis con las que trabaja el MSAT, indicaría que la estrategia de seguridad del negocio no es la adecuada para el negocio produciendo un ambiente de vulnerabilidad dentro del mismo.

En la siguiente tabla podremos observar los resultados obtenidos respecto a la Distribución de defensa de riesgos y la madurez de la seguridad del Centro de Educación Continua CEC-EPN.

Tabla 1-1: Resumen de Resultados
Fuente: Informe de la herramienta MSAT

Áreas de Análisis	Distribución de defensa de Riesgos	Madurez de la Seguridad
Personal	🟡	🔴
Operaciones	🟡	🟢
Aplicaciones	🔴	🟢
Infraestructura	🔴	🟢
Leyenda	🟢 Distribucion Pareja 🟡 Disparidad leve 🔴 Disparidad significativa	🟢 Optimizada 🟡 Estandar 🔴 Basica

De la comparación entre el Perfil de Riesgos del Negocio (BRP) y el índice de defensa a Profundidad (DiDI) obtendremos la distribución de defensa de riesgos mismo que nos mostrará el balance entre los riesgos y las medidas para prevenir los mismos que posee el Centro de Educación Continua, Podemos observar que es necesaria una considerable mejora en el área de Aplicaciones e Infraestructura así como una ligera mejora en las áreas de Personal y Operaciones. Con el fin de obtener un balance adecuado entre ellos generando así un ambiente estable en el negocio.

Podemos observar que el nivel de madurez es el adecuado al negocio en casi todas las áreas de análisis exceptuando el área de Personal lo cual podría generar inestabilidad en el negocio.

1.2.1.1. Medidas de Defensa

Con el estado del nivel de madures de las áreas de análisis, podremos observar si el negocio cumple con las mejores prácticas para así saber que mejorar dentro de las mismas.

En base a las respuestas sobre la evaluación de riesgos la herramienta ha calificado las medidas de defensa que posee el Centro de educación continua de la siguiente manera.

Tabla 1-2: Medidas de Defensa

Fuente: Informe de la herramienta MSAT

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus -Equipos de escritorio	
Antivirus -Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	
Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado -Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión -Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	
Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

Leyenda:

- Cumple las mejores prácticas recomendadas
- Necesita Mejorar
- Carencias Severas

A continuación se muestran los resultados obtenidos de la herramienta MSAT para cada área de análisis, así como para cada sub área de las mismas.

1.2.1.1.1. Infraestructura

El estudio de esta área de análisis se centra en el funcionamiento de la red, los procesos comerciales que se deben implantar, la creación y uso de hosts y la gestión y el mantenimiento de la red.

Reglas y filtros de Cortafuegos

- Se ha instalado cortafuegos en todas las oficinas.
- El cortafuegos se comprueba regularmente para asegurarse de que funciona correctamente
- Existen varios segmentos DMZ para proteger los recursos corporativos accesibles a través de Internet.
- Se utiliza software de cortafuegos basados en hosts para proteger los servidores.

Antivirus

- Los Pc del negocio utilizan soluciones antivirus.
- Se utilizan soluciones antivirus en el nivel del servidor.

Segmentación

- Se implantado la segmentación de la red en su entorno.

Sistema de detección de intrusiones (IDS)

- No se utiliza ningún hardware ni software de detección de intrusiones.

Inalámbrico

- No existe la opción de conexión inalámbrica a su red

Autenticación

Usuarios internos

- Actualmente se requiere sólo autenticación de contraseñas complejas para que los usuarios accedan a la red interna y a los hosts.

Usuarios de acceso remoto

- Actualmente la autenticación no existe o sólo existe autenticación de contraseñas sencillas para el acceso remoto a la red interna y a los hosts.

Directivas de contraseñas

Directivas de contraseñas-Cuenta de usuario

- Las cuentas de usuarios utilizan directivas de contraseñas
- Directivas de contraseñas-Cuenta de acceso remoto
- Las cuentas de acceso remoto no utilizan directivas de contraseñas.

Gestión y control

Informes sobre incidentes y respuesta

- Las estaciones de trabajo no se crean conforme a ninguna documentación ni simulación formal.

Creación segura

- Se han instalado cortafuegos particulares en todas las estaciones de trabajo del entorno
- Los procesos de creación de los dispositivos de infraestructura están documentados.
- La creación del sistema no incluye ningún procedimiento para reforzar el host.
- El software de acceso remoto del cliente se ha instalado en las estaciones de trabajo que se conectan remotamente a la red de servidores.
- Los procesos de creación de los servidores están documentados.
- No se utiliza ningún software de cifrado de discos en el entorno.
- Se utiliza un software de control/gestión remota en el entorno.
- No se utiliza ningún protector de pantalla protegido por contraseña en el entorno.
- No se utilizan módems en el entorno.

Seguridad física

- Se han instaurado controles de seguridad física para proteger los activos de la empresa.
- Se ha instalado un sistema de alarma para detectar e informar de intrusiones.
- Los Controles de entrada y de visitantes no están implementados.

- Los equipos de la red se hallan en una habitación cerrada con acceso restringido.
- Los equipos de red se encuentran en rack bajo llave.
- Las estaciones de trabajo no están protegidas con cables de seguridad.
- Los ordenadores portátiles están protegidos con cables de seguridad.
- Los materiales impresos confidenciales se almacenan en armarios con llave.

1.2.1.1.2. Aplicaciones

El objetivo de la evaluación consistió en realizar una revisión de las aplicaciones de del CEC-EPN y valorarlas desde el punto de vista de la seguridad y disponibilidad

Implementación y uso

- No se utilizan equilibradores de carga en el entorno.

Clústeres

- No se utiliza la agrupación en clústeres en el entorno.

Aplicación y recuperación de datos

- No se tiene ninguna línea de aplicaciones empresariales
- No se realizan periódicamente pruebas de la recuperación de aplicaciones y datos.

Fabricante de software independiente (ISV)

- Otros fabricantes han desarrollado una o más de las aplicaciones principales del entorno.
- No todos los fabricantes independientes de software suelen ofrecer revisiones ni actualizaciones de seguridad.

Desarrollado internamente

- El equipo interno de desarrollo de software ofrece revisiones y actualizaciones de seguridad.
- No se utiliza macros personalizadas en las aplicaciones ofimáticas del negocio.

Vulnerabilidades

- Actualmente no se conocen vulnerabilidades para la seguridad en ninguna aplicación de su entorno.

Diseño de aplicaciones

Autenticación

- Se usa una autenticación de contraseñas complejas en las aplicaciones principales.

Directivas de contraseñas

- No se usan controles de contraseñas complejas en todas las aplicaciones principales.
- La caducidad de las contraseñas se controla en todas las aplicaciones principales.
- No se utilizan controles de bloqueo de cuentas en todas las aplicaciones principales.

Autorización y control de acceso

- Se limita el acceso a datos y funciones confidenciales según los privilegios de la cuenta en las aplicaciones principales.

Registro

- Hay varios eventos registrados por las aplicaciones del entorno. Las aplicaciones deben registrar todos los eventos según las prácticas recomendadas.
- Se registran los intentos fallidos de autenticación.
- Se registran los intentos de autenticación correctos.
- Se registran los errores de las aplicaciones.
- Si se registran los accesos denegados a los recursos.
- No se registran los accesos correctos a los recursos.
- Se registran los cambios en los datos.
- No se registran los cambios en las cuentas de usuario.

Validación de datos de entrada

- Se validan los datos de entrada de todos los usuarios finales.
- Se validan todos los datos de entrada de las aplicaciones de cliente.
- No se validan los datos de entrada que proceden de un feed de datos.

Metodologías de desarrollo de seguridad de software

- La organización no proporciona formación sobre metodologías de seguridad para software para su personal de desarrollo.
- Las aplicaciones no cifran los datos confidenciales antes de transmitirlos. Su respuesta indica que las aplicaciones principales del entorno no cifran los datos confidenciales cuando están almacenados.

Cifrado –Algoritmo

- Se utiliza el algoritmo de hash MD5.

1.2.1.1.3. Operaciones

Esta sección de la evaluación revisa aquellos procesos de la empresa que regulan las directivas de seguridades corporativas, los procesos de recursos humanos, así como la formación y la divulgación de materias de seguridad para los empleados.

Requisitos de seguridad

- El CEC-EPN posee un modelo para la asignación de niveles de gravedad a cada componente del entorno informático.

Evaluaciones de seguridad

- La evaluación de los medios de seguridad no es realizada por empresas independientes al CEC-EPN
- Las evaluaciones de la seguridad de la empresa no las realiza personal interno.

Comprobaciones del historial personal

- No se llevan a cabo comprobaciones del historial personal como parte integral del proceso de contratación.

1.2.1.1.4. Personal

Directiva de recursos humanos

- No existe ninguna directiva formal para los empleados que dejan la empresa.

Relaciones con terceros

- Los sistemas se configuran por parte de personal interno
- El CEC-EPN gestiona el entorno informático.
- No existe ninguna directiva para las relaciones con terceros.

Conocimiento de seguridad

- No se ha asignado a ningún individuo ni grupo la seguridad de la empresa.
- No existe ningún programa de divulgación de las medidas de seguridad en la empresa.

Formación sobre seguridad

- No existe la capacitación adecuada en temas de seguridad para el personal del CEC-EPN

1.2.2. INICIATIVAS DE SEGURIDAD

Después de la Evaluación realizada, la herramienta MSAT considera que los siguientes aspectos no cumplen las mejores prácticas recomendadas y deben dirigirse a aumentar la seguridad dentro del CEC-EPN

Prioridad Alta	Prioridad intermedia	Prioridad Baja
• **Creación Segura** • **Cifrado** • **Relaciones con Terceros** • **Fabricante de software independiente(ISV)** • **Cifrado - Algoritmo**	• Segmentación • Seguridad Física • Usuarios Administrativos • Directivas de Contraseñas	• Host de gestión-servidores • Host de gestión-Dispositivos de red • Protocolos y servicios • Uso aceptable • Copias de seguridad

Tabla 1-3: Iniciativas de Seguridad
Fuente: Informe CompletoCEC-EPN

1.2.3. ANALISIS DE RIESGOS DEL CENTRO DE EDUCACION CONTINUA

Para el Análisis de riesgos se necesitara identificar los activos informáticos que posea el Centro de Educación Continua e identificar las vulnerabilidades y riesgos a los que estos están expuestos, para que de esta manera podamos

seleccionar los controles más adecuados para mitigar estos riegos y evitar o disminuir la ocurrencia de los mismo.

1.2.3.1. Recopilación de Activos Informáticos del Centro de Educación Continua.

Los activos informáticos comprenden todos los recursos de hardware y software que posee la organización, con el fin de proteger a estos de cualquier riesgo se diseñara el Plan de gestión de seguridad de la información presente.

A continuación listaremos los activos informáticos que posee el Centro de Educación Continua (CEC-EPN):

1.2.3.1.1. Hardware

Los activos informáticos de hardware que posee el CEC-EPN por el tipo de servicio que estos prestan dentro de la organización, se indican a continuación.

Laboratorios

El Centro de Educación continua posee 11 salas preparadas con infraestructuras de red comunicaciones y equipo de computación y proyección

- 144 equipos fijos
- 45 equipos portátiles
- 11 proyectores de video

Aulas

El Centro de Educación Continua posee 18 salas para el aprendizaje de Idiomas equipadas con

- Equipo de computación (1 por aula)
- Proyector de video
- Pantalla interactiva

Administrativo

El Centro de Educación Continua posee 3 salas distribuidas en las tres sedes, para uso de instructores, equipadas con 20 equipos de computación en total.

El Centro de Educación continua posee 88 equipos de computación distribuidos en las tres sedes para uso del personal administrativo en el desarrollo de sus actividades.

1.2.3.1.2. Software

A continuación listaremos los activos informáticos de software que posee el CEC-EPN.

Convenios Académicos

- SPSS
- Adobe

Software de Terceros administrado o supervisado por personal CGT CEC

- Olympo – Sistema de Facturación
- McAfee- Solución de antivirus perimetral
- Q-Matic-Sipse – Control de turnos de atención
- OTRS – Help desk
- Quipux-Sistema de gestión documental del sector público
- E-SIGEF- Sistema contable del sector público
- Intranet- Portal de servicios internos
- Google Apps- Sistema de comunicación – correo electrónico y mensajería

Software Desarrollado por personal CGT CEC

- Sistema SIICECW- Sistema de Gestión Académica
- Gestión de matrículas, cursos y estudiantes
- Portal de Servicios web
  - Matrículas
  - Evaluaciones a instructores
  - Historial académico
  - Registro de Notas

1.2.3.1.3. Comunicaciones

A continuación listaremos los activos informáticos de comunicaciones que posee el CEC-EPN agrupados por el tipo de servicio que estos prestan dentro de la organización.

Red LAN

- El Centro de Educación Continua posee 3 sedes cada una de ellas con Red con cableado UTP categoría 6 – 6A, interconectadas a través de un anillo de fibra óptica.
- La Red Soporta servicios de transmisión de datos, voz (telefonía IP) y video. Siendo por tanto una red convergente.

Internet

- El Centro de Educación Continua posee un servicio para comunicación interna y externa basada en protocolos TCP/IP

Servidores

- El centro de Educación continua posee 9 servidores físicos redundantes distribuidos en chasis de servidores y racks, que brindan los siguientes servicios

- Telefonía ip
- Almacenamiento de documentos
- Directorio Activo
- Servidores de aplicaciones
- Firewall
- Base de datos
- Respaldos
- Antivirus corporativo
- Pruebas
- Control de Código

1.2.3.2. Metodología

Para la realización del presente Análisis de Riesgos se utilizó la guía NIST 800-30 la misma que se detalla en este apartado. [4]

La Metodología NIST SP 800-30 está compuesta por 9 pasos básicos para el análisis de riesgo:

1. Caracterización del sistema.
2. Identificación de amenaza.
3. Identificación de vulnerabilidades.
4. Control de análisis.
5. Determinación de la Probabilidad.
6. Análisis de impacto.
7. Determinación del riesgo.
8. Recomendaciones de control.
9. Resultado de la implementación o documentación.

Paso 1 Caracterización del sistema:

En este paso identificaremos el alcance que tendrá nuestra evaluación de riesgos, así como los recursos tanto de hardware y software que constituyen el sistema, este paso se lo realizara en el apartado 1.2.3.2.1.

Paso 2 Identificación de la Amenaza:

En este paso se identificaremos y listaremos las posibles amenazas, las cuales podrían producir un incidente en la organización, Así como evaluar la probabilidad de ocurrencia de las mismas, este paso se lo realizara en el apartado 1.2.3.2.2.

Paso3 Identificación de vulnerabilidades:

En este paso se elaborara una lista de vulnerabilidades del sistema, estas vulnerabilidades pueden ser provocadas o alteradas por las fuentes de amenaza, este paso se lo realizara en el apartado 1.2.3.2.3.

Paso 4 Control de Análisis:

En este paso se analiza los controles que se encuentran implementados o están planeados con el objetivo de que exista una mínima probabilidad de que una amenaza se cumpla sobre las vulnerabilidades del Sistema, este paso se lo realizara en el apartado 1.2.3.2.4.

Paso 5 Determinación de la Probabilidad:

En este paso se determina la probabilidad de que una vulnerabilidad pueda ser ejecutada en un ambiente de amenazas relacionado, este paso se lo realizara en el apartado 1.2.3.2.5.

Paso 6 Análisis de impacto:

En este paso se determina el impacto desfavorable que tendría la ejecución de una amenaza sobre una vulnerabilidad, este paso se lo realizara en el apartado 1.2.3.2.5.

Paso 7 Determinación del riesgo:

En este paso se evalúa el nivel de riesgo de una amenaza o vulnerabilidad a través de una matriz de riesgo, este paso se lo realizara en el apartado 1.2.3.2.5.

Paso 8 Recomendaciones de control:

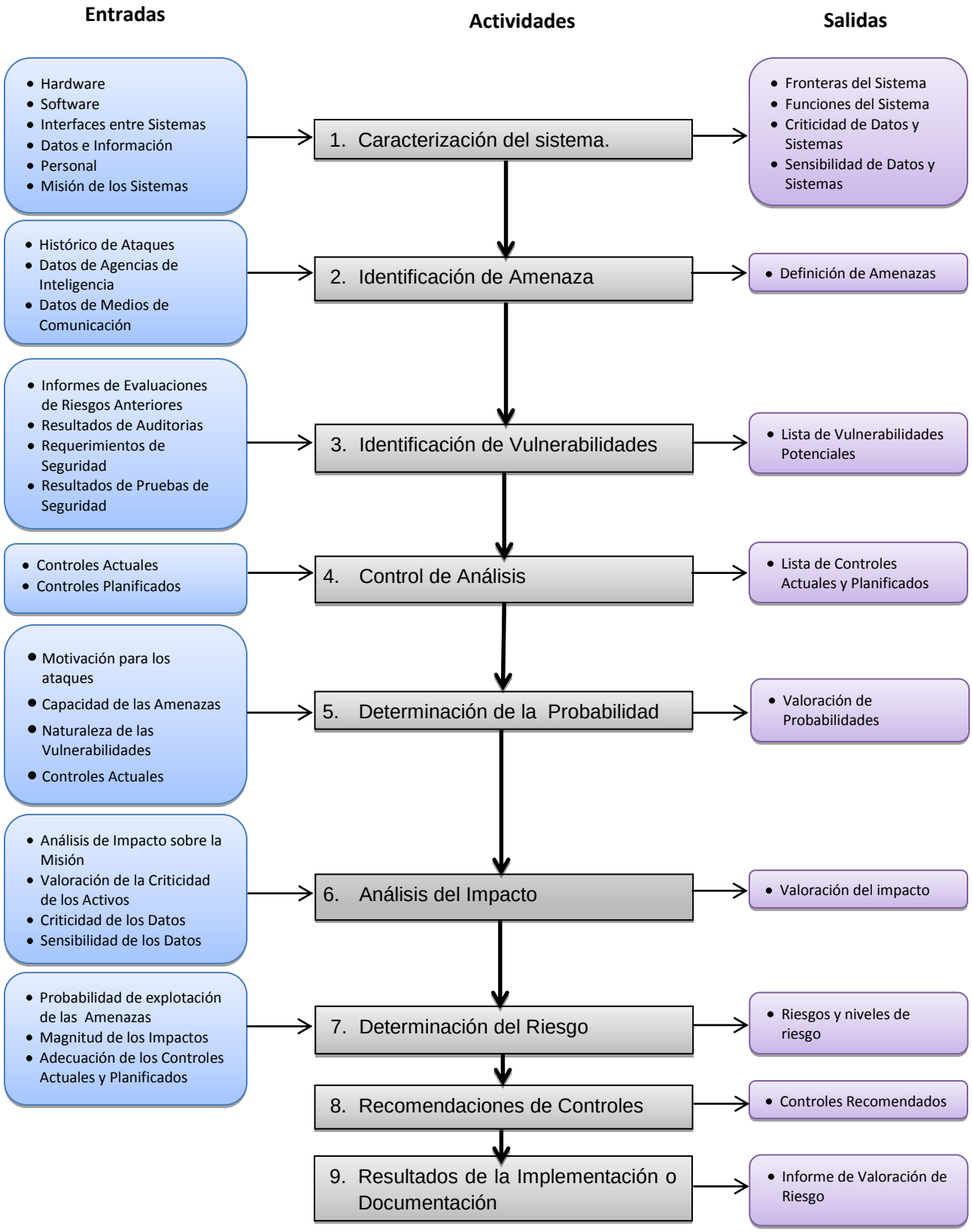
En este paso se proveen los controles necesarios para mitigar o eliminar los riesgos encontrados en la organización, este paso se lo realizara en el apartado 2.3.

Paso 9 Resultado de la implementación o documentación:

Este es el paso final en el cual llevaremos una adecuada documentación de los resultados obtenidos una vez terminada la evaluación de riesgos, el presente proyecto no contempla la etapa de implementación por lo cual este paso no fue tomado en cuenta en la aplicación de la NIST 800-30.

La Figura 1-3 muestra el proceso de análisis de riesgos.

Figura 1-3: Metodología de la Evaluación de Riesgos [4]



Fuente: Nist SP 800-30

1.2.3.2.1. Caracterización del Sistema

Para realizar nuestro análisis de riesgos el primer paso a seguir será identificar todos los activos informáticos y aplicaciones que forman parte del CEC-EPN.

1.2.3.2.1.1. Aplicaciones y Servicios del CEC-EPN

En este apartado se analizarán las principales aplicaciones, servicios que posee el Centro de Educación Continua, así como la infraestructura que estos poseen.

1.2.3.2.1.1.1. Aplicaciones

Portal del CEC-EPN

El portal Web del Centro de Educación Continúa, tiene como principal función mostrar el portafolio de Servicios que ofrece el CEC-EPN.

Figura 1-4: Portal del CEC-EPN

Dirección: http://www.cec-epn.edu.ec/

Usuarios:

Los usuarios de este Portal son los administradores del sitio y toda persona que esté interesada en recibir información de los cursos que ofrece el CEC-EPN, ya sean de Lingüística o de Capacitación Tecnológica o empresarial.

Portal de Servicios

El Portal de Servicios del Centro de Educación Continua posee varios servicios de la organización como son inscripciones online en los cursos que esta ofrece, así como historial académico y evaluaciones a los instructores.

Figura 1-5: Portal de Servicios del CEC-EPN

Dirección: http://aps.cec-epn.edu.ec/portal

Usuarios:

Los usuarios de este Portal son los administradores del portal, instructores y alumnos del Centro de Educación Continua que deseen tomar uno de sus cursos.

SIICECW

El Sistema Integrado de Información del CEC, es un sistema de uso interno del Centro de Educación Continua el cual es utilizado para la gestión y el registro de los alumnos del CEC-EPN en los diferentes cursos que este brinda. Solo se puede acceder a este sitio desde las Instalaciones del CEC-EPN.

Figura 1-6: Sistema Integrado de Información del CEC

Software:

- apache
- php
- mysql
- Joomla

Hardware:

- 2 Quad-Core Intel Xeon 2.3 GHz. Memoria RAM: 6GB (BLADE Proliant BL460c G6)

Dirección: http://aps.cec-epn.edu.ec/siiscecw

Usuarios:

Los usuarios de este Sistema son los administradores del mismo, y el personal del CEC-EPN.

1.2.3.2.1.1.2. Servidores

Servidor de Base de Datos

El servidor de BDD del Centro de Educación Continua es el encargado de almacenar la información de algunas de las aplicaciones internas que posee el Centro de Educación continua, este servidor almacena las siguientes BDD:

- CEC_RECAUDA
- AUDITORIA
- SISINFCEC

Sistema Operativo: Windows Server 2008

Software:

- SQL 2008 Server R2

Hardware:

- 2 Quad-Core Intel Xeon 2.40 GHz. Memoria RAM: 6GB (BLADE Proliant BL460c G7)

Dirección IP: 192.168.57.2

Ubicación:

Edificio de Aulas y Relación con el Medio Externo

Servidor de Aplicaciones

Este servidor se encuentra virtualizado sobre una plataforma Windows utilizando Vvmware, este almacena las siguientes aplicaciones:

- Intranet
- SIICECW
- OTRS
- Sistema de Gestión de Calidad
- Sistema de Información de Mercados

Sistema Operativo: Linux Centos 6 (Virtual)

Software:

- SQL 2008 Server R2
- apache
- php
- mysql
- Joomla
- ssl

Hardware:

- 2 Quad-Core Intel Xeon 2.3 GHz. Memoria RAM: 6GB (BLADE Proliant BL460c G6)
- VMWARE

Dirección IP: 192.168.57.56

Ubicación:

Edificio de Aulas y Relación con el Medio Externo

Servidor de Archivos

El servidor de Archivos es el encargado de almacenar la documentación de los diferentes departamentos que forman al Centro de Educación Continua.

Sistema Operativo: Windows Server 2008

Software:

- Ninguno

Hardware:

- Intel Xeon E5620 3.20 GHz. Memoria RAM: 1GB

Dirección IP: 192.168.57.5

Ubicación:

Edificio de Aulas y Relación con el Medio Externo

Usuarios:

Empleados de los departamentos que forman el CEC-EPN

Servidor de Antivirus

Este servidor es el encargado de brindar el servicio de antivirus a todos los computadores que se encuentran en las instalaciones del Centro de Educación Continua, mediante la utilización de McAfee un software de administración centralizada de la seguridad.

Sistema Operativo: Windows Server 2008

Software:

- EPO 4.6 McAfee

Hardware:

- 2 Quad-Core Intel Xeon 2.3 GHz. Memoria RAM: 6GB (BLADE Proliant BL460c G6)

Direction IP: 192.168.57.7

Ubicación:

Edificio de Aulas y Relación con el Medio Externo

Active Directory

Este servidor brinda los siguientes servicios:

- Servidor Secundario Active directory
- Servidor DNS
- Servidor de Políticas de dominio GPO

Sistema Operativo: Windows Server 2003

Software:

- Ninguno

Hardware:

- Intel Xeon E5420 2.50 GHz. Memoria RAM: 2GB (BLADE)

Dirección IP: 192.168.57.10

Ubicación:

Edificio de Aulas y Relación con el Medio Externo

Servidor de Backup

El servidor de Backup es utilizado principalmente para el respaldo de las bases de Datos de las aplicaciones internas del Centro de Educación continua mismas que se encuentran almacenadas en el Servidor de Base de Datos.

Sistema Operativo: Windows Server 2003

Software:

- HP Data Protector

Hardware:

- Intel Xeon E5310 1.86 GHz. Memoria RAM: 3.25 GB (BLADE)

Dirección IP: 192.168.57.13

Ubicación:

Edificio de Aulas y Relación con el Medio Externo

Central Telefónica IP

Sistema Operativo: Centos

Software:

- Elastix

Hardware:

- Intel Xeon E5620 2.40 GHz. Memoria RAM: 6GB

Dirección IP: 192.168.57.95

1.2.3.2.2. Identificación de Amenazas

Una amenaza es un suceso que puede ocurrir sobre un activo informático que puede ser causado por una entidad natural, humana o artificial, estas pueden ocurrir ya sea de manera natural u ocasionada intencionalmente aprovechando las vulnerabilidades del mismo. [5]

En este apartado se identificarán las posibles amenazas que podrían afectar al Centro de Educación Continua.

Amenaza	Posibles Amenazas
Amenazas Naturales	• Terremotos. • Inundaciones. • Tormenta Eléctrica.
Amenazas Humanas	• Filtrado de información interna • Vandalismo • Hacking • Robo
Amenazas Infraestructurales	• Incendios • Cortes de Energía • Humedad
Amenazas Tecnológicas	• Falla del Servicio de Internet • Fallas en los Activos Informáticos • Mal funcionamiento de las Aplicaciones internas.
Amenazas Organizacionales	• Falta de Personal • Falta de planes de Seguridad y Contingencia. • No se controla la utilización de los recursos de la organización.

Tabla 1-4: Identificación de Amenazas
Fuente: Elaborado por el Autor

Una vez que se identificó las posibles amenazas se procedió a listar las posibles consecuencias de las mismas.

Amenazas Naturales

Posibles Amenazas	Consecuencias de la Amenaza
Terremotos	• Daños en las instalaciones de la Organización. • Daños en el Personal de la Organización
Inundaciones	• Daños en las instalaciones dela Organización. • Daños en los Activos de Hardware
Tormenta Eléctrica	• Daños en los Activos de Hardware. • Fallas Eléctricas(Cortes de Energía, Variaciones en los niveles de energía)

Amenazas Humanas

Posibles Amenazas	Consecuencias de la Amenaza
Filtrado de Información Interna	• Sabotaje a los sistemas de la Organización • Chantaje • Fraude • Acceso no autorizado a los sistemas de la Organización
Vandalismo	• Daños a los activos informáticos de la Organización. • Sabotaje a los sistemas de la organización
Hacker	• Sabotaje a los sistemas de la organización • Ingeniería Social. • Manipulación de la Información Interna de la Organización.
Robo	• Perdida de Activos Informáticos • Equipos insuficientes para cubrir la demanda de los trabajadores. • Altos costes para reposición de Activos Informáticos

Amenazas Infraestructurales

Posibles Amenazas	Consecuencias de la Amenaza
Incendios	• Daños en las instalaciones de la Organización. • Daños en el Personal de la Organización
Cortes de Energía	• Daños en los Activos Informáticos • Inoperatividad de los Servicios que brinda la Organización.
Humedad	• Daños en las instalaciones de la Organización. • Daños en los Activos Informáticos

Amenazas Tecnológicas

Posibles Amenazas	Consecuencias de la Amenaza
Falla del Servicio de Internet	• Inoperatividad de los Servicios que brinda la Organización los cuales necesiten una conexión a internet.
Fallas en los Activos Informáticos	• Equipos insuficientes para cubrir la demanda de los trabajadores y clientes de la Organización.
Mal funcionamiento de las Aplicaciones internas.	• Perdida de la integridad de la Información de la Organización. • Fallos en el sistema.

Amenazas Organizacionales

Posibles Amenazas	Consecuencias de la Amenaza
Falta de Personal	• Baja en la calidad de los Servicios que brinda la organización. • Horarios de Trabajo excesivos • Perdida de Personal
Falta de planes de Seguridad y Continuidad.	• Mayor tiempo para recuperarse de una catástrofe. • Inadecuada Gestión de la información de la Organización.
No se controla la utilización de los recursos de la organización.	• Daño en los Activos Informáticos • Perdida de los Activos Informáticos

1.2.3.2.3. Identificación de vulnerabilidades

Una vez seleccionadas las posibles amenazas dentro de la organización se pasó a la detección de las posibles vulnerabilidades, las cuales podrían ser explotadas por dichas amenazas.

Vulnerabilidades/Amenazas Naturales

Vulnerabilidad	Fuente de la Amenaza
• No se realiza mantenimiento sobre la planta de energía auxiliar.	Tormenta Eléctrica
• No tener un adecuado sistema de drenaje en las instalaciones de la organización.	Inundaciones

Tabla 1-5: Identificación de Vulnerabilidades
Fuente: Elaborado por el Autor

Vulnerabilidades/Amenazas Humanas

Vulnerabilidad	Fuente de la Amenaza
• Se terceriza el mantenimiento de activos informáticos como servidores. • No se tiene cláusulas de seguridad en los contratos de los servicios que se tercerizan. • No hay proceso formal para la eliminación de datos en medios electrónicos y formato impreso.	Filtrado de información interna
• No existe un monitoreo continuo de los accesos realizados en los servidores. • No existe un cifrado sobre la información en las BDD de la empresa. • No se tiene un número límite de intentos fallidos sobre el ingreso a sus sistemas. • No se lleva un registro de eventos producidos en los host y los dispositivos.	Hacking
• No existen controles físicos para garantizar la seguridad de los activos de la empresa. • No se investiga a fondo al personal nuevo previo a su contratación. • No existe un proceso formal de salida de los empleados.	Robo

Vulnerabilidades/Amenazas Infraestructurales

Vulnerabilidad	Fuente de la Amenaza
• No se tiene suficientes rutas de escape en las instalaciones.	Incendios
• No se realiza mantenimiento sobre la planta de energía auxiliar.	Cortes de Energía
• No se realiza revisiones periódicas de las tuberías de las instalaciones.	Humedad

Vulnerabilidades/Amenazas Tecnologicas

Vulnerabilidad	Fuente de la Amenaza
• No existe una red inalámbrica propia dentro del CEC-EPN. • No se tiene una planificación para dar mantenimiento a la red del CEC-EPN	Falla del Servicio de Internet
• Desconocimiento de las vulnerabilidades actuales de las aplicaciones de la empresa. • Se desconoce la arquitectura y el flujo de datos de las aplicaciones. • No se tiene una planificación para el mantenimiento de las aplicaciones.	Mal funcionamiento de las Aplicaciones internas.

Vulnerabilidades/Amenazas Organizacionales

Vulnerabilidad	Fuente de la Amenaza
• No se verifica que los equipos informáticos se utilicen de manera correcta.	No se controla la utilización de los recursos de la organización.
• No se tienen directivas y procedimientos para notificar problemas de seguridad. • No se tiene procedimientos de contingencia ante incidentes formales. • No se evalúa el impacto de un nuevo servicio antes de implementarlo. • No existe departamento de seguridad en la empresa • Se desconoce el estado actual en la seguridad interna del CEC-EPN.	Falta de reglas y controles

1.2.3.2.4. Control de Análisis

A continuación se listara los diferentes controles y políticas de seguridad que posee actualmente el CEC-EPN.

Cuentas de correo Electrónico

- Queda totalmente prohibido transferir programas de música o video, ya que el tamaño de estos archivos puede disminuir el desempeño del servidor de correo.

- Los usuarios son responsables de todas las actividades realizadas con la cuenta de correo electrónico proporcionada por el CEC-EPN. Esta

responsabilidad supone el cuidado de los recursos que integran dicha cuenta y, particularmente, de los elementos, como la contraseña, que pueden permitir el acceso de terceras personas a dicha cuenta.

- El correo es de uso personal e intransferible.
- No están permitidos los mecanismos y sistemas que intenten ocultar la identidad del emisor de correo.

- Está prohibida la suplantación de identidad de otra persona en el envío de mensajes de correo electrónico.

- Es obligación del usuario utilizar destinatarios precisos y evitar los mensajes en cadenas o series.

- Únicamente el personal de la Coordinación de Gestión Tecnológica (CGT) está autorizado a realizar tareas de envió correo masivo, previa solicitud de la Dirección o una de las Unidades del CECEPN

- En caso de falla en la recepción o entrega de un correo debe ser informada a la Coordinación de Gestión Tecnológica (CGT), para darle el seguimiento respectivo y establecer las posibles causas.

Controles en los Servidores.

- La Coordinación de Gestión Tecnológica se responsabiliza de garantizar la disponibilidad e integridad de toda la información mantenida en los servidores o carpetas establecidas para este fin.

- Por ningún motivo la Coordinación de Gestión Tecnológica se responsabiliza de información relevante para el CEC-EPN que no haya sido

almacenada en los servidores o carpetas comunicadas por la Coordinación de Gestión Tecnológica.

- La Coordinación de Gestión Tecnológica será responsable de garantizar la disponibilidad e integridad de la información almacenada en el correo (bandeja de entrada)

- En caso de requerirse los respaldos por causas de perdida de la información, o siniestro, la Coordinación de Gestión Tecnológica se compromete a entregar dichos respaldos en un plazo de 48 horas. Para pérdidas de información que impliquen un proceso largo, el Coordinador y el Subcoordinador asignado analizarán el tiempo de respuesta.

- Los Coordinadores del CEC-EPN tienen la responsabilidad de capacitar y comunicar a sus subordinados, sobre los servidores o carpetas que la Coordinación de Gestión Tecnológica ha destinado para el almacenamiento de la información.

- El personal del CEC-EPN se responsabiliza de guardar toda la información de tipo laboral en los servidores o carpetas destinadas por la Coordinación de Gestión Tecnológica y debidamente informados por sus Coordinadores.

- El personal de CEC-EPN tiene prohibido subir a los servidores carpetas compartidas, todo tipo de información personal como por ejemplo música, video, fotos o documentos personales.

- Es responsabilidad del personal del CEC-EPN mantener depurados los documentos con el fin de que los repositorios no se llenen con información obsoleta o innecesaria.

- El responsabilidad del personal del CEC-EPN mantener depurado su bandeja de correo libre de spam, cadenas de correo o información no

relevante para su trabajo, con el bien de hacer más eficiente el procesos de backup.

Controles sobre los Equipos del CEC-EPN

- Todo equipo que forme parte de la red administrativa del CEC-EPN, tendrá Asignado un NOMBRE DE EQUIPO y pertenecerá a un GRUPO DE TRABAJO asignado por la Coordinación de Gestión Tecnológica. La asignación de nombre del equipo se la realizará de la siguiente forma.

  Sede_Coordinación _ USUARIO

  Para la actualización de contraseñas cada equipo debe seguir las siguientes reglas:

  1. La vigencia máxima de una contraseña es de 60 días
  2. Longitud mínima de la contraseña 8 caracteres
  3. Se puede utilizar caracteres numéricos, alfanuméricos, letras
  4. mayúsculas, letras minúsculas y símbolos.

- Se prohíbe el uso de programas o recursos para los cuales no exista una licencia o autorización de uso válido a nombre de la institución.

- Está prohibido el uso de programas de descarga p2p para música, videos, imágenes, etc.

- La Coordinación de Gestión Tecnológica, se encargará del mantenimiento preventivo y correctivo de las computadoras, en el caso de existir un daño en un equipo de computación se debe informar al siguiente correo electrónico: tecnologia@cec-epn.edu.ec.

- De detectarse un daño causado por negligencia o mal uso del equipo, el funcionario deberá reponer el bien afectado o en su defecto cubrir el monto económico del mismo.

- Queda restringido el uso de unidades USB, quemadoras de CD o DVD, para uso personal.

- Una estación de trabajo es de uso exclusivo de la o las personas a las que se les ha asignado el equipo, por lo tanto se prohíbe el préstamo de equipos a terceros aun cuando sean parte del CEC-EPN.

- Está prohibido instalar y usar cualquier sistema de mensajería o chat como msn Messenger, yahoo messenger o cualquier similar, a excepción de las personas autorizadas dentro de cada Unidad.

- Que prohibido el acceso a televisión, música o videos vía internet, ya que esto atenta contra la calidad del servicio.

- No se permite la instalación de programas mediante descarga directa de vía internet.

- Todos los bienes del CEC-EPN deben estar correctamente registrados e inventariados para su mejor control y manejo.

- Todos los bienes deben estar codificados y etiquetados para su mejor identificación y control. Debido a las dos fases de registro en inventarios existentes, es necesario etiquetar el bien con el código interno asignado por el sistema de inventarios del CEC-EPN, hasta su codificación definitiva por parte del Departamento de Bienes de la Escuela Politécnica Nacional.

Controles sobre el manejo de la Información

- Para el manejo de la información institucional, la Coordinación de Gestión Tecnológica se encargará de proveer de unidades de red donde se almacenará la información que permita el desarrollo de las actividades de las diferentes Unidades. Cabe a aclarar que la Coordinación de Gestión Tecnológica realiza respaldos únicamente de las unidades de red.

- No se permite la creación de accesos directos a documentos que se encuentran en las unidades de red.

- Se prohíbe la revelación intencionada de información sensible perteneciente al CEC-EPN, utilizando Internet como medio de comunicación.

1.2.3.2.5. Valoración del Riesgo

Para el siguiente apartado se utilizó las definiciones de probabilidad de amenaza y magnitud de impacto, las cuales fueron tomadas de la guía NIST SP 800-30.

Probabilidad de la Amenaza	Impacto		
	Bajo (10)	Medio (50)	Alto (100)
Alta (1.0)	Bajo 10 x 1.0 = 10	Medio 50 x 1.0 = 50	Alto 100 x 1.0 = 100
Media (0.5)	Bajo 10 x 0.5 = 5	Medio 50 x 0.5 = 25	Medio 100 x 0.5 = 50
Baja (0.1)	Bajo 10 x 0.1 = 1	Bajo 50 x 0.1 = 5	Bajo 100 x 0.1 = 10

Tabla 1-6: Matriz de Nivel de Riesgo
Fuente: Guía NIST SP 800-30

En la siguiente tabla podremos observar las definiciones de la probabilidad de que una amenaza explote a las vulnerabilidades que tiene la organización.

Nivel	Definición de la Probabilidad
Alto	La causa de la amenaza se encuentra altamente motivada, por lo que los controles para prevenir que se explote una vulnerabilidad son ineficientes.
Medio	La causa de la amenaza se encuentra motivada, los controles implantados pueden prevenir que se explote una vulnerabilidad.
Bajo	La causa de la amenaza carece de motivación o los controles implantados impiden de manera significativa que se explote una vulnerabilidad

Tabla 1-7: Definición de la Probabilidad
Fuente: Guía NIST SP 800-30

En la siguiente tabla podremos observar las definiciones del impacto que tendría sobre la organización de ejecutarse una amenaza.

Nivel	Definición de la Magnitud de Impacto
Alto	La explotación de una vulnerabilidad (1) Puede resultar en costosas pérdidas de los principales activos o recursos tangibles; (2) Puede violar o dañar de manera significativa el cumplimiento de la misión, los intereses o la reputación de una organización; (3) Puede generar pérdidas humanas o lesiones en los empleados de una organización.
Medio	La explotación de una vulnerabilidad (1) Puede resultar en costosas pérdidas de activos o recursos tangibles; (2) Puede violar o dañar el cumplimiento de la misión, los intereses o la reputación de una organización; (3) Pueden ocasionarse lesiones en los empleados.
Bajo	La explotación de una vulnerabilidad (1) Puede resultar en la perdida de algunos activos o recursos tangibles; (2) puede afectar notablemente la misión de una organización, la reputación o los intereses.

Tabla 1-8: Definición de la Magnitud de Impacto
Fuente: Guía NIST SP 800-30

La siguiente tabla muestra los diferentes niveles de riesgo que pueden estar afectando a la organización.

Tabla 1-9: Escala de Riesgo y acciones necesarias
Fuente: Guía NIST SP 800-30

Nivel	Descripción de riesgos y acciones necesarias
Alto	Si una observación o descubrimiento es evaluado como un alto riesgo, existe la fuerte necesidad de medidas correctivas. Un sistema existente puede seguir operando. Pero un plan de acciones correctivas debe ponerse en marcha lo más pronto posible.
Medio	Si una observación está clasificado como de riesgo medio, se necesitan medidas correctivas y un plan debe ser desarrollado para incorporar dentro estas acciones en un periodo de tiempo razonable.
Bajo	Si una observación está clasificado como de riesgo bajo. El administrador del sistema debe decidir si se toman medidas correctivas o si el riesgo es aceptable.

A continuación se muestra la valoración de riesgo utilizando las definiciones de la guía NIST SP 800-30.

Amenazas Naturales

Tabla 1-10: Valoración de Riesgos
Fuente: Elaborada por el Autor

Vulnerabilidad	Fuente de la Amenaza	Probabilidad de la Amenaza	Impacto	Valoración del Riesgo
1. No se realiza mantenimiento sobre la planta de energía auxiliar.	Tormenta Eléctrica	Bajo	Media	Bajo

Vulnerabilidad	Fuente de la Amenaza	Probabilidad de la Amenaza	Impacto	Valoración del Riesgo
2. No tener un adecuado sistema de drenaje en las instalaciones de la organización.	Inundaciones	Bajo	Medio	Bajo

Amenazas Humanas

Vulnerabilidad	Fuente de la Amenaza	Probabilidad de la Amenaza	Impacto	Valoración del Riesgo
1. Se terceriza el mantenimiento de activos informáticos como servidores.		Baja	Medio	Medio
2. No se tiene cláusulas de seguridad en los contratos de los servicios que se tercerizan.	Filtrado de información interna	Media	Medio	Medio
3. No hay proceso formal para la eliminación de datos en medios electrónicos y formato impreso.		Media	Medio	Medio

Vulnerabilidad	Fuente de la Amenaza	Probabilidad de la Amenaza	Impacto	Valoración del Riesgo
4. No existe un monitoreo continuo de los accesos realizados en los servidores.		Media	Medio	Medio
5. No existe un cifrado sobre la información en las BDD de la empresa.	Hacking	Baja	Medio	Bajo
6. No se tiene un número límite de intentos fallidos sobre el ingreso a sus sistemas.		Baja	Medio	Bajo
7. No se lleva un registro de eventos producidos en los host y los dispositivos.		Media	Medio	Medio
8. No existen controles físicos para garantizar la seguridad de los activos de la empresa.		Alta	Medio	Medio
9. No se investiga a fondo al personal nuevo previo a su contratación.	Robo	Media	Medio	Medio
10. No existe un proceso formal de salida de los empleados.		Alta	Medio	Medio

Amenazas Infraestructurales

Vulnerabilidad	Fuente de la Amenaza	Probabilidad de la Amenaza	Impacto	Valoración del Riesgo
1. No se tiene suficientes rutas de escape en las instalaciones.	Incendios	Baja	Medio	Bajo
2. No se realiza mantenimiento sobre la planta de energía auxiliar.	Cortes de Energía	Baja	Bajo	Bajo
3. No se realiza revisiones periódicas de las tuberías de las instalaciones.	Humedad	Baja	Bajo	Bajo

Amenazas Técnicas

Vulnerabilidad	Fuente de la Amenaza	Probabilidad de la Amenaza	Impacto	Valoración del Riesgo
1. No existe una red inalámbrica propia dentro del CEC-EPN.	Falta del Servicio de Internet	Media	Bajo	Bajo
2. No se tiene una planificación para dar mantenimiento a la red del CEC-EPN		Alta	Medio	Medio

Vulnerabilidad	Fuente de la Amenaza	Probabilidad de la Amenaza	Impacto	Valoración del Riesgo
3. Desconocimiento de las vulnerabilidades actuales de las aplicaciones de la empresa.	Mal funcionamiento de las Aplicaciones internas.	Alta	Medio	Medio
4. Se desconoce la arquitectura y el flujo de datos de las aplicaciones.		Medio	Baja	Baja
5. No se tiene una planificación para el mantenimiento de las aplicaciones.		Alta	Medio	Medio

Amenazas Organizacionales

Vulnerabilidad	Fuente de la Amenaza	Probabilidad de la Amenaza	Impacto	Valoración del Riesgo
1. No se verifica que los equipos informáticos se utilicen de manera correcta.	No se controla la utilización de los recursos de la organización	Baja	Bajo	Bajo
2. No se tienen directivas y procedimientos para notificar problemas de seguridad.	Falta de reglas y controles	Media	Medio	Medio
3. No se tiene procedimientos de contingencia ante incidentes formales.		Alta	Medio	Medio

4. No se evalúa el impacto de un nuevo servicio antes de implementarlo.		Media	Alto	Medio
5. No existe departamento de seguridad en la empresa	Falta de reglas y controles	Alta	Medio	Medio
6. Se desconoce el estado actual en la seguridad interna del CEC-EPN.		Media	Medio	Medio

1.2.3.2.6. Plan de Tratamiento de Riesgos

Pasó 1: Una vez realizado la valoración del riesgo el CEC-EPN toma como riesgos aceptables a todas las vulnerabilidades que hayan tenido una valoración baja, el CEC-EPN deberá tratar en un periodo de tiempo razonable todas las vulnerabilidades que posean una valoración del riesgo media o mayor de manera que estas puedan ser mitigadas.

Pasó 2: Utilizando la guía NIST 800-30 se procederá a seleccionar los requerimientos de seguridad para el CEC-EPN, se seleccionara estos requerimientos en base a las vulnerabilidades que posean una valoración de riesgo media o mayor.

Pasó 3: Tomando en cuenta las vulnerabilidades que tuvieron una valoración del riesgo media o mayor, y utilizando los controles del estándar ISO/IEC 27002, seleccionaremos los controles adecuados para mitigar estas vulnerabilidades.

Pasó 4: Una vez seleccionados los controles del estándar ISO/IEC 27002 y los requerimientos de seguridad de la organización, seleccionaremos los controles que servirán para que se cumpla con cada uno de los requerimientos de seguridad.

Pasó 5: Con cada uno de los controles seleccionados en el paso 3, verificaremos el estado actual con el fin de ver si se encuentran implementados o son aplicables en la organización.

Pasó 6: Con aquellos controles que tiene un estado aplicable en la organización, se realizara una propuesta para que estos puedan ser implementados en la organización.

Pasó 7: Se realizara una guía de implementación para las soluciones que se plantearon en el paso 6.

1.3. DETERMINACIÓN DE LOS REQUERIMIENTOS DE SEGURIDAD

Una vez identificadas las vulnerabilidades y amenazas del Centro de Educación Continua se realizara la determinación de los Requerimientos de Seguridad necesarios para la organización basados en los criterios de seguridad que se encuentran dentro de la Guía NIST SP 800-30.

Las áreas de seguridad que tomarán en cuenta serán las siguientes:

- Seguridad Administrativa.
- Seguridad Operacional.
- Seguridad Técnica.

La siguiente tabla muestra los criterios de seguridad que corresponden a cada área de Seguridad.

	Criterios de Seguridad
Seguridad Administrativa	• Asignación de responsabilidades • Continuidad del soporte • Capacidad de respuesta a incidentes • Revisión Periódica de los controles de Seguridad • Liquidación e investigación a fondo del Personal. • Evaluación de Riesgos. • Capacitación Técnica y de Seguridad. • Autorización y Re-Autorización del Sistema. • Sistema o plan de seguridad de las aplicaciones
Seguridad Operacional	• El control de los contaminantes transportados por el aire (humo, polvo, productos químicos) • Controles para garantizar la calidad del suministro eléctrico • Acceso y Disposición de medios de almacenamiento • Distribución y etiquetado de Datos externos. • Protección de las instalaciones (por ejemplo, sala de informática, centro de datos, oficina) • Control de Humedad • Control de Temperatura
Seguridad Técnica	• Comunicaciones (por ejemplo, acceso telefónico, de interconexión de sistemas, enrutadores) • Criptografía • Control de Acceso Discrecional • Identificación y autenticación • Auditoría en detección de intrusiones • Reutilización de objetos • Auditoria al Sistema.

Tabla 1-11: Criterios de Seguridad
Fuente: Guía NIST SP 800-30

En base a los criterios de seguridad tomados de la Guía NIST SP 800-30 y la valoración de riesgos hecha en el apartado 1.2.3.2.5. Seleccionaremos los requerimientos de seguridad necesarios para el CEC-EPN.

Tabla 1-12: Requerimientos de Seguridad
Fuente: Elaborada por el Autor

	Criterios de Seguridad	Vulnerabilidades Asociadas	Requerimiento
Seguridad Administrativa	Asignación de responsabilidades de respuesta a incidentes	Organizacionales: 2, 3, 4, 6	SI
	Continuidad del soporte	Humanas: 1,8 Técnicas: 2, 3, 5	SI
	Capacidad de respuesta a incidentes	Humanas: 7, 8 Técnicas: 2, 3, 5 Organizacionales: 1,2,3,5	SI
	Revisión Periódica de los controles de Seguridad	Técnicas: 2 Organizacionales: 2,3,5,6	SI
	Liquidación e investigación a fondo del Personal.	Humanas: 4, 7, 9, 10 Organizacionales: 5	SI
	Evaluación de Riesgos.	Humanas: 1, 2, 7, 8 Técnicas: 2, 3 Organizacionales: 2, 3, 4, 5, 6	SI

	Capacitación Técnica y de Seguridad.	Organizacionales: 5	No
	Observación: El personal del CEC-EPN recibe una capacitación continua en el área técnica. Sin embargo se recomienda la capacitación en el área de seguridades a todo el personal, ya que al momento solo la recibe el área de Tecnologías		
	Autorización y Re-Autorización del Sistema.	Humanas: 4,7	SI
	Sistema o plan de seguridad de las aplicaciones	Humanas: 2 Técnicas: 3, 5 Organizacionales:2, 4, 5,6	SI
Seguridad Operacional	Controles para garantizar la calidad del suministro eléctrico		No
	Observación: El CEC-EPN cuenta con generadores de energía secundarios y unidades UPS en su sala de servidores. Se recomienda realizar un mantenimiento planificado de los generadores secundarios.		
	Acceso y Disposición de medios de almacenamiento	Humanas:3, 4, 7	SI
	Distribución y etiquetado de Datos externos.	Humanas: 4, 7, 8 Organizacionales: 4	SI
	Protección de las instalaciones	Técnicas: 2	SI

	Control de Humedad		SI
	Control de Temperatura		No
	Observación: Las salas de servidores y laboratorios cuentan con la ventilación necesaria para preservar la integridad de los activos informáticos.		
Seguridad Técnica	Comunicaciones (por ejemplo, acceso telefónico, de interconexión de sistemas, enrutadores)	Técnicas: 2	SI
	Criptografía	Humanas: 4, 7 Técnicas: 2, 5 Organizacionales:2,3,4,5	SI
	Control de Acceso Discrecional	Humanas: 4, 7, 8 Técnicas: 3 Organizacionales:2, 4 ,5	SI
	Identificación y autenticación	Humanas: 4, 6, 7 Organizacionales:2, 5	SI
	Auditoría en detección de intrusiones	Humanas: 4,7 ,8 Técnicas: 3, 5 Organizacionales:2,3,5,6	SI
	Reutilización de objetos	Humanas: 3 Técnicas: 3 Organizacionales:2	SI
	Auditoria al Sistema	Humanas: 3, 4, 7, 8 Técnicas: 2, 3, 5 Organizacionales: 2,3,4,5,6	SI

CAPITULO 2: PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN EL ESTÁNDAR ISO/IEC 27000.

2.1. SÍNTESIS DE LAS PRÁCTICAS DE SEGURIDAD ISO/IEC 27000 A APLICARSE EN EL CENTRO DE EDUCACIÓN CONTINUA

ISO/IEC 27001

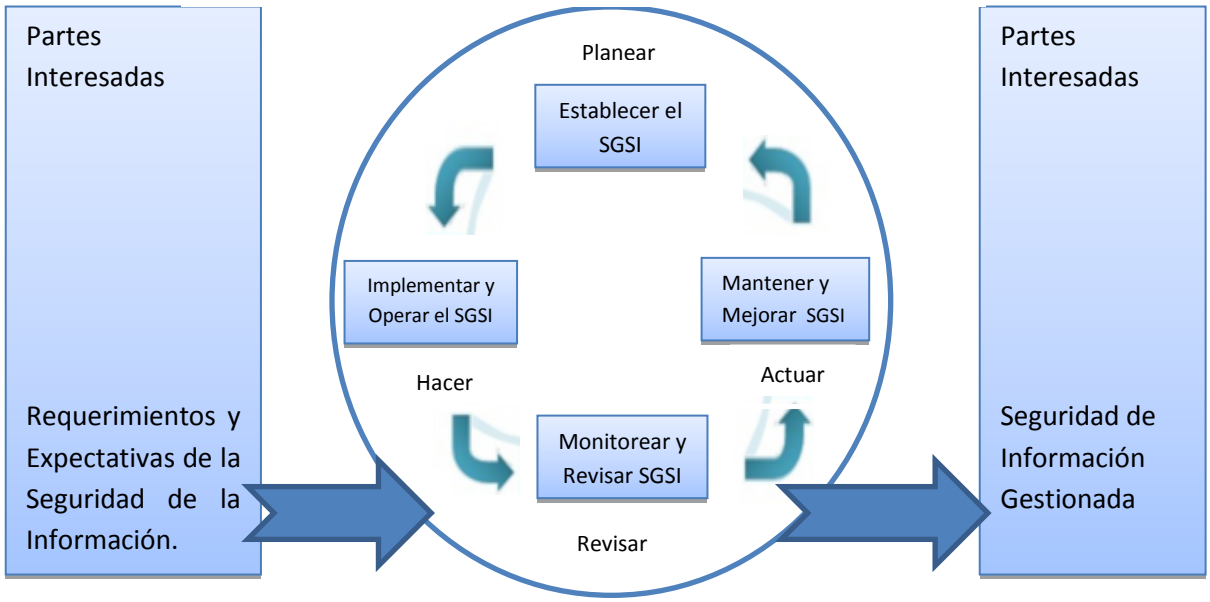
Este estándar nos permite plantear un modelo para la implementación, la operación, el monitoreo, la revisión, mejora y mantenimiento de un Sistema de Gestión de Seguridad de la Información. [6]

El estándar se centra en entender los requerimientos de seguridad de la organización así como la necesidad de implementar controles para mitigar los riesgos de seguridad de la información, teniendo en cuenta un sistema de mejora continua sobre el Sistema de Gestión de Seguridad de la Información.

El Estándar posee un modelo de procesos Planear -Hacer-Revisar-Actuar que se muestra en la figura a continuación.

Figura 1-7: Modelo Aplicado a los procesos SGSI [7]

Fuente: Estándar ISO/IEC 27001:2005



El presente proyecto realizara la etapa de planeación ya que el alcance del proyecto al ser una propuesta de Plan de Gestión de Seguridad no contempla una etapa de implementación del mismo, la misma que será realizada por el personal de la Coordinación de Gestión Tecnológica del CEC-EPN.

ISO/IEC 27002

El documento ISO/IEC 27002 anteriormente denominada ISO/IEC 17799:2005 es indispensable para la aplicación de éste estándar. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. De esta forma este estándar es el encargado de minimizar cualquier tipo falla en la seguridad de la información de la organización.

Estructura

El Estándar Internacional ISO/IEC 27002 contiene 11 dominios los mismos que se listan a continuación. [8]

- Política de seguridad.
- Aspectos organizativos de la seguridad de la información.
- Gestión de activos.
- Seguridad ligada a los recursos humanos.
- Seguridad física y ambiental.
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Gestión de incidentes en la seguridad de la información.
- Gestión de la continuidad del negocio.
- Cumplimiento.

2.2. ALCANCE Y LÍMITES PLAN DEL SEGURIDAD DE LA INFORMACIÓN

El plan de gestión de seguridad de la Información que se propone a continuación para el Centro de Educación Continua se enfoca en el mejoramiento de las actividades de TI que tienen lugar en el Departamento de Tecnología del Centro de Educación Continua de la Escuela Politécnica Nacional, con el fin de asegurar la seguridad de la información que la organización maneja. Se tomará en cuenta al personal que labora en la organización, los equipos informáticos, la infraestructura de la red y la infraestructura de las instalaciones de la organización.

El plan considera las instalaciones del CEC-EPN de la calle Ladrón de Guevara, las instalaciones en la Escuela Politécnica Nacional y las que se encuentran en el edifico Araucaria, así como las aplicaciones que se encuentran administradas por la unidad virtual del CEC-EPN

Basándonos en el estándar ISO/IEC 27001 trataremos de comprender las necesidades de seguridad de la organización, para lo cual se realizó en el apartado 1.2.3 la aplicación de la guía NIST 800-30 con lo cual pudimos evaluar las vulnerabilidades y riesgos de la organización para que con ello en el apartado 1.3 podamos evaluar y seleccionar los requerimientos de seguridad necesarios para la organización.

Mediante la utilización del estándar ISO/IEC 27002:2005 definiremos los objetivos de control y controles necesarios para los requerimientos de seguridad que se seleccionaron anteriormente.

Una vez seleccionados los objetivos de control y controles evaluaremos cada uno para seleccionar solo aquellos que sean aplicables dentro de la organización. Hecho esto realizaremos una guía de implementación para los controles que sean aplicables en la organización.

En la guía se recomendará herramientas, se creará plantillas y se dará recomendaciones para implementar estos controles de la mejor manera.

2.3. DETERMINACIÓN DE LOS OBJETIVOS DE CONTROL Y CONTROLES PARA LAS VULNERABILIDADES Y RIESGOS DENTRO DEL CENTRO DE EDUCACIÓN CONTINUA.

En base a los resultados obtenidos con la herramienta MSAT y la valoración de riesgos realizada en el apartado 1.2.3.2.5, se analizó junto con el personal de la Coordinación de Gestión Tecnológica del CEC-EPN los controles de la norma ISO/IEC 27002, con el fin de seleccionar los controles que se ajusten a las necesidades de la organización . [5]

Tabla 1-13: Determinación de los objetivos de control y controles
Fuente: Elaborada por el Autor

Riesgo Humano

Vulnerabilidad	Controles del estándar ISO/IEC 27002
Se terceriza el mantenimiento de activos informáticos como servidores.	• **6.1.5.** Acuerdos de confidencialidad • **7.1.1** Inventario de Activos • **10.2.2.** Supervisión y revisión de los servicios prestados por terceros.
No se tiene cláusulas de seguridad en los contratos de los servicios que se tercerizan.	• **6.1.5.** Acuerdos de confidencialidad • **10.2.2.** Supervisión y revisión de los servicios prestados por terceros.
No hay proceso formal para la eliminación de datos en medios electrónicos y formato impreso.	• **6.1.4.** Proceso de autorización para el tratamiento de la Información. • **10.5.1.** Copias de Seguridad de la Información • **10.7.4** Seguridad de la Documentación del Sistema.

No existe un monitoreo continuo de los accesos realizados en los servidores.	• **10.6.1** Controles de Red • **10.6.2** Seguridad de los servicios de Red. • **10.9.2** Transacciones en línea. • **11.2.1** Registro de usuario • **11.2.3** Gestión de contraseñas de usuario • **11.5.2** Identificación y autenticación de usuario • **11.5.3** Sistema de gestión de Contraseñas
No se lleva un registro de eventos producidos en los host y los dispositivos.	• **13.2.3** Recopilación de Evidencias • **13.1.1** Notificación de los eventos de seguridad de la información • **13.1.2** Notificación de puntos débiles de seguridad. • **10.10.5.** Registro de Fallas. • **11.4.3.** Identificación de los equipos en las redes • **11.4.6.** Control de la conexión de red • **11.5.1.** Procedimientos seguros de inicio de sesión.
No existen controles físicos para garantizar la seguridad de los activos de la empresa.	• **9.1.1** Perímetro de seguridad física • **9.1.2** Controles físicos de entrada • **9.1.3** Seguridad en oficinas, despachos e instalaciones • **9.2.7** Retirada de materiales propiedad de la empresa • **11.3.3** Política de puesto de trabajo despejado y pantalla limpia.
No se investiga a fondo al personal nuevo previo a su contratación.	• **8.1.2** Investigación de Antecedentes • **8.1.3** Términos y condiciones de Contratación
No existe un proceso formal de salida de los empleados.	• **8.3.1** Responsabilidad del cese o cambio. • **8.3.2** Devolución de activos • **8.3.3** Retirada de los derechos de acceso

Riesgo Técnico

Vulnerabilidad	
No se tiene una planificación para dar mantenimiento a la red del CEC-EPN	• **9.2.1** Emplazamiento y protección de equipos • **9.2.3** Seguridad del cableado • **9.2.4** Mantenimiento de Equipos • **11.4.1** Política sobre el uso de los servicios en red
Desconocimiento de las vulnerabilidades actuales de las aplicaciones de la empresa.	• **10.1.1.** Documentación de los procedimientos de operación • **12.1.1** Análisis y especificación de los requerimientos de Seguridad • **12.2.1** Validación de los datos de entrada • **12.3.1.** Política de uso de los controles criptográficos • **12.3.2** Gestión de claves • **12.4.1** Control de Software en Explotación
No se tiene una planificación para el mantenimiento de las aplicaciones.	• **10.10.2** Supervisión del uso del sistema • **12.5.2.** Revisión técnica de las aplicaciones tras efectuar cambios en el Sistema Operativo

Riesgo Organizacional

Vulnerabilidad	
No se tienen directivas y procedimientos para notificar problemas de seguridad.	• **13.1.1** Notificación de los eventos de seguridad de la información • **13.1.2** Notificación de puntos débiles de seguridad
No se tiene procedimientos de contingencia ante incidentes formales.	• **12.5.1** Procedimientos de Control de Cambios • **15.1.3** Protección de Documentos de la Organización

	• **15.1.4** Protección de datos y privacidad de la información de carácter personal • **12.5.4** Fugas de Información
No se evalúa el impacto de un nuevo servicio antes de implementarlo.	• **12.5.1** Procedimientos de Control de cambios. • **14.1.2** Continuidad del Negocio y evaluación de Riesgos. • **13.2.2** Aprendizaje de los incidentes de seguridad de la información.
No existe departamento de seguridad en la empresa	• **10.1.3** Segregación de tareas • **6.1.3** Asignación de Responsabilidades relativas a la seguridad de la información
Se desconoce el estado actual en la seguridad interna del CEC-EPN.	• **15.2.1** Cumplimiento de las políticas y normas de seguridad. • **15.2.2** Comprobación del cumplimiento técnico. • **15.3.1** Controles de Auditoría de Sistemas de Información • **10.10.1** Registro de Auditoria

A continuación se muestra el listado de controles seleccionados, así como a que área de seguridad pertenecen estos.

Tabla 1-14: Segregación de áreas de seguridad para los de los objetivos de control y controles seleccionados

Fuente: Elaborada por el Autor

Controles	Seguridad Administrativa	Seguridad Operacional	Seguridad Técnica
6.1.3. Asignación de Responsabilidades relativas a la seguridad de la información	X		
6.1.4. Proceso de autorización para el tratamiento de la Información	X		

Controles	Seguridad Administrativa	Seguridad Operacional	Seguridad Técnica
6.1.5. Acuerdos de confidencialidad	X		
6.1.8. Revisión independiente de la seguridad de la información	X		
6.2,1. Identificación de los riesgos derivados del accesos de terceros	X		X
7.1.1. Inventario de Activos	X		X
7.2.2. Etiquetado y manipulado de la Información		X	
8.1.1. Funciones y Responsabilidades	X		
8.1.2. Investigación de Antecedentes	X		
8.1.3. Términos y condiciones de Contratación	X		
8.3.1. Responsabilidad del cese o cambio	X		
8.3.2. Devolución de activos	X		
8.3.3. Retirada de los derechos de acceso	X		
9.1.1. Perímetro de seguridad física	X	X	X
9.1.2. Controles físicos de entrada.	X		X
9.1.3. Seguridad en oficinas, despachos e instalaciones		X	X
9.2.1. Emplazamiento y protección de equipos		X	
9.2.3. Seguridad del cableado			X
9.2.4. Mantenimiento de equipos	X		
9.2.7. Retirada de materiales propiedad de la empresa			X

Controles	Seguridad Administrativa	Seguridad Operacional	Seguridad Técnica
10.1.1. Documentación de los procedimientos de operación	X		
10.1.2. Gestión de Cambios	X		
10.1.3. Segregación de tareas	X		
10.2.2. Supervisión y revisión de los servicios prestados por terceros	X		
10.5.1. Copias de Seguridad de la Información			X
10.6.1. Controles de Red	X		X
10.6.2. Seguridad de los servicios de Red	X		X
10.7.4. Seguridad de la documentación del sistema		X	
10.8.1. Políticas y procedimientos de intercambio de información	X		
10.9.2. Transacciones en línea			X
10.10.1. Registro de Auditoría			X
10.10.2. Supervisión del uso del sistema	X		
10.10.5. Registro de Fallas			X
11.2.1. Registro de usuario			X
11.2.3. Gestión de contraseñas de usuario			X
11.3.3. Política de puesto de trabajo despejado y pantalla limpia.	X		
11.4.1. Política sobre el uso de los servicios en red	X		X
11.4.3. Identificación de los equipos en las redes			X

Controles	Seguridad Administrativa	Seguridad Operacional	Seguridad Técnica
11.4.6. Control de la conexión de red			X
11.5.1. Procedimientos seguros de inicio de sesión.	X		X
11.5.2. Identificación y autenticación de usuario			X
11.5.3. Sistema de gestión de Contraseñas			X
11.6.1. Restricciones del acceso a la Información			X
12.1.1. Análisis y especificación de los requerimientos de Seguridad	X		
12.2.1. Validación de los datos de entrada	X		X
12.3.1. Política de uso de los controles criptográficos	x		X
12.3.2. Gestión de Claves			X
12.4.1. Control del Software en Explotación.	X		
12.5.1. Procedimientos de Control de Cambios	X		
12.5.2. Revisión técnica de las aplicaciones tras efectuar cambios en el Sistema Operativo	X		
12.5.4. Fugas de Información			X
13.1.1. Notificación de los eventos de seguridad de la información	X		X
13.1.2. Notificación de puntos débiles de seguridad.	X		X
13.2.2. Aprendizaje de los incidentes de seguridad de la información.	X		X
13.2.3. Recopilación de evidencias	X		X

Controles	Seguridad Administrativa	Seguridad Operacional	Seguridad Técnica
14.1.2. Continuidad del Negocio y evaluación de Riesgos	X		
15.1.2. Derechos de Propiedad Intelectual		X	
15.1.3. Protección de documentos de la organización		X	X
15.1.4. Protección de datos y privacidad de la información de carácter personal		X	
15.2.1. Cumplimiento de las políticas y normas de seguridad.	X		
15.2.2. Comprobación del cumplimiento técnico.	X		
15.3.1. Controles de Auditoría de Sistemas de Información	X		X

2.3.1. SEGREGACIÓN DE ÁREAS DE SEGURIDAD PARA LOS DE LOS OBJETIVOS DE CONTROL Y CONTROLES SELECCIONADOS

Una vez seleccionados los controles que se ajustan a las necesidades de la organización, se seleccionó los controles necesarios para cada uno de los requerimientos de seguridad para cada área de seguridad de la organización.

SEGURIDAD ADMINISTRATIVA.

Asignación de responsabilidades de respuesta a incidentes

6.1 Organización Interna

6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.

7.1 Responsabilidad de los Activos

7.1.2 Propiedad de los Activos

8.1 Antes del Empleo

8.1.3 Términos y condiciones de contratación.

8.3 Cese del empleo o cambio de puesto de trabajo.

8.3.2 Devolución de activos.

8.3.3 Retirada de los derechos de acceso.

10.1 Responsabilidades y procedimientos de operación.

10.1.1 Documentación de los procedimientos de operación.

10.1.3 Segregación de Tareas

10.8 Intercambio de información.

10.8.1 Políticas y procedimientos de intercambio de información.

11.3 Responsabilidades de usuario.

11.3.3 Política de puesto de trabajo despejado y pantalla limpia.

11.5 Control de acceso al sistema operativo.

11.5.1 Procedimientos seguros de inicio de sesión.

Continuidad del soporte

9.2 Seguridad de los equipos.

9.2.4 Mantenimiento de los equipos.

10.1 Responsabilidades y procedimientos de operación.

10.1.2 Gestión de cambios.

14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

14.1.2 Continuidad del negocio y evaluación de riesgos.

Capacidad de respuesta a incidentes

6.2 Terceros.

6.2.1 Identificación de los riesgos derivados del acceso de terceros.

13.1 Notificación de eventos y puntos débiles de seguridad de la información.

13.1.1 Notificación de los eventos de seguridad de la información.

13.1.2 Notificación de puntos débiles de seguridad.

13.2 Gestión de incidentes y mejoras de seguridad de la información.

13.2.3 Recopilación de evidencias.

Revisión Periódica de los controles de Seguridad

10.2 Gestión de la provisión de servicios por terceros.

10.2.2 Supervisión y revisión de los servicios prestados por terceros.

10.10 Supervisión.

10.10.2 Supervisión del uso del sistema.

12.5 Seguridad en los procesos de desarrollo y soporte.

12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.

15.2.1 Cumplimiento de las políticas y normas de seguridad.

15.2.2 Comprobación del cumplimiento técnico.

Liquidación e investigación a fondo del Personal.

8.1 Antes del empleo.

8.1.2 Investigación de antecedentes.

8.3 Cese del empleo o cambio de puesto de trabajo.

8.3.1 Responsabilidad del cese o cambio.

8.3.2 Devolución de activos.

8.3.3 Retirada de los derechos de acceso

Evaluación de Riesgos.

6.1 Organización interna.

6.1.8 Revisión independiente de la seguridad de la información.

6.2 Terceros.

6.2.1 Identificación de los riesgos derivados del acceso de terceros.

10.2 Gestión de la provisión de servicios por terceros.

10.2.2 Supervisión y revisión de los servicios prestados por terceros.

10.10 Supervisión.

10.10.2 Supervisión del uso del sistema.

12.1 Requisitos de seguridad de los sistemas de información.

12.1.1 Análisis y especificación de los requisitos de seguridad.

12.5 Seguridad en los procesos de desarrollo y soporte.

12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

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

14.1.2 Continuidad del negocio y evaluación de riesgos.

Autorización y Re-Autorización del Sistema.

6.1 Organización interna.

6.1.4 Proceso de autorización de recursos para el tratamiento de la información

12.2 Tratamiento correcto de las aplicaciones.

12.2.1 Validación de los datos de entrada.

Sistema o plan de seguridad de las aplicaciones

6.1 Organización interna.

6.1.1 Compromiso de la Dirección con la seguridad de la información.

6.1.2 Coordinación de la seguridad de la información.

6.1.5 Acuerdos de confidencialidad.

6.2 Terceros.

6.2.1 Identificación de los riesgos derivados del acceso de terceros.

7.1 Responsabilidad sobre los activos.

7.1.1 Inventario de activos.

9.1 Áreas seguras.

9.1.1 Perímetro de seguridad física.

9.1.2 Controles físicos de entrada.

10.1 Responsabilidades y procedimientos de operación.

10.1.1 Documentación de los procedimientos de operación.

10.1.2 Gestión de cambios.

10.6 Gestión de la seguridad de las redes.

10.6.1 Controles de red.

10.6.2 Seguridad de los servicios de red.

10.8 Intercambio de información.

10.8.1 Políticas y procedimientos de intercambio de información.

11.4 Control de acceso a la red.

11.4.1 Política de uso de los servicios en red.

12.1 Requisitos de seguridad de los sistemas de información.

12.1.1 Análisis y especificación de los requisitos de seguridad.

12.3 Controles criptográficos.

12.3.1 Política de uso de los controles criptográficos.

12.4 Seguridad de los archivos de sistema.

12.4.1 Control del software en explotación.

12.5 Seguridad en los procesos de desarrollo y soporte.

12.5.1 Procedimientos de control de cambios.

12.6 Gestión de la vulnerabilidad técnica.

12.6.1 Control de las vulnerabilidades técnicas.

15.3 Consideraciones sobre las auditorías de los sistemas de información.

15.3.1 Controles de auditoría de los sistemas de información.

SEGURIDAD OPERACIONAL.

Acceso y Disposición de medios de almacenamiento

7.2 Clasificación de la información.

7.2.2 Etiquetado y manipulado de la información.

9.1 Áreas seguras.

9.1.1 Perímetro de seguridad física.

10.7 Manipulación de los soportes.

10.7.4 Seguridad de la documentación del sistema.

15.1 Cumplimiento de los requisitos legales.

15.1.2 Derechos de propiedad intelectual (DPI).

15.1.3 Protección de los documentos de la organización.

15.1.4 Protección de datos y privacidad de la información de carácter personal.

Distribución y etiquetado de Datos externos.

7.2 Clasificación de la información.

7.2.2 Etiquetado y manipulado de la información.

15.1 Cumplimiento de los requisitos legales.

15.1.3 Protección de los documentos de la organización.

Protección de las instalaciones

9.1 Áreas seguras.

9.1.3 Seguridad de oficinas, despachos e instalaciones.

Control de Humedad

9.1 Áreas seguras.

9.1.3 Seguridad de oficinas, despachos e instalaciones.

9.2 Seguridad de los equipos.

9.2.1 Emplazamiento y protección de equipos.

SEGURIDAD TÉCNICA.

Comunicaciones (por ejemplo, acceso telefónico, de interconexión de sistemas, enrutadores)

9.2 Seguridad de los equipos.

9.2.3 Seguridad del cableado.

10.6 Gestión de la seguridad de las redes.

10.6.1 Controles de red.

10.6.2 Seguridad de los servicios de red.

11.4 Control de acceso a la red.

11.4.1 Política de uso de los servicios en red.

11.4.6 Control de la conexión a la red.

Criptografía

10.5 Copias de seguridad.

10.5.1 Copias de seguridad de la información.

10.9 Servicios de comercio electrónico.

10.9.2 Transacciones en línea.

11.6 Control de acceso a las aplicaciones y a la información.

11.6.1 Restricción del acceso a la información.

12.2 Tratamiento correcto de las aplicaciones.

12.2.1 Validación de los datos de entrada.

12.3 Controles criptográficos.

12.3.1 Política de uso de los controles criptográficos.

12.3.2 Gestión de claves.

12.4 Seguridad de los archivos de sistema.

12.4.3 Control de acceso al código fuente de los programas.

12.5 Seguridad en los procesos de desarrollo y soporte.

12.5.4 Fugas de información.

15.1 Cumplimiento de los requisitos legales.

15.1.3 Protección de los documentos de la organización.

Control de Acceso Discrecional

7.1 Responsabilidad sobre los activos.

7.1.1 Inventario de activos.

9.1 Áreas seguras.

9.1.1 Perímetro de seguridad física.

9.1.2 Controles físicos de entrada.

9.1.3 Seguridad de oficinas, despachos e instalaciones.

Identificación y autenticación

11.2 Gestión de acceso de usuario.

11.2.1 Registro de usuario.

11.2.3 Gestión de contraseñas de usuario.

11.4 Control de acceso a la red.

11.4.3 Identificación de los equipos en las redes.

11.5 Control de acceso al sistema operativo.

11.5.1 Procedimientos seguros de inicio de sesión.

11.5.2 Identificación y autenticación de usuario.

11.5.3 Sistema de gestión de contraseñas.

Auditoría en detección de intrusiones

6.2 Terceros.

6.2.1 Identificación de los riesgos derivados del acceso de terceros.

10.10 Supervisión.

10.10.1 Registros de auditoría.

13.2 Gestión de incidentes y mejoras de seguridad de la información.

13.2.3 Recopilación de evidencias.

Auditoria al Sistema

10.10 Supervisión.

10.10.1 Registros de auditoría.

10.10.5 Registro de fallos.

13.1 Notificación de eventos y puntos débiles de seguridad de la información.

13.1.1 Notificación de los eventos de seguridad de la información.

13.1.2 Notificación de puntos débiles de seguridad.

15.3 Consideraciones sobre las auditorías de los sistemas de información.

15.3.1 Controles de auditoría de los sistemas de información

2.4. DETERMINACIÓN DE LOS OBJETIVOS DE CONTROL Y CONTROLES APLICABLES DEL CENTRO DE EDUCACIÓN CONTINUA.

Una vez seleccionados los controles que se necesitarían para mitigar los riesgos del CEC-EPN, evaluaremos cada uno de estos estos con el fin de ver el estado actual de los mismos en la organización.

Tabla 1-15: Determinación de Controles Aplicables.
Fuente: Elaborada por el Autor

	Justificación	Estado
6.1 Organización Interna		
6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.	Una vez que sea aprobada la propuesta de Plan de gestión de seguridad del presente proyecto, la dirección del CEC-EPN será la encargada de asignar a su personal las funciones correspondientes a la implementación del Plan de gestión de la seguridad; en caso de no tener el personal capacitado para dicho plan; se recomienda buscar la asesoría necesaria para realizar esta tarea.	Aplicable
6.1.4 Proceso de autorización de recursos para el tratamiento de la información	Una vez que se haya asignado las tareas correspondientes a la implementación del presente Plan, se debe asignar los recursos necesarios que exijan los encargados del proceso de implementación con el fin de implementar estas políticas de la mejor manera.	Aplicable
	El CEC-EPN no incluye ningún acuerdo de confidencialidad al momento que terceriza un servicio, como por ejemplo el mantenimiento de sus servidores, lo que podría	

6.1.5 Acuerdos de confidencialidad.	comprometer la información interna de la organización ya que no existe un respaldo legal que proteja la misma. Por ello se realizara una propuesta de acuerdo de confidencialidad en la guía de implementación del presente proyecto.	Aplicable
6.1.8 Revisión independiente de la seguridad de la información.	De momento no se cuenta con ninguna empresa o ente externo el cual evalué el nivel de seguridad de la organización.	Aplicable
6.2 Terceros.		
6.2.1 Identificación de los riesgos derivados del acceso de terceros.	El acceso a la sala de servidores solo es permitido para el personal del área de tecnología por lo cual se garantiza la seguridad de los mismos hacia terceros, sin embargo el CEC-EPN al ser un centro de educación tiene un constante flujo de personas en sus instalaciones lo cual podría ocasionar riesgos a la seguridad.	Aplicable
7.1 Responsabilidad de los Activos		
7.1.1 Inventario de activos.	Al momento se encuentran implementadas las políticas que pudimos observar en el apartado 1.2.3.2.4.	Implementado
7.1.2 Propiedad de los Activos	Al momento se encuentran implementadas las políticas que pudimos observar en el apartado 1.2.3.2.4; sin embargo se recomienda una revisión de los activos asignados al personal en periodos más cortos de tiempo.	Implementado

7.2 Clasificación de la información.		
7.2.2 Etiquetado y manipulado de la información.	Los Coordinadores del CEC-EPN tienen la responsabilidad de capacitar y comunicar a sus subordinados, sobre los servidores o carpetas que la CGT ha destinado para el almacenamiento de la información.	Implementado
8.1 Antes del Empleo		
8.1.2 Investigación de antecedentes.	No existe ningún control sobre los antecedentes del personal que va a ser contratado por el CEC-EPN. El no hacer esto puede repercutir en un alto riesgo de robo, fraude o uso inadecuado de las instalaciones.	Aplicable
8.1.3 Términos y condiciones de contratación.	Los términos de contratación así como las responsabilidades que tiene el personal a ser contratado por el CEC-EPN se encuentran detallados en el contrato de dicho empleado.	Implementado
8.3 Cese del empleo o cambio de puesto de trabajo.		
8.3.1 Responsabilidad del cese o cambio.	Una vez que el empleado es retirado de su cargo, el departamento de Recursos Humanos del CEC-EPN le notificará el proceso a seguir para el cese de sus servicios.	Implementado
8.3.2 Devolución de activos.	Una vez que un empleado termine su relación laboral con el CEC-EPN, deberá llenar un formulario indicando los bienes que este poseía con el fin de devolverlos, sin embargo en algunas ocasiones no se notifica de esto al Departamento de Tecnología haciendo que esta entrega de bienes no se realice como debería.	Implementado

8.3.3 Retirada de los derechos de acceso.	El ingreso al área de oficinas no es restringido en lo absoluto lo cual podría ocasionar riesgos en la seguridad interna del CEC-EPN. Todas las cuentas de usuario o el ingreso a cualquiera de los sistemas del CEC-EPN son eliminadas.	Aplicable
9.1 Áreas seguras.		
9.1.1 Perímetro de seguridad física.	Se han instaurado controles de seguridad física para proteger los activos de la empresa.	Implementado
9.1.2 Controles físicos de entrada.	El departamento de Tecnología así como la sala de servidores cuentan con los controles físicos necesarios para asegurar únicamente el ingreso del personal autorizado.	Implementado
9.1.3 Seguridad de oficinas, despachos e instalaciones.	El ingreso al área de oficinas no es restringido en lo absoluto lo cual podría ocasionar riesgos en la seguridad interna del CEC-EPN.	Aplicable
9.2 Seguridad de los equipos.		
9.2.1 Emplazamiento y protección de equipos.	Los equipos de red se hallan en una habitación cerrada con el acceso restringido, además los equipos portátiles están protegidos con cables de seguridad.	Implementado
9.2.3 Seguridad del cableado.	El cableado ya sea de red o de energía se encuentra correctamente protegido contra cualquier amenaza.	Implementado
9.2.4 Mantenimiento de los equipos.	Actualmente se tiene una planificación para el mantenimiento de los equipos por parte del departamento de Tecnología.	Implementado

9.2.7 Retirada de materiales propiedad de la empresa.	No existe control con la salida o ingreso de activos informáticos por parte del personal de seguridad de la EPN.	Aplicable
10.1 Responsabilidades y procedimientos de operación.		
10.1.1 Documentación de los procedimientos de operación.	El CEC-EPN cuenta con los manuales de operación de los sistemas que han sido implantados dentro de la organización.	Implementado
10.1.2 Gestión de cambios.	El CEC-EPN cuenta con un proceso de gestión de cambios.	Implementado
10.1.3 Segregación de Tareas	Cuando sea conveniente, se debería Implementar la segregación de tareas para reducir el riesgo de uso inadecuado deliberado o negligente del sistema	Aplicable
10.2 Gestión de la provisión de servicios por terceros.		
10.2.2 Supervisión y revisión de los servicios prestados por terceros.	Previo a la contracción de un servicio a tercerizar se realiza un concurso de merecimientos para la contratación con el fin de seleccionar la mejor oferta y tener un servicio más eficiente.	Implementado
10.5 Copias de Seguridad		
10.5 Copias de seguridad.	Se realizan bakups de las bases de datos de los sistemas de información.	Implementado
10.5.1 Copias de seguridad de la información.	El CEC-EPN posee un servidor de respaldos por lo cual el personal de la CGT se responsabiliza en garantizar la disponibilidad e integridad de la información almacenada en este.	Implementado

10.6 Gestión de la seguridad de las redes.		
10.6.1 Controles de red.	El CEC-EPN cuenta con firewalls en sus instalaciones, tanto para sus oficinas como para la protección de sus servidores.	Implementado
10.6.2 Seguridad de los servicios de red.	No se utiliza ningún hardware ni software para la detección de intrusiones lo que generaría riesgos en la seguridad de los servicios.	Aplicable
10.7 Manipulación de los soportes.		
10.7.4 Seguridad de la documentación del sistema.	La documentación del sistema se encuentra almacenada en un repositorio al cual solo tienen acceso los miembros de la CGT.	Implementado
10.8 Intercambio de información.		
10.8.1 Políticas y procedimientos de intercambio de información.	Se deberían establecer políticas, procedimientos y controles formales de intercambio con objeto de proteger la información mediante el uso de todo tipo de servicios de comunicación.	Aplicable
10.9 Servicios de comercio electrónico.		
10.9.2 Transacciones en línea.	Las aplicaciones no cifran los datos confidenciales antes de transmitirlos. Su respuesta indica que las aplicaciones principales del entorno no cifran los datos confidenciales cuando están almacenados	Aplicable
10.10 Supervisión.		
10.10.1 Registros de auditoría.	Se lleva un registro de todas las auditorías realizadas dentro del CEC-EPN.	Implementado

10.10.2 Supervisión del uso del sistema.	No se realizan tareas de monitoreo sobre los sistemas de la organización.	Aplicable
10.10.5 Registro de fallos.	Los fallos en los sistemas se registran en el help desk del CEC-EPN	Implementado
11.1 Requisitos de negocio para el control de acceso.		
11.2 Gestión de acceso de usuario.		
11.2.1 Registro de usuario.	La CGT es la encargada de la creación de cuentas de usuario en los sistemas que forman parte del CEC-EPN.	Implementado
11.2.3 Gestión de contraseñas de usuario	Todo equipo tiene configurado un nombre de usuario y contraseña, los mismos que serán asignados dentro del Directorio Activo que administra el Centro.	Implementado
11.3 Responsabilidades de usuario.		
11.3.3 Política de puesto de trabajo despejado y pantalla limpia.	No se tiene una política de puesto de trabajo despejado y pantalla limpia.	Aplicable
11.4 Control de acceso a la red.		
11.4.1 Política de uso de los servicios en red.	Al momento se encuentran implementadas las políticas que pudimos observar en el apartado 1.2.3.2.4.	Implementado
11.4.3 Identificación de los equipos en las redes.	Todo equipo que forme parte de la red administrativa del CEC-EPN, tendrá asignado un NOMBRE DE EQUIPO y pertenecerá a un GRUPO DE TRABAJO / DOMINIO asignado por la CGT.	Implementado

11.4.6 Control de la conexión a la red.	No se tiene un control de autenticación de usuarios para las conexiones remotas.	Aplicable
11.5 Control de acceso al sistema operativo.		
11.5.1 Procedimientos seguros de inicio de sesión.	No existen procedimientos de inicio de sesión.	Aplicable
11.5.2 Identificación y autenticación de usuario.	Se registran los intentos fallidos y correctos de autenticación.	Implementado
11.5.3 Sistema de gestión de contraseñas.	El CEC-EPN posee un sistema de contraseña compleja el cual modifica las contraseñas de sus aplicaciones	Implementado
11.6 Control de acceso a las aplicaciones y a la información.		
11.6.1 Restricción del acceso a la información.	Se limita el acceso a datos y funciones confidenciales según los privilegios de la cuenta en las aplicaciones principales.	Implementado
12.1 Requisitos de seguridad de los sistemas de información.		
12.1.1 Análisis y especificación de los requisitos de seguridad.	Actualmente no se conocen las vulnerabilidades para la seguridad en ninguno de los sistema del CEC-EPN	Aplicable
12.2 Tratamiento correcto de las aplicaciones.		
12.2.1 Validación de los datos de entrada.	Se validan los datos de entrada de todos los usuarios finales y todos los datos de entrada de las aplicaciones de cliente.	Implementado
12.3 Controles criptográficos.		
12.3.1 Política de uso de los controles criptográficos.	No se utiliza ningún software de cifrado de discos en el entorno. Además Las aplicaciones no cifran los datos confidenciales antes de transmitirlos. Las aplicaciones principales del entorno no cifran los datos confidenciales cuando están	Aplicable

	almacenados	
12.3.2 Gestión de claves.	Al momento se encuentran implementadas las políticas que pudimos observar en el apartado 1.2.3.2.4.	Implementado
12.4 Seguridad de los archivos de sistema.		
12.4.1 Control del software en explotación.	Los fabricantes independientes de software no ofrecen revisiones ni actualizaciones de seguridad.	Aplicable
12.5 Seguridad en los procesos de desarrollo y soporte.		
12.5.1 Procedimientos de control de cambios.	El CEC-EPN cuenta con procedimientos de control de cambios.	Implantado
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	No se realiza revisiones regulares sobre las aplicaciones del CEC-EPN	Aplicable
12.5.4 Fugas de información.	No se tiene implementado un DLP (Data Loss Prevention) dentro del CEC-EPN.	Aplicable
12.6 Gestión de la vulnerabilidad técnica.		
12.6.1 Control de las vulnerabilidades técnicas.	Actualmente no se conocen las vulnerabilidades para la seguridad en ningún área.	Aplicable
13.1 Notificación de eventos y puntos débiles de seguridad de la información.		
13.1.1 Notificación de los eventos de seguridad de la información.	No se lleva un registro de los eventos de seguridad de la información.	Aplicable
13.1.2 Notificación de puntos débiles de seguridad.	Actualmente no se conocen las vulnerabilidades para la seguridad en ningún área.	Aplicable

13.2 Gestión de incidentes y mejoras de seguridad de la información.		
13.2.3 Recopilación de evidencias.	El CEC-EPN no cuenta con un departamento encargado de la seguridad de la información de la organización.	Aplicable
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio		
14.1.2 Continuidad del negocio y evaluación de riesgos.	El CEC-EPN no cuenta con planes de continuidad ni de gestión de seguridad de la información.	Aplicable
15.1 Cumplimiento de los requisitos legales.		
15.1.2 Derechos de propiedad intelectual (DPI).	El CEC-EPN prohíbe el uso de programas o recursos para los cuales no exista una licencia o autorización de uso válido a nombre de la institución.	Implementado
15.1.3 Protección de los documentos de la organización.	La CGT es la responsable de la protección de los documentos de la organización mismos a los cuales solo tendrá acceso el personal autorizado.	Implementado
15.1.4 Protección de datos y privacidad de la información de carácter personal.	La CGT no se responsabiliza por la pérdida de información de tipo personal que los funcionarios mantengan en sus equipos. Además las aplicaciones no cifran los datos confidenciales antes de transmitirlos.	Aplicable
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.		
15.2.1 Cumplimiento de las políticas y normas de seguridad.	No se verifica si las políticas establecidas actualmente por el CEC-EPN se cumplen a cabalidad.	Aplicable

15.2.2 Comprobación del cumplimiento técnico.	No se verifica si las políticas implantadas actualmente por el CEC-EPN se cumplen a cabalidad.	Aplicable
15.3 Consideraciones sobre las auditorías de los sistemas de información.		
15.3.1 Controles de auditoría de los sistemas de información.	El CEC-EPN realiza auditorias sobre sus procesos más no sobre los sistemas de información de la organización.	Aplicable

CAPITULO 3: GUÍA DE IMPLEMENTACIÓN DEL PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

3.1. DETERMINACIÓN DE LOS ELEMENTOS CRÍTICOS ENCONTRADOS EN EL CENTRO DE EDUCACIÓN CONTINUA

Una vez definidos los objetivos de control y controles implementados y aplicables en la organización, se realizara un enfoque en aquellos que aún no hayan sido implementados, para lo cual a continuación se listarán estos y se plantearán la posible solución para estos.

Tabla 1-16: Determinación de Elementos Críticos.
Fuente: Elaborada por el Autor

	Solución
6.1 Organización Interna	
6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.	Se realizará una propuesta de segregación de tareas y funciones de la siguiente manera: • Responsable de la Información. • Responsable del Servicio • Administrador de la seguridad del Sistema
6.1.4 Proceso de autorización de recursos para el tratamiento de la información	Se recomienda el diseño de un proceso de gestión de autorizaciones para los nuevos recursos de tratamiento de la información, se recomienda la utilización de un check list con el fin de verificar si los nuevos recursos cumplen con lo que necesita la organización.
6.1.5 Acuerdos de confidencialidad.	Se realizará una propuesta de acuerdo de confidencialidad el cual podrá ser utilizado en los contratos de los servicios a tercerizar por el CEC-EPN
6.1.8 Revisión independiente de la seguridad de la información.	Se recomienda la contratación de una empresa externa o ente externo a la organización el cual realice una evaluación de la seguridad de la información de la organización.

6.2 Terceros.	
6.2.1 Identificación de los riesgos derivados del acceso de terceros.	Se recomienda la implementación de un sistema de tarjetas magnéticas o de aproximación para las personas que visiten el área administrativa de la organización para que solamente tengan acceso a su lugar de destino, además se recomienda la separación de la zona administrativa con la de los laboratorios para evitar posibles riesgos en la seguridad de la información.
8.1 Antes del Empleo	
8.1.2 Investigación de antecedentes.	Se recomienda realizar una investigación del historial laboral del personal previo a la contratación.
8.3 Cese del empleo o cambio de puesto de trabajo.	
8.3.3 Retirada de los derechos de acceso.	En caso de que un miembro del personal fuese despedido o separado del personal de la empresa, el personal correspondiente deberá notificarlo al personal de la Coordinación de Gestión Tecnológica para que estos procedan a la eliminación de toda cuenta de usuario que este posea.
9.1 Áreas seguras.	
9.1.3 Seguridad de oficinas, despachos e instalaciones.	Se realizará una propuesta de áreas seguras. La cual incluirá una propuesta de tarjetas magnéticas las cuales servirán tanto para el personal como para los visitantes para que de esta manera cada empleado solo tenga acceso a su departamento asignado y los visitantes solo puedan tener acceso al lugar al cual estos deseen visitar, de igual manera se propone la utilización de un libro de visitas con el fin de tener un registro de las personas que ingresan a las oficinas del CEC-EPN.
9.2 Seguridad de los equipos.	
9.2.7 Retirada de materiales propiedad de la empresa.	Se recomienda colocar un sistema de etiquetas magnéticas en los activos informáticos de la organización con el fin de evitar que estos se saquen sin permiso de las instalaciones del CEC-EPN.
10.1 Responsabilidades y procedimientos de operación.	
10.1.3 Segregación de Tareas	Se realizara una propuesta de segregación de tareas y funciones de la siguiente manera:

	• Responsable de la Información. • Responsable del Servicio • Administrador de la seguridad del Sistema
10.6 Gestión de la seguridad de las redes.	
10.6.2 Seguridad de los servicios de red.	Se recomienda la implantación de una herramienta IPS la cual nos permita controlar los accesos en la red de la organización y así proteger los sistemas del CEC-EPN de ataques y abusos. [10]
10.8 Intercambio de información.	
10.8.1 Políticas y procedimientos de intercambio de información.	Se recomienda la utilización de la guía ISO/IEC 27010:2012 con el fin de mejorar la seguridad de la información en las comunicaciones inter-organizacionales e intersectoriales.
10.9 Servicios de comercio electrónico.	
10.9.2 Transacciones en línea.	La información que se almacena dentro de los sistemas en línea del CEC-EPN, debe ser encriptada en su totalidad para evitar el plagio de la misma.
10.10 Supervisión.	
10.10.2 Supervisión del uso del sistema.	Se recomienda la utilización de un Sistema de Administración de red NMS (Network Management System).
11.3 Responsabilidades de usuario.	
11.3.3 Política de puesto de trabajo despejado y pantalla limpia.	Se recomienda la implantación y la concientización de una política de puesto de trabajo despejado y pantalla limpia en los ordenadores de la organización.
11.4 Control de acceso a la red.	
11.4.6 Control de la conexión a la red.	Se recomienda la implantación de un IDS para la detestación de accesos no autorizados a la red de la organización. [9]
11.5 Control de acceso al sistema operativo.	
11.5.1 Procedimientos seguros de inicio de sesión.	Cada estación de trabajo deberá contar con una contraseña robusta con el fin de que esta sea de uso exclusivo de la persona a la que le fue asignada.

12.1 Requisitos de seguridad de los sistemas de información.	
12.1.1 Análisis y especificación de los requisitos de seguridad	Se deberá realizar la planificación de evaluaciones periódicas de los niveles de seguridad de la organización con el fin de analizar el estado actual de los mismo y tener el conocimiento de los posibles riesgos que afecten a la organización.
12.3 Controles criptográficos.	
12.3.1 Política de uso de los controles criptográficos.	Se recomienda encriptar la información de sus sistemas de información previo a su almacenamiento en los servidores de la organización.
12.4 Seguridad de los archivos de sistema.	
12.4.1 Control del software en explotación.	Toda actualización o modificación sobre los sistemas de información que maneje la organización deberá ser documentada de manera correcta, para conocer qué cambio se realizó sobre el mismo y el responsable de este cambio.
12.5 Seguridad en los procesos de desarrollo y soporte.	
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Tras cualquier tipo de modificación ya sea en los sistemas de información o en sistemas operáticos sobre los cuales estos funcionan, se deberá verificar que no exista ningún tipo de impacto adverso para las actividades o seguridad de la Organización.
12.5.4 Fugas de información.	Se recomienda la implementación de un DLP dentro de la organización.
12.6 Gestión de la vulnerabilidad técnica.	
12.6.1 Control de las vulnerabilidades técnicas.	Se recomienda la planificación adecuada e implantación de herramientas las cuales muestren el estado actual de los activos de TI.
13.1 Notificación de eventos y puntos débiles de seguridad de la información.	
13.1.1 Notificación de los eventos de seguridad de la información.	Se recomienda la utilización del check list de la guía de auditoria del estándar ISO 27000, con el fin de realizar un análisis del estado actual del CEC-EPN. En caso de encontrar alguna anomalía en la seguridad de la información nos comunicaremos con el coordinador de la CTG del CEC-EPN con el fin de infórmale la anomalía encontrada.
13.1.2 Notificación de puntos débiles de seguridad.	

13.2 Gestión de incidentes y mejoras de seguridad de la información.	
13.2.3 Recopilación de evidencias.	En caso de encontrarse alguna anomalía que amenace la seguridad del CEC-EPN el personal correspondiente deberá realizar un informe ejecutivo el cual será entregado a la alta dirección de la organización para que esta tenga conocimiento de lo sucedido. Y así se proceda a la respectiva investigación de lo sucedido.
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio	
14.1.2 Continuidad del negocio y evaluación de riesgos.	Se recomienda la realización de un análisis de impacto en el negocio (BIA), con el fin de identificar los eventos que podrían causar interrupciones a los procesos de negocio y sus consecuencias para la seguridad de información. [11]
15.1 Cumplimiento de los requisitos legales.	
15.1.4 Protección de datos y privacidad de la información de carácter personal.	Se recomienda encriptar la información de sus sistemas de información previo a que esta se almacenada en los servidores de la organización.
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.	
15.2.1 Cumplimiento de las políticas y normas de seguridad.	Se recomienda la utilización del check list de la guía de auditoria del estándar ISO 27000, con el fin de realizar un análisis del estado actual del CEC-EPN.
15.2.2 Comprobación del cumplimiento técnico.	Se recomienda la utilización del check list de la guía de auditoria del estándar ISO 27000, con el fin de realizar un análisis del estado actual del CEC-EPN.
15.3 Consideraciones sobre las auditorías de los sistemas de información.	
15.3.1 Controles de auditoría de los sistemas de información.	Se recomienda la utilización del check list de la guía de auditoria del estándar ISO 27000.

3.2. GUÍA DE IMPLEMENTACIÓN DEL PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN,

Una vez determinadas las posibles soluciones a cada uno de los controles que seleccionamos, nos enfocaremos en ofrecer una guía para que el personal del CEC-EPN realice la implementación de los mismos.

3.2.1. ACUERDO DE CONFIDENCIALIDAD.

A continuación se planteará un acuerdo de confidencialidad para los servicios que contrata el CEC-EPN el mismo que se recomienda que se incluya para salvaguardar la seguridad de la organización. [12]

Figura 1-8: Propuesta de Contrato de Confidencialidad
Fuente: Elaborado por el autor

CONTRATO DE CONFIDENCIALIDAD DE SERVICIOS

EL CENTRO DE EDUCACIÓN CONTINUA DE LA ESCUELA POLITECNICA NACIONAL REPRESENTADA POR EL SEÑOR _____, A QUIEN EN LO SUCESIVO SE LE DENOMINARA "EL CONTRATANTE", Y POR LA OTRO LADO LA EMPRESA_____, REPRESENTADA POR EL SEÑOR _____, EN ADELANTE DENOMINADO "EL CONTRATISTA", AL TENOR DE LAS SIGUIENTES CLAUSULAS.

CLAUSULAS

Primera: De ser necesario cualquier tipo de información del tipo confidencial "EL CONTRATANTE" deberá brindársela a "EL CONTRATISTA "con el fin que este desempeñe sus servicios.

"EL CONTRATISTA" una vez realizado el presente contrato no tendrá derecho a divulgar ningún tipo de información brindada por "EL CONTRANTE" así mismo no tendrá derecho a copiarla, ni tratar de sacar lucro personal de la misma.

"EL CONTRATISTA" también debe comprometer a todo el personal involucrado en la prestación del servicio a cumplir con lo estipulado anteriormente.

"EL CONTRATANTE" podrá reclamar o solicitar se le devuelva la "información confidencial" en cualquier tiempo mediante comunicación que haga a "EL CONTRATISTA".

"EL CONTRATISTA" deberá eliminar cualquier tipo de copia de la información prestada así como devolver cualquier tipo de documentación que se le haya sido entregada por parte de "EL CONTRATANTE" una vez finalizado sus servicios.

Segunda: "EL CONTRATANTE" debe autorizar a "EL CONTRATISTA" mediante un documento escrito en caso de que sea deseo de "EL CONTRATANTE", o necesidad de "EL CONTRATISTA" divulgar todo o parte de la "información confidencial" a un tercero.

Tercera: "EL CONTRATISTA" en caso de incumplir el presente contrato o sus servicios deberá ofrecer una indemnización correspondiente a daños y perjuicios equivalente al costo del servicio contratado más el costo de abogados o de cualquier servicio que "EL CONTRATANTE" requiera para hacer cumplir esta cláusula.

Cuarta: La vigencia de este contrato será de _____ años contados a partir de la celebración de firma del presente contrato.

Quinta: En caso de necesitarse una modificación en el presente contrato, deberá realizarse mediante un documento escrito por "EL CONTRATANTE".

Sexta: "EL CONTRATANTE" y "EL CONTRATISTA" aceptan que las cláusulas escritas en este convenio dejan sin efecto cualquier acuerdo o negociación sostenido por ellas previamente, prevaleciendo lo dispuesto en este Documento.

Una vez estipuladas las clausulas a cumplir y siendo aceptadas por ambas partes, lo suscriben por duplicado en la ciudad de Quito, Provincia de Pichincha siendo el _____ de _____de _____.

_____ _____

"EL CONTRATANTE" "EL CONTRATISTA"

3.2.2. POLITICAS DE PERSONAL.

3.2.2.1. Segregación de tareas

De momento el Centro de Educación Continua de la Escuela Politécnica Nacional no cuenta con una unidad responsable de la seguridad de la información por lo que es prioritario que se la implemente. A continuación se presenta una propuesta de segregación de tareas y funciones de la siguiente manera: [13]

- Responsable de la Información.
- Responsable del Servicio
- Administrador de la seguridad del Sistema

3.2.2.2. Responsable de la Información

El responsable de la información debe ser una persona que forme parte de la alta dirección de la organización ya que este será el responsable del cuidado y del uso que se le dé a la información de la organización.

Por ende sobre el recaerá la responsabilidad de cualquier error o negligencia en la confidencialidad de la información de la organización.

Este será el encargado de determinar los niveles de seguridad de la información.

3.2.2.3. Responsable del Servicio

Este será el encargado de determinar los niveles y requisitos de seguridad de los servicios que brinda el CEC-EPN.

El responsable del servicio debe cuidar que los servicios y la información de los mismos estén disponibles cumpliendo con los requisitos de seguridad de los mismos.

3.2.2.4. Administrador de la seguridad del Sistema

Será el responsable de la implementación de medidas de seguridad necesarias en los sistemas de información, así como de la gestión, configuración de hardware y software en los equipos en los cuales funcionan dichos servicios.

En caso de necesitar un cambio en los requisitos de seguridad de la información, el Administrador de la Seguridad del Sistema será el responsable de rechazar o aprobar dichos cambios

Este estará a cargo de realizar evaluaciones para saber el estado en el que se encuentra la seguridad de la información del CEC-EPN

Este será el responsable de monitorear y hacer que se mantenga la seguridad de la información y será el encargado de promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad

3.2.2.5. Fugas de Información.

Para evitar las fugas de información se propone la implementación de un DLP dentro de la organización.

Mediante este DLP podremos supervisar como se usa la información de la organización en los equipos sea dentro o fuera de la red de la organización mediante la detección de comunicaciones salientes.

3.2.3. POLITICAS DE SEGURIDAD FISICA Y DE RED.

En este apartado se presentarán y difundirán hacia la organización las medidas que se podrían tomar para mejorar la seguridad física en el CEC-EPN, con el fin de crear perímetros de seguridad y de esta forma prevenir cualquier tipo de acceso no autorizado a la misma. [14]

3.2.3.1. Zonas de acceso restringido

En estas zonas será donde se deberá almacenar la información que se considera confidencial para el CEC-EPN, por tanto se deberá tener las medidas de seguridad adecuadas para asegurar la protección de la misma; el perímetro de esta zona deberá estar claramente definido para que solo el personal autorizado tenga acceso a la misma, por ello estas zonas deberán contar con los mecanismos de control o el personal de seguridad el cual controle la entrada y salida a las mismas. [15]

Estas zonas deberán contar con un sistema de vigilancia CCTV que cubra todos los accesos a las mismas para detectar cualquier tipo de intrusión no autorizada.

Estas zonas deberán estar disponibles solo para el personal autorizado para el manejo de la información dentro del CEC-EPN.

3.2.3.2. Acceso sobre las Áreas administrativas

De momento el CEC-EPN no controla el ingreso a la zona administrativa de ninguna manera, debido a que estas zonas comparten espacio con el área de laboratorios en donde se tiene un flujo significativo de personas por los cursos que la organización imparte, por ello es recomendable que el área administrativa y el área de laboratorios sean ubicadas en sectores diferentes de la organización con el fin de evitar amenazas a la seguridad del CEC-EPN.

Se recomienda la instalación de un sistema de puertas con cerradura electrónica en todas las oficinas del área administrativa del CEC-EPN y de esta manera evitar riesgos a la seguridad de la información por parte de gente ajena a la organización.

Se recomienda la implementación de un sistema de tarjetas magnéticas o de aproximación para los visitantes para que así estos tengan acceso solo a su lugar de destino, de igual manera se recomienda llevar un registro de las personas que ingresan al área de oficinas de la organización mediante un libro de visitas, por ello se propone ubicar al personal de seguridad calificado en los ingresos de estas zonas con el fin de que se lleve un registro de las personas ajenas a la organización que entran a dichas áreas.

Con esto en caso de suceder cualquier tipo de acceso no autorizado a las zonas restringidas se tendría un registro de los posibles culpables.

Figura 1-9: Propuesta de Libro de Visitas
Fuente: Elaborado por el autor

Registro de Visitas

Nombre	Cedula	Hora de Ingreso	Hora de Salida	Firma
Fecha:				

3.2.3.3. Vulnerabilidades Técnicas

La Coordinación de Gestión Tecnológica (CGT) del Centro de Educación Continua deberá enfocarse en fortalecer la planificación que se tiene actualmente para la revisión del estado de hardware y software de los equipos, la misma que se debe realizarse periódicamente con el fin de verificar el correcto funcionamiento de los equipos y verificar que en los mismos no se encuentren instalados ningún tipo de software que pueda atentar contra la seguridad de los usuarios de los equipos.

Una vez realizada la revisión sobre los equipos se deberá realizar un informe de cualquier irregularidad o novedad encontrada en los equipos con el fin notificarla a la alta dirección de la organización en caso de ameritarlo, o simplemente para llevar un registro de la evaluación realizada.

En caso de existir alguna falla en sus equipos se la deberá notificar al personal encargado, el mismo que está encargado de realizar las reparaciones necesarias en los equipos.

Herramientas de Monitoreo

Para salvaguardar la información y la seguridad de los usuarios de los equipos se recomienda la implantación de una herramienta la cual nos permita construir un perfil detallado del software y hardware que se encuentren instalados en los equipos de la organización.

A continuación se indican algunas herramientas las cuales podrían servir para este cometido:

SQLMap: Es una herramienta open source, en inglés, que automatiza el proceso de detección de vulnerabilidades de inyección SQL.

SECUNIA: Proporciona una serie de herramientas de escaneo de vulnerabilidades de software y gestión de parches. Dispone de versiones gratuitas para uso personal no comercial.

GFI: Es una herramienta, en español, que permite hacer gestión de actualizaciones, gestión de vulnerabilidades, auditoría de red y de software, inventario, gestión de cambios y análisis de riesgos y cumplimiento.

OCS Inventory: Es una herramienta de software libre que permite a los usuarios administrar el inventario de sus activos de TI.

3.2.3.4. Seguridad en la Red

En este apartado se presentan procedimientos y herramientas de monitoreo de red, los mismos que ayudaran a preservar la seguridad al utilizar la red de la organización

Autenticación de usuarios en conexiones externas.

De momento no existe manera de realizar conexiones externas a los distintos servidores del Centro de Educación Continua, lo cual dificultaría que el personal autorizado acceda desde afuera de las instalaciones de la organización. Por ello, se debe implementar un sistema de autenticación para conexiones externas, el mismo que solo deberá estar disponible para el rol de Administrador de la Seguridad del Sistema propuesto en el apartado 3.2.2.

En caso de necesitar conectarse externamente a uno de los servidores se deberá hacer una petición al Administrador de la seguridad del Sistema el cual autorizara o denegara la misma, en caso se aceptar la solicitud se creara una cuenta temporal para que el funcionario autorizado pueda ingresar de manera remota por el tiempo necesario.

Herramientas de Monitoreo de red

Mediante estas herramientas se podrá realizar la monitorización de la seguridad de la red de la organización así como detectar cualquier tipo de problema que se suscite en esta, con el fin de notificar al personal de la Coordinación de Gestión Tecnológica para que se realicen las acciones necesarias para mitigar dichos problemas.

A continuación se listará algunas herramientas las cuales podrían servir para este cometido:

Spiceworks: Es una herramienta gratuita de gestión, monitorización y resolución de problemas de red, creación automática de mapas de red, helpdesk.

Wireshark: Es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos..

Nmap: Herramienta de exploración de redes y auditoría de seguridad. Útil para inventario de red, planificación de actualizaciones y monitorización de disponibilidad de servidores o servicios.

Md5deep and hashdeep: Set de herramientas para comprobar el hash de los ficheros y su estado en relación a los originales para comprobar posibles alteraciones

3.2.4. POLITICAS DE MANEJO DE LOS SISTEMAS DE INFORMACIÓN.

Los sistemas de información que pertenecen al Centro de Educación Continua no son sometidos a pruebas para evaluar cualquier tipo de falla en los mismos, de momento no existe una planificación de mantenimiento sobre los mismos lo que puede dar como resultado que no se conozcan las vulnerabilidades de seguridad que se podrían presentar o en su defecto que los sistemas estén funcionando de manera defectuosa.

Al realizar el presente trabajo se pudo constatar que las aplicaciones del CEC-EPN de momento no encriptan de ninguna la manera la información que estas reciben antes de que esta se almacene en las bases de datos lo que podría representar una grave amenaza a la confidencialidad de la información.

Notificación de eventos y puntos débiles de seguridad de la información.

Con el fin de conocer el estado actual de la seguridad de los sistemas de información y en sí de toda la organización, se recomienda la utilización del Check List de Auditoria de la ISO/IEC 27000 para que de esta manera la organización realice una autoevaluación de sus niveles de seguridad. La implementación de este Check List recaerá sobre el Responsable del Servicio, este rol fue planteado en el apartado 3.2.2.

Se debe concientizar a los usuarios de los sistemas de información del CEC-EPN, que en caso de detectar una irregularidad o un desperfecto en el mismo se debe notificar de manera inmediata a la Coordinación de Gestión Tecnológica para que la misma tome las acciones correctivas necesarias con el fin de reparar dicho desperfecto. Este desperfecto debe ser notificado a la alta dirección de inmediato.

CAPITULO 4: CONCLUSIONES Y RECOMENDACIONES.

4.1. CONCLUSIONES

Una vez realizado el presente proyecto se obtienen las siguientes conclusiones.

- Al contar con un número significativo de alumnos y empleados, el Centro de Educación Continua requiere de un nivel adecuado de seguridad de la información, motivo por el cual requiere de las medidas de control necesarias para salvaguardar su información. Sin embargo, de momento adolece de falencias en el tema de seguridad de la información.

- La determinación de los requerimientos de seguridad de la organización será un factor de vital importancia, por lo cual se debe realizar de manera cuidadosa ya que de esta manera determinaremos los requerimientos que necesitan ser tratados con prioridad con el fin de que la organización obtenga un nivel adecuado de seguridad de la información.

- La evaluación de riegos realizada determinó que al momento no existe ningún riesgo de Alto nivel pero si varios de Medio nivel los mismos que pueden ser mitigados si se siguen la recomendaciones de los objetivos de control y controles que fueron seleccionados en el presente trabajo.

- Con el fin de mitigar los riegos de manera correcta, la selección de los objetivos de control y controles del estándar ISO/IEC 27002:2005 se debe realizar de manera minuciosa y ajustándose a las necesidades de la organización sobre la cual se va a implantar en Plan de Gestión de Seguridad de la Información.

- Los riegos del Centro de Educación Continua más significativos que se pudieron observar en los resultados de la herramienta MSAT, fueron los riesgos que se encuentran relacionados con el personal de la organización, debido a que de momento no existen políticas de seguridad dentro de la organización con un enfoque en el personal de la misma.

- Con el fin de obtener un punto de vista más profundo sobre el nivel de la seguridad de la información en el Centro de Educación Continua se utilizó la guía NIST 800-30 para seleccionar las falencias que necesitan ser atendidas con prioridad así como la identificación de los requerimientos de seguridad de la organización.

- La correcta implantación y ejecución del presente Plan de Gestión de Seguridad de la Información en el Centro de Educación Continua dependerá del compromiso de todo el personal de la misma, por ende se necesitara el compromiso de los coordinadores de los diferentes departamentos de la organización para que el plan brinde los mejores resultados en la organización.

4.2. RECOMENDACIONES.

- Se debe delegar a una persona o departamento, en específico, la etapa de implantación del Plan de Gestión de la Información, este será el responsable de verificar el cumplimiento de las políticas de seguridad en el Centro de Educación Continua y verificar que esté funcione de manera correcta con el paso del tiempo, asegurando de esta manera que los niveles de seguridad sean los adecuados en la organización.

- Se debe realizar tareas de monitoreo constantes sobre la red de la organización con el fin de evitar posibles fugas de información o ataques sobre la misma, por ello se debería realizar la implementación de una herramienta que ayude a proteger la seguridad de la información en la red de la organización.

- Se recomienda la utilización del Check List de auditoria del estándar ISO/IEC 27000 con el fin de que se realicen auditorías internas en la organización para conocer el estado en el que se encuentra la misma, esto debe ser delegado a un miembro de la Coordinación de Gestión Tecnológica el mismo que estará encargado tanto de su implementación como del análisis de los resultados obtenidos.

- Fortalecer las tareas de mantenimiento de red, equipos y aplicaciones que forman parte del Centro de Educación Continua para detectar posibles amenazas a la seguridad de los mismos y en si para mantener la seguridad de la organización.

- Utilizar más de una herramienta en caso de que se desee realizar un nuevo análisis de vulnerabilidades y riesgos en la organización ya que de esta manera se podrá tener una mejor visión para determinar los niveles de riesgo a los que se enfrenta la organización.

- En caso de necesitarse nuevas medidas de control para mitigar futuras amenazas dentro del Centro de Educación Continua, se recomienda la utilización de estándares de la familia ISO/IEC 27000 ya que estos proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

- Se recomienda la capacitación en el tema de seguridad informática a todo el personal administrativo de la organización ya que de momento solo se lo hace con miembros de la Coordinación de Gestión Tecnológica, para que de esta manera el personal del Centro de Educación Continua realice sus labores teniendo una noción de que deben realizar para mantener segura la información de la organización.

- Los encargados de la implantación del presente plan o aquellas personas que queden a cargo del cumplimento del mismo, deben tener un enfoque de mejora continua buscando así siempre mejores soluciones para las amenazas que podrían afectar al Centro de Educación Continua.

BIBLIOGRAFÍA

- [1] Escuela Politécnica Nacional – Centro de Educación Continua – Historia http://www.cec-epn.edu.ec/?categoria=1000 Ultimo Acceso Enero de 2014
- [2] Centro de Educación Continua – Manual de Calidad del CEC-EPN
- [3] TechNet - Herramienta de Evaluación de Seguridad de Microsoft (MSAT) http://technet.microsoft.com/es-es/library/cc185712.aspx Ultimo Acceso Enero de 2014
- [4] Metodología de la Evaluación de Riesgos – Guía Nist 800-30
- [5] Gestión de Riesgos - http://www.slideshare.net/xhagix/riesgos-2012 Ultimo Acceso Marzo de 2014
- [6] ISO 27000 - www.iso27000.es Ultimo Acceso Junio de 2014
- [7] El Anexo de ISO 27001 en español - https://iso27002.wiki.zoho.com Ultimo Acceso Julio de 2014
- [8] Controles de la ISO 27002:2005 http://www.iso27000.es/download/ControlesISO27002-2005.pdf Ultimo Acceso Julio de 2014
- [9] Sistema de prevención de intrusos - http://es.wikipedia.org/wiki/Sistema_de_prevenci%C3%B3n_de_intrusos Ultimo Acceso Junio de 2014
- [10] Sistema de detección de intrusos - http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos Ultimo Acceso Junio de 2014
- [11] Seguridad de la Información en Colombia - http://seguridadinformacioncolombia.blogspot.com/ Ultimo Acceso Agosto de 2014
- [12] Ideas para Pymes – Contrato de Confidencialidad http://www.ideasparapymes.com/herramientas/legal/machote-contrato-de-confidencialidad.dbsp Ultimo Acceso Agosto de 2014

- [13] Esquema Nacional de Seguridad - Responsabilidades y Funciones https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/801-Responsabilidades_en_el_ENS/801_ENS-responsabilidades_feb-11.pdf Ultimo Acceso Julio de 2014
- [14] Normas ISO 27000 – Protección Física y Ambiental http://www.cpciba.org.ar/archivos/adjuntos/seguridad.pdf Ultimo Acceso Junio de 2014
- [15] Seguridad Física - http://www.cni.es/comun/recursos/descargas/NS-03_Seguridad_Fisica.pdf Ultimo Acceso Agosto de 2014