ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERIA DE SISTEMAS

PROPUESTA DE POLITICAS DE SEGURIDAD DE LA INFORMACION PARA LA ESCUELA POLITECNICA NACIONAL

PROYECTO PREVIO A LA OBTENCIÓN DEL GRADO DE MAGISTER (MSc.) EN GESTION DE LAS COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN

MARCO OSWALDO SANTORUM GAIBOR
mosg81@hotmail.com

DIRECTOR: MSc. ING. GUSTAVO SAMANIEGO
gsamanie@server.epn.edu.ec

Quito, Marzo 2008

NDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCION

La Unidad de Gestión de la Información (UGI) de la Escuela Politécnica Nacional (EPN) encargada de la Gestión de las Tecnologías de la Información requiere elaborar las Políticas de Seguridad de la Información que le permita formalizar sus esfuerzos para que la información guarde los principios básicos de Seguridad de la Información como son la Integridad, Disponibilidad y Confidencialidad; esto quiere decir que la información sea correcta, completa y esté siempre a disposición, además que ésta sea utilizada sólo por aquellos que tienen autorización para hacerlo y además que los recursos tecnológicos sean aprovechados de manera adecuada y óptima.

Actualmente existen algunas Políticas de Seguridad de la Información en la UGI que se encuentran aisladas, sin embargo se requiere diseñar formalmente un cuerpo integral de Políticas de manera que interactúen con los procesos propios de la universidad y se consiga apoyar los objetivos estratégicos basándose en recomendaciones y mejores prácticas indicadas en los marcos de referencia.

Para esto se deberá hacer una caracterización del problema donde se determine la importancia y prioridades en cuanto a información y recursos tecnológicos de un ambiente universitario.

Estas políticas deben ser elaboradas en colaboración con los involucrados y además deben estar alineadas a las necesidades y objetivos estratégicos de la Escuela Politécnica Nacional. Todo este esfuerzo deberá ser ejecutado no de manera aislada sino a través de una correcta campaña de difusión que permita concienciar y garantizar el éxito en la implantación de estas políticas en la Escuela Politécnica Nacional.

Esta propuesta de políticas será analizada por la Unidad de Gestión de la información de la EPN junto al abogado de la Institución quienes emitirán sus observaciones, para que a continuación se constituya en una propuesta oficial de Políticas de Seguridad de la Información, las mismas que serán sometidas a la aprobación de Consejo Politécnico para que puedan ser oficialmente implantadas en la Escuela Politécnica Nacional.

Mediante la evaluación y validación desde el punto de vista legal, económico, organizacional, técnico y operacional se podrá determinar la validez y aplicabilidad de dichas políticas en el ambiente de la Escuela Politécnica Nacional.

CAPITULO 1
CARACTERIZACION DEL AMBIENTE DE LA ESCUELA POLITECNICA NACIONAL

1.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Hoy en día resulta frecuente encontrarse con que las personas directamente involucradas con la seguridad de la información (PSI) tengan una visión limitada de lo que significa desarrollar las políticas de seguridad de la información, puesto que no es suficiente el escribirlas y tratar de ponerlas en práctica. Se incluye la asignación de responsables, se procura difundirlas, y se supervisa su cumplimiento, pero aún esto no es suficiente.

Muchas veces estas políticas de seguridad de la información fallan precisamente por el desconocimiento de lo que implica el desarrollarlas y mas aún si estas políticas están destinadas a un ambiente universitario, por esto se requieren definir adecuadamente que es una política de seguridad de la información, caracterizar el ambiente de implantación y establecer el proceso formal de desarrollo de las mismas tomando en cuenta el marco de referencia propuesto por el Instituto SANS.

1.1.1 DEFINICION DE POLITICA

Una política es típicamente un documento en el que se esbozan los requisitos específicos o normas que deben cumplirse. Las políticas son generalmente un punto específico que abarca un espacio único. Por ejemplo, una “Política de Uso

Aceptable" abarcaría las normas y reglamentos para el uso adecuado de las instalaciones de computación. 1

“Declaración general de principios que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías “. 2

Tomando en cuenta estas definiciones resulta importante aclarar el término política desde el comienzo, ya que existen términos utilizados en seguridad informática todos los días, pero algunas veces son utilizados indistintamente sin entender su real significado, por esto a continuación se definen los siguientes términos correctamente.

ESTÁNDAR

Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares sirven como especificaciones para la implementación de las políticas y son diseñados para promover la implementación de las políticas de alto nivel de la organización antes que crear nuevas políticas.

---

[1] Tomado de: The SANS Security Policy Project
[2] Tomado de: Guía para elaboración de políticas de seguridad. Patrick D. Howard.

MEJOR PRÁCTICA

Es una regla de seguridad específica a una plataforma que es aceptada a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la organización.

GUÍA

Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son, esencialmente recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

PROCEDIMIENTO

Los procedimientos definen específicamente cómo las políticas, estándares, mejores prácticas y guías serán implementados en una situación dada. Los procedimientos son dependientes de la tecnología o de los procesos y se refieren a plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada a dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema.

Los procedimientos seguirán las políticas de la institución, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

1.1.2 POR QUÉ REDACTAR POLÍTICAS DE SEGURIDAD DE LA INFORMACION PARA LA EPN

Existen varias razones por las cuales es recomendable tener políticas escritas en una universidad como la Escuela Politécnica Nacional.

La siguiente es una lista de algunas de estas razones:

1. Para cumplir con regulaciones legales o técnicas.
2. Como guía para el comportamiento profesional y personal.
3. Permite unificar la forma de trabajo de las personas en las diferentes dependencias universitarias que tengan responsabilidades y tareas similares.
4. Permite establecer mejores prácticas en el trabajo universitario.
5. Permiten asociar los objetivos estratégicos de la universidad al ejercicio diario de las labores y actividades universitarias.
6. Se constituyen en un referente a la hora de detectar situaciones anormales en el trabajo.

1.2 LA INFORMACIÓN UNIVERSITARIA

La información universitaria se la puede considerar como un componente fundamental de la estructura universitaria, y está relacionada con:

- Profesores
- Estudiantes
- Personal Administrativo
- Trabajadores
- Actividades de Docencia
- Actividades de Investigación
- Actividades de Vinculación
- Gestión Administrativa
- Equipamiento
- Capital Intelectual
- Etc.

Esta información se la puede encontrar en forma de archivos, bases de datos, tablas o simplemente como texto, pero cualquiera sea el caso, fluye internamente y también hacia el exterior.

Siendo esta Información crítica para el desenvolvimiento de las labores de la Escuela Politécnica Nacional, para su categorización y caracterización se la puede enfocar desde el punto de vista técnico, legal, institucional.

A continuación se busca evidenciar la necesidad del establecimiento de políticas de seguridad de la información en la Escuela Politécnica Nacional.

1.2.1 EL ENFOQUE TÉCNICO

Los puntos principales a tratar desde este enfoque son:
a) El Soporte
b) Los Mecanismos de Almacenamiento y Modificación
c) Los Mecanismos de Acceso
d) El Mantenimiento
e) Compatibilidad de la información

El Soporte

Los soportes típicos de la universidad, son los ficheros, carpetas, libros y en computadores.

A pesar de existir computadores en casi todas las dependencias universitarias, todavía existe un gran uso de archivadores y documentación en papel.

Es necesario entonces la generación de políticas que potencien la migración gradual de la información hacia el almacenamiento en un computador, brindar los medios para permitir compatibilidad y facilitar el acceso a la comunidad politécnica.

Los Mecanismos de Almacenamiento y Modificación

Una vez que la información es almacenada por un computador, al igual que cuando se poseía información en papel, se deberá asignar un responsable quien deberá gestionar el ingreso, modificación, eliminación de la misma quedando bajo su autorización cualquier proceso sobre la misma. Ante un problema de cualquier tipo con la información, no se diluyen las responsabilidades de las dependencias involucradas.

Para esto será aconsejable que la información que esa sección genere no salga de ese lugar, que existan códigos de almacenamiento y modificación de información diferentes a los de acceso. Procurar que esta información sea centralizable y no esté centralizada con el fin de proteger la información ante posibles daños intencionales e intromisiones no autorizadas.

Los Mecanismos de Acceso

Al igual que en el Almacenamiento, nadie podrá acceder a determinada información salvo que el responsable lo permita. Esto no quiere decir que un responsable pueda negar información debidamente solicitada, sino que es el único que autoriza el acceso.

Cuando una dependencia necesite trabajar con información de otra dependencia, sólo deberá tener acceso y a lo estrictamente necesario.

El Mantenimiento

Deberá existir un plan de mantenimiento y servicios técnicos propios así como mantenimiento de los sistemas y equipos que se desarrollen y adquieran para la institución.

El mantenimiento debe estar previsto en el diseño original del Sistema, caso contrario no será conveniente llevar un proyecto a la práctica puesto que un sistema sin un mantenimiento planificado podría resultar en un peligro potencial para al Institución.

Las políticas de servicios y gastos de mantenimiento deben plantearse en función de prioridades de la Institución.

Compatibilidad de la información

Como en toda institución se evidencian problemas de incompatibilidad de la información, de manera que cuando se compara datos tomados de diferentes fuentes, sistemas o dependencias, estos suelen ser incompatibles ocasionando que esta información sea inútil. Por ejemplo si se pregunta el número de estudiantes por docente se generan varias respuestas debido a la interpretación que se podría dar al dato "docente", ya que se lo podría tomar como persona, o como un cargo o como horas de profesores.

Es necesario entonces establecer las políticas que garanticen el flujo de la información diseñando adecuadamente la estructura de ésta y de sus ficheros contenedores. Para estos casos las políticas deben ser generadas en una etapa de planificación previa, tomando como parámetros los indicadores que la Institución considere válidos para su estructura, evaluación y corrección de ser necesario, de manera que se garantice el flujo y compatibilidad de la información en la institución.

1.2.2 EL ENFOQUE NORMATIVO - LEGAL

La legislación ecuatoriana contempla sanciones y tipifica delitos como la omisión de responsabilidades en la difusión de información, el perder o difundir información no autorizada, el vulnerar información confidencial, etc.
La legislación ecuatoriana y los convenios internacionales firmados por el Ecuador evidencian la necesidad de elaborar Políticas de Seguridad de la Información que permitan garantizar la integridad, confidencialidad y disponibilidad de la información.

La elaboración de estas políticas deberán ceñirse a normas internacionales que garanticen el éxito de las mismas además de la validez de su aplicación, para esto en el presente trabajo se ha considerado el marco de referencia propuesto por el Instituto SANS, esto además de brindar calidad, garantiza la preocupación y seriedad de la Institución ante la Información Universitaria.

1.2.3 EL ENFOQUE INSTITUCIONAL

Las autoridades de la Escuela Politécnica Nacional deberán apoyar la implantación de las políticas de seguridad de la información tomando en cuenta la importancia de las mismas y en pos de apoyar los objetivos institucionales, garantizando de esta manera el cumplimiento y la aceptación de las mismas.

Para esto, estas políticas deben ser elaboradas a medida, es decir, ajustándose a la realidad de la institución. Por lo tanto, es necesario conocer la estructura de la institución, además de definir las responsabilidades de la misma como el priorizar dicha implantación por etapas, fijar los objetivos y evaluar continuamente el funcionamiento de dichas políticas.

1.3 ORGANIZACIÓN DE LA UNIVERSIDAD

La Escuela Politécnica Nacional es una de las instituciones de educación superior más antiguas del país. Fue fundada el 27 de agosto de 1869, mediante decreto expedido por la Convención Nacional del Ecuador, por iniciativa del Presidente Gabriel García Moreno, con el fin de poner al servicio del país un centro de investigación y formación de profesionales en ingeniería y ciencias.

Al iniciar su vida académica cuenta con el concurso de destacados catedráticos alemanes tales como el Padre Juan Bautista Menten y el Padre Teodoro Wolf, y el italiano Padre Luis Sodiro. Posteriormente se unieron los profesores jesuitas alemanes Luis Dressel, José Kolberg y Emilio Muellendorf, entre otros.

La EPN tiene como misión: “Generar, asimilar y adaptar, transmitir y difundir, aplicar, transferir y gestionar el conocimiento científico y tecnológico, para contribuir al desarrollo sostenido y sustentable de nuestro país, como resultado de una dinámica interacción con los actores de la sociedad ecuatoriana y la comunidad internacional”.

Según el Estatuto vigente desde Octubre del 2006, en su artículo 6, Título II, establece la siguiente estructura institucional:

NIVEL DIRECTIVO:

- Consejo Politécnico
    - Comisión de Evaluación Interna,
    - Comisión de Vinculación con la Colectividad
- Consejo Académico
    - Comisión de Docencia
    - Comisión de Investigación y Extensión
- Consejo de Facultad
- Consejo de Departamento.

NIVEL EJECUTIVO:

- Rectorado
    - Dirección de Auditoria Interna,
    - Dirección de Asesoría Jurídica,
    - Dirección de Planificación,
    - Dirección de Relaciones Institucionales,
    - Dirección Administrativa,
    - Dirección Financiera,
    - Dirección de Recursos Humanos,
    - Secretaría General,
    - Unidad de Gestión de Proyectos,
    - Unidad de Gestión de la Información.
- Vicerrectorado,
    - Unidad de Admisión,
    - Unidad de Desarrollo Curricular,
    - Unidad de Bienestar Estudiantil y Social,
- Decanato de Facultad
- Subdecanato de Facultad
- Jefatura de Departamento

NIVEL CONSULTIVO

- Asamblea Politécnica

Los profesores, funcionarios administrativos y trabajadores, usuarios de la red de la Escuela Politécnica Nacional, en adelante en esta tesis serán mencionados como funcionarios de la EPN.

1.4 UNIDAD DE GESTIÓN DE LA INFORMACIÓN (UGI)

La UGI fue creada en el año de 1968, en el rectorado del Ing. Rubén Orellana. Inicialmente fue llamada Instituto de Informática y Computación (ICC) y en aquel tiempo en la Escuela Politécnica Nacional no había ninguna carrera que hiciera referencia al ámbito de la informática o computación.

Era necesario realizar una gran inversión para la compra de un equipo de tercera generación, cuyo uso inicial serviría para los estudiantes de tesis de las carreras de ingeniería. Su demanda fué tal que acudían personas de diversas instituciones para utilizar sus servicios como las personas del Banco Central, CEPE, Diners Club, entre otros.

Al fenecer la máquina también la ICC llegó a su final, pero se observó que surgía la necesidad de un centro de cómputo que permita gestionar la información y tecnologías relacionadas. Es por esto que se crea el “Centro de Cómputo de la EPN” bajo la dirección del Ing. Xavier García y en el rectorado del Ing. Alfonso Espinosa. Durante este período se realiza el proyecto del backbone para la EPN, creándose la Polired (Nombre de la Red de la EPN).

El antiguo Centro de Cómputo actualmente se denomina Unidad de Gestión de la Información (UGI) de la Escuela Politécnica Nacional.

1.4.1 MISIÓN

La Unidad de Gestión de la Información (UGI) es el organismo de la Escuela Politécnica Nacional encargado de administrar los recursos de la institución brindando apoyo en la gestión de redes, comunicaciones, soporte y asesoramiento técnico interno y externo además de la elaboración de la planificación estratégica de sistemas de la institución.

1.4.2 VISIÓN

La Unidad de Gestión de la Información será reconocida como la unidad más eficiente y eficaz de la Escuela Politécnica Nacional brindando un soporte eficiente a la comunidad politécnica y a los usuarios externos basados siempre en los más altos principios éticos y apoyados en el compromiso y experiencia del personal.

1.4.3 OBJETIVOS GENERALES

- Administrar los Recursos computacionales e informáticos.
- Apoyar los análisis de procesos y procedimientos
- Recomendar estructuras
- Brindar soporte en los Recursos computacionales e informáticos
- Capacitar en los recursos computacionales e informáticos

1.4.4 OBJETIVOS ESPECIFICOS

- Asesorar a las autoridades y usuarios de la comunidad politécnica en la adquisición de los recursos computacionales de la institución y en la optimización de su utilización.
- Desarrollar y mantener sistemas informáticos para el manejo de la información estudiantil y académica de la Escuela Politécnica Nacional.
- Proponer políticas para el desarrollo de los procesos internos y uso de recursos computacionales e informáticos.
- Proponer la actualización y renovación de los sistemas de computación, de acuerdo con los avances tecnológicos y las necesidades de la Institución.
- Proporcionar información gerencial como apoyo a la toma de decisiones.
- Mantener la información de recursos computacionales e informáticos que dispone la Politécnica.

- Centralizar información académica y estudiantil.
- Gestionar soluciones a problemas de redes y comunicaciones.
- Implantar y gestionar políticas, procesos y procedimientos para el funcionamiento de los servicios de Internet e Intranet.
- Apoyar en prácticas de laboratorio en redes y comunicaciones.

1.4.5 DEFINICIÓN DE POLÍTICAS BÁSICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA ESCUELA POLITÉCNICA NACIONAL

La definición de políticas básicas de seguridad de la información de la Escuela Politécnica Nacional se desarrolla con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información considerada sensible en la institución y ante los requerimientos legales de la legislación ecuatoriana y tratados internacionales a los cuales se ha sumando el Estado Ecuatoriano y por ende sus instituciones para la lucha contra delitos informáticos.

El desarrollo de este Proyecto de Tesis forma parte de esta definición de políticas. Una vez elaboradas las Políticas de Seguridad de la Información se revisará y oficializará la propuesta de aprobación de dichas políticas ante Consejo Politécnico.

Como se contempla más adelante, las etapas de desarrollo de políticas de seguridad de la información son 11, entre las cuales se encuentra la creación de las políticas, etapa que es motivo de la presente tesis.

1.5 EL INSTITUTO SANS (SYSADMIN AUDIT NETWORK SECURITY)

“SANS es una importante y confiable fuente de capacitación y certificación en Seguridad de la Información a nivel mundial; que desarrolla, mantiene y pone a disposición del público sin costo alguno, la mayor colección de documentos de investigación sobre diversos aspectos de la Seguridad de la Información. “ 3.

El Instituto SANS (SysAdmin Audit Network Security) fue creado en 1989 como una organización de investigación cooperativa y de educación. Sus programas ahora llegan a más de 165.000 profesionales de la seguridad en todo el mundo. Una serie de personas como auditores, administradores de red, jefes de seguridad de la información, etc. comparten las lecciones que aprenden y conjuntamente encuentran soluciones a los desafíos que se enfrentan. A través de SANS interactúan muchos profesionales de la seguridad de diversas organizaciones mundiales, profesionales de universidades, y otros quienes colaboran con la seguridad de la información de toda esta comunidad.

Más de 1200 documentos de investigación relacionados con el ámbito de la Seguridad de la Información se comparten y se ponen a disposición de los usuarios de SANS.

El proyecto “Sans Security Policy Project” se constituye en un proyecto de investigación, consenso y participación de toda la comunidad SANS. El objetivo final del proyecto es el de ofrecer los recursos necesarios para el rápido desarrollo y aplicación de Políticas de Seguridad de la Información.

---

[3] Tomado de: The SANS Security Policy Project

SANS proporciona un gran conjunto de recursos entre estos las plantillas para la elaboración de Políticas de Seguridad de la Información que permitan cumplir los requerimientos planteados por marcos de referencia como ISO27001, ITIL, COBIT, etc.

Estas plantillas proporcionadas por SANS son una recopilación de documentos o plantillas genéricas que son un conjunto de mejores prácticas que se constituyen en la base esencial de la elaboración de Políticas de Seguridad de la Información que garanticen los principios básicos de Seguridad de la Información como son la Integridad, Confidencialidad y Disponibilidad.

SANS propone el análisis de dichos documentos de acuerdo al ambiente de implantación. Una vez que estos hayan sido analizados, las observaciones, comentarios, conclusiones emitidas retroalimentan al proyecto.

Además aclara que hay una serie de normas y certificaciones que se pueden utilizar como base del marco de Políticas de Seguridad de la Información, para esto se deberá tomar cuenta lo siguiente:

- ¿Cuál marco se ajusta a la cultura organizacional?
- ¿Qué requisitos reglamentarios se deben cumplir?
- ¿Qué es lo que dictan sus principios rectores?
- ¿Qué desafíos ha experimentado en el Pasado?
- ¿Cuál es la tecnología de futuro incluida en su planificación?
- ¿Qué recursos se posee para cumplir las regulaciones?

El autor Sheldon Borkin ha realizado una comparación entre el estándar HIPAA Health Insurance Portability and Accountability Act y el estándar de seguridad de la información ISO/IEC 17799.

HIPPA contempla la elaboración de Políticas de Seguridad de la Información para lo cual toma en cuenta las mejores prácticas propuestas por SANS.

Comparación de Estándares por by Sheldon Borkin

ISO ~ HIPPA	19	En los tópicos analizados los requisitos propuestos por ISO e HIPPA son aproximadamente los mismos.
ISO > HIPPA	12	En los tópicos analizados los requerimientos de ISO incluyen los requerimientos de HIPPA y además un número sustancial de requerimientos adicionales.
HIPPA > ISO	11	En los tópicos analizados el estándar HIPPA incluye al menos un requerimiento no contemplado entre los requerimientos de ISO. Esta designación puede ser utilizada aún si existieran substancialmente más requerimientos ISO para el tópico.

CONCLUSIONES

1.- El cumplir la norma HIPPA no garantiza el cumplimiento de la norma ISO en su totalidad.

2.- Si se cumple la norma ISO no se garantiza el cumplimiento en su totalidad de los requisitos propuestos por HIPPA.

3.- La estrategia adecuada para cumplir las dos normas debe ser entonces realizar auditorias internas y externas que permitan evaluar el cumplimiento de las mismas.

Si bien todas las mejores prácticas propuestas garantizan que su aplicación resultará beneficiosa para el ámbito de aplicación de las mismas, sin embargo no se constituyen en una ley a ser cumplida a cabalidad puesto que las diferentes estructuras organizacionales requieren de una aplicación caracterizada para su propio ámbito.

Por lo tanto, la aplicación de las mejores prácticas propuestas por SANS para la elaboración de las Políticas de Seguridad de la Información, resulta beneficiosa y positiva puesto que los objetivos de seguridad perseguidos como son la Confidencialidad, Integridad y Disponibilidad de la Información, son los mismos principios básicos que son perseguidos también por marcos de referencia como ITIL e ISO.

La propuesta de políticas generada en base a las mejores prácticas propuestas por SANS será puesta a consideración sin perjuicio de ser modificada, aumentada o disminuida, puesto que se constituye en un esfuerzo inicial totalmente perfectible y abierto para ser sometido a discusión en espera de la obtención de las Políticas de Seguridad de la Información definitivas que serán aprobadas por Consejo Politécnico.

CAPITULO 2
ELABORACION DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

2.1 ETAPAS DE DESARROLLO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El ciclo de vida de las Políticas comprenden 11 etapas que pueden ser agrupadas en 4 fases: Fase de Desarrollo, Fase de Implementación, Fase de Mantenimiento y Fase de Eliminación.

El alcance de este proyecto de tesis contempla dentro de la primera fase de este ciclo, las etapas de creación y revisión.

A continuación se describe el ciclo de vida de las políticas, véase Figura 2.1.

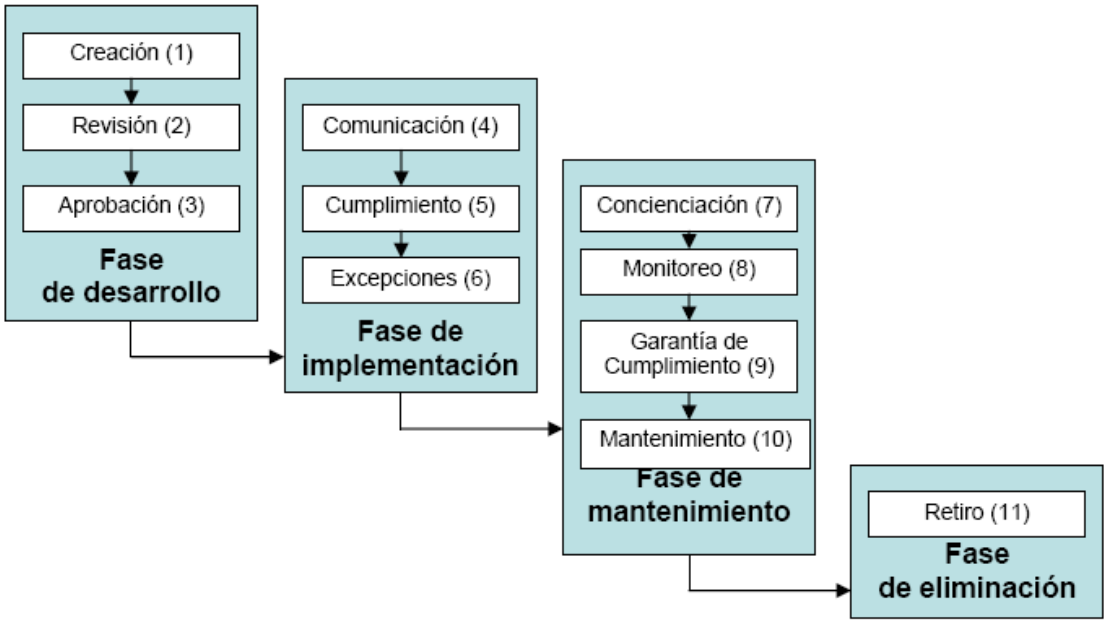

Figura 2.1 Etapas de Desarrollo PSI

Tomado de: Guía para elaboración de políticas de seguridad. Patrick D. Howard

2.1.1 FASE DE DESARROLLO

Durante esta fase las políticas son creadas, revisadas y aprobadas.

Creación

La creación de las políticas implica identificar la necesidad de crear las mismas, por ejemplo debido a requerimientos legales, regulaciones técnicas, contractuales u operacionales de la Escuela Politécnica Nacional.

Se debe determinar el alcance y la aplicabilidad de la política, los roles y las responsabilidades inherentes a la aplicación de la política y garantizar la factibilidad de su implementación. La creación de una política también incluye la investigación para determinar los requerimientos universitarios para desarrollar las políticas, es decir, que autoridades deben aprobarla, bajo que supervisión se debe coordinar el desarrollo, los formatos de redacción y la investigación de las mejores prácticas para su aplicabilidad a las necesidades institucionales.

De esta etapa se tendrá como resultado las políticas documentadas de acuerdo con los procedimientos y estándares seleccionados, al igual que la coordinación con la Unidad de Gestión de la Información de la EPN para obtener información necesaria y la aceptación de dichas políticas.

Revisión

Una vez documentadas las políticas creadas bajo la coordinación de la UGI, éstas deberán ser remitidas a un individuo o grupo independiente que posea una perspectiva diferente que la persona que redactó las políticas para su evaluación antes de su aprobación final. Esto trae consigo un apoyo más amplio para dichas políticas debido al incremento en el número de individuos involucrados, también el

aumento de credibilidad en las políticas gracias a la información recibida de diferentes especialistas que forman parte del grupo de revisión.

Propio de esta etapa será la presentación de las políticas a los revisores, a quienes se expondrá cualquier punto que puede ser importante en la revisión, explicando sus objetivos, el contexto y los beneficios potenciales de las políticas justificando la necesidad de las mismas.

Como parte de esta revisión, se espera entonces que el creador de las políticas recopile los comentarios y las recomendaciones para realizar los cambios en las políticas y así efectuar todos los ajustes y las revisiones necesarias para obtener una versión final de las políticas que se encontrarán listas para la aprobación por Consejo Politécnico, organismo universitario encargado de dicha oficialización.

Aprobación

El paso final en la fase de desarrollo de las políticas es la aprobación. El objetivo de esta etapa será el obtener el apoyo de Consejo Politécnico, a través de la aprobación y oficialización de las mismas.

La aprobación permite iniciar la implementación de las políticas. Se requiere que la UGI como organismo proponente de dichas políticas haga una presentación formal ante las autoridades y Consejo Politécnico, quienes emitirán recomendaciones para que una vez contempladas, dichas políticas sean aceptadas por la administración.

Puede ocurrir que por incertidumbre de las autoridades sea necesaria una aprobación temporal.

2.1.2 FASE DE IMPLEMENTACIÓN

En esta fase las políticas son comunicadas y acatada.

Comunicación

La comunicación de la política es la primera etapa que se realiza en la fase de implementación. La política debe ser inicialmente difundida a los miembros de la comunidad universitaria o a quienes sean afectados directamente por la política (contratistas, proveedores, usuarios de cierto servicio, etc.).

Esta etapa implica determinar el alcance y el método inicial de distribución de la política. Debe planificarse esta etapa con el fin de determinar los recursos necesarios y el enfoque que debe ser seguido para mejorar la visibilidad de la política.

Cumplimiento

La etapa de cumplimiento incluye actividades relacionadas con la ejecución de la política.

Implica trabajar con autoridades de la universidad, Rector, Vicerrector, Decanos, Subdecanos, Jefes de Departamento y los Jefes de dependencias, para interpretar cuál es la mejor manera de implementar la política en diversas situaciones y dependencias; asegurando que la política es entendida por aquellos que requieren implementarla, monitorearla, hacerle seguimiento, reportar regularmente su cumplimiento y medir el impacto inmediato de la política en las actividades operativas. Dentro de estas actividades está la elaboración de informes a la administración del estado de la implementación de la política.

Excepciones

Aprobar las excepciones donde la implementación no es posible.

Debido a problemas de coordinación, falta de personal y otros requerimientos operacionales, no todas las políticas pueden ser cumplidas de la manera que se pensó al comienzo. Por esto, cuando los casos lo ameriten, es probable que se requieran excepciones a la política para permitir a ciertas dependencias o personas el no cumplimiento de la política.

Debe establecerse un proceso para garantizar que las solicitudes de excepciones son registradas, seguidas, evaluadas, enviadas para aprobación o desaprobación, documentadas y vigiladas a través del periodo de tiempo establecido para la excepción. El proceso también debe permitir excepciones permanentes a la política al igual que la no aplicación temporal por circunstancias de corta duración.

2.1.3 FASE DE MANTENIMIENTO

Los usuarios deben ser conscientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se le debe dar mantenimiento actualizándola si se requiriese.

Concienciación

Garantiza la concienciación permanente de la política.

La etapa de concienciación de la fase de mantenimiento comprende los esfuerzos continuos realizados para garantizar que las personas estén conscientes de la política y buscan facilitar su cumplimiento. Esto es hecho al definir las necesidades de concienciación de las diversas audiencias dentro de la universidad tales como

Estudiantes, Profesores, Empleados Administrativos, Trabajadores, Autoridades, etc. En relación con la adherencia a la política se determinan los métodos de concienciación más efectivos para cada grupo de audiencia. Por ejemplo: reuniones informativas, cursos de entrenamiento, mensajes de correo, etc. Se define también el desarrollo y difusión de material de concienciación como presentaciones, afiches, circulares, etc. La etapa de concienciación también incluye esfuerzos para integrar el cumplimiento de la política y retroalimentación sobre el control realizado para su cumplimiento. La tarea final es medir la concienciación de los miembros de la comunidad universitaria con la política y ajustar los esfuerzos de acuerdo con los resultados de las actividades medidas.

Monitoreo

Seguimiento y reporte del cumplimiento de la política.

Durante la fase de mantenimiento, la etapa de monitoreo es realizada para seguir y reportar la efectividad de los esfuerzos en el cumplimiento de la política. Esta información se obtiene de la observación de los profesores, estudiantes, empleados administrativos y los cargos de supervisión, mediante auditorias formales, evaluaciones, inspecciones, revisiones y análisis de los reportes de contravenciones y de las actividades realizadas en respuesta a los incidentes.

Esta etapa incluye actividades continuas para monitorear el cumplimiento o no de la Política a través de métodos formales e informales y el reporte de las deficiencias encontradas a las autoridades apropiadas.

Garantía de cumplimiento

Afrontar las contravenciones de la política.

La etapa de garantía de cumplimiento de las políticas incluye las respuestas de la administración a actos u omisiones que tengan como resultado contravenciones de la Política, con el fin de prevenir que siga ocurriendo. Esto significa que una vez que una contravención sea identificada, la acción correctiva debe ser determinada y aplicada a los procesos (esto es, la revisión del proceso y su mejoramiento), a la tecnología (actualización) y a las personas (acciones disciplinarias) con el fin de reducir la probabilidad de que vuelva a ocurrir. Se deberá entonces incluir información sobre las acciones correctivas adelantadas para garantizar el cumplimiento en la etapa de concienciación.

Mantenimiento

La etapa de mantenimiento está relacionada con el proceso de garantizar la vigencia y la integridad de la política. Esto incluye hacer seguimiento a las tendencias de cambios en la tecnología, en los procesos, en las personas, en la institución, en el enfoque del negocio, que pudieran afectar la política. Se deberá entonces recomendar y coordinar las modificaciones, documentándolas en la política y registrando las actividades de cambio.

Esta etapa también garantiza la disponibilidad continuada de la política para todas las partes afectadas por ella, al igual que el mantenimiento de la integridad de la política a través de un control de versiones efectivo. Cuando se requieran cambios a la política, las etapas realizadas antes deben ser re-visitadas, en particular las etapas de revisión, aprobación, comunicación y garantía de cumplimiento.

2.1.4 FASE DE ELIMINACIÓN

La política se retira cuando no se la requiera más.

Retiro

Prescindir de la política cuando no se la necesite más.

Después que la política ha cumplido con su finalidad y ya no es necesaria, entonces debe ser retirada, esto se daría por ejemplo cuando la universidad cambió la tecnología a la cual aplicaba o se creó una nueva política que la reemplazó.

La etapa de retiro corresponde a la fase de eliminación del ciclo de vida de la política, y es la etapa final del ciclo. Esta función implica retirar una política superflua del inventario de políticas activas para evitar confusión, archivarla para futuras referencias y documentar la información sobre la decisión de retirar la política es decir, la justificación, quién autorizó, la fecha, etcétera.

Estas cuatro fases del ciclo de vida reúnen 11 etapas diferentes que deben seguirse durante el ciclo de vida de una política específica. No importa como se agrupen, tampoco importa si estas etapas son abreviadas por necesidades de inmediatez, pero cada etapa debe ser realizada. Si en la fase de desarrollo la universidad intenta crear una política sin una revisión independiente, se tendrán políticas que no estarán bien concebidas ni serán bien recibidas por la comunidad universitaria. En otras circunstancias, y por falta de visión, puede desearse omitir la etapa de excepciones de la fase de implementación, pensando equivocadamente que no existirán circunstancias para su no cumplimiento. También se podría descuidar la etapa de mantenimiento, olvidando la importancia de mantener la integridad y la vigencia de las políticas. Muchas veces se encuentran políticas inoficiosas en los documentos de importantes organizaciones, indicando que la etapa de retiro no está siendo realizada.

No sólo se requiere que las once etapas sean realizadas, algunas de ellas deben ser ejecutadas de manera cíclica, en particular mantenimiento, concienciación, monitoreo, y garantía de cumplimiento.

2.2 DECLARACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN A ELABORAR

El Principal objetivo del proyecto emprendido por el Instituto SANS es el de proveer las recomendaciones y las mejores prácticas organizacionales a la hora de desarrollar las Políticas de Seguridad de la Información.

Para esto sugiere el uso de plantillas de Políticas que han sido desarrolladas y probadas por un grupo de experimentados profesionales en seguridad con una amplia experiencia en proyectos gubernamentales y comerciales quienes han debido someter a cada una de estas políticas a un riguroso proceso de aprobación, constituyéndose estas plantillas en el punto de partida de este trabajo.

Para el mejor uso de las políticas, estas se agrupan considerando los siguientes criterios:

POLITICAS DE ADMINISTRACION DE RECURSOS

- PSI.AR.01 Política de Uso Adecuado
- PSI.AR.02 Política de Correo Electrónico
- PSI.AR.03 Política de reenvío de correo electrónico
- PSI.AR.04 Política de retención de correo electrónico
- PSI.AR.05 Política de auditoría y evaluación de vulnerabilidades
- PSI.AR.06 Política de evaluación de riegos
- PSI.AR.07 Política de Sensibilidad de la Información
- PSI.AR.08 Política de bases de datos de credenciales
- PSI.AR.09 Política de instalación de software

POLITICAS DE DISPOSITIVOS DE SEGURIDAD

- PSI.DS.01 Política de protección de servidores contra el Malware
- PSI.DS.02 Política de uso de antivirus

PSI.DS.03 Política de seguridad de la zona desmilitarizada DMZ

POLITICAS DE DISPOSITIVOS PERIFERICOS

PSI.DP.01 Política de uso de líneas telefónicas para transmisión de datos

PSI.DP.02 Política de conexión y acceso telefónico dial-in

PSI.DP.03 Política de uso de Dispositivos de Comunicación Personal y voicemail

PSI.DP.04 Política de uso de dispositivos de almacenamiento removible

POLITICAS DE CIFRADO

PSI.C.01 Política de Cifrado Aceptable

PSI.C.02 Política de Contraseñas

POLITICAS DE SEGURIDAD FISICA

PSI.SF.01 Política de seguridad de servidores

POLITICAS DE REDES

PSI.R.01 Política de seguridad de enrutadores

PSI.R.02 Política de red privada virtual de la Polired

PSI.R.03 Política de Acceso Remoto

PSI.R.04 Política de la Extranet

PSI.R.05 Política de comunicación Inalámbrica

PSI.R.06 Política de Seguridad de redes LAN internas

A continuación se presenta una descripción de las Políticas de seguridad de la Información sugeridas las mismas que serán motivo de análisis para validar su aplicabilidad en la Escuela Politécnica Nacional.

DESCRIPCION DE POLITICAS DE ADMINISTRACION DE RECURSOS

PSI.AR.01 Política de Uso Adecuado

El objetivo de esta política es determinar los parámetros aceptables para el uso de equipos de cómputo en la Escuela Politécnica Nacional.

PSI.AR.02 Política de Correo Electrónico

Esta política se refiere al uso de correo electrónico que es remitido desde el dominio y servidores de correo de la Escuela Politécnica Nacional (epn.edu.ec) y que se aplica a todos los funcionarios que operan en nombre de esta.

PSI.AR.03 Política de reenvío de correo electrónico

La presente política cubre el reenvío automático de correo electrónico, previniendo la transmisión indebida de información sensible por parte de funcionarios de la EPN.

PSI.AR.04 Política de retención de correo electrónico

La política de retención de correo electrónico permite a los funcionarios determinar cual información enviada o recibida debe ser retenida y por cuanto tiempo.

PSI.AR.05 Política de auditoría y evaluación de vulnerabilidades

El propósito de este documento es establecer un acuerdo para inspecciones de seguridad de la Red y equipos de la Escuela Politécnica Nacional ha ser realizadas por auditores internos o externos.

PSI.AR.06 Política de evaluación de riegos

Esta política tiene como propósito autorizar a la entidad a cargo del proceso de evaluación de riesgos, realizar evaluaciones periódicas de riesgos de seguridad de la información con el propósito de determinar áreas de vulnerabilidad e iniciar una remediación inmediata.

PSI.AR.07 Política de Sensibilidad de la Información

La Política de Sensibilidad de la Información permite a los funcionarios de la EPN determinar a qué información pueden tener acceso las personas que no son miembros de la EPN, así como la sensibilidad relativa de la información que no debe ser revelada fuera de la Escuela Politécnica Nacional sin la autorización apropiada.

PSI.AR.08 Política de bases de datos de credenciales

Esta política establece los requisitos mínimos de seguridad para el almacenamiento y recuperación de nombres de usuarios y contraseñas de manera segura en la base de datos conocida como base de datos de credenciales ha ser usada por programas, aplicativos, sistemas que requieran autenticarse mediante esta, a través de la red de la Escuela Politécnica Nacional.

PSI.AR.09 Política de instalación de software

El propósito de esta política es reducir al mínimo el riesgo de pérdida de funcionalidad en programas, la exposición de información sensible contenida dentro de la red de la Escuela Politécnica Nacional, el riesgo de introducir malware y la exposición ilegal de software no autorizado en ejecución.

DESCRIPCION DE POLITICAS DE DISPOSITIVOS DE SEGURIDAD

PSI.DS.01 Política de protección de servidores contra el Malware

El propósito de esta política es determinar la necesidad de proporcionar una protección adecuada contra las amenazas malware, como virus, gusanos, SPAM y aplicaciones spyware entre otros, en los equipos de la institución.

PSI.DS.02 Política de uso de antivirus

Establecer los requisitos y procedimientos que deben cumplirse por todas las computadoras conectadas a las redes de la EPN para asegurar un eficaz descubrimiento y prevención de virus.

PSI.DS.03 Política de seguridad de la zona desmilitarizada DMZ

Esta política establece los requerimientos de seguridad de la información para todos los equipos conectados a la Polired localizados en la “Zona Desmilitarizada” (DMZ). El cumplimiento de estos requerimientos minimizará el riesgo potencial de daño de la imagen pública de la EPN causado por el uso no autorizado de los recursos de la institución y de la pérdida de datos confidenciales y propiedad intelectual de la EPN.

DESCRIPCIÓN DE POLITICAS DE DISPOSITIVOS PERIFERICOS

PSI.DP.01 Política de uso de líneas telefónicas para transmisión de datos

El presente documento explica las políticas y procedimientos de uso aceptable de las líneas telefónicas de la Escuela Politécnica Nacional utilizadas en la transmisión de datos.

PSI.DP.02 Política de conexión y acceso telefónico dial-in

El propósito de esta política es el de proteger la información electrónica de la Escuela Politécnica Nacional definiendo apropiadamente el acceso dial-in a la Polired y que sea realizado solamente por personal autorizado.

PSI.DP.03 Política de uso de Dispositivos de Comunicación Personal y voicemail

Esta política aplica al uso de cualquier Dispositivo de Comunicación Personal y de voicemail de la EPN otorgados por la misma o usados para fines de la institución.

PSI.DP.04 Política de uso de dispositivos de almacenamiento removible

El propósito de esta política es minimizar el riesgo de pérdida o exposición de información sensible de la Escuela Politécnica Nacional y reducir el riesgo de adquirir infecciones de virus y malware en computadoras operadas en la Escuela Politécnica Nacional durante el uso de dispositivos de almacenamiento removible.

DESCRIPCIÓN DE POLITICAS DE CIFRADO

PSI.C.01 Política de Cifrado Aceptable

El propósito de esta política es brindar una orientación para el uso del cifrado con algoritmos que han obtenido un reconocimiento público y que han demostrado que trabajan eficazmente. Además, esta política brinda orientación para asegurar el cumplimiento de regulaciones internacionales.

PSI.C.02 Política de Contraseñas

El propósito de esta política es establecer una norma para la creación de contraseñas seguras, la protección de esas contraseñas y la frecuencia de cambio.

DESCRIPCIÓN DE POLITICAS DE SEGURIDAD FISICA

PSI.SF.01 Política de seguridad de servidores

El propósito de esta política es establecer las normas para la configuración de los servidores de la Escuela Politécnica Nacional. La puesta en práctica eficaz de esta política reducirá al mínimo el acceso no autorizado a la red de la Escuela Politécnica Nacional y a su información propietaria.

DESCRIPCIÓN DE POLITICAS DE REDES

PSI.R.01 Política de seguridad de enrutadores

El propósito de este documento es describir los requerimientos mínimos de seguridad en la configuración de todos los routers y switches conectados a la Polired de la EPN.

PSI.R.02 Política de red privada virtual (VPN) de la Polired

El propósito de esta política es proporcionar las normas para las conexiones remotas IPSec o L2TP que conforman una Red Privada Virtual (VPN) con la Polired de la Escuela Politécnica Nacional.

PSI.R.03 Política de Acceso Remoto

El propósito de esta política es definir las normas de conexión a la Polired desde cualquier beneficiario o usuario externo de la Escuela Politécnica Nacional. Estas normas se diseñan para minimizar el posible riesgo potencial de daños y perjuicios que puede afectar a la Polired debido al uso no autorizado de los recursos de la Escuela Politécnica Nacional.

PSI.R.04 Política de la Extranet

Describe la política bajo la cual las organizaciones o personas externas pueden conectarse a las redes de la Escuela Politécnica Nacional con la finalidad de realizar transacciones relacionadas con la institución.

PSI.R.05 Política de comunicación Inalámbrica

Esta política especifica las condiciones que deben cumplir los dispositivos de la infraestructura inalámbrica para conectarse a la Polired de la Escuela Politécnica Nacional.

PSI.R.06 Política de Seguridad de redes LAN internas

Esta política establece los requisitos de seguridad de información para las redes de la Escuela Politécnica Nacional mantenidas en el Campus Politécnico para asegurar que no se divulgue información confidencial, que las tecnologías no estén comprometidas y que las actividades de los laboratorios de la Escuela Politécnica Nacional estén protegidas.

PSI.R.07 Política de red de área local virtual (VLAN)

El propósito de esta política es proporcionar las normas para conexiones VLAN’s al interior de la Polired de la Escuela Politécnica Nacional.

2.3 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA ESCUELA POLITÉCNICA NACIONAL

2.3.1 PSI.AR.01 POLÍTICA DE USO ADECUADO

1.0 DESCRIPCIÓN

La intención de la Escuela Politécnica Nacional al publicar una política de uso aceptable, es no imponer disposiciones contrarias a la cultura o costumbre del ambiente de la Escuela Politécnica Nacional, estableciendo una cultura de apertura, de confianza y de integridad. El Comité de Seguridad se compromete a proteger a los funcionarios y dependencias de la Escuela Politécnica Nacional, de acciones ilegales o perjudiciales cometidas por individuos que actúen conscientemente o sin saberlo.

Los equipos y dispositivos pertenecientes a Internet / Intranet / Extranet sin limitarse a equipos de cómputo, software, sistemas operativos, medios de almacenamiento, red de suministro de cuentas de correo electrónico, navegación WWW, FTP, etc. son propiedad de la Escuela Politécnica Nacional. Estos sistemas se utilizarán en servicio a los intereses de la Institución, de nuestras dependencias, de nuestro personal.

La efectividad de la seguridad es un esfuerzo de equipo, con la participación y el apoyo de cada funcionario y dependencia de la Escuela Politécnica Nacional que interactúe con información y / o sistemas de información. Es responsabilidad de cada funcionario conocer estas directrices y actuar con criterio de acuerdo a sus actividades.

2.0 PROPÓSITO

El objetivo de esta política es determinar los parámetros aceptables para el uso de equipos de cómputo en la Escuela Politécnica Nacional. Estas normas se han establecido para proteger al funcionario y a la Escuela Politécnica Nacional. El uso

inadecuado de equipos de cómputo expone a la Escuela Politécnica Nacional a riesgos como ataques de virus, vulnerabilidad de los sistemas, redes y servicios, además de problemas legales.

3.0 ALCANCE

Esta política se aplica a los funcionarios, contratistas, consultores de la Escuela Politécnica Nacional, incluso todo el personal afiliado a terceros. Esta política se aplica a todo el equipo que es de propiedad o que es arrendado por la Escuela Politécnica Nacional.

4.0 POLÍTICA

4.1 Uso general y Propiedad

1. Mientras la administración de la red de la Escuela Politécnica Nacional proporcione un nivel razonable de privacidad, los usuarios deben ser conscientes que los datos que ellos crean en los sistemas de la institución siguen siendo propiedad de la Escuela Politécnica Nacional. Debido a la necesidad de proteger la red de la Escuela Politécnica Nacional, la gestión no puede garantizar la confidencialidad de la información almacenada en cualquier dispositivo de red que pertenece a la Escuela Politécnica Nacional.

2. Los funcionarios son responsables por el ejercicio de buen juicio con respecto a la racionabilidad del uso personal. Los distintos departamentos son responsables de crear las normas y procedimientos para el uso de los sistemas, equipos e Internet/Intranet/Extranet.

En ausencia de tales normas, los funcionarios deben consultar a su supervisor o jefe inmediato.

3. El Comité de Seguridad recomienda que cualquier información que los usuarios

consideren sensible o vulnerable sea cifrada. Para obtener información sobre la clasificación de información, consultar la Política de Sensibilidad de la información.

4. Por razones de seguridad y de mantenimiento de la red, las personas autorizadas dentro de la Escuela Politécnica Nacional pueden controlar los equipos, sistemas y el tráfico de la red en cualquier momento.

5. La Escuela Politécnica Nacional se reserva el derecho a la auditoria de redes y sistemas en forma periódica para garantizar el cumplimiento de esta política.

4.2 Seguridad y Propiedad de la Información

1. La información contenida en Internet/Intranet/Extranet y los sistemas relacionados debería ser clasificada como confidencial, o no confidencial, cuyos detalles se pueden encontrar en las políticas de sensibilidad de la información.

Ejemplos de la información confidencial incluye, pero no se limita a: la empresa privada, las estrategias empresariales, información de la competencia, los secretos comerciales, especificaciones, listas de usuarios, datos de investigación. Los funcionarios deben tomar todas las medidas necesarias para evitar el acceso no autorizado a esta información.

2. Mantener las contraseñas seguras y no compartir cuentas. Los usuarios autorizados son responsables de la seguridad de sus contraseñas y cuentas. Las contraseñas de sistemas deberán cambiarse trimestralmente, y las contraseñas de usuarios deberán cambiarse cada seis meses.

3. Todos los computadores de escritorio, computadores portátiles y estaciones de trabajo deben ser aseguradas con un protector de pantalla protegido con contraseña con la función de activación automática cada 10 minutos o menos, o por la salida de sesión.

(control-alt-suprimir), cuando el usuario no se encuentre usándolo.

4. El uso de cifrado de información permite el cumplimiento de la política de cifrado Aceptable.

5. Debido a que la información contenida en los computadores portátiles es especialmente vulnerable, debe tenerse un cuidado especial. Proteger los computadores portátiles de acuerdo con los "consejos de seguridad para computadores portátiles".

6. Los anuncios creados por parte de los funcionarios de la Escuela Politécnica Nacional, por ejemplo en grupos de noticias, deberán contener una cláusula de exención de responsabilidad que indique que las opiniones expresadas en estos son estrictamente de su responsabilidad, y no necesariamente refleja la posición de la Escuela Politécnica Nacional, a menos que la publicación lo amerite para concretar por ejemplo un negocio y bajo la autorización correspondiente.

7. Todos los hosts utilizados por el funcionario que estén conectados a la Internet/Intranet/Extranet de la Escuela Politécnica Nacional, ya sea de propiedad del funcionario o de la Escuela Politécnica Nacional, deberán continuamente ejecutar escaneo de programas antivirus con una base de datos de virus actualizada.

8. Los funcionarios deben tener una extrema precaución al abrir archivos adjuntos de correo electrónico recibidos de remitentes desconocidos, que pueden contener virus, SPAM, caballos de Troya, Malware en general.

4.3 Prohibiciones de Uso

En general, se prohíben las siguientes actividades. Los funcionarios pueden quedar exentos de estas restricciones solamente en el caso del ejercicio de sus legítimas responsabilidades adheridas al puesto de trabajo.

En ningún caso un funcionario de la Escuela Politécnica Nacional está autorizado a participar en una actividad ilegal según la legislación local, estatal, federal o el derecho internacional.

La siguiente lista no es exhaustiva, pero intenta proporcionar una descripción de las actividades que entran en la categoría de uso inaceptable.

Sistemas y actividades de la red

Las siguientes actividades están estrictamente prohibidas, sin excepción:

1. Violaciones de los derechos de cualquier persona o empresa protegida por derechos de autor, secreto comercial, patentes u otra propiedad intelectual, o de las leyes o reglamentos similares, incluyendo pero no limitado a la instalación o la distribución de productos “piratas” de software que no son debidamente autorizados para su uso por la Escuela Politécnica Nacional.

2. Está estrictamente prohibido la copia no autorizada de material protegido por derechos de autor, lo que incluye la digitalización y distribución de fotografías de revistas, libros u otras fuentes con derechos de autor, derechos de autor de música, y la instalación de cualquier software protegido por derechos de autor para los cuales la Escuela Politécnica Nacional o el usuario final no tenga una licencia activa.

3. Está prohibido la exportación de software, información técnica, tecnología o software de encriptación, violación de los controles de las leyes de exportaciones internacionales o regionales. La gestión adecuada debe ser consultada previamente a la exportación de cualquier material.

4. Introducción de programas maliciosos en la red o servidor por ejemplo, virus, gusanos, caballos de Troya, etc.

5. Permitir el uso de contraseñas o cuentas personales a terceros, permitir la utilización de su cuenta personal por otros. Esto incluye la familia y otros miembros de la familia cuando se está trabajando en el hogar.

6. Utilizar la Escuela Politécnica Nacional como parte activa en el reclutamiento o la transmisión de material que viole las leyes de la jurisdicción local del usuario, material de acoso sexual, o material hostil al lugar de trabajo.

7. Hacer ofertas fraudulentas de los productos, elementos o servicios procedentes de cualquier cuenta de la Escuela Politécnica Nacional.

8. Efectuar violaciones o interrupciones de seguridad o perturbaciones a la red de comunicaciones. Las violaciones de seguridad incluyen, pero no se limitan a, tener acceso a datos de que el funcionario no es un destinatario o acceder a un servidor o cuenta que el funcionario no está expresamente autorizado a acceder, a menos que estas actividades estén incluidas dentro del ámbito de sus funciones ordinarias. Para los fines de esta sección, "interrupción" incluye, pero no se limita, al sniffing de la red, inundaciones con ping, spoofing de paquetes, la denegación de servicio, alteración de información de enrutamiento para propósitos maliciosos.

9. Escaneo de Puertos o escaneos de seguridad, están expresamente prohibidos, a menos que la notificación previa sea realizada al Comité de Seguridad.

10. Ejecutar cualquier forma de supervisión de la red en la que se intercepte datos no destinados al funcionario, a menos que esta actividad sea parte del trabajo normal del funcionario.

11. Eludir la autenticación de usuario o la seguridad de cualquier computador, red o cuenta.

12. Interferir o denegar el servicio a un funcionario a los equipos que no sean de su uso personal.

13. El uso de cualquier programa / script / comando o enviar mensajes de cualquier tipo con la intención de interferir con o desactivar una sesión de terminal del usuario a través de cualquier medio a nivel local o por medio de Internet / Intranet / Extranet.

14. Proporcionar información institucional o listas de los funcionarios de la Escuela Politécnica Nacional a terceros.

Correo electrónico y actividades de comunicación

1. Envío de mensajes de correo electrónico no solicitado, incluyendo el envío de "correo basura" o de otro tipo de material publicitario a personas que no hayan solicitado este tipo de material (email SPAM).

2. Cualquier forma de acoso a través del correo electrónico, teléfono o mensajería personal, ya sea a través del lenguaje, la frecuencia, o el tamaño de los mensajes.

3. El uso no autorizado, o falsificación, de la información de encabezado del correo electrónico.

4. Solicitud de correo electrónico para cualquier otra dirección de correo electrónico, que no sea la de la cuenta propia, con la intención de hostigar o para recoger las direcciones de respuesta.

5. La creación o transmisión de "cartas en cadena", "Ponzi" o "Pirámide" de esquemas de cualquier tipo.

6. El uso de correo electrónico no solicitado generado dentro de la Escuela

Politécnica Nacional o en otras redes de Internet / Intranet / Extranet de los proveedores de servicios en nombre de, o para publicitar cualquier servicio auspiciado por la Escuela Politécnica Nacional o conectados a través de la red de la Escuela Politécnica Nacional.

5.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.2 PSI.AR.02 POLÍTICA DE CORREO ELECTRONICO

1.0 PROPÓSITO

Prevenir una mala interpretación y evitar la afectación de la imagen pública de la Escuela Politécnica Nacional cuando se envía correo electrónico fuera de la misma ya que las personas externas tienden a pensar que dicho mensaje expresa una declaración y posición oficial de la Escuela Politécnica Nacional.

2.0 ALCANCE

Esta política se refiere al uso de correo electrónico que es remitido desde el dominio y servidores de correo de la Escuela Politécnica Nacional (epn.edu.ec) y que se aplica a todos los funcionarios que operan en nombre de esta.

3.0 POLÍTICA

3.1 Uso no autorizado

El sistema de correo electrónico de la Escuela Politécnica Nacional, no debe ser usado para la creación o distribución de cualquier mensaje discriminador u ofensivo, incluyendo entre otros comentarios del color de piel, invalidez, edad, orientación sexual, pornografía, las creencias religiosas y la práctica de las diferentes creencias políticas o el origen nacional.

No es permitido el envío de correos electrónicos masivos, cadenas o SPAM.

Los funcionarios que reciban cualquier correo electrónico con este tipo de contenido, deben informar inmediatamente a su jefe superior.

3.2 Uso personal

Usar los recursos del correo electrónico de manera consciente y limitada; hasta cierta medida su uso para fines personales es aceptable, pero no dentro de las horas de

trabajo. Está prohibido el envío de cadenas de correos, correos con bromas o similares y presentaciones que son envidas con propósito ofensivos. Virus u otras advertencias de correo malicioso y envío de correos en masa serán bloqueados por los servidores antispam de la Escuela Politécnica Nacional.

3.3 Monitoreo

Los funcionarios de la Escuela Politécnica Nacional no tendrán ninguna expectativa de privacidad en cualquier cosa que almacenen, envíen o reciban en la cuenta de correo electrónico de la institución.

La Escuela Politécnica Nacional puede monitorizar el correo electrónico institucional sin previo aviso, sin embargo no está obligada a controlar los mensajes de correo electrónico.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.3 PSI.AR.03 POLÍTICA DE REENVIO AUTOMATICO DE CORREO ELECTRÓNICO

1.0 PROPOSITO

El propósito de esta política es prevenir el uso no autorizado o no consentido de la información considerada crítica para la Escuela Politécnica Nacional.

2.0 ALCANCE

La presente política cubre el reenvío automático de correo electrónico, previniendo la transmisión indebida de información sensible por parte de funcionarios de la EPN.

3.0 POLÍTICA

Todas las personas que conforman la EPN, deben tener una extrema precaución al enviar un correo electrónico relacionado con información considerada sensible para la institución a una red exterior, a menos que sea aprobado por el encargado de manejar dicha información; dichos mensajes tampoco deberán ser transmitidos automáticamente a un destino externo.

La información sensible según lo definido en la Política de Sensibilidad de la Información, no será remitida vía ningún medio, a menos que este correo electrónico sea crítico para la EPN y esté cifrado en concordancia con la Política de Cifrado Aceptable.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.4 PSI.AR.04 POLÍTICA DE RETENCIÓN DE CORREO ELECTRONICO

1.0 PROPÓSITO

La política de retención de correo electrónico permite a los funcionarios determinar cual información enviada o recibida debe ser retenida y por cuanto tiempo.

La información cubierta en estas normas incluye, entre otras, información que se guarda o comparte vía correo electrónico o tecnologías de mensajería instantánea.

Todos los funcionarios deben familiarizarse con el tema de retención de correo electrónico.

Si se tiene preguntas sobre como clasificar un determinado tipo de información debe consultarse al jefe inmediato.

2.0 ALCANCE

Cualquier correo electrónico que contenga información sensible de la institución debe ser tratada de esa manera.

Toda la información del correo de la Escuela Politécnica Nacional se categorizará en de la siguiente manera:

- La Correspondencia administrativa (4 años)
- La Correspondencia fiscal (4 años)
- La Correspondencia general (1 año)
- La Correspondencia efímera (Reténgala hasta leer luego y destrúyala)

3.0 POLÍTICA

3.1 Correspondencia Administrativa

La Correspondencia Administrativa de la Escuela Politécnica Nacional involucra toda la información etiqueta como sensible y relacionada con las autoridades y dependencias administrativas y deberá ser retenida de la siguiente manera.

Para asegurar que la Correspondencia Administrativa sea retenida, el buzón admin@epn.edu.ec será creado. Se deberá incluir esta dirección en los envíos de correos electrónicos institucionales que contengan este tipo de información en la sección CC, de esta manera esta información será gestionada adecuadamente.

3.2 Correspondencia Fiscal

La Correspondencia Fiscal de la Escuela Politécnica Nacional involucra toda la información relacionada al presupuesto, crédito, gastos, etc. por parte de la EPN.

Para asegurar que la Correspondencia Fiscal sea retenida, el buzón fiscal@epn.edu.ec será creado. Se deberá incluir esta dirección en los envíos de correos electrónicos institucionales que contengan este tipo de información en la sección CC, de esta manera esta información será gestionada adecuadamente.

3.3 Correspondencia General

La correspondencia general de la Escuela Politécnica Nacional involucra toda la información relacionada a la interacción de la institución con usuarios externos o internos y los servicios prestados por la EPN.

El funcionario es responsable de la retención del correo electrónico de correspondencia general.

3.4 Correspondencia efímera

La correspondencia efímera es la categoría más común e incluye el correo electrónico personal, peticiones de recomendaciones o revisiones, el correo

electrónico relacionado con el desarrollo del producto, actualizaciones e informes de estado.

3.5 Correspondencia de Mensajería Instantánea

La correspondencia de la mensajería instantánea de la Escuela Politécnica Nacional debe ser guardada con una función de identificación del mensajero instantáneo o copiado en un archivo o guardado. Las conversaciones instantáneas que son de naturaleza administrativa o fiscal deben ser copiadas en un mensaje de correo y enviado a la respectiva dirección de retención.

3.6 Comunicación Cifrada

La infomación cifrada debe ser guardada de una forma consistente de acuerdo a las políticas de sensibilidad de la Información de la Escuela Politécnica Nacional. En general debe guardarse la información en un formato de cifrado.

3.7 Correo electrónico Anulado o recuperado por medios de respaldo

La Escuela Politécnica Nacional mantiene medios de respaldos del servidor de correo. No se modificará o removerá información de correos electrónicos de los medios de respaldo.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.5 PSI.AR.05 POLÍTICA DE AUDITORIA Y EVALUACION DE VULNERABILIDADES

1.0 PROPOSITO

El propósito de este documento es establecer un acuerdo para inspecciones de seguridad de la Red y equipos de la Escuela Politécnica Nacional ha ser realizadas por auditores internos o externos. Dicha auditoria se encargará de examinar las redes de usuarios y/o firewalls o cualquier sistema que pertenezca a la Escuela Politécnica Nacional.

Estas auditorias estarán orientadas a los siguientes ámbitos:

- Asegurar la integridad, confidencialidad y disponibilidad de la información manejada.
- Investigar los posibles incidentes de seguridad en conformidad a las políticas de seguridad de la EPN.
- Monitorear las actividades de los usuarios o sistemas de manera apropiada.

2.0 ALCANCE

La presente política abarca todas las computadoras y dispositivos de comunicación pertenecientes u operados por la EPN. Esta política también abarca cualquier computadora o dispositivo de comunicación que se encuentre dentro de las instalaciones de la EPN aunque no pertenezca a ésta.

3.0 POLÍTICA

Cuando se requiera y con el propósito de realizar la auditoria, se permitirá que los auditores puedan acceder a las redes y Firewalls pertenecientes a la EPN.

La EPN proveerá los protocolos, información de direcciones y conexiones para que los auditores utilicen el Software requerido para realizar la inspección de la red.

Este acceso debe incluir:

- Nivel de acceso de usuario y/o sistema para cualquier computadora o dispositivo de comunicación.
- Acceso a la información (electrónica, almacenada en discos duros) que pueda ser producida, transmitida o almacenada en los equipos de la EPN.
- Acceso a las áreas de trabajo (laboratorios, dependencias, áreas de almacenamiento, etc.).
- Acceso para monitorear interactivamente los registros de tráfico en las redes de la EPN.

3.1 Control de la Red.

Los auditores internos y/o externos de la Escuela Politécnica Nacional realizarán inspecciones de seguridad del tráfico y actividades de los funcionarios de la EPN usuarios de la Polired en horarios y fechas establecidas sin previo aviso.

3.2 Degradación y/o Interrupción del Servicio.

El desempeño y/o disponibilidad de la red podría afectar a la inspección de esta. La EPN libera a los auditores internos y /o externos de cualquier responsabilidad por daños que podrían surgir por las restricciones de disponibilidad de la red causadas por la inspección realizada.

3.3 Punto de contacto con el usuario durante el proceso de evaluación

La EPN asignará a una persona por escrito para que esté disponible si los auditores internos y/o externos tienen alguna duda o requieren ayuda sobre los datos descubiertos durante la inspección.

3.4 Período de examinación

La EPN y los auditores internos y /o externos establecerán por escrito las fechas en las cuales el equipo de auditoria puede examinar las instalaciones.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.6 PSI.AR.06 POLÍTICA DE EVALUACIÓN DE RIESGOS

1.0 PROPÓSITO

Esta política tiene como propósito autorizar a la entidad a cargo del proceso de evaluación de riesgos, realizar evaluaciones periódicas de riesgos de seguridad de la información con el propósito de determinar áreas de vulnerabilidad e iniciar una remediación inmediata.

2.0 ALCANCE

Las evaluaciones de riesgos pueden ser conducidas por alguna entidad interna de la Escuela Politécnica Nacional o alguna entidad externa que tenga firmado un acuerdo de terceras partes con la EPN. Las evaluaciones de riesgos pueden ser dirigidas sobre alguna información del sistema que incluyan aplicaciones, servidores, redes y cualquier proceso o procedimiento por el cual estos sistemas son administrados y/o sostenidos.

3.0 POLÍTICA

La ejecución, desarrollo e implementación de programas de corrección es responsabilidad tanto de la entidad a cargo, como del departamento responsable de los sistemas que estén siendo evaluados. Los funcionarios deben cooperar completamente con todo proceso de evaluación que esté siendo conducido sobre sistemas sobre los cuales son partes responsables. Los funcionarios además deberán trabajar con el equipo responsable del proceso de evaluación para generar un plan de remediación.

4.0 PROCESO DE EVALUACIÓN DEL RIESGO

Referirse a los Procedimientos de Evaluación del riesgo.

5.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.7 PSI.AR.07 POLÍTICA DE SENSIBILIDAD DE LA INFORMACION

1.0 PROPÓSITO

La Política de Información Sensible permite a los funcionarios de la EPN determinar a qué información pueden tener acceso las personas que no son miembros de la EPN, así como la sensibilidad relativa de la información que no debe ser revelada fuera de la Escuela Politécnica Nacional sin la autorización apropiada.

La información proporcionada en estas normas incluye, pero no se limita a, información que se guarda o es compartida vía cualquier medio. Esto incluye: la información electrónica, la información sobre el papel y la información que se compartió oralmente o visualmente (como en el teléfono y la video conferencia).

Todos los funcionarios deben familiarizarse con la información y directrices de etiquetado. Cabe señalar que las directrices de sensibilidad de la información se crearon para dar énfasis al sentido común que el funcionario puede tomar para proteger la información Confidencial de la Escuela Politécnica Nacional por ejemplo, la información Confidencial de la Escuela Politécnica Nacional no debe ser divulgada ni desatendida abandonándola en alguna habitación.

Nota: El impacto de estas normas en la actividad diaria debe ser mínimo.

Deben dirigirse preguntas sobre la clasificación apropiada de un fragmento específico de información a su jefe inmediato. Deben dirigirse preguntas sobre estas normas a la UGI.

2.0 ALCANCE

Toda la información de la Escuela Politécnica Nacional debe ser categorizada en dos categorías:

- Pública
- Confidencial

La información Pública es la información que se ha sido declarada de conocimiento público por alguien con la autoridad para hacerlo y que se puede distribuir libremente a cualquiera sin ningún posible daño a los intereses y propiedad intelectual de la Escuela Politécnica Nacional.

En la Escuela Politécnica Nacional la información Confidencial comprende toda la otra información que no cae en la categoría de pública. Esto es un proceso continuo a través del cual se determina que cierta información es más sensible que otra y debe protegerse de una manera más segura. Se incluye la información que debe protegerse muy cuidadosamente como los secretos comerciales, programas de desarrollo, el potencial de adquisición de objetivos y otro tipo de información integral para el éxito de nuestra institución. También se incluye como información confidencial de la Escuela Politécnica Nacional aquella menos crítica, como los directorios del teléfono, la información general de la institución, la información del personal, etc. que no requiere un riguroso grado de protección.

Un subconjunto de la información confidencial de la Escuela Politécnica Nacional es la información confidencial de terceras partes de la Escuela Politécnica Nacional. Esta es información confidencial perteneciente a terceros que han confiado en la Escuela Politécnica Nacional y con quienes se ha firmado acuerdos de no divulgación. Ejemplos de este tipo de información incluyen, desde los esfuerzos de desarrollo conjunto, los pedidos de usuarios y la información del proveedor. La información de esta categoría oscila entre extremadamente sensible.

En general toda aquella información considerada como excepción en la Ley de Transparencia y acceso a la Información Pública del Ecuador, será considerada confidencial.

El personal de la Escuela Politécnica Nacional debe usar el sentido común para proteger la información confidencial tomando las medidas necesarias. Si un funcionario tiene dudas respecto de la sensibilidad de un fragmento particular de información, debe consultar a su jefe inmediato.

3.0 POLÍTICA

Las directrices de Sensibilidad que se detallan a continuación proporcionan los detalles de cómo proteger la información en diferentes niveles de sensibilidad. Se debe usar estas normas como una referencia, de acuerdo a la información confidencial puede ser necesario tomar medidas más severas dependiendo de las circunstancias y la naturaleza de protección de la información Confidencial en cuestión.

3.1 Sensibilidad mínima

La marcación queda a discreción del propietario o custodio de la información.

Se puede marcar usando las palabras "EPN - Confidencial" esto puede ser por escrito o en un lugar visible dependiendo de la información de que se trate. Otras etiquetas que pueden utilizarse podría ser los "Propiedad de la EPN" o etiquetas similares a la discreción individual de su unidad de negocio o departamento.

Aun cuando ninguna señal esté presente, se presumirá que la información es confidencial salvo que expresamente se haya determinado dicha información de la Escuela Politécnica Nacional es pública por un funcionario de la Escuela Politécnica Nacional con la autoridad para hacerlo.

3.2 Información de Sensibilidad Media

Incluye información comercial, financiera, técnica e información personal.
Este tipo de información deberá ser marcada como “Confidencial - EPN” y considera a la información en medios electrónicos y a la impresa.

3.3 Información muy sensible

Se considera como información muy sensible a los secretos transaccionales, operacionales, personales, financieros, códigos fuentes y a la información técnica requerida para el éxito de la institución.

Nota: cualquiera de estas normas puede usarse con la marcación de la información como: "Escuela Politécnica Nacional - Confidencial" o "Propiedad de la Escuela Politécnica Nacional ", o etiquetar la información "Sólo para uso interno de la Escuela Politécnica Nacional " u otras etiquetas similares a la discreción de su unidad educativa individual o departamento. Si este tipo de información Confidencial de la Escuela Politécnica Nacional se ha marcado los usuarios deben ser conscientes que esta información es muy sensible y se debe proteger como tal.

Para estas categorías se debe definir los siguientes parámetros:

Acceso: Tendrán acceso todos los funcionarios, contratistas, personas con una necesidad comercial que requieran conocer este tipo de información de la Escuela Politécnica Nacional.

Distribución dentro de la Escuela Politécnica Nacional: El envío por correo electrónico es aceptado así como los métodos de transmisión de archivos electrónicos entre dependencias internas.

Distribución fuera de la Escuela Politécnica Nacional: Se deberá usar métodos de envío de correo electrónico públicos o privados que hayan sido públicamente aprobados y aceptados.

Distribución electrónica: No existe restricción siempre que los destinatarios sean aceptados.

Almacenamiento: Mantener fuera de vista de personas no autorizadas; borrar pizarrones y no dejar a la vista. Deben administrarse los equipos con seguridad de nivel medio. Para proteger la pérdida de información electrónica se debe tener los controles de acceso individuales dónde es posible y apropiado.

Disposición/Destrucción: Información antigua debe ser almacenada en cajas especialmente marcadas; los datos electrónicos deben ser limpiados o borrados.

Sanción por divulgación deliberada o inadvertida de información: Penalización civil o penal en caso de divulgar información confidencial de la institución que perjudique los intereses de la misma.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.8 PSI.AR.08 POLÍTICA DE BASES DE DATOS DE CREDENCIALES

1.0 PROPÓSITO

Esta política establece los requisitos mínimos de seguridad para el almacenamiento y recuperación de nombres de usuarios y contraseñas de manera segura en la base de datos conocida como base de datos de credenciales ha ser usada por programas, aplicativos, sistemas que requieran autenticarse mediante esta, a través de la red de la Escuela Politécnica Nacional.

Aquellos programas que se ejecutan sobre la red de la Escuela Politécnica Nacional usualmente requieren acceder a uno de los servidores de bases de datos internos. Para acceder a una base de datos el programa se debe autenticar ante esta mediante credenciales permitidas. Estas credenciales otorgaran las restricciones de acceso respectivas; si estas son almacenadas inadecuadamente se podría comprometer el acceso a los recursos.

2.0 ALCANCE

La presente política es aplicable a todos los programas que accedan a bases de datos de autenticación de la Escuela Politécnica Nacional.

3.0 POLÍTICAS

3.1 General

Para mantener la seguridad de las bases de datos internas de la Escuela Politécnica Nacional, el acceso a programas solo debe concederse a través de la autenticación por medio de credenciales, las mismas que no deben estar en texto plano dentro del cuerpo principal del programa, así como también no deberán ser almacenadas en lugares que puedan ser accedidos a través de un servidor Web.

3.2 Especificación de Requerimientos

3.2.1. Almacenamiento de Nombres de Usuario y Contraseñas en la base de datos

- Los nombres de usuario y las contraseñas de la base de datos deben ser guardados en un archivo independiente del cuerpo del código del programa. Este archivo no debe ser legible.
- Las credenciales de la base de datos pueden residir en el servidor de base de datos, En este caso un número de comprobación hash que las identifica puede ser almacenado en el cuerpo del código del programa.
- Las credenciales de la base de datos pueden ser almacenadas como parte de un servidor de autenticación como un servidor de LDAP usado para la autenticación de usuarios. La autenticación de la base de datos puede ocurrir durante la ejecución de un programa como parte del proceso de autenticación de usuarios ante el servidor de autenticación. En este caso, no hay necesidad de uso programado de credenciales de base de datos.
- Las credenciales de la base de datos pueden no residir en el árbol de documentos del servidor Web.
- El paso de autenticación no debe permitir el acceso a la base de datos basándose solamente en la autenticación de un usuario de manera remota.
- Contraseñas o frases de paso usadas para el acceso a la base de datos deberían ser incluidas en las políticas de contraseña.

3.2.2. Recuperación de Nombres y Contraseñas

- Si el almacenamiento se realiza en un archivo de datos aparte del código fuente del programa, entonces los nombres de usuario y contraseñas de la base de datos deben ser buscados justo antes de ser usados. Para continuar con la autenticación, el nombre del usuario y la contraseña deben ser borrados.

- El medio dentro del cual se guardan las credenciales de la base de datos debe estar separado físicamente de los directorios del código fuente.
- Los lenguajes que ejecutan código fuente y validan las credenciales, no deben residir en el mismo árbol de directorios en el que reside el cuerpo del código ejecutado.

3.3.3. Acceso a la base de datos de Nombres y Contraseñas

- Cada programa o cada colección de programas que implemente una determinada función comercial debe tener su propia base de datos de credenciales. No se permite compartir credenciales entre programas.
- Las contraseñas usadas por los programas permiten niveles de acceso al sistema y esto es definido por la Política de Contraseñas.
- Los grupos de desarrollo deben tener un proceso interno para asegurar que las contraseñas de la base de datos sean controladas y cambiadas de acuerdo con la Política de Contraseña. Este proceso debe incluir un método para restringir el conocimiento de contraseñas de la base de datos ante personas no autorizadas.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.9 PSI.AR.09 POLITICA DE INSTALACION DE SOFTWARE

1.0 ANTECEDENTES

El permitir a los funcionarios instalar software sobre dispositivos o equipos de la institución somete a la institución a una exposición de riesgo innecesaria.

Versiones de archivo conflictivas o DLL's son los que pueden impedir correr a programas, la introducción de malware desde software de instalación infectado, software inautorizado que podría ser descubierto en una auditoria y los programas que pueden ser usados para "hackear" la red de la institución son los ejemplos de los problemas que pueden ser presentados cuando los funcionarios instalan el software sobre el equipo de la institución

2.0 PROPOSITO

Reducir al mínimo: el riesgo de pérdida de funcionalidad de programas, la exposición de información sensible contenida dentro de la red de la Escuela Politécnica Nacional , el riesgo de introducir malware, y la exposición ilegal de software inautorizado en ejecución.

3.0 ALCANCE

Esta política cubre todos los computadores, servidores, PDAs, smartphones, y otros dispositivos que funcionan dentro de la red de la Escuela Politécnica Nacional.

4.0 POLÍTICA

Los funcionarios no pueden instalar el software sobre los dispositivos de la EPN administrados dentro de la Polired de la Escuela Politécnica Nacional.

Los requerimientos de nuevo software deberán ser solicitados para ser aprobados por el jefe inmediato para luego ser enviados a la Unidad de Gestión de la Información por escrito o vía correo electrónico.

El software debe ser seleccionado de una lista de software aprobado, mantenido por la UGI, en el caso de que ninguno de estos cumpla con los requisitos solicitados se considerará la solicitud.

La UGI obtendrá y rastreará las licencias, probará el nuevo software en caso de cualquier conflicto de compatibilidad, y realizará la instalación.

5.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.10 PSI.DS.01 POLÍTICA DE PROTECCION DE SERVIDORES CONTRA EL MALWARE

1.0 ANTECEDENTES

La Escuela Politécnica Nacional otorga la responsabilidad al personal profesional que realiza la gestión de los servidores de la Institución. Inherentes a esta responsabilidad esta la obligación de proporcionar una protección adecuada contra las amenazas malware, como virus, gusanos y aplicaciones spyware entre otros. La aplicación efectiva de esta política limitará la exposición y el efecto de las amenazas de malware comunes a los sistemas que cubren.

2.0 PROPÓSITO:

El propósito de esta política es determinar la necesidad de proporcionar una protección adecuada contra las amenazas malware, como virus, gusanos , SPAM y aplicaciones spyware entre otros, en los equipos de la institución.

3.0 ALCANCE:

Esta política se aplica a todos los servidores administrados en la Polired. –se incluye explícitamente cualquier sistema para el cual la Escuela Politécnica Nacional tenga una obligación contractual de administrar. También se incluye toda disposición de los sistemas servidor para uso interno de la Escuela Politécnica Nacional tiene obligación administrativa o no.

4.0 POLÍTICA:

El personal técnico considerará esta política a fin de determinar los servidores que requieren tener anti-virus y/o aplicaciones anti-spyware instalados y configurarlos adecuadamente.

4.1 ANTI-VIRUS

Todos los servidores DEBEN tener instalado un antivirus que ofrezca escaneo en tiempo real para la protección de archivos y aplicaciones que se ejecutan en el sistema destino, si se ajustan una o varias de las condiciones siguientes:

- No administrativas, usuarios que tienen la capacidad de acceso remoto
- El sistema es un servidor de archivos
- El acceso de parte de NBT / Microsoft está disponible en este servidor para los usuarios sin derechos administrativos
- El acceso HTTP / FTP está abierto al Internet.
- Otros protocolos / aplicaciones que posean riesgos estarán disponibles para Internet a discreción del Administrador de Seguridad

4.2 ANTI-VIRUS DEL SERVIDOR DE CORREO

Si el sistema objeto de ataque es un servidor de correo DEBE tener instalado una aplicación antivirus externa como interna que analice todo el correo con destino hacia y desde el servidor de correo. La ejecución local de la aplicación antivirus puede ser desactivada durante la obtención de copias de seguridad o respaldos si una aplicación externa de antivirus todavía escanea los mensajes de correo electrónico entrantes mientras que la copia de seguridad se está realizando.

4.3 ANTI-SPYWARE

Todos los servidores deberán tener una aplicación anti-spyware instalada, que ofrezca protección en tiempo real al sistema objeto del ataque si se cumple una o más de las siguientes condiciones:

- Cualquier sistema en el que usuarios no-técnicos o no-administrativos tienen acceso remoto a la red y cualquier acceso de salida permitido al Internet.
- Cualquier sistema en el que usuarios no técnicos o no administrativos tienen la capacidad de instalar software en su propio.

4.4 ANTISPAM

Todos los servidores de correo deberán tener una aplicación antispam instalada, que ofrezca protección en tiempo real al sistema objeto del ataque.

Si desde una cuenta del dominio de la EPN, se envían mensajes no solicitados el momento que se detecte dichos envíos no autorizados la cuenta será dada de baja inmediatamente sin mediar aviso previo.

No se deberá enviar ningún mail a una dirección para ser "removido". La Escuela Politécnica Nacional no solicita confirmaciones masivas para remover direcciones de cadenas de correo electrónico.

4.5 EXCEPCIONES

Una excepción a lo anterior por lo general se concederá con un mínimo de resistencia y documentación de una de las siguientes condiciones que se aplican a un sistema:

- El sistema es un servidor de SQL
- El sistema se utiliza como un servidor de correo dedicado
- El sistema no es una plataforma basada en Windows

5.0 CUMPLIMIENTO

La responsabilidad de aplicar esta política pertenece a todo el personal técnico operativo de la Unidad de Gestión de la Información. La responsabilidad de garantizar que los sistemas nuevos y existentes permanezcan bajo el cumplimiento de esta política recae en el oficial de seguridad. Cualquier funcionario que haya violado esta política puede ser objeto de medidas disciplinarias, e incluyendo la terminación del empleo.

2.3.11 PSI.DS.02 POLÍTICA DE USO DE ANTIVIRUS

1.0 PROPÓSITO

Establecer los requisitos y procedimientos que deben cumplirse por todas las computadoras conectadas a las redes de la EPN para asegurar un eficaz descubrimiento y prevención de virus.

2.0 ALCANCE

Esta política aplica a todos los equipos conectados a la POLIRED de la EPN ya sean computadores o aquellos que posean directorios de archivos de PC compartidos. Esto incluye, pero no se limita a, las computadoras de escritorio, computadoras portátiles, servidores de archivos/ftp/tftp/proxy y cualquier computador de un laboratorio generador de tráfico en la red.

3.0 POLÍTICA

Todos los computadores de la EPN deben cumplir las normas establecidas por la institución, se deben respaldar por un software anti-virus instalado y programado para correr en intervalos regulares de tiempo. Además este debe actualizar constantemente la base de datos y archivos de patrones de virus.

Aquellos computadores infectados con virus deben ser desconectados de la red hasta que se notifiquen como libres de virus. Los jefes de laboratorio son responsables de crear procedimientos que aseguren que el software antivirus se ejecute a intervalos regulares de tiempo y que se verifiquen las computadoras como libres de virus.

Se prohíbe cualquier actividad con intención de crear y/o distribuir programas malévolos en las redes de la EPN (por ejemplo: virus, gusanos, troyanos, bombas de correo electrónico, etc.) de acuerdo con la Política de Uso Aceptable.

Procesos recomendados de Anti-Virus

A continuación se presentan procesos recomendados para prevenir problemas de virus:

- Siempre correr la versión corporativa estándar del software antivirus que la EPN haya adquirido que se encontrará disponible en el sitio compartido de descargas y ejecutar la versión más actual; descargar e instalar las actualizaciones para el anti-virus apenas estas estén disponibles.
- NUNCA abrir archivos o macros adjuntos a un correo electrónico desde una fuente desconocida, sospechosa o no confiable. Borrar estos archivos adjuntos inmediatamente luego “borrarlos doblemente” vaciando la papelera de reciclaje.
- Borrar el SPAM, cadenas y demás tipos de correo basura.
- Nunca descargar archivos desde fuentes sospechosas o desconocidas.
- Evitar la compartición de un disco dando acceso de lectura/escritura a menos que haya un requerimiento absoluto del negocio para hacerlo.
- Siempre escanear los dispositivos removibles (memorias flash, disquetes, etc.) en busca de virus antes de usarlos.
- Respaldar la información crítica y configuraciones del sistema sobre una base regular y guardar la información en un lugar seguro.
- Si existen conflictos con el software anti-virus durante las pruebas de laboratorio, se deberá probar el software anti-virus sobre una máquina limpia y determinar el software incompatible.
- Nuevos virus son descubiertos casi todos los días. Periódicamente chequear actualizaciones para el antivirus.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.12 PSI.DS.03 POLÍTICA DE SEGURIDAD DE LA ZONA DESMILITARIZADA DMZ

1.0 PROPÓSITO

Esta política establece los requerimientos de seguridad de la información para todos los equipos conectados a la Polired localizados en la "Zona Desmilitarizada" (DMZ). El cumplimiento de estos requerimientos minimizará el riesgo potencial de daño de la imagen pública de la EPN causado por el uso no autorizado de los recursos de la institución y de la pérdida de datos confidenciales y propiedad intelectual de la EPN.

2.0 ALCANCE

Los equipos y dispositivos como ruteadores, conmutadores, hosts, etc. conectados a la Polired que están expuestos al Internet sin pasar por los firewalls de la institución, son considerados como parte de la DMZ y están sujetos a esta política. Esto incluye las áreas DMZ en localidades primarias y remotas de los Proveedores de Servicio de Internet (ISP). Todo equipamiento existente y futuro, que falle y este bajo el alcance de esta política deberá ser configurado de acuerdo a los documentos referenciados. Esta política no se aplica a los equipos y laboratorios que residen dentro de los firewalls de la EPN. Las normas a cumplir por estos equipos se definen en la Política de Seguridad de Laboratorio Interno.

3.0 POLÍTICA

3.1 Propiedad y Responsabilidades

1. Todas las aplicaciones, sistemas computacionales, etc. que se requiera sean puestas en los servidores de la DMZ, deberán presentar una justificación adecuada para ser aprobada por el Comité de Seguridad de la EPN y este deberá mantener las justificaciones archivadas.

2. Las áreas académicas y administrativas son responsables de la asignación de responsables de estos equipos y de la información que está publicada es estos, definiendo un punto de contacto primario (PC) y uno de reserva en caso de requerirse para solucionar una contingencia.

3. Los cambios en la conectividad, configuración y/o requerimientos de nuevas conexiones o equipos en la DMZ deberán ser solicitados al Comité de Seguridad de la EPN para que sean aprobadas previamente por este Comité.

4. Todas las conexiones de los ISP deberán mantenerse por la UGI, unidad que realizará la administración y estudios técnicos necesarios.

5. La UGI deberá mantener un dispositivo firewall entre la DMZ y el Internet.

6. La EPN y el Comité de Seguridad de la EPN se reservan el derecho de interrumpir las conexiones de los equipos si existiera un riesgo de seguridad.

7. Los laboratorios DMZ proveerán y mantendrán los dispositivos de red desarrollados en el laboratorio DMZ sobre el punto de demarcación de la Organización de Soporte de Red.

8. La UGI deberá almacenar toda la información de contactos actuales y espacios de direcciones de la DMZ.

9. El acceso inmediato a equipos y registros del sistema deberá ser concedido por los miembros de la UGI y el Comité de Seguridad de la EPN sobre solicitud de acuerdo a la Política de Auditoria.

10. Las cuentas individuales de la DMZ deberán ser borradas dentro de 3 días cuando estas no sean autorizada por más tiempo. La clave de las cuentas grupales

deberá cumplir con la Política de Claves y deberá ser cambiada dentro de los 3 días por un miembro del grupo.

3.2 Requerimientos generales de configuración

1. Los recursos de producción deberán ser independientes de los recursos de las redes DMZ.

2. Los equipos de la DMZ no deberán estar conectados a las redes internas de la EPN ni directamente ni a través de conexiones inalámbricas.

3. Los equipos de la DMZ deberán estar físicamente en un cuarto separado de cualquier red interna. Si esto no es posible, el equipo deberá estar en un lugar físicamente sellado con acceso limitado. Adicionalmente, el administrador de la DMZ deberá mantener una lista de quien tiene acceso al equipo.

4. El administrador de la DMZ es el responsable del cumplimiento de las siguientes políticas relacionadas:

a. Política de contraseñas
b. Política de comunicacion inalámbrica
c. Política de Anti-Virus

5. La UGI mantendrá dispositivos firewalls que deberán estar configurados de acuerdo a los principios de menor acceso y a las necesidades de la DMZ. Todos los filtros del firewall serán administrados por la UGI.

6. El dispositivo Firewall deberá ser el único punto de acceso entre la DMZ y el resto de las redes de la EPN y/o el Internet. Cualquier tipo de conexión cruzada las cuales eviten el firewall están estrictamente prohibidas.

7. La configuración original del firewall y cualquier cambio deberá ser revisado y aprobado por la UGI. La UGI adicionalmente podrá disponer las medidas de seguridad que sean necesarias.

8. El tráfico de la DMZ hacia la red interna, incluyendo el acceso VPN, está comprendido en la Política de Acceso Remoto.

9. Los sistemas operativos de todos los servidores internos a los servicios corrientes del Internet en la DMZ se deben configurar bajo estándares de seguridad en la instalación y la configuración del servidor.

10. Los Servicios y usos que no son utilizados deben ser deshabilitados.

3.3 Propiedad y Responsabilidades de equipos en la DMZ

Los equipos y aplicaciones que caen dentro del alcance de esta política deben ser administrados por la UGI en el sistema de gestión de la DMZ, aplicaciones y/o redes.

Los grupos de administración nombrados por la UGI serán responsables de lo siguiente:

- Los equipos deben ser registrados en un sistema de gestión de activos de la institución. La siguiente información es requerida:
  - Los responsables de los Host y su ubicación
  - Hardware y versión del sistema operativo
  - Funciones Principales y aplicaciones
  - Grupos de contraseñas para las contraseñas privilegiadas.
- Las interfaces de red deben ser registradas adecuadamente en el Servidor de Nombres de Dominio (mínimo de registros A y PTR graba).
- Las contraseñas grupales deben ser administradas de acuerdo con el proceso de administración de contraseñas.

- Debe concederse acceso inmediato al equipo y registros del sistema a los miembros de la UGI bajo demanda tomando en cuenta la política de Auditoria.
- Los cambios realizados sobre el equipo existente e instalación de nuevos equipos deben seguir reglas de la institución de administración del proceso de cambio.

Para verificar el cumplimiento de esta política, la UGI periódicamente auditará los equipos de la DMZ conforme la Política de Auditoria.

3.4 Política de Configuración General de equipos de la DMZ

Todos los equipos deben obedecer la siguiente política de Configuración:

- El hardware, sistemas operativos, servicios y aplicaciones deben ser aprobados por la UGI como parte de la fase de pre-despliegue.
- La configuración del sistema operativo debe hacerse según los estándares de configuración de host y router de manera segura.
- Todos los parches recomendados por el vendedor del equipo y la UGI deben ser instalados. Esto aplica a todos los servicios instalados, aunque esos servicios pueden estar temporalmente o permanentemente desactivados. Los administradores deberán establecer un proceso de actualización periódico.
- Deben desactivarse los servicios y aplicaciones que no sirven para los requisitos comerciales.
- Las relaciones de confianza entre sistemas serán aprobadas solamente en caso de un requerimiento institucional plenamente justificado aprobado por la UGI.
- Los servicios y aplicaciones que no sean para el acceso general deben ser restringidas por las listas de control de acceso.
- Servicios inseguros o protocolos deberán reemplazarse con equivalentes más seguros siempre que estos existan.
- La administración remota debe realizarse sobre canales seguros (por ejemplo, conexiones de red cifradas que usan SSH o IPSEC) o acceso por consola

independiente de las redes de DMZ. Donde una metodología para las conexiones de canal seguras no esté disponible, las contraseñas one-time (DES/SofToken) deben usarse para todos los niveles de acceso.

- Todo host que requiera conexión para actualizaciones deben ejecutarse sobre canales seguros.
- Los eventos de seguridad y rastros de la auditoria deben ser guardados en registros logs aprobados por la UGI. Los eventos de seguridad incluyen (pero no se limita a) lo siguiente:
    - Fallas de ingreso de Usuarios
    - Fallas al obtener acceso privilegiado
    - Violaciones en la Política de Acceso
- La UGI aprobará excepciones a la política en caso de ser requerido.

3.5 Nuevas Instalaciones y Procedimientos de Administración del Cambio

Todas las nuevas instalaciones y cambios a la configuración de equipos y aplicaciones existentes deben seguir las políticas y procedimientos siguientes:

- Las nuevas instalaciones deben hacerse vía el Proceso de Instalación de Equipos DMZ.
- Los cambios de configuración deben seguir los Procedimientos de Administración de Cambio (CM).
- La UGI ejecutará auditorias de sistema y aplicación antes del despliegue de nuevos servicios.
- La UGI deberá aprobar de manera directa o vía el proceso administración de configuración todos los nuevos despliegues y cambios de la configuración.

3.6 Equipos de Proveedores de Servicio Externo

La responsabilidad de proteger los equipos instalados por los proveedores de servicios externos debe ser claramente especificada en el contrato con el proveedor de servicios. El departamento de Recursos Humanos o contratante será responsable del cumplimiento de esta política.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.13 PSI.DP.01 POLÍTICA DE USO DE LINEAS TELEFONICAS PARA TRANSMISION DE DATOS

1.0 PROPÓSITO

El presente documento explica las políticas y procedimientos de uso aceptable de las líneas telefónicas de la Escuela Politécnica Nacional utilizadas en la transmisión de datos.

Dicha política abarca dos diferentes usos de las líneas telefónicas las líneas que se han conectado con el único propósito de enviar y recibir fax, y las líneas que van a ser conectadas a las computadores.

2.0 ALCANCE

Esta política sólo se refiere a las líneas telefónicas utilizadas en la transmisión de datos que se conectan a un punto dentro de los edificios y otras localidades de la EPN. No se especifica a las líneas de teléfono que están siendo utilizadas en la comunicación de voz a través de centrales telefónicas tradicionales y de la telefonía pública.

3.0 POLÍTICA

3.1 Escenarios y las repercusiones sobre las instituciones

Hay dos importantes escenarios que implican el uso indebido de las líneas telefónicas contra los que hay que protegerse a través de esta política. El primero es un atacante del exterior, que pide una serie de números de línea telefónica, con la esperanza de conectarse a un equipo que tiene un módem. Si dicho módem de la EPN responde dentro de sus instalaciones, entonces existe la posibilidad de violar la red interna de la EPN a través de ese computador. Por lo menos, la información contenida en dicho computador puede verse comprometida. Esto potencialmente resulta en una pérdida económica al valorar la información institucional comprometida.

El segundo escenario es la amenaza de que cualquier persona que tenga acceso físico a una instalación de la EPN pueda utilizar un computador de escritorio o portátil equipado con un módem. En este caso, el intruso podría ser capaz de conectarse a la red de confianza (intranet) de la EPN a través de la conexión Ethernet de dicho computador y, a continuación, llamar a un sitio sin control mediante el módem, con la capacidad de filtrar información de la EPN a un lugar desconocido. Esto también podría dar lugar a la pérdida de información vital.

A continuación se exponen los procedimientos específicos para hacer frente a los riesgos de seguridad inherentes a cada uno de estos escenarios.

3.2 Máquinas de Fax

Por regla general, se aplica lo siguiente a las solicitudes de líneas telefónicas para fax.

- Las líneas de Fax están aprobadas para uso departamental exclusivo.
- No existirán líneas de fax instaladas para su uso personal.
- El fax debe ser colocado en un área administrativa centralizada designada para uso departamental.
- A un computador que sea capaz de hacer una conexión de fax no se le debe permitir usar una línea telefónica para este fin.

Las excepciones a la anterior política de líneas telefónicas para fax serán analizadas caso por caso, después de examinar la necesidad de la dependencia con respecto al nivel de sensibilidad y de seguridad de la solicitud.

En la conexión el uso de una línea telefónica para fax está sujeto a que el solicitante cumpla plenamente con los requisitos que se indican a continuación. Estos requisitos son responsabilidad del usuario autorizado para cumplirlos en todo momento:

- La línea de fax será utilizada únicamente como se especifica en la solicitud.

- Sólo las personas autorizadas para utilizar la línea deben tener acceso a esta.
- Cuando no esté en uso, la línea ha de ser físicamente desconectada del computador.
- Cuando este en uso, el computador ha de ser físicamente desconectado de la red interna de la EPN.
- La línea se utilizará únicamente para actividades exclusivas de la EPN, y no para actividades y/o motivos personales.
- Todos los materiales descargados, antes de ser introducidos en los sistemas y redes de la EPN, deben haber sido escaneados por un antivirus de servicio público (por ejemplo, McAfee VirusScan), que se mantenga vigente a través de actualizaciones periódicas.

3.3 Computador con Conexión de línea telefónica

La política general es que las solicitudes de los computadores u otros dispositivos inteligentes a conectarse con líneas telefónicas dentro de la EPN, no sean aprobadas por razones de seguridad. Líneas telefónicas representan una importante amenaza para la seguridad de la EPN, intrusiones activas se han puesto en marcha en contra de tales líneas por parte de los hackers. Exenciones a la política anterior se concederán examinando caso por caso. Reemplazo de líneas, como las solicitadas a causa de un movimiento, corresponden a la categoría de "nuevas" líneas. También serán objeto de un examen caso por caso.

3.4 Solicitar una Línea telefónica

Una vez aprobado por un administrador, la persona que solicite una línea telefónica debe proporcionar la siguiente información al Proveedor:

- Un requerimiento claramente detallado con las razones por las que otras conexiones seguras disponibles en la EPN no se pueden utilizar.
- El objetivo del requerimiento por el cual la línea telefónica se va a utilizar.
- El software y hardware a ser conectado a la línea y que se utilice a través de la línea.

- Las conexiones externas a las que el solicitante intente acceder.

La descripción del requerimiento debe responder, como mínimo, las siguientes preguntas:

- ¿Qué requerimientos de comunicación de información se llevarán a cabo sobre la línea?
- ¿Por qué una computadora de escritorio de la EPN equipado con capacidad de acceso a Internet no puede realizar las mismas tareas que la línea telefónica propuesta?
- ¿Por qué las conexiones actuales de acceso de la EPN no pueden realizar las mismas tareas como una línea telefónica?

Además, el solicitante debe estar preparado para responder a las siguientes preguntas suplementarias relacionadas con el perfil de seguridad de la petición:

- ¿Las máquinas que están usando las líneas telefónicas serán físicamente desconectadas de la red interna de la EPN?
- ¿Dónde serán colocadas las líneas telefónicas? Un cubículo/dependencia o laboratorio?
- ¿Está la línea dentro y donde la EPN la necesita?
- ¿Cuántas líneas se solicitan, y el número de personas que utilizarán la línea?
- ¿Con qué frecuencia se utiliza la línea? Una vez a la semana, 2 horas por día?
- ¿Cuál es la fecha más temprana en que la línea termina el servicio?
- ¿La línea debe finalizar su asignación tan pronto como ya no esté en uso?
- ¿Qué otros medios se utilizarán para garantizar la línea de un uso no autorizado?
- ¿Se trata de una línea de la sustitución de una antigua ubicación? ¿Cuál era el propósito original de dicha línea?
- ¿Qué tipo de protocolos se llevarán a cabo sobre la línea?

- ¿Será instalado un antivirus autorizado por la EPN en la/s máquina/s que utilizarán la línea telefónica?
- ¿El solicitante debe utilizar el Formulario de solicitud de línea telefónica para abordar estas cuestiones y presentar una solicitud?

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.14 PSI.DP.02 POLÍTICA DE CONEXIÓN Y ACCESO TELEFONICO DIAL-IN

1.0 PROPÓSITO

El propósito de esta política es el de proteger la información electrónica de la Escuela Politécnica Nacional definiendo apropiadamente el acceso dial-in a la Polired y que sea realizado solamente por personal autorizado.

2.0 ALCANCE

El alcance de esta política es el definir apropiadamente el acceso dial-in y que este usado por el personal autorizado.

3.0 POLÍTICA

Los funcionarios de la Escuela Politécnica Nacional y terceras partes autorizadas pueden usar conexión dial-in para tener acceso a la red. El acceso dial-in debe ser estrictamente controlado, usando una única contraseña de autentificación, esta contraseña deberá ser emitida por la UGI

Es una responsabilidad de los funcionarios con privilegios de acceso dial-in el asegurar que la conexión con la red de la Escuela Politécnica Nacional no sea usada por personas ajenas a la institución para obtener acceso a la información de la compañía.

Un funcionario a quien se la ha otorgado los privilegios de conexión dial-in debe estar constantemente consciente de que la conexión dial-in entre su ubicación y la Escuela Politécnica Nacional es una literal extensión de la red de la Escuela Politécnica Nacional y que esto proporciona una potencial entrada a la información sensible de la institución. El funcionario y/o la tercera parte autorizada deben tomar toda medida razonable de protección del activo de la Escuela Politécnica Nacional

Los teléfonos análogos o que no sean GSM, no podrán ser usados para conectarse a la red de la Escuela Politécnica Nacional, ya que estas señales pueden ser escaneadas y/o hackeadas por individuos no autorizados. Únicamente los teléfonos que trabajen bajo el estándar GSM pueden ser considerados suficientemente seguros para conectarse a la red de la Escuela Politécnica Nacional. Para información adicional sobre acceso inalámbrica a la red de la Escuela Politécnica Nacional, consulte la política de comunicación inalámbrica.

Nota: Las cuentas dial-in son consideradas como cuentas necesarias. La actividad de la cuenta es monitoreada y si la cuenta dial-in no es usada en un periodo de seis meses, la cuenta expira. Si la cuenta dial-in es subsecuentemente requerida, el individuo debe hacer una petición para una nueva cuenta, como se describe abajo.

La persona que necesite tener acceso por dial-in deberá presentar una solicitud por escrito al director de UGI en la cual se exponga la razón por la que se requiere dicho servicio. El director de la UGI será quien vea si es pertinente el permitir el acceso de dicha persona.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.15 PSI.DP.03 POLÍTICA DE USO DE DISPOSITIVOS DE COMUNICACIÓN PERSONALES Y DE VOICEMAIL

1.0 PROPÓSITO

Este documento describe los requisitos de Seguridad de Información para los Dispositivo de Comunicación Personales y Voicemail de la EPN.

2.0 ALCANCE

Esta política aplica al uso de cualquier Dispositivos de Comunicación Personal y de voicemail de la EPN otorgados por la misma o usados para fines de la institución.

3.0 POLÍTICA

3.1 Política de emisión

Los dispositivos de comunicación personales (PCDs) sólo se asignarán al personal de la EPN que tenga deberes que les exijan estar en contacto inmediato y frecuente cuando se encuentren fuera de su lugar normal de trabajo. Para el propósito de esta política, se definen PCDs para incluir dispositivos inalámbricos portátiles, teléfonos celulares, tarjetas inalámbricas portátiles y beepers. La eficaz distribución de los varios dispositivos tecnológicos debe limitarse a personas para quienes la productividad mejorada es apropiada en relación con los costos incurridos.

Pueden asignarse dispositivos inalámbricos portátiles, para una eficiencia operacional, al personal de la EPN que necesita dirigir inmediatamente, asuntos críticos de la misma. Estos individuos generalmente están en el nivel ejecutivo y de dirección. Además del contacto verbal, es necesario que ellos posean la capacidad para revisar y poseer respuestas documentadas a problemas críticos.

3.2 Bluetooth

Los dispositivos de mano libres, como Bluetooth, pueden otorgarse a personal autorizado de la EPN que ha recibido la aprobación para ello. Se debe tener cuidado

para evitar ser captados al utilizar adaptadores Bluetooth, los dispositivos Bluetooth 2.0 de clase 1 tienen un rango de alcance de 330 pies.

3.3 Voicemail

Los buzones de Voicemail pueden otorgarse a personal de la EPN que requieren un método para que otros les puedan dejar mensajes en caso de que ellos no estén disponibles. Los buzones de Voicemail deben ser protegidos por un CÓDIGO que nunca debe estar igual que los últimos cuatro dígitos del número del teléfono del buzón del voicemail.

3.4 Pérdida y Robo

No pueden guardarse en PCDs archivos que contengan datos confidenciales o sensibles, a menos que estos estén protegidos por un método de encriptación aprobada. Nunca se guardarán datos confidenciales o sensibles en un PCD. Los cargos de reparación debido al mal uso de los equipos o de los servicios pueden ser responsabilidad del funcionario, para ello se analizará en una base caso por caso. El costo de cualquier artículo extraviado también será responsabilidad del funcionario. La pérdida o robo de los equipos deben informarse inmediatamente.

3.5 Uso personal

Los PCDs y el voicemail se emiten para actividades propias de la EPN. El uso personal debe limitarse al uso mínimo e incidental.

3.6 Seguridades de PCD

El realizar o atender llamadas telefónicas así como el uso de PCDs mientras se conduce puede ser un riesgo de seguridad. Los conductores deben usar los PCDs cuando el vehículo se encuentre parqueado o ellos se encuentren fuera del vehículo. Si los funcionarios deben usar un PCD mientras manejan, deberán usar dispositivos manos libres.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable de haber violado esta política puede ser sujeto a acciones disciplinarias que llevan a ser inelegible para el uso continuo de PCDs. Los casos extremos podrían llevar a disciplina adicional, llegando incluso al despido del funcionario.

2.3.16 PSI.DP.04 POLITICA DE USO DE DISPOSITIVOS DE ALMACENAMIENTO REMOVIBLE

1.0 ANTECEDENTES

Los medios removibles son una fuente muy conocida de infecciones de virus malware y ocasionan directamente una pérdida de información sensible en muchas instituciones.

2.0 PROPÓSITO

El propósito de esta política es minimizar el riesgo de pérdida o exposición de información sensible de la Escuela Politécnica Nacional y reducir el riesgo de adquirir infecciones de virus y malware en computadoras operadas en la Escuela Politécnica Nacional durante el uso de dispositivos de almacenamiento removible.

3.0 ALCANCE

Esta política cubre todas las computadoras y servidores que operan en la Escuela Politécnica Nacional.

4.0 POLÍTICA

El personal administrativo de la Escuela Politécnica Nacional sólo puede usar los medios removibles entre computadoras de trabajo de la institución, los cuales deberán estar adecuadamente protegidos según lo establece la Política de Antivirus.

Los medios removibles de la Escuela Politécnica Nacional no pueden ser conectados o usados en computadoras que no sean aquellos de propiedad o arrendados por la Escuela Politécnica Nacional sin el permiso explícito del personal de seguridad de la institución o UGI. La información catalogada como sensible deberá ser guardada en medios removibles solo cuando se requiera para el normal desempeño de servicios o cumplimiento de deberes exigidos por el estado. Cuando

la información sensible esta almacenada en medios removibles, esta debe ser cifrada de acuerdo a las políticas de Cifrado aceptadas por la Escuela Politécnica Nacional.

5.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.17 PSI.C.01 POLÍTICA DE CIFRADO ACEPTABLE

1.0 PROPÓSITO

El propósito de esta política es brindar una orientación para el uso del cifrado con algoritmos que han obtenido un reconocimiento público y que han demostrado que trabajan eficazmente. Además, esta política brinda orientación para asegurar el cumplimiento de regulaciones internacionales.

2.0 ALCANCE

Esta política se aplica a todas las dependencias, y a todos los funcionarios de la Escuela Politécnica Nacional.

3.0 POLITICA

Algoritmos que han demostrado su trabajo eficaz como DES, Blowfish, RSA, RC5 e IDEA deben ser usados como base para las tecnologías de cifrado. Estos algoritmos representan actualmente los mecanismos de cifrado de aplicaciones aprobadas.
La longitud de la clave de un sistema de cifrado simétrico debe ser de por lo menos 56 bits.

Las claves de los sistema de cifrado asimétricos deben ser de una longitud que proporcione una firmeza equivalente.

Los requerimientos de la longitud de la clave de la Escuela Politécnica Nacional serán revisados anualmente y actualizados como la tecnología lo permita.

El uso de los algoritmos de cifrado no autorizados por la UGI se encuentra prohibido, a menos que sea revisado por expertos calificados y sea aprobado por el Comité de Seguridad de la EPN.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.18 PSI.C.02 POLÍTICA DE CONTRASEÑAS

1.0 ANTECEDENTE

Las contraseñas son un aspecto importante de seguridad de la computadora. Ellos son la línea delantera de protección para las cuentas del usuario. Una contraseña pobremente escogida puede comprometer la Polired de la EPN.

Como tal, todos los funcionarios con acceso a sistemas computacionales de la EPN son responsables de tomar las medidas necesarias para protección de sus contraseñas.

2.0 PROPÓSITO

El propósito de esta política es establecer una norma para la creación de contraseñas seguras, la protección de esas contraseñas, y la frecuencia de cambio.

3.0 ALCANCE

El alcance de esta política incluye todo el personal que tiene o es responsable de una cuenta (o cualquier forma de acceso que soporta o requiere una contraseña) en cualquier equipo o sistema computacional que reside en la EPN, que tiene acceso a la Polired o guarda cualquier información no pública de la EPN.

4.0 POLÍTICA

4.1 General

- Todas las contraseñas a nivel de sistema (por ejemplo, Root, administrador de NT, cuentas de administración, etc.) deben cambiarse en un período de por lo menos un trimestre.
- Toda la producción de contraseñas a nivel de sistema deben ser administradas por la UGI gestionado a través de la base de datos de contraseñas.

- Todas las contraseñas a nivel de usuario (por ejemplo, el correo electrónico, Web, computador de escritorio, etc.) deben cambiarse cada seis meses por lo menos. El intervalo de cambio recomendado es cada cuatro meses.
- Las cuentas de usuario que tienen los privilegios a nivel de sistema concedidas a un número de miembros o grupo deben tener una única contraseña.
- No deben insertarse las contraseñas en mensajes de correo electrónico u otros formularios de comunicación electrónica.
- Todas las contraseñas de nivel de usuario y nivel de sistema deben satisfacer a las normas descritas a continuación.

4.2 Normas

A. Normas de Construcción de Contraseña Generales

Las contraseñas son usadas para varios propósitos en la EPN. Algunos de los usos más comunes incluyen: cuentas a nivel de usuario, cuentas Web, cuentas de correo electrónico, protección del protector de pantalla, contraseña del voicemail, y el login del router local. Subsecuentemente muy pocos sistemas tienen passwords temporales, por lo tanto se debe estar consciente de cómo seleccionar las contraseñas seguras.

Las contraseñas débiles tienen las siguientes características:

- La contraseña contiene menos de quince caracteres.
- La contraseña es una palabra encontrada en un diccionario (inglés o extranjero).
- La contraseña es una palabra de uso común como:
    - Nombres de familia, mascotas, los amigos, colaboradores, caracteres imaginarios, etc.
    - Términos y nombres de computadores, comandos, sitios, compañías, hardware, software.

- Las palabras "EPN ", "UGI", "sistema" o cualquier derivación.
- Cumpleaños y otra información personal como las direcciones y números de teléfono.
- Palabras o moduelos de número como el aaabbb, qwerty, el zyxwvuts, 123321, etc.,
- Cualquiera deletreó al revés.
- Cualquiera de lo anterior precedido o seguido por un dígito (por ejemplo, secret1, 1secret)

Las contraseñas fuertes tienen las características siguientes:

- Contienen los caracteres mayúscula y minúscula (por ejemplo, un-z, UN-Z)
- Tiene dígitos y caracteres de puntuación así como las cartas por ejemplo, 0-9! @ #$% ^ & * () _+ | ~ - = \ ` {} []: "; '<>?. /)
- Son por lo menos quince caracteres largos alfanuméricos y son un passphrase (Ohmy1stubbedmyt0e).
- No es una palabra de cualquier idioma, dialecto, lengua, etc.
- No se basan en información personal, los nombres de familia, etc.
- Las contraseñas nunca deben apuntarse o guardarse en línea.
- Intente crear contraseñas que pueden recordarse fácilmente. Una manera de hacer esto es crear una contraseña basada en un título de la canción, afirmación, u otra frase. Por ejemplo, la frase podría ser: "Este mayo Es Una Manera de Recordar" y la contraseña podría ser: "TmB1w2R! " o "Tmb1W>r ~ " o alguna otra variación.

NOTA: No use ambos ejemplos como contraseñas.

B. Estándares de Protección de Contraseñas

No use la misma contraseña para las cuentas de la EPN para varios accesos por ejemplo cuenta SAE, cuenta correo electrónico, etc.

No comparta las contraseñas de la EPN con cualquiera, incluyendo a ayudantes administrativos o secretarias. Todas las contraseñas serán tratadas como información confidencial sensible de la EPN.

A continuación se presenta una lista de cosas que no se deben hacer:

- No revele una contraseña por el teléfono a CUALQUIERA.
- No revele una contraseña en un mensaje del correo electrónico
- No revele una contraseña al jefe
- No hable sobre una contraseña delante de otros
- No indique al formato de una contraseña (por ejemplo, "nombre de mi nombre")
- No revele una contraseña en encuestas o formularios de seguridad
- No comparta una contraseña con los miembros familiares
- No revele una contraseña a los colaboradores mientras está en vacación

Si alguien requiere una contraseña, refiérase a este documento o llame a alguien en el Departamento de Seguridad de Información.

No usar la opción "Recordar Contraseña" de aplicaciones (por ejemplo., Eudora, Outlook, Messenger de Netscape).

De nuevo, no apunte y no guarde las contraseñas en cualquier parte en su dependencia.

No guarde las contraseñas en un archivo en CUALQUIER computadora (incluso Palm Pilots o dispositivos similares) sin cifrado.

Cambie por lo menos una vez las contraseñas cada seis meses (excepto contraseñas de nivel de sistema que deben cambiarse trimestralmente). El intervalo de cambio recomendado es cada cuatro meses.

Si una cuenta o la contraseña es motivo de desconfianza o se sospecha que ha sido revelada, se debe denunciar el incidente inmediatamente a la UGI.

Se debe ejecutar intentos de crackeado o adivinanza de contraseñas estas pueden ser ejecutados periódicamente o en períodos randómicos por la UGI o sus delegados. Si una contraseña es adivinada o crackeado durante uno de estas examinaciones, el usuario exigirá sea cambiada.

C. Estándares de Desarrollo de Aplicaciones

Los diseñadores de la aplicación deben asegurar que sus programas contienen las precauciones de seguridad siguientes.

Las aplicaciones:

- Deben apoyar la autenticación de usuarios individuales, no grupales.
- No se deben guardar las contraseñas en texto legible o en cualquier manera fácilmente reversible.
- Debe proveer facilidades de administración de contraseñas para que el usuario autorizado otorgue la restauración de contraseñas sin tener que conocerlas.

D. Uso de Contraseñas y Passphrases para los Usuarios de Acceso Remoto

El acceso a la Polired de la EPN vía acceso remoto debe usar una autenticación de contraseñas con claves publicas/privadas y con un passphrase fuerte de acceso.

E. Passphrases

Los Passphrases son usados para la autenticación de claves publica/privada. Un sistema de claves publicas/privadas define una relación de seguridad fuerte a través

de una clave pública que es conocida por todos, y un clave privada que sólo es conocida por el usuario. Sin el passphrase para "desbloquear" la clave privada, el usuario no puede obtener acceso.
Un passphrase no es igual que una contraseña. Un passphrase es una versión más larga de una contraseña y es por consiguiente más seguro. Un passphrase está típicamente compuesto de múltiples palabras. Debido a esto, un passphrase está más seguro contra los "ataques de diccionario."

Un passphrase bueno es relativamente largo y contiene una combinación de letras minúsculas y mayúsculas, caracteres numéricos y de puntuación. Un ejemplo de un passphrase bueno sería por ejemplo:

"The *? #> * @ TrafficOnThe101Was * & #! #ThisMorning"

Todas las reglas que aplican a las contraseñas aplican a passphrases.

5.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.19 PSI.SF.01 POLÍTICAS DE SEGURIDAD DE SERVIDORES

1.0 PROPÓSITO

El propósito de esta política es establecer las normas para la configuración de los servidores de la Escuela Politécnica Nacional. La puesta en práctica eficaz de esta política reducirá al mínimo el acceso no autorizado a la red de la Escuela Politécnica Nacional y a su información propietaria.

2.0 EL ALCANCE

Esta política se aplica a todos los servidores de la Escuela Politécnica Nacional, y a los servidores registrados bajo cualquier dominio interno de la Escuela Politécnica Nacional.

Esta política está expresamente orientada a los equipos servidores de la Polired y a la configuración segura de servidores ubicados en el área DMZ de la Escuela Politécnica Nacional.

3.0 POLÍTICA

3.1 La propiedad y Responsabilidades

Todos los servidores internos de la Escuela Politécnica Nacional deben ser manejados por un grupo operacional responsable de la administración del sistema.

Las guías de configuración de servidores aprobadas deben ser respetadas y aplicadas por cada grupo operacional responsable, basado en las políticas institucionales. Los grupos operacionales deben supervisar el cumplimiento de la

configuración y de ser necesario solicitar la aprobación de las excepciones a la política para ser adaptada a su ambiente, esto será revisado y aprobado por la UGI.

Los servidores deben ser registrados dentro del sistema de gestión corporativa de la EPN. Como mínimo, se requiere la siguiente información que lo identifique:

- Identificar el responsable o contacto y la localización del servidor y un contacto de reserva.
- El Hardware y la versión del Sistema operativo.
- Funciones Principales y usos, de ser aplicable

La Información en el sistema de gestión corporativo de la institución debe mantenerse actualizada.

Los Cambios de Configuración en los servidores de producción deben seguir los procedimientos de dirección de cambio apropiados.

3.2 Directrices de Configuración Generales

La configuración del Sistema operativo debe ser conforme a las directrices aprobadas por la UGI.

Los servicios y aplicaciones que no serán usados deben ser deshabilitados.

El acceso a servicios debe ser registrado y/o protegido por métodos de control de acceso como encapsulamiento, de ser posible.

Los parches de seguridad más recientes deben ser instalados sobre el sistema tan pronto como sean liberados, la única excepción se da cuando el uso inmediato interferiría con la funcionalidad de los servicios institucionales.

Las relaciones de confianza entre sistemas son un riesgo de seguridad y su empleo debería ser evitado. No usar una relación de confianza cuando exista algún otro método de comunicación.

No utilizar cuentas privilegiadas como root cuando una cuenta no privilegiada pueda ser usada.

Si una metodología para la conexión de canal seguro está disponible, deberá ser aplicada, y el acceso privilegiado debe ser realizado sobre canales seguros, (por ejemplo cifrado conexiones de red que usan SSH o IPSEC).

Los servidores físicamente deben ser ubicados en un ambiente cuyo acceso sea controlado.

Los servidores expresamente tienen prohibido funcionar dentro de ambientes que no estén controlados.

3.3 Monitoreo

Todos los acontecimientos de seguridad relacionados con sistemas críticos o sensibles deben ser registrados y los rastros de auditorias guardados de la siguiente manera:

- Todos los incidentes de seguridad se mantendrán en línea mínimo 1 semana.
- Los medios de respaldo como DVD, CD, cintas diarias serán conservados durante al menos 1 mes.
- Respaldos semanales serán conservados durante al menos 1 mes.
- Respaldos mensuales serán conservados para un mínimo de 2 años.
- Los acontecimientos relacionados con la seguridad serán reportados a la UGI, que informará de incidentes al Comité de Seguridad de la Información. Se

tomarán las medidas correctivas como sean necesarias. Cualquier acontecimiento relacionado con la Seguridad incluye, pero no se limita, a:

- Ataques y Exploración de puertos
- Evidencias de accesos no autorizados con cuentas privilegiadas
- Ocurrencias anómalas que no son relacionadas con usos específicos sobre el servidor

3.4 Auditorias

- Las auditorias serán realizadas regularmente por la Unidad de Gestión de la Información dentro de la Escuela Politécnica Nacional.
- Las auditorias serán manejadas por un grupo interno de auditoria designado por la UGI, conforme a la política de auditoria. La UGI filtrará conclusiones no relacionadas con un grupo específico operacional y luego presentará las conclusiones al personal de apoyo apropiado para la nueva mediación o la justificación.
- Se hará el esfuerzo necesario para impedir que las auditorias causen fallas operacionales o interrupciones.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado por haber violado esta política puede ser sujeto a la acción disciplinaria, incluyendo la terminación del contrato laboral.

2.3.20 PSI.R.01 POLÍTICA DE SEGURIDAD DE ENRUTADORES

1.0 PROPÓSITO

Este documento describe los requerimientos mínimos de seguridad en la configuración de todos los routers y switches conectados a la Polired de la EPN.

2.0 ALCANCE

Esta política cubre todos los routers y switches conectados a la Polired y con salida hacia el Internet. Los routers y switches de laboratorios internos que no tienen salida al Internet no están cubiertos por esta política. Los routers y switches dentro de las áreas DMZ deben ser configurados de acuerdo a la política de la zona desmilitarizada DMZ de la EPN.

3.0 POLÍTICA

Todo router debe cumplir con los siguientes estándares de configuración:

1. Las cuentas de los usuarios locales no deben ser configuradas en el router local. Estos deberán usar autenticación de usuarios usando otros mecanismos.
2. La contraseña de habilitación del router debe ser guardada de manera segura y con un método de cifrado. Esta contraseña deberá ser almacenada en un router de una organización externa que brinde soporte a la institución.
3. Se debe deshabilitar lo siguiente:
    a. Envío de broadcast directo.
    b. El ingreso de paquetes al router con direcciones inválidas como las referenciadas en RFC 1918.
    c. Servicios TCP y UDP que no hayan sido plenamente justificados.
    d. Todas las fuentes de enrutamiento
    e. Todos los servicios Web que estén corriendo en el router.
4. Usar cadenas estandarizadas SNMP
5. Las reglas de acceso deben ser añadidas según las necesidades de la institución.

6. El router debe estar incluido en el sistema de administración corporativo de la institución con un punto de contacto designado.
7. Cada router debe tener las siguientes instrucciones mostradas en un punto claramente visible: EL ACCESO SIN AUTORIZACIÓN A ESTE DISPOSITIVO DE RED ESTÁ PROHIBIDO.

Se debe tener permisos explícitos para acceder o configurar este dispositivo. Todas las actividades realizadas sobre este dispositivo son registradas y las violaciones de esta política puede dar como resultado una acción disciplinaria; las violaciones serán reportadas para la respectiva aplicación de la ley.

8. Telnet nunca debe ser usado sobre la red para administrar un router, a menos que exista un túnel de seguridad que proteja todo el canal de comunicación. SSH es el protocolo más conveniente para esta administración.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable de haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.21 PSI.R.02 POLÍTICA DE RED PRIVADA VIRTUAL (VPN) DE LA POLIRED

1.0 PROPÓSITO

El propósito de esta política es proporcionar las normas para las conexiones remotas IPSec o L2TP que conforman una Red Privada Virtual (VPN) con la Polired de la Escuela Politécnica Nacional.

2.0 ALCANCE

La presente política se aplica a todos los usuarios de la Polired de la Escuela Politécnica Nacional ya sean personas internas o externas a la institución que utilizan VPN's como conexión. Esta política se aplica a las implementaciones de VPN enlazadas a través de un concentrador.

3.0 POLÍTICA

Esta política se aplica a los funcionarios y al personal relacionado a terceras partes que puede utilizar los beneficios de VPNs de la Escuela Politécnica Nacional que es el servicio de" manejo de usuario". Esto significa que el usuario es responsable para seleccionar un Servicio de Proveedor de Internet (ISP), coordinando la instalación, configurando e instalando cualquiera software requerido, y cancelando un pago por el servicio. Pueden encontrarse detalles extensos en la Política de Acceso Remota.

Adicionalmente

Es responsabilidad de funcionarios con privilegios de VPN asegurar que no se permita el acceso a usuarios no autorizados a las redes internas de la Escuela Politécnica Nacional

El uso de VPN debe ser controlado usando una de contraseña de autentificación tal como un sistema de clave pública o privada con una contraseña o frase fuerte de paso.

Cuando está conectado activamente a la Polired, las VPN's forzarán todo el tráfico a y desde el PC sobre el túnel VPN, todo el tráfico restante será eliminado.

El hacer un túnel Dual no está permitido; sólo se permite una conexión de red.

Las entradas de VPN serán preparadas y se administrarán por los responsables de la Unidad de Gestión de Información.

Todos los equipos conectados a la Polired de la Escuela Politécnica Nacional vía VPN o cualquier otra tecnología debe usar un software anti-virus actualizado establecido por la UGI, esto incluye los computadores personales.

Los usuarios de VPN serán desconectados automáticamente de una red después de treinta minutos de inactividad. El usuario debe entonces loguearse de nuevo para reconectase a la red. Ping's u otro mecanismo de conexión artificial no deben ser usados para mantener la conexión abierta.

El concentrador de VPN se limita a un tiempo de conexión absoluto de 24 horas.

Los usuarios de computadoras externas de la Escuela Politécnica Nacional deben configurar el equipo para cumplir con las políticas VPN y políticas de la Polired.

Solo pueden acceder usuarios VPN aprobados por la UGI.

Los usuarios que usando tecnología VPN con equipos personales, deben entender que sus máquinas son una extensión de la Polired y como tal están sujetos a las mismas reglas y regulaciones que se aplican a los equipos de la Escuela Politécnica Nacional, es decir, sus máquinas deben configurarse para obedecer las Políticas de Seguridad de la UGI.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.22 PSI.R.03 POLITICAS DE ACCESO REMOTO

1.0 PROPÓSITO

El propósito de esta política es definir las normas de conexión a la Polired desde cualquier beneficiario externo de la Escuela Politécnica Nacional. Estas normas se diseñan para minimizar el posible riesgo potencial de daños y perjuicios que puede afectar a la Polired debido al uso no autorizado de los recursos de la Escuela Politécnica Nacional. Los daños y perjuicios incluyen la pérdida de datos sensibles confidenciales, la propiedad intelectual, daños a la imagen pública, daños críticos de los sistemas internos, etc.,

2.0 ALCANCE

Esta política aplica a todos los funcionarios de la Escuela Politécnica Nacional. Esta política aplica a las conexiones de acceso remotas usadas para trabajar en la Escuela Politécnica Nacional, incluyendo la lectura, envío de correo electrónico y los recursos de la estructura de la intranet.

Las aplicaciones de acceso remotas que son cubiertas por esta política incluyen, pero no se limitan a, los dial-in módems, frame relay, ISDN, DSL, VPN, SSH, cable módems, etc.

3.0 POLÍTICA

3.1 General

Es responsabilidad de los usuarios con privilegios de acceso remoto a la Polired asegurar que su conexión de acceso remoto, esté protegida bajo las mismas consideraciones que rigen la conexión de los usuarios locales de la Escuela Politécnica Nacional.

El acceso general a la Internet para el uso recreativo de los miembros de la casa a través de la Polired en los computadores personales no es permitida, el miembro de la EPN es responsable de asegurar que su familia no viole ninguna de las políticas, no realice actividades ilegales y no use el acceso para intereses de negocio personales y externos a la institución. El miembro de la EPN es responsable por las consecuencias de su mal uso.

3.2 Requisitos

La seguridad en un acceso remoto debe ser estrictamente controlada. El control será realizado vía autenticación de la contraseña o por claves publicas/privadas. Véase la política de contraseñas.

En ningún momento el usuario de la Polired proporcionará su login o contraseña de conexión o correo electrónico a cualquier persona incluyendo a los miembros de su familia.

Los usuarios de la Polired con privilegios de acceso remoto deben asegurar que su computadora personal o puesto de trabajo con el cual se conecta a la institución, no se conecte al mismo tiempo a cualquier otra red, con la excepción de redes personales que están bajo el completo control del usuario.

Los usuarios de la Polired con privilegios de acceso remoto a la red corporativa no deben usar cuentas de correo electrónico públicas (es decir, Hotmail, Yahoo, AOL), u otros recursos externos para realizar actividades institucionales, asegurando que los asuntos institucionales no se confundan con los personales.

Los Routers de líneas ISDN dedicadas configuradas para el acceso remoto a la Polired deben reunir requisitos de autenticación mínimos.

La reconfiguración de los equipos personales de los usuarios con el propósito de Split-tunneling o dual homing no está permitida de ninguna manera.

Frame Relay debe reunir requisitos mínimos de autenticación.

La configuración del hardware no estandarizado debe ser aprobado por los Servicios de Acceso Remoto, y la UGI debe aprobar las configuraciones de seguridad para el acceso al hardware.

Todos los equipos conectados a la Polired vía las tecnologías de acceso remoto deben usar un software anti-virus actualizado esto incluye a las computadoras personales. Las conexiones de terceros deben obedecer a los requisitos declarados en el acuerdo de terceras partes.

El equipo personal usado para conectarse a la Polired debe reunir los requisitos de seguridad mínimos especificados para equipos locales de la Institución.

Las organizaciones o individuos que desean implementar soluciones de Acceso Remota no estandarizadas a la Polired deben obtener la aprobación de la UGI.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.23 PSI.R.04 POLÍTICA DE LA EXTRANET

1.0 PROPÓSITO

Este documento describe la política bajo la cual las organizaciones o personas externas pueden conectarse a las redes de la Escuela Politécnica Nacional con la finalidad de realizar transacciones relacionadas con la institución.

2.0 ALCANCE

Las conexiones de terceros que requieren el acceso a los recursos no públicos de la Escuela Politécnica Nacional están dentro de esta política, independientemente si un circuito de telecomunicaciones (tales como frame relay o RDSI) o si la tecnología VPN es usada para la conexión. Conectividad de terceros, como proveedores de servicios de Internet (ISP) que ofrecen acceso a Internet para la Escuela Politécnica Nacional o a la red telefónica pública conmutada NO recaen bajo esta política

3.0 POLÍTICA

3.1 Pre-Requisitos

3.1.1 Análisis de la Seguridad

Todas las conexiones extranet nuevas pasarán por una revisión de seguridad realizada por la Unidad de Gestión de la Información. Las revisiones son para garantizar el acceso a todos los puntos de conexión de la mejor manera posible.

3.1.2 Participación de terceros en la conexión de un acuerdo

Todas las nuevas solicitudes de conexión entre terceros y la Escuela Politécnica Nacional requieren firmar un acuerdo previo entre las partes. Este acuerdo debe ser firmado entre el Jefe de la UGI y un representante de terceros parte que esté legalmente facultado para firmar en nombre de ellos.

El documento firmado se mantendrá en los archivos de la UGI. Los documentos relativos a las conexiones dentro de los laboratorios de la Escuela Politécnica

Nacional son almacenados en un archivo a nombre del equipo encargado de seguridad de los laboratorios.

3.1.3 Caso de negocios

Todas las conexiones a la Extranet deben ir acompañadas de una justificación válida por escrito, que será aprobada por el administrador de la Extranet.

3.1.4 Punto de contacto (PoC)

Los Terceros deben designar una persona que va a ser el punto de contacto (POC) para la conexión Extranet. El PoC actúa en nombre de los Terceros y permitirá establecer el contacto entre las partes de esta política. En el caso de que se cambie el PoC, el Tercero deberá avisar sin demora.

3.2 Establecimiento de Conectividad

Las dependencias de la Escuela Politécnica Nacional que deseen establecer conectividad con Terceros tienen que presentar una solicitud al administrador de la Extranet. El administrador de la Extranet establecerá los mecanismos de seguridad inherentes a dicha conexión. La dependencia de la Institución debe proporcionar información plena y completa en cuanto a la naturaleza de la conexión a la Extranet.

En ningún caso se confiará en la tercera parte para proteger los recursos de la red de la Escuela Politécnica Nacional.

3.3 Modificación o Cambio de Conectividad y Acceso

Todos los cambios en el acceso deben ir acompañados de una justificación válida de negocio y están sujetos a revisión de seguridad. Los cambios se llevarán a cabo a través de proceso de gestión de cambios. La dependencia o los terceros son responsables de notificar al administrador de la Extranet cuando haya un cambio en la información original proporcionada a fin de que la seguridad y la conectividad también evolucionen.

3.4 Finalización de Acceso

Cuando el acceso ya no es necesario, la dependencia de la institución debe notificar al administrador de la Extranet, que se terminará el acceso. Esto puede significar una modificación de los permisos existentes para que ponga fin al circuito, según el caso. Se debe llevar a cabo una auditoria de la Extranet y de los equipos de seguridad con sus respectivas conexiones sobre una base anual para asegurar que todas las conexiones existentes siguen siendo necesarias.

Las conexiones que se determine que ya no están siendo utilizadas por la institución se darán por terminadas inmediatamente. En caso de que un incidente de seguridad o de que una conexión vaya ser eliminada de la Extranet, el administrador notificará al POC de la Institución Patrocinadora de los cambios antes de tomar cualquier acción.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.24 PSI.R.05 POLÍTICA DE COMUNICACIÓN INALÁMBRICA

1.0 ANTECEDENTES

El propósito de esta política es garantizar y proteger los activos de información de propiedad de la Escuela Politécnica Nacional. La EPN proporciona dispositivos de computadora, redes y otros sistemas de información electrónicos para cumplir con los objetivos institucionales.

La Escuela Politécnica Nacional autoriza el acceso a estos recursos como un privilegio y debe gestionarlos de manera responsable para garantizar la confidencialidad, integridad y disponibilidad de todos los activos de la información.

Esta política especifica las condiciones que deben cumplir los dispositivos de la infraestructura inalámbrica para conectarse a la Polired de la Escuela Politécnica Nacional. Sólo los dispositivos de la infraestructura inalámbrica que cumplan con las especificaciones de esta política o aquellas excepciones aprobadas por la Unidad de Gestión de la Información tienen permitido la conectividad a la Polired de la Escuela Politécnica Nacional.

2.0 APLICACION

Todos los funcionarios, contratistas, consultores de la Escuela Politécnica Nacional, incluso todo el personal afiliado a terceras partes que deseen mantener un dispositivo de infraestructura inalámbrica en la Polired de la EPN deben adherirse a esta política. Esta política se aplica a todos los dispositivos de infraestructura inalámbrica que se conectan a la Polired de la Escuela Politécnica Nacional, incluye pero no se limita a computadoras portátiles, desktops, teléfonos celulares y asistentes personales digitales (PDAs). Esto incluye cualquier forma de dispositivo de comunicación inalámbrico capaz de transmitir paquetes de datos.

La UGI deberá aprobar las excepciones a esta política.

3.0 DECLARACIÓN DE LA POLÍTICA

3.1 Requisitos Generales de Acceso a la Red

Todos los dispositivos inalámbricos que residen en un sitio de la Escuela Politécnica Nacional, que se conecten a la Polired y que tengan acceso a información clasificada como confidencial, muy Confidencial, deben cumplir con los siguientes requisitos:

3.1.1 Cumplir con las normas especificadas en el estándar de Comunicación Inalámbrica.

3.1.2 Haber instalado, con el apoyo y mantenimiento de un equipo de soporte de la Institución.

3.1.3 Usar los protocolos de autenticación aceptados para dispositivos inalámbricos de la Escuela Politécnica Nacional.

3.1.4 Usar los protocolos de cifrado aceptados por la Escuela Politécnica Nacional.

3.1.5 Mantener un registro de las direcciones MAC para que puedan ser autenticadas y rastreadas.

3.1.6 No interferir con las instalaciones inalámbricas que pertenecen a otras Organizaciones.

3.1.7 Usar como Protocolo de Autenticación el Protocolo de Autenticación Extensible Rápido (EAP-RÁPIDO), el Protocolo de Autenticación Extensible Protegido (PEAP), o el Protocolo de Autenticación Extensible de Seguridad de la Capa de Traducción (EAP-TLS).

3.1.8 Usar el Protocolo de Integridad de Clave Temporal (TKIP) o protocolos del Sistema de Cifrado Avanzado (AES) con una longitud de clave mínima de 128 bits.

3.2 Requisitos de dispositivos inalámbricos de Laboratorio y Aislados

Aquellos laboratorios y dispositivos inalámbricos a los que no se proporciona conectividad a la red general de la Escuela Politécnica Nacional deben cumplir con los siguientes requisitos:

3.2.1 Estar aislados de la red Polired y cumplir con la Política de Seguridad de la Zona Desmilitarizada o Política de Seguridad de Laboratorios internos.

3.2.2 No interferir en el despliegue de acceso inalámbrico mantenidos por otras organizaciones de apoyo.

3.2.3 El identificador de conjuntos de servicios de dispositivos de laboratorio (SSID) debe ser diferente del dispositivo EPN de producción SSID.

3.2.4 La transmisión del dispositivo del laboratorio SSID debe ser desactivada

4.0 REFERENCIAS

En apoyo de esta norma, las siguientes políticas, pautas, y recursos son:

- La Política de Sensibilidad de información
- La Política de Comunicación inalámbrica

5.0 CUMPLIMIENTO

Cualquier funcionario que se encuentre que haya violando la política puede estar sujeto a acciones disciplinarias, e incluso a la terminación de empleo. Cualquier violación de la política por un funcionario temporal, contratista o vendedor puede producir la terminación de su contrato o trabajo con la EPN.

2.3.25 PSI.R.06 POLITICA DE SEGURIDAD DE REDES LAN INTERNAS

1.0 PROPÓSITO

Esta política establece los requisitos de seguridad de información para las redes de la Escuela Politécnica Nacional mantenidas en el Campus Politécnico para asegurar que no se divulgue información confidencial, que las tecnologías no estén comprometidas y que las actividades de los laboratorios de la Escuela Politécnica Nacional estén protegidas.

2.0 ALCANCE

Esta política aplica a todos los usuarios y redes LAN internas de la Escuela Politécnica Nacional. Deben configurarse todos los equipos existentes y futuros que caigan bajo el alcance de esta política.

Los Laboratorios de DMZ autosuficientes están exentos de esta política. Los laboratorios de DMZ deben obedecer a la Política de seguridad de la zona desprotegida DMZ

3.0 POLÍTICA

3.1 Responsabilidades de propiedad

1. Cada laboratorio en las dependencias de la EPN es responsable de asignar encargados de laboratorio, un punto de contacto y uno de reserva para cada laboratorio. Los responsables del laboratorio deben mantener la información de los computadores actualizada y el equipo de gestión de la red. El contacto con los encargados del laboratorio o su reserva, se deben mantener disponibles en casos de contingencias, si no las acciones serán tomadas sin su participación.

2. Los administradores del laboratorio son responsables de la seguridad de sus laboratorios y del impacto del laboratorio en la Polired y cualquier otra red. Los administradores de laboratorio son responsables de la adhesión a esta política y los

procesos asociados. Donde las políticas y procedimientos son indefinidos, los administradores del laboratorio deben hacer lo mejor de sí para salvaguardar a la EPN de las vulnerabilidades de seguridad.

3. Los administradores de laboratorio son responsables de la conformidad del laboratorio con todas las políticas de seguridad de la EPN. Las siguientes son particularmente importantes: La Política de contraseñas para conectar dispositivos a una red de computadoras, de servidores, política de seguridad inalámbrica, política de anti-virus, y de seguridad física.

4. Los administradores de laboratorio son responsables de controlar el acceso al laboratorio. El acceso a cualquier laboratorio dado, sólo será concedida por el administrador del laboratorio. Esto incluye supervisar la lista de acceso continuamente para asegurar que aquéllos que ya no requieran el acceso sean eliminados.

5. La Unidad de Gestión de la Información debe mantener un dispositivo firewall entre la Polired y los equipos del laboratorio.

6. La Unidad de Gestión de la Información se reserva el derecho de interrumpir las conexiones del laboratorio que impactan negativamente o proponen un riesgo de seguridad a la Polired.

7. La Unidad de Gestión de la Información debe grabar todas las direcciones IP del laboratorio que son ruteadas dentro de la Polired de la EPN en la base de datos correspondiente junto con la información actual del contacto para ese laboratorio.

8. Cualquier dependencia que quiera agregar una conexión externa debe proporcionar un diagrama y la documentación requerida a la UGI con la justificación debida. La UGI revisará la seguridad involucrada antes de aprobarla.

9. Todas las contraseñas de usuario deben cumplir con la política de Contraseñas de la EPN. Las cuentas de usuario individuales de cualquier dispositivo de laboratorio deben eliminarse cuando el usuario deje de pertenecer a la institución. Las contraseñas de cuentas grupales deben ser cambiadas al menos una vez trimestralmente.

3.2 Requisitos de la Configuración General

Todo el tráfico entre la Internet y la Polired debe pasar por un cortafuego mantenido por la UGI. Los dispositivos de red de laboratorio (incluyendo wireless) no deben realizar un bypass a otras redes de la Polired.

Cualquier cambio en las configuraciones originales del cortafuego será realizado por la UGI para implementar mejoras según se requiera para implementar seguridad.

Se prohíbe en la Polired de la EPN la exploración de puertos de red, (la auto-exploración de la Polired, genera tráfico SPAMming/flooding) y otras actividades similares que afecten negativamente la Polired. Estas actividades deben estar restringidas dentro del laboratorio.

El tráfico entre la Polired y las redes de laboratorios, así como el tráfico entre redes de laboratorio separadas, se basa en las necesidades de la institución y siempre que este tráfico no impacte negativamente en otras redes será permitido. Los laboratorios no deben anunciar los servicios de red o poner la información confidencial del laboratorio en riesgo.

La UGI se reserva el derecho de intervenir todos los datos de las redes internas y su administración a cualquier hora, incluye pero no se limita a los paquetes entrantes y salientes, los cortafuegos y los dispositivos periféricos de la red.

Los dispositivos de gateway son necesarios para obedecer a todas las seguridades del producto en la EPN y se deben autenticar contra los servidores de Autenticación Corporativos.

Las contraseñas de administración de todos los dispositivos del laboratorio deben ser diferentes de todas las otras contraseñas de equipos del laboratorio. La contraseña debe ser de acuerdo con la política de contraseñas de la EPN. La contraseña sólo se proporcionará a aquéllos usuarios autorizados para administrar la red del laboratorio.

Todas las peticiones de conexión externa del laboratorio deben ser autorizadas por la UGI. Las líneas análogas o ISDN se las debe configurar para aceptar solamente números de llamada confiables. Las contraseñas se deben utilizar para la autenticación.

Todas las redes de los laboratorios con conexiones externas no deben conectarse a la Polired o a ninguna otra red interna directamente o vía una conexión inalámbrica.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

2.3.26 PSI.R.07 POLÍTICA DE RED DE ÁREA LOCAL VIRTUAL (VLAN)

1.0 PROPÓSITO

El propósito de esta política es proporcionar las normas para conexiones VLAN's al interior de la Polired de la Escuela Politécnica Nacional

2.0 ALCANCE

La presente política se aplica a todos los usuarios y dependencias que se conectan a la Polired de la Escuela Politécnica Nacional utilizando VLAN's como medio conexión.

3.0 POLÍTICA

Esta política se aplica a los funcionarios y dependencias de la Escuela Politécnica Nacional que puede utilizar los beneficios de VLANs. Esto significa que aquellos usuarios o dependencias que requieran acceder a las facilidades prestadas por una VLAN deberán solicitar dicho servicio a la UGI.

Adicionalmente

Es responsabilidad de funcionarios con privilegios de VLAN asegurar que no se permita el acceso a usuarios no autorizados a las redes internas de la Escuela Politécnica Nacional

El uso de VLAN debe ser controlado usando una de contraseña de autentificación tal como un sistema de clave pública o privada con una contraseña o frase fuerte de paso.

Las conexiones VLAN serán configuradas y se administrarán por los responsables de la Unidad de Gestión de Información.

Todos los equipos conectados a la Polired de la Escuela Politécnica Nacional vía VLAN o cualquier otra tecnología deben usar un software anti-virus actualizado establecido por la UGI, esto incluye los computadores personales.

Los usuarios de VLAN serán desconectados automáticamente de una red después de treinta minutos de inactividad. El usuario debe entonces loguearse de nuevo para reconectase a la red. Ping's u otro mecanismo de conexión artificial no deben ser usados para mantener la conexión abierta.

Los usuarios de las dependencias que han solicitado el uso de VLAN de la Escuela Politécnica Nacional deben configurar el equipo para cumplir con las políticas VLAN y políticas de la Polired en general.

Solo pueden acceder usuarios VLAN aprobados por la UGI.

4.0 CUMPLIMIENTO

Cualquier funcionario encontrado culpable por haber violado esta política puede estar sujeto a acciones disciplinarias, llegando incluso al despido del funcionario.

CAPITULO 3
EVALUACIÓN DE LA APLICABILIDAD

Una vez desarrollada la propuesta de políticas de seguridad de la información, se realiza la evaluación de la aplicabilidad cuyo como objetivo fundamental es validar dicha propuesta, es decir determinar si es factible aplicar la propuesta en la Escuela Politécnica Nacional tomando en cuenta varios aspectos tales como legales, económicos, técnicos, operacionales, organizacionales y operacionales.

3.1 ASPECTOS LEGALES

La Escuela Politécnica Nacional forma parte del Sistema Nacional de Educación Superior Ecuatoriano, creada de conformidad con la Constitución Política y la Ley del Estado Ecuatoriano, por lo tanto se constituye en una Institución del Estado obligada a cumplir con la legislación nacional.

El Ecuador desde el año 2004 confirmó su decisión de combatir los delitos de explotación sexual, trata, tráfico, pornografía infantil y otras formas de explotación de niños, niñas, adolescentes, mujeres, los mismos que constituyen violaciones de los derechos humanos.

El Estado Ecuatoriano además ha ratificado una serie de instrumentos internacionales en materia de derechos humanos que lo comprometen por un lado a respetar sus contenidos y por otro lado a implementar las medidas necesarias para cumplir con los compromisos y la vigencia de los mismos.

Estos tratados se constituyen en el marco jurídico que le permite a las instituciones del Ecuador adoptar las medidas necesarias en pos de cumplir dichos compromisos y tener el respaldo jurídico para dichas acciones.

Por ejemplo La Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos en su considerando destaca la necesidad de establecer los mecanismos que permitan el uso adecuado de las tecnologías de la información en beneficio de la población y las instituciones del país.

La Escuela Politécnica Nacional como institución educativa y en atención a la Ley de Educación Superior tiene tres funciones sustantivas como son la docencia, la investigación y la vinculación con la comunidad, por esto requiere la elaboración de políticas de seguridad de la información que le permitan normar el uso de los recursos tecnológicos por parte de funcionarios y estudiantes miembros de la comunidad politécnica, para que estos ayuden a cumplir con las funciones encomendadas a la institución.

A continuación se presenta un compendio de algunas leyes ecuatorianas que contemplan aspectos relativos a la información, propiedad intelectual, comunicaciones, tecnologías de la información, etc., las mismas que se constituyen en la base legal que respalda la creación de las Políticas de Seguridad de la Información que presenta esta propuesta.

3.1.1 LEY DE EDUCACIÓN SUPERIOR

La ley de Educación Superior dentro de los artículos 2, 6 y 27 y dentro de la disposición general segunda contempla aspectos relativos a la necesidad de normar a través de políticas de seguridad de la información lo siguiente.

Estos han sido tomados en cuenta y se presentan a continuación los extractos de los mismos.

Art. 2

Es incompatible con los principios de la Ley de Educación Superior toda forma de violencia, intolerancia y discriminación.

e) Desarrollar sus actividades de investigación científica en armonía con la legislación nacional de ciencia y tecnología y la Ley de Propiedad Intelectual.

Art. 6

La vigilancia y el mantenimiento del orden interno son de competencia y responsabilidad de sus autoridades.

Art. 27

Para su gobierno las universidades y escuelas politécnicas definirán los órganos colegiados de carácter académico y administrativo, así como las unidades de apoyo. Su organización, integración, deberes y atribuciones constarán en sus respectivos estatutos y reglamentos, en concordancia con su misión y las disposiciones establecidas en esta ley.

Disposición General Segunda

Todos los centros de educación superior elaborarán planes operativos cada año y un plan estratégico de desarrollo institucional concebido a mediano y largo plazo, según su propia orientación, que contenga los siguientes aspectos: visión, misión, estrategia, objetivos, resultados esperados y líneas de acción. Cada institución deberá realizar la evaluación de estos planes y elaborar el correspondiente informe, que deberá ser presentado al CONESUP y al Consejo Nacional de Evaluación y Acreditación.

3.1.2 LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

La ley de comercio electrónico, firmas electrónicas y mensajes de datos contempla dentro de los artículos:5, 9, 57, 58, 59, 60, 61, 62, 63, 64 aspectos relativos a la confidencialidad de la información electrónica, su protección, los daños y demás aspectos que se han tomado en cuenta en la propuesta de políticas de seguridad de la información.

La Política de cifrado aceptable, sensibilidad de la información, contemplan los extractos de la ley que se presentan a continuación.

Art. 5 Confidencialidad y reserva

Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.

Art. 9 Protección de datos

Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

Art. 57 Infracciones informáticas

Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Art. 58

El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionadas con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.

Art. 59

Serán reprimidos con tres a seis años de reclusión menor, todo funcionario público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo.

Art. 60 Falsificación electrónica

Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1 Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
2 Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3 Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este capítulo.

Art. 61 Daños informáticos

El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica.

Art. 62 Apropiación ilícita

Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente

sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1 Inutilización de sistemas de alarma o guarda;
2 Descubrimiento descifrado de claves secretas o encriptadas;
3 Utilización de tarjetas magnéticas o perforadas;
4 Utilización de controles o instrumentos de apertura a distancia; y,
5 Violación de seguridades electrónicas, informáticas u otras semejantes.".

Art. 63

Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.".

Art. 64

Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

3.1.3 LEY ESPECIAL DE TELECOMUNICACIONES

La ley especial de telecomunicaciones contempla dentro de los artículos: 7, 9, 11, 14, 27, 28, 29 aspectos relativos a la necesidad de normar a través de políticas de seguridad de la información lo siguiente.

Art. 7

Es atribución del Estado dirigir, regular y controlar todas las actividades de telecomunicaciones.

Art. 9

El Estado regulará, vigilará y contratará los servicios de telecomunicaciones en el País.

Art. 11 Uso Prohibido

Es prohibido usar los medios de telecomunicación contra la seguridad del Estado, el orden público, la moral y las buenas costumbres. La contravención a esta disposición será sancionada de conformidad con el Código Penal y más leyes pertinentes.

Art. 14 Derecho al secreto de las telecomunicaciones

El Estado garantiza el derecho al secreto y a la privacidad de las telecomunicaciones. Es prohibido a terceras personas interceptar, interferir, publicar o divulgar sin consentimiento de las partes la información cursada mediante los servicios de telecomunicaciones.

Art. 27 Delitos contra las telecomunicaciones

Los delitos cometidos contra los medios y servicios de telecomunicaciones serán los tipificados en el Código Penal y serán sancionados de conformidad con lo dispuesto en dicho código.

Art. 28 Infracciones

Constituyen infracciones a la presente Ley, las siguientes:

a. El ejercicio de actividades o la prestación de servicios sin la correspondiente concesión o autorización, así como la utilización de frecuencias radioeléctricas sin permiso o en forma distinta de la permitida.

b. El ejercicio de actividades o la prestación de servicios que no correspondan al objeto o al contenido de las concesiones o autorizaciones.

c. La conexión de otras redes a la red de telecomunicaciones sin autorización o en forma distinta a la autorizada o a lo previsto en esta Ley y sus Reglamentos.

d. La instalación, la utilización o la conexión a la red de telecomunicaciones de equipos que no se ajusten a las normas correspondientes.

e. La producción de daños a la red de telecomunicaciones como consecuencia de conexiones o instalaciones no autorizadas.

f. La importación, fabricación, distribución, venta o exposición para la venta de equipos o aparatos que no dispongan de los certificados de homologación y de cumplimiento de las especificaciones técnicas que se establezcan en los Reglamentos.

g. La competencia desleal en la prestación de los servicios de telecomunicaciones.

h. Cualquiera otra forma de incumplimiento o violación de las disposiciones legales, reglamentarias o contractuales en materia de telecomunicaciones.

Se consideran infracciones graves las siguientes:

a. La conducta culposa o negligente que ocasione daños, interferencias o perturbaciones en la red de telecomunicaciones en cualquiera de sus elementos o en su funcionamiento.

b. La alteración o manipulación de las características técnicas de los equipos, aparatos o de terminales homologados o la de sus marcas, etiquetas o signos de identificación.

c. La producción deliberada de interferencias definidas como perjudiciales en el Convenio Internacional de Telecomunicaciones.

d. La violación a la prohibición constante en el artículo 14 de la presente Ley.

Art. 29 Sanciones

La persona natural o jurídica que incurra en cualquiera de las infracciones señaladas en el artículo anterior sin perjuicio de la reparación de los daños ocasionados será sancionada por las autoridades indicadas en el artículo 30 con una de las siguientes sanciones según la gravedad de la falta, el daño producido y la reincidencia en su comisión:

a. Amonestación escrita.

b. Sanción pecuniaria de uno hasta cincuenta salarios mínimos vitales generales.

c. Suspensión temporal de los servicios.

d. Suspensión definitiva de los servicios.

e. Cancelación de la concesión o autorización y negativa al otorgamiento de nuevas.

Art. 30.- Juzgamiento

Corresponde al Superintendente de Telecomunicaciones juzgar al presunto infractor, graduando la aplicación de la sanción según las circunstancias, mediante resolución motivada y notificada al infractor.

3.1.4 LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

La ley orgánica de transparencia y acceso a la información pública contempla dentro los artículos 3, 5, 6, 13, 17 aspectos relativos a la información pública, confidencial, su difusión y resguardo. Estos han sido tomados en cuenta en la política de sensibilidad de la información.

Ámbito de Aplicación de la Ley

Art. 3

Esta Ley es aplicable a:

a) Los organismos y entidades que conforman el sector público en los términos del artículo 118 de la Constitución Política de la República;

De la información pública y su difusión

Art. 5

Información Pública.- Se considera información pública todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del

Estado.

Art. 6

Información Confidencial.- Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República.

El uso ilegal que se haga de la información personal, o su divulgación, dará lugar a las acciones legales pertinentes.

No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas.

Art. 17

De la Información Reservada.- No procede el derecho a acceder a la información pública, exclusivamente en los siguientes casos:

a) Los documentos calificados de manera motivada como reservados por el Consejo de Seguridad Nacional, por razones de defensa nacional, de conformidad con el artículo 81, inciso tercero, de la Constitución Política de la República y que son:

    1) Los planes y órdenes de defensa nacional, militar, movilización, de operaciones especiales y de bases e instalaciones militares ante posibles amenazas contra el Estado;

2) Información en el ámbito de la Inteligencia, específicamente los planes, operaciones e informes de Inteligencia y Contrainteligencia militar, siempre que existiera conmoción nacional;

3) La información sobre la ubicación del material bélico cuando esta no entrañe peligro para la población; y,

4) Los fondos de uso reservado exclusivamente destinados para fines de la defensa nacional; y,

b) Las informaciones expresamente establecidas como reservadas en leyes vigentes.

3.1.5 LEY PROPIEDAD INTELECTUAL

Art. 1.

El Estado reconoce, regula y garantiza la propiedad intelectual adquirida de conformidad con la ley, las Decisiones de la Comisión de la Comunidad Andina y los convenios internacionales vigentes en el Ecuador.

La propiedad intelectual comprende:

1. Los derechos de autor y derechos conexos.

2. La propiedad industrial, que abarca, entre otros elementos, los siguientes:

a. Las invenciones;
b. Los dibujos y modelos industriales;
c. Los esquemas de trazado (topografías) de circuitos integrados; d. La información no divulgada y los
secretos comerciales e industriales;
e. Las marcas de fábrica, de comercio, de servicios y los lemas comerciales;

f. Las apariencias distintivas de los negocios y establecimientos de comercio;
g. Los nombres comerciales;
h. Las indicaciones geográficas; e,
i. Cualquier otra creación intelectual que se destine a un uso agrícola, industrial o comercial.

3. Las obtenciones vegetales.

Art. 11.

Únicamente la persona natural puede ser autor. Las personas jurídicas pueden ser titulares de derechos de autor, de conformidad con el presente Libro.

Art. 28.

Los programas de ordenador se consideran obras literarias y se protegen como tales. Dicha protección se otorga independientemente de que hayan sido incorporados en un ordenador y cualquiera sea la forma en que estén expresados, ya sea en forma legible por el hombre (código fuente) o en forma legible por máquina (código objeto), ya sean programas operativos y programas aplicativos, incluyendo diagramas de flujo, planos, manuales de uso, y en general, aquellos elementos que conformen la estructura, secuencia y organización del programa.

Art. 129.

El derecho a la patente sobre una invención desarrollada en cumplimiento de un contrato pertenece al mandante o al empleador, salvo estipulación en contrario.

La misma disposición se aplicará cuando un contrato de trabajo no exija del empleado el ejercicio de una actividad inventiva, si dicho empleado ha efectuado la invención utilizando datos o medios puestos a su disposición en razón de su empleo.

En el caso previsto en el inciso anterior, el empleado inventor tendrá derecho a una remuneración única y equitativa en la que se tenga en cuenta la información y medios brindados por la empresa y la aportación personal del trabajador, así como la importancia industrial y comercial de la invención patentada, la que en defecto de acuerdo entre las partes será fijada por el juez competente, previo informe del IEPI.

En las circunstancias previstas en el inciso primero de este artículo, el empleado inventor tendrá un derecho similar cuando la invención sea de importancia excepcional y exceda el objeto implícito o explícito del contrato de trabajo. El derecho a la remuneración prevista en éste inciso es irrenunciable.

A falta de estipulación contractual o de acuerdo entre las partes sobre el monto de dicha retribución, será fijada por el juez, competente previo informe del IEPI. Dicha retribución tiene el carácter de irrenunciable.

En el caso de que las invenciones hayan sido realizadas en el curso o con ocasión de las actividades académicas de universidades o centros educativos, o utilizando sus medios o bajo su dirección, la titularidad de la patente corresponderá a la universidad o centro educativo, salvo estipulación en contrario. Quien haya dirigido la investigación tendrá derecho a la retribución prevista en los incisos anteriores.

3.1.6 LA PORNOGRAFIA INFANTIL Y EL DERECHO DE PRIVACIDAD

Se define pornografía infantil “toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales”. “Cualquier material audiovisual que utiliza niños en un contexto sexual”.

Al ser Internet una red pública a la cual cualquier individuo que posea los medios de conexión necesarios puede conectarse sin una identidad válida necesaria, carece de una regulación jurídica específica, así como de límites y control externo.

Cualquier intento de un gobierno por controlar los contenidos o el uso de Internet se considera una intromisión o violación de privacidad y un atentado contra la naturaleza de la red que es la libertad de información. Por esto el momento de tomar las medidas necesarias para combatir delitos informáticos como la pornografía infantil se puede encontrar muchos escollos al no poseer una base jurídica clara y contundente, que respalde acciones como la intervención de computadores de la institución en busca de este tipo de material prohibido.

La dimensión internacional de Internet y algunas de sus características tales como el uso masivo, la descentralización, la ausencia de territorialidad, y el automatismo, se constituyen en serios obstáculos a la hora de regular jurídicamente su utilización.

La solución a esto empieza con la firma de los tratados internacionales a los cuales el estado ecuatoriano se ha sumando, así de esta manera estos convenios instan a los estados miembros a estimular y favorecer sistemas de autorregulación que incluyan organismos representativos de los proveedores de servicios y de los usuarios de Internet.

También resulta importante el avance del estado ecuatoriano al tipificar en su código penal los delitos de pornografía infantil ejercida por cualquier medio de difusión.

Las diferentes legislaciones de cada país permiten que el cuerpo policial sólo pueda perseguir los delitos en el Estado al cual pertenecen y no tiene competencias en otros estados

La Escuela Politécnica Nacional requiere de un sustento legal que le permita proceder bajo el respaldo de la ley en el momento que requiera tomar acciones en

contra del personal de la institución al cual se le haya encontrado infringiendo las Políticas de seguridad de la información.

La manera legal de proceder ante un caso de pornografía infantil en la institución es que una vez detectada la fuente de almacenamiento o difusión de contenido pornográfico infantil en un servidor alojado dentro la institución, se deberá notificar a la policía quienes tratarán de salvaguardar la mayor cantidad de información del sitio, de manera que no se pierdan las posibles pistas que puedan ayudar en el posterior proceso judicial. Para esto el estado ecuatoriano a través de un juez deberá autorizar el procedimiento de pesquisa para poder intervenir los computadores de los involucrados, sin perjuicio de violar derechos de privacidad.

3.1.7 CODIGO PENAL DE LA REPUBLICA DEL ECUADOR

El código penal de la república del Ecuador tipifica los delitos de explotación sexual y pornografía infantil, a continuación se presenta el extracto relativo a dichos delitos.

Ley Nro. 2005-2 R.O.No.45 de 23/05/2005

Explotación sexual: “Quien produjere, publicare o comercializare imágenes pornográficas, materiales audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato, u organizare espectáculos en vivo, con escenas pornográficas en que participen menores de edad, será reprimido con la pena de seis a nueve años de reclusión menor ordinaria, el comiso de objetos y de los bienes producto del delito, la inhabilidad para el empleo, profesión u oficio…”

También constituye explotación sexual, la facilitación del acceso a espectáculos pornográficos o el suministro de este tipo de material en cuyas imágenes participen menores de edad.

Se establecen circunstancias agravantes cuando la víctima es menor de doce años, discapacitada o adolece de una enfermedad incurable; o en el caso de que el infractor sea padre, madre, pariente hasta el cuarto grado de consanguinidad y segundo de afinidad, tutores, representantes legales, curadores o cualquier otra persona del contorno íntimo de la familia, ministros de culto, profesores u otra persona que se haya valido de su posición para cometer delito.

Se comete también abuso sexual cuando mediante violencia o amenazas se utilice a personas mayores de edad en espectáculos que impliquen la exhibición de su cuerpo con fines sexuales.

3.1.8 PLAN NACIONAL PARA COMBATIR LA TRATA, EXPLOTACIÓN SEXUAL, LABORAL Y OTROS MEDIOS DE EXPLOTACIÓN DE PERSONAS, EN PARTICULAR MUJERES, NIÑOS, NIÑAS Y ADOLESCENTES

La prevención se constituye en el primer esfuerzo para cumplir con la obligación que los estados han adquirido al ratificar las diferentes convenciones internacionales.

Este plan nacional para cumplir de manera operativa con los objetivos planteados, se ejecuta a través de varios ejes. El primero de estos, se constituye en la base que sustenta el desarrollo de esta propuesta de tesis, este es el eje de Prevención que plantea lo siguiente:

“El conjunto de políticas, estrategias, proyectos, acciones, entre otros, que deben ser programadas y coordinadas para generar conciencia sobre la dimensión y gravedad del problema y lograr que las diferentes estancias del Estado y otros sectores sociales, articulen respuestas efectivas, que busquen la eliminación y/o modificación de las condiciones, causas y factores de riesgo y de vulnerabilidad que originan las conductas delictivas y de victimización”.

Este conjunto de políticas planteadas deberán estar dirigidas entre otros a los funcionarios de las instituciones del estado con el objetivo de que conozcan cuales son estos delitos y el impacto que tienen sobre sus victimas, además de que sepan cual es el papel que deben jugar como funcionarios del estado ante estas violaciones de derechos humanos.

El eje de investigación y sanción contempla:

“El sistema jurídico se pone en acción a través de la investigación, que tiene por objetivo establecer a través de un procedimiento lógico legal y pertinente si un hecho que esta en consideración del Ministerio Público es constitutivo de delito. Establecer como sucedieron los hechos, quienes son los responsables, que grado de participación tienen los imputados y en qué figura tipificada en el código penal se encuadra el hecho pesquisado.

La investigación busca una comprensión de los delitos materia del Plan y toda su complejidad para que las diligencias, la recolección de las evidencias, la formulación de hipótesis, los peritajes y la determinación del tipo penal, cumplan con el objetivo de hacer justicia a las víctimas.

La investigación debe garantizar la recolección de todos los elementos que posteriormente serán analizados por los tribunales respectivos, para imponer sanciones adecuadas que correspondan a la gravedad de los delitos cometidos.”

Los compromisos adquiridos por el estado en la adopción de convenios internacionales en los que se menciona entre otros los delitos de explotación sexual, pornografía infantil, etc. se contemplan dentro de los artículos: 1, 3, 9:

Art. 1 Los estados deben prohibir la pornografía infantil.
Art. 3 El estado debe tipificar en las leyes penales la pornografía infantil.
Art. 9 Los estados deben adoptar y aplicar medidas administrativas, políticas y sociales para la prevención de estos delitos.

Declárese como política prioritaria del estado el combate al plagio de personas, tráfico ilegal de migrantes, explotación sexual y laboral; y otros modos de explotación y prostitución de mujeres, niños, niñas y adolescentes, pornografía infantil y corrupción de menores. Por tanto es responsabilidad del estado y de sus instituciones, en el marco del enfoque de derechos y las disposiciones legales y reglamentarias vigentes, desarrollar, dirigir y ejecutar políticas y estrategias para cumplir estos propósitos.

Pornografía Infantil es la representación de un niño o niña por cualquier medio con actividades sexuales explicitas, reales o simuladas o la representación de los genitales de un niño o niña con fines primordialmente sexuales.

La constitución política del Estado Ecuatoriano también contempla la lucha contra estos delitos, así el Art. 50 manifiesta lo siguiente:

Art. 50.

El Estado adoptará las medidas que aseguren a los niños y adolescentes las siguientes garantías:

1. Atención prioritaria para los menores de seis años que garantice nutrición, salud, educación y cuidado diario.
2. Protección especial en el trabajo, y contra la explotación económica en condiciones laborales peligrosas, que perjudiquen su educación o sean nocivas para su salud o su desarrollo personal.
3. Atención preferente para su plena integración social, a los que tengan discapacidad.
4. Protección contra el tráfico de menores, pornografía, prostitución, explotación sexual, uso de estupefacientes, sustancias psicotrópicas y consumo de bebidas alcohólicas.

5. Prevención y atención contra el maltrato, negligencia, discriminación y violencia.
6. Atención prioritaria en casos de desastres y conflictos armados.
7. Protección frente a la influencia de programas o mensajes nocivos que se difundan a través de cualquier medio, y que promuevan la violencia, la discriminación racial o de género, o la adopción de falsos valores.

A continuación se presenta un mapa conceptual que resume los aspectos legales tomados en cuenta. Véase Fig 3.1.

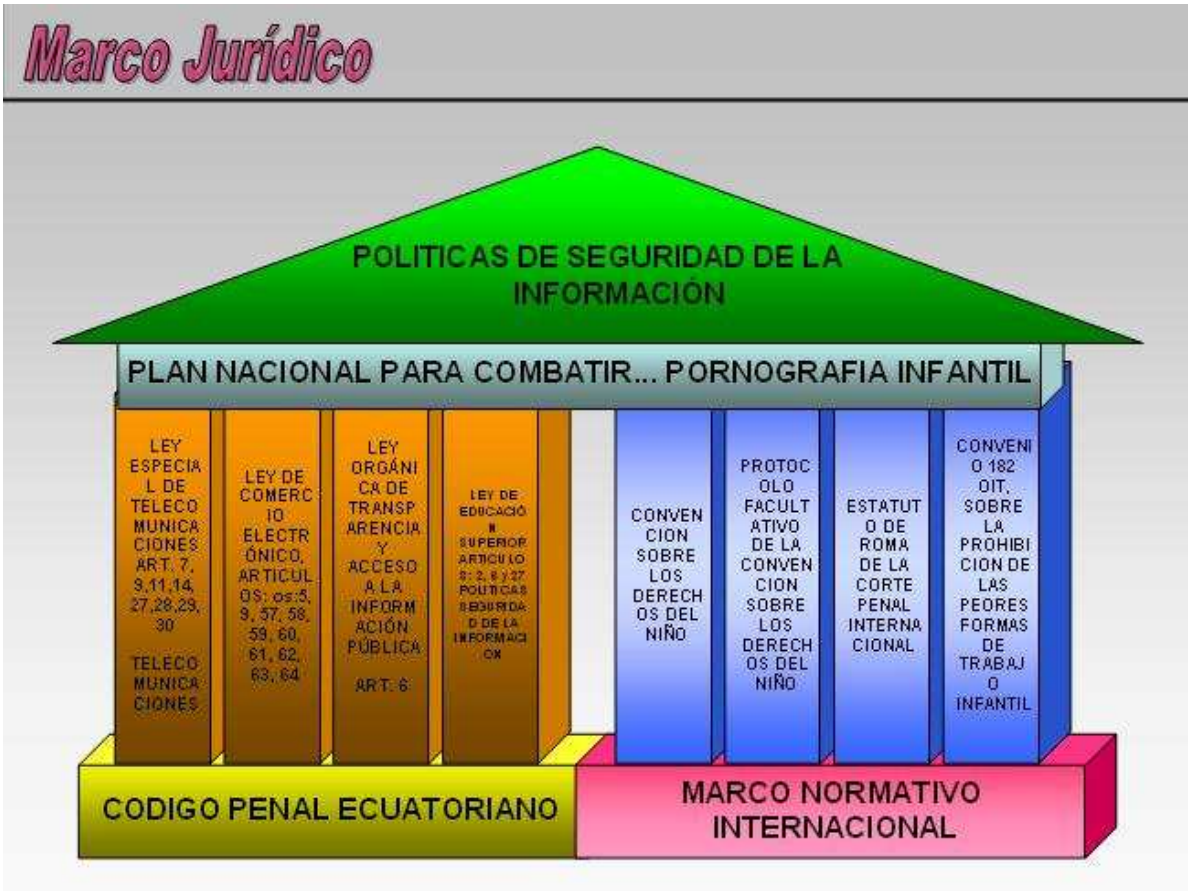

Figura 3.1 Mapa conceptual aspectos legales

Autor: Ing. Marco Santórum G.

3.2 ASPECTOS OPERACIONALES

3.2.1 DEFINICION DE ROLES DEL RECURSO HUMANO

Para poder establecer la planificación inicial se deberá definir el perfil del recurso humano requerido para dicha implantación.

A continuación se definen los roles necesarios a ser desempeñados por el recurso humano de la EPN, cabe notar que se presenta una descripción del perfil de cada rol mas no la designación específica de una persona de la institución, a excepción de las autoridades cuya participación es necesaria.

Rector (R): Autoridad de la EPN y miembro de Consejo Politécnico responsable de la aprobación de las políticas.

Vicerrector (VR): Autoridad de la EPN y miembro de Consejo Politécnico responsable de la aprobación de las políticas.

Consejo Politécnico (CP): Organismo de la EPN responsable de la aprobación de las políticas que rigen a la institución conformado por representantes de todos los sectores de la comunidad politécnica.

Consejo Politécnico está conformado por: Rector, Vicerrector, Docentes (6), Estudiantes (3), Trabajador (1).

Representante Legal (RL): Persona con la autoridad requerida para representar legalmente a la EPN, responsable del asesoramiento, análisis y cumplimiento legal de las políticas.

Encargado del Proyecto (EP): Persona(s) de la Institución que bajo el encargo de la UGI sea el responsable directo de la implantación de las Políticas de Seguridad de la Información en la EPN.

Jefe Proyecto UGI (JP): Persona con la autoridad requerida para representar a la UGI ante las autoridades de la EPN, responsable de aprobar la propuesta de Políticas de Seguridad de la Información y de presentar formalmente la propuesta ante Consejo Politécnico.

Este rol podría ser desempeñado por el Jefe de la Unidad de Gestión de la Información.

Comité de Seguridad de la Información (CS): El establecimiento de un comité de seguridad de la información proporciona un foro de amplio espectro para revisar y evaluar la viabilidad de POLÍTICAS que afectan a toda la universidad.

La responsabilidad del comité de seguridades garantizar que las POLÍTICAS, estén bien redactadas, sean comprensibles, estén coordinadas y sean viables en términos de las personas, procesos y tecnologías que afecta.

Para este proyecto este comité estará conformado por el Encargado de proyecto, el Jefe del Proyecto y personal de la UGI relacionado con la temática que se esté tratando.

Decanos (D): Autoridades de gestión representantes de las Facultades de la EPN, encargados de la difusión, cumplimiento, monitoreo y definición de las políticas y sus excepciones..

Sub Decanos (SD): Autoridades académicas representantes de las Facultades de la EPN, encargados de la difusión, cumplimiento, monitoreo y definición de las políticas y sus excepciones.

Jefes de Departamento (JD): Autoridades investigativas y de vinculación con la colectividad representantes de los departamentos de la EPN, encargados de la difusión, cumplimiento, monitoreo y análisis y definición de las políticas y sus excepciones.

Promotor(es) (P): Persona(s) responsables de la difusión, promoción, concienciación de las políticas.

3.2.2 CUESTIONARIO DE ANÁLISIS OPERATIVO

Para establecer la factibilidad operativa además se ha realizado una encuesta a miembros de la comisión del proceso de selección del hardware y software involucrados en el proyecto se seguridad periférica de la EPN.

ANÄLISIS	SI	NO
1. ¿Existe el apoyo del nivel directivo para realizar la implementación de la propuesta de políticas de seguridad de la información?	x	
2. ¿Los procesos administrativos de la institución son factibles de adaptarse a la propuesta?	x	
3. ¿El estándar propuesto para la elaboración de las políticas es factible de ser adaptado a la realidad de la EPN?	x	
¿El recurso humano de la Unidad de Gestión de la Información esta capacitado para aplicar la propuesta?	x	
¿Considera que la propuesta generará beneficio a la institución?	x	

Tabla 3.1 Recurso humano responsable ciclo de vida de las PSI
Fuente: Ing. Gustavo Samaniego.

3.2.3 CRONOGRAMA Y PLANIFICACIÓN DE RECURSOS

A continuación se presenta un diagrama de Gantt a través del cual se ha planificado las tareas, el personal requerido, y tiempo de dedicación, con el fin de determinar el esfuerzo humano requerido. Véase Figura 3.2.

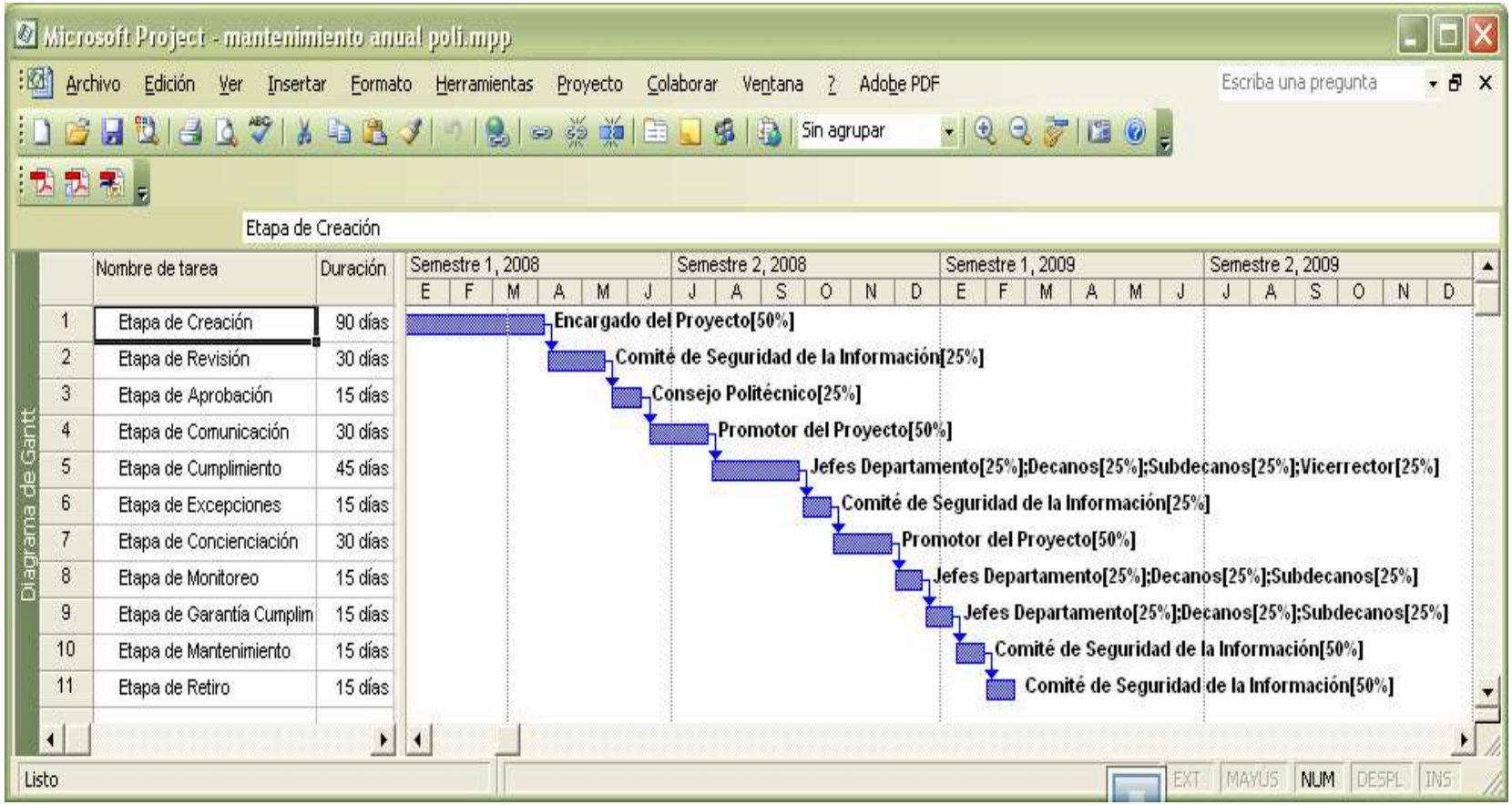

Figura 3.2: Cronograma y planificación de recursos

Autor: Ing. Marco Santórum G.

3.2.4 RESULTADOS DE LA FACTIBILIDAD OPERACIONAL

La Escuela Politécnica Nacional posee el recurso humano necesario para la realización del proceso.

Se cuenta con el apoyo de las autoridades de la Institución para la realización del proyecto.

Muestra del apoyo de las autoridades es el presupuesto asignado para la adquisición del software y hardware necesarios para la implementación.

Los equipos han sido adquiridos por la institución.

El recurso humano en este momento se ha capacitado para la operación de los equipos.

Las políticas de seguridad de la información por la tanto permiten establecer los lineamientos en base a los cuales los equipos adquiridos deben funcionar.

El tiempo de implementación de la propuesta esta retrasado con respecto a los requerimientos, sin embargo la planificación se adapta a la realidad de la institución y el recurso humano de la misma esperando cumplir con la aprobación y puesta en marcha de las políticas a corto plazo.

3.3 ASPECTOS ORGANIZACIONALES

Al validar la propuesta tomando en cuenta los aspectos organizacionales se busca determinar la factibilidad de la implantación de las mismas en la Escuela Politécnica Nacional.

Con este análisis organizacional se designa los responsables para cada etapa del ciclo de vida de las políticas.

3.3.1 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Es importante determinar los involucrados en el desarrollo de las Políticas de seguridad de la información.

Para esto se deberá conformar un Comité de Seguridad de la Información encargado de llevar a cabo la ejecución del proceso durante el ciclo de vida de las políticas.

De manera ideal este Comité deberá ser integrado por el Jefe de la Unidad de Gestión de la Información de la EPN, ya que esta unidad es responsable de la Administración de los Recursos de TI de la Institución y quienes deberán durante todo el proceso ser los responsables directos de la ejecución del proyecto de implantación de estas políticas y posteriormente de su monitoreo y mantenimiento.

Miembros del Comité de Seguridad de la Información

El Comité de Seguridad de la Información deberá ser conformado de manera ideal por el Jefe de de la Unidad de Gestión de la Información para desempeñar funciones como la Gestión General del proyecto y los demás miembros de la UGI en un papel de apoyo cuando así se lo requiera.

Se requiere la participación del nivel directivo de la EPN representado ya sea por el Rector o Vicerrector quienes considerarán y aprobarán las resoluciones del comité de seguridad.

El jefe de la UGI deberá necesariamente ser el Jefe de proyecto, siendo este el responsable oficial de la propuesta de políticas de seguridad de la información ante Consejo Politécnico.

De la UGI intervendrán además los administradores de los servicios de acuerdo a los requerimientos según la plataforma o servicio que administre en caso de ser necesario.

Se requiere la participación del asesor jurídico de la institución quien debe examinar las políticas una vez que los documentos se hayan redactado. Este debe proporcionar asesoramiento sobre la legislación nacional e internacional, dar criterios de cierto tipo de información que se debe proteger, así como sobre otras cuestiones jurídicas.

Durante la etapa de revisión de documentos de las políticas, puede ser útil trabajar con los usuarios para garantizar la aceptación y el éxito de la política.

Una vez redactadas las políticas, el comité de seguridad será responsable de las etapas de revisión, excepciones, mantenimiento y retiro de las mismas, posteriormente el comité estará disponible para contestar preguntas y consultas sobre las políticas.

Para la evaluación de este proyecto se ha planificado la participación de dos miembros permanentes del comité, estos serán el jefe de proyecto y el encargado del proyecto.

Funciones del Comité de Seguridad de la Información.

Serán funciones del Comité de Seguridad de la Información las siguientes:

1. Revisar y proponer a Consejo Politécnico para su aprobación, la propuesta de Políticas de Seguridad de la Información y las responsabilidades generales en materia de seguridad de la información.

2. Llevar a cabo el proceso de implantación de las Políticas de Seguridad de la Información de la Escuela Politécnica Nacional.

3. Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

4. Tomar conocimiento y supervisar la investigación y el monitoreo de los incidentes relativos a la seguridad.

5. Aprobar las principales iniciativas para incrementar la seguridad de la información.

6. Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.

7. Garantizar que la seguridad sea parte del proceso de planificación de la información.

8. Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

9. Promover la difusión y apoyo, a la seguridad de la información dentro de la institución.

3.3.2 ASIGNACIÓN DE RESPONSABLES DURANTE EL CICLO DE VIDA

Se determina los responsables por etapa del ciclo de vida de las políticas tomando en cuenta los roles definidos en la etapa de aspectos operativos. Estos serán quienes deberán cumplir los requisitos necesarios para la implantación de las políticas en cada etapa. Se definirá los funcionarios que desempeñarán cada rol en caso de implantarse las políticas.

A continuación se exponen las etapas del proceso desde la aprobación, la primera es cubierta en este documento, las diez restantes están fuera del alcance del proyecto de tesis.

Etapa de Creación

El objetivo de esta etapa es la definición y redacción de las políticas documentadas de acuerdo con los procedimientos y estándares seleccionados.

Esta etapa es cubierta por este proyecto de tesis, por lo que el responsable directo es el autor de la Tesis, o en el caso del presente análisis el responsable es:

- Encargado del Proyecto

Etapa de Revisión

Propio de esta etapa será la presentación de las políticas a los revisores, a quienes se expondrá cualquier punto que puede ser importante en la revisión, explicando sus objetivos, el contexto y los beneficios potenciales de las políticas justificando la necesidad de las mismas.

En el caso del presente análisis se requiere del siguiente recurso humano:

- Comité de Seguridad de la Información.

Etapa de Aprobación

Las políticas de seguridad que afectan toda la universidad deben ser aprobadas y firmadas por la máxima autoridad tal como es el Consejo Politécnico, para garantizar el nivel necesario de énfasis y visibilidad de las políticas a través de la aprobación y oficialización de las mismas.

Para esto se requiere del siguiente recurso humano:

- Rector
- Vicerrector
- Representante Legal
- Consejo Politécnico

Etapa de Comunicación

La política debe ser inicialmente difundida a los miembros de la comunidad universitaria o a quienes sean afectados directamente por la política.

Para esto se requiere la participación de la Dirección de Relaciones Institucionales. En el caso del presente análisis se denomina:

- Promotor

Etapa de Cumplimiento

La etapa de cumplimiento implica trabajar con otras personas de la Universidad, Vicerrector, Decanos, Jefes de Departamento y los Jefes de dependencias para interpretar cuál es la mejor manera de implementar la política en diversas situaciones y dependencias.

Para esto se requiere de los funcionarios con responsabilidades de supervisión en la universidad:

- Vicerrector
- Decanos
- Subdecanos
- Jefes de Departamento

Etapa de Excepciones

Debido a problemas de coordinación, falta de personal y otros requerimientos operacionales, no todas las políticas pueden ser cumplidas de la manera que se pensó al comienzo. Por esto, cuando los casos lo ameriten, es probable que se requieran excepciones a la política para permitir a ciertas dependencias o personas el no cumplimiento de la política.

Para esto se requiere del siguiente recurso humano:

- Comité de seguridad de la información

Etapa de Concienciación

La etapa de concienciación comprende los esfuerzos continuos realizados para garantizar que las personas están conscientes de la política y buscan facilitar su cumplimiento.

Para esto se requiere del siguiente recurso humano:

- Promotor

Etapa de Monitoreo

Esta etapa incluye actividades continuas para monitorear el cumplimiento o no de la Política a través de métodos formales e informales y el reporte de las deficiencias encontradas a las autoridades apropiadas.

Para esto se requiere de los funcionarios con responsabilidades de supervisión en la universidad:

- Decanos
- Subdecanos
- Jefes de Departamento

Etapa de Garantía de cumplimiento

Se deben determinar y aplicar las acciones correctivas a los procesos que se han contravenido o han fallado.
La revisión de los procesos y su mejoramiento así como la actualización de la tecnología y acciones disciplinarias son necesarios con el fin de reducir la probabilidad de que vuelva a ocurrir.

Para esto se requiere de los funcionarios con responsabilidades de supervisión en la universidad:

- Decanos
- Subdecanos
- Jefes de Departamento

Etapa de Mantenimiento

Esta etapa incluye hacer seguimiento a las tendencias de cambios en la tecnología, en los procesos, en las personas, en la institución, en el enfoque del negocio, que pudieran afectar la política. Se deberá entonces recomendar y coordinar modificaciones documentándolos en la política y registrando las actividades de cambio.

Para esto se requiere del siguiente recurso humano:

- Comité evaluación de políticas

Etapa de Retiro

Después que la política ha cumplido con su finalidad y no es necesaria entonces debe ser retirada, esto se daría por ejemplo cuando la universidad cambió la tecnología a la cual se aplicaba la política o se creó una nueva política que la reemplazó.

Para esto se requiere del siguiente recurso humano:

- Comité de seguridad de la información

A continuación se presenta un resumen de los responsables por etapa.
Véase Tabla 3.1.

Etapa	Políticas
Creación	Cubierta en el proyecto de tesis , Encargado del proyecto
Revisión	Comité de seguridad de la información.
Aprobación	Rector, Vicerrector, Representante legal, Consejo Politécnico
Comunicación	Promotor
Cumplimiento	Funcionarios con responsabilidades de supervisión
Excepciones	Comité de seguridad de la información
Concienciación	Promotor
Monitoreo	Funcionarios con responsabilidades de supervisión
Garantizar cumplimiento	Funcionarios con responsabilidades de supervisión
Mantenimiento	Comité de seguridad de la información
Retiro	Comité de seguridad de la información

Tabla 3.2 Recurso humano responsable ciclo de vida de las PSI

Autor: Ing. Marco Santórum G.

Una vez determinados los aspectos organizacionales y la designación de responsables se puede concluir lo siguiente:

- La Escuela Politécnica Nacional posee el personal requerido para la ejecución del proyecto.
- Las horas invertidas por el personal de la EPN se consideran parte de la carga asignada semestralmente o parte de sus funciones administrativas por lo que no representan un gasto adicional.
- Se requiere la participación del nivel directivo de la EPN en el proceso de implantación junto a los involucrados con el fin de garantizar el éxito de las políticas.

- Como todo proceso que involucra la participación de varios sectores de la institución acostumbrados a no poseer políticas regulatorias en su accionar, generará resistencia por parte del personal quienes deberán poner el hombro para que el proyecto cumpla con sus objetivos planteados.
- El impacto a la institución será alto, sin embargo a largo plazo permitirá conducir la institución a través de procesos de TI seguros.

3.4 ASPECTOS ECONÓMICOS

A continuación se presenta un análisis que permita evaluar la factibilidad de la implantación de las políticas de seguridad de la información tomando en cuenta los aspectos económicos.

En primer lugar se va a determinar el esfuerzo que involucra llevar adelante la implementación de la propuesta.

Se tomará en cuenta los siguientes aspectos:

- El tiempo requerido para dicha implantación.
- El personal requerido que involucra la implementación de las políticas.
- Los recursos tecnológicos que se requieren, como software y hardware.
- Los recursos materiales requeridos.

3.4.1 PRODUCTIVIDAD LABORAL Y DATOS ESTADISTICOS

Al definir productividad del trabajo se puede observar que “es el rendimiento o eficiencia de la actividad productiva de los hombres expresada por la correlación entre el gasto de trabajo y la cantidad de bienes materiales producidos en una unidad de tiempo. Se determina por la cantidad de tiempo invertido en elaborar la unidad de producción o por la cantidad de producción fabricada en la unidad de tiempo”[4].

---

4 Tomado de: Diccionario de economía política de Borísov, Zhamin y Makárova

Un factor muy importante a la hora de mejorar la productividad de una institución es la tecnología, por ejemplo la tecnología permite tener una mayor rapidez en la atención a los usuarios y brindar un mejor servicio, ayudan a reducir costes, o a vender más, a ser más productivos en general.

Sin embargo si esta tecnología se constituye en un factor que en lugar de mejorar la productividad hace que los funcionarios pierdan su tiempo por ejemplo accediendo a sitios Web con información vaga o irrelevante o para realizar actividades no relacionadas con su trabajo, si estos forman parte de cadenas de correo electrónico basura, si el computador se constituye en un elemento distractor, la productividad de la institución se va reducir en lugar de aumentar.

Es por esto que tomando en cuenta el dato estadístico proporcionado por firma de recursos humanos, Kelly Services [5], se puede llegar a varias conclusiones.

La firma precisó que para esta encuesta buscó puntos de vista de aproximadamente 70,000 personas en 28 países incluyendo a Ecuador.

La encuesta buscó identificar la incidencia de correos no deseados conocidos como SPAM, así como el impacto que tienen en la productividad en el trabajo.

El 41% de los trabajadores contestó que reciben un gran número de correos que son inútiles. El SPAM es cada vez más común, ya que el 29% de los usuarios de esta

---

[5] Tomado de : Firma de recursos humanos, Kelly Services

herramienta contestaron que más del 20% de los correos que reciben a diario son SPAM.

La encuesta encontró que el uso de las herramientas de comunicación en línea se ha extendido a la mayoría de la fuerza laboral.

El 81% de los trabajadores usan el correo y otros recursos de Internet, 11% utilizan únicamente el correo y 2% se limitan a navegar para consultas diversas, solamente el 3% no usa ninguna de estas herramientas.

De acuerdo a estos resultados, la tecnología impacta positivamente en la calidad del trabajo ya que el 85% de los encuestados dijo que el uso de las TI ayuda a mejorar su productividad.

Sin embargo así mismo si se toma en cuenta datos estadísticos propuestos por empresas como yahoo, dicen que el 40 % [6]del tráfico de la red no es productivo, es decir que si los funcionarios acceden a Internet el 40 % de su tiempo lo destinan a actividades ajenas a las legítimamente encomendadas.

La jornada laboral considerada en la Escuela Politécnica Nacional es de 8 horas diarias, 40 semanales, 160 horas mensuales.

En la institución como en todas existe tiempo no productivo del funcionario tiempo en el cual desarrolla sus actividades como trasladarse de la entrada a la dependencia, de la dependencia a la salida, tiempo de refrigerio, ir al baño, tiempo de actividades varias, tiempo entre comidas, cafés, pasillos, reuniones mal convocadas e innecesarias, Internet, etc.

---

[6] Tomado de Ing. Pablo Sosa . Maestría Gestión de TIC's EPN. Seguridad Informática.

Para nuestro caso se considera entonces que apenas una hora es destinada a las actividades no productivas en la institución.

Horas Productivas

Actividades Principales:	30%
Actividades Administrativas:	20%
Actividades Investigativas:	20%
Actividades relacionadas con TI:	30%

	100% (7 horas)

Horas no productivas

Actividades no productivas	1 hora

(Entrada, Salida, Coffe Break, baño, teléfono, etc.)

3.4.2 IDENTIFICACIÓN DE COSTOS

Implantación de las Políticas

Para la identificación de los costos que involucra el proyecto respecto del recurso humano se ha considerado una escala estimada de valores tomando en cuenta un valor promedio de ingresos por cada nivel remunerativo en la EPN como se muestra a continuación:

Nivel gerencial: 3200 dólares (mensuales * 160 horas de trabajo)
Nivel ejecutivo: 3000 dólares (mensuales * 160 horas de trabajo)
Nivel profesores: 2500 dólares (mensuales * 160 horas de trabajo)
Nivel técnico: 1500 dólares (mensuales * 160 horas de trabajo)
Nivel operativo: 800 dólares (mensuales * 160 horas de trabajo)

Se debe notar además que estos valores son considerados dentro de la remuneración que percibe el recurso humano de la Escuela Politécnica Nacional por lo que no representaría un egreso adicional.

A continuación se presenta una tabla con la identificación de los valores asociados a la participación del recurso humano en el proyecto.

Código	Descripción	Tipo de Recurso	Costo estimado por hora
CP	Consejo Politécnico (10 personas)	Gerencial	175.63 USD.
R	Rector	Gerencial	20 USD.
VR	Vicerrector	Gerencial	20 USD.
RL	Representante Legal	Ejecutivo	15.63 USD.
D	Decanos	Ejecutivo	18.75 USD.
SD	Sub Decanos	Ejecutivo	18.75 USD.
JD	Jefes de Departamento	Ejecutivo	18.75 USD.
JP	Jefe Proyecto UGI	Ejecutivo	18.75 USD.
EP	Encargado Proyecto	Ejecutivo	9.38 USD.
CS	Comité de seguridad de la información EP+JP	Ejecutivo	26.25 USD.
P	Promotor	Operativo	9.38 USD.

Tabla 3.3: Costos estimados del personal involucrado

Autor: Ing. Marco Santórum G.

	Nombre del recurso	Tipo	Iniciales	Capacidad máxima	Tasa estándar
1	Jefe UGI	Trabajo	JP	100%	$ 18,75/hora
2	Representante Legal	Trabajo	R	100%	$ 15,63/hora
3	Rector	Trabajo	R	100%	$ 20,00/hora
4	Vicerrector	Trabajo	VR	100%	$ 20,00/hora
5	Jefes Departamento	Trabajo	JD	100%	$ 18,75/hora
6	Decanos	Trabajo	D	100%	$ 18,75/hora
7	Subdecanos	Trabajo	SD	100%	$ 18,75/hora
8	Encargado del Proyecto	Trabajo	EP	100%	$ 9,38/hora
9	Comité de Seguridad de la Información	Trabajo	CS	100%	$ 26,25/hora
10	Consejo Politécnico	Trabajo	CP	100%	$ 175,63/hora
11	Promotor del Proyecto	Trabajo	P	100%	$ 9,38/hora

Figura 3.4: Recurso humano del Proyecto

Autor: Ing. Marco Santórum G.

Una vez realizado el cálculo del costo del proyecto en recurso humano tomando en cuenta las horas necesarias los niveles salariales y fases del proyecto se ha proyectado un costo inicial de 58.000 dólares en recurso humano necesario para ejecutar el proyecto.

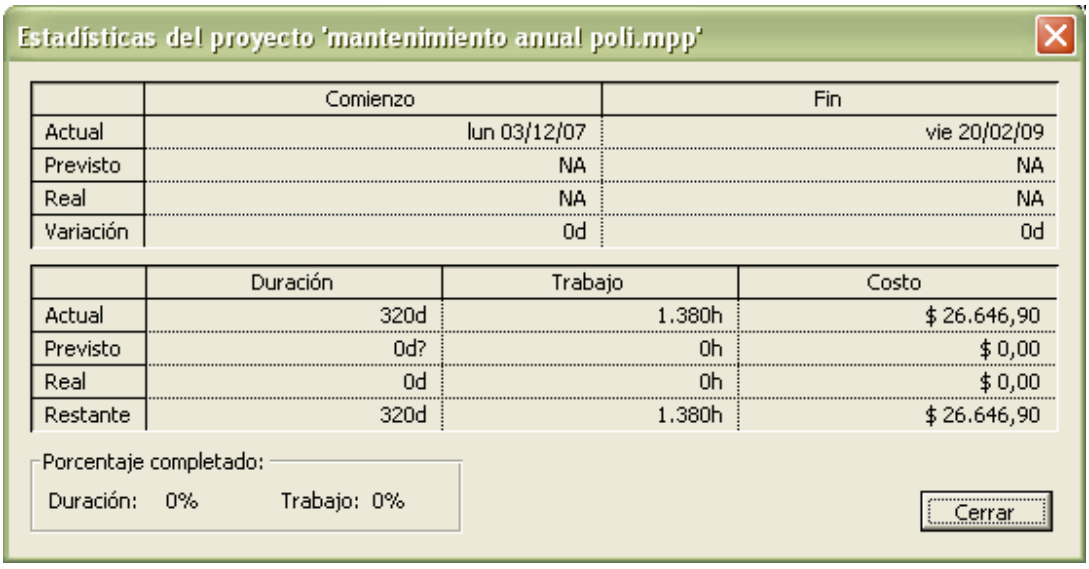

Figura 3.5: Estadísticas del Proyecto

Autor: Ing. Marco Santórum G.

La implantación de estas políticas requiere la implantación de dispositivos de seguridad periférica que permitan monitorear las actividades de los host internos de la institución.

Para esto entre otros la Unidad de Gestión de la Información requiere la adquisición de 4 servidores para dar un servicio básico y confiable de red, un Servidor de Monitoreo para el proyecto Estación de Trabajo y Redes Avanzadas, un Servidor de Antivirus, con el cual poder monitorear y actualizar las PC's de la Escuela Politécnica Nacional, un Servidor de DNS y DHCP para la asignación de direcciones IP dinámicamente, un Servidor de Correo Electrónico, un Firewall, etc.

La Escuela Politécnica Nacional ha presupuestado en el año 2008 la inversión en renovación de servidores y laboratorios de la institución, para esto ha considerado la inversión en equipamiento para la Unidad de Gestión de la Información de 150000 dólares.

Mantenimiento de las Políticas

Durante la fase de mantenimiento de las políticas se busca concienciar a los funcionarios de la Escuela Politécnica Nacional de la importancia de las políticas, y para garantizar el cumplimiento y su efectividad se deberá monitorear, garantizar su cumplimiento y de ser necesario corregirlas o actualizarlas.

A continuación se identifican los costos involucrados en el mantenimiento anual de las Políticas de Seguridad de la Información.

El siguiente diagrama de Gant presenta la planificación de la etapa de mantenimiento de las políticas de seguridad de la información.

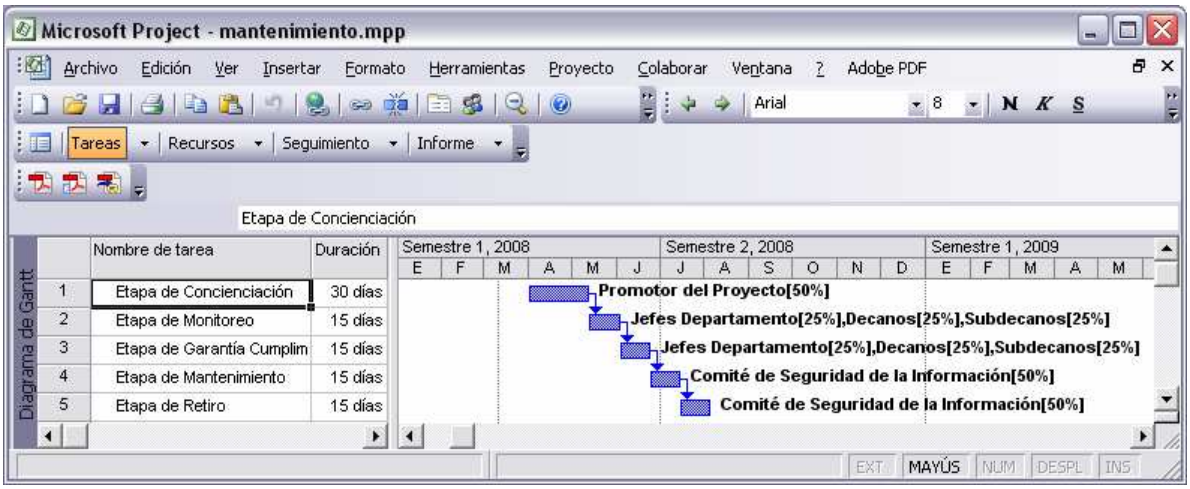

Figura 3.6: Planificación de la fase de mantenimiento

Autor: Ing. Marco Santórum G.

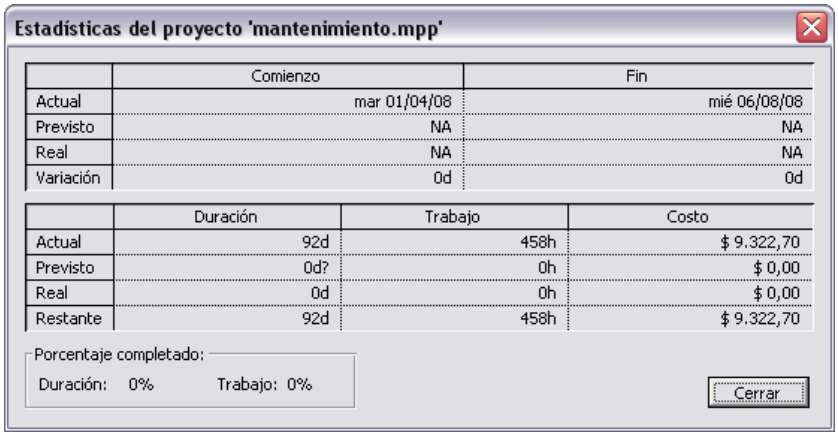

Figura 3.7: Costos anuales de la fase de mantenimiento

Autor: Ing. Marco Santórum G.

Una vez identificados los costos involucrados en el proyecto por concepto del recurso humano requerido en la fase de mantenimiento, se procede a identificar los demás costos del proyecto.

COSTOS DE MANTENIMIENTO	
Costos de sueldos y salarios	9322,72
Costos de promoción	1000
Costos Comunicación y Papelería	1000
Costos de Administración	1000
Otros	500
TOTAL COSTOS	12822,72

Tabla 3.4: Costos de mantenimiento

Autor: Ing. Marco Santórum G.

Estos costos de mantenimiento anual se lo toman en cuenta durante el ciclo de vida del proyecto tomando en cuenta el porcentaje de inflación anual provisto por el Banco Central del Ecuador. [7]

AÑOS	CICLO DE VIDA DEL PROYECTO				
	0	1	2	3	4
	0	12822,72	13207,40	13603,62	14011,73

Tabla 3.5: Proyección de costos

Autor: Ing. Marco Santórum G.

3.4.3 PROYECCIÓN DE COSTOS DURANTE LA VIDA ÚTIL DEL PROYECTO

Si se considera un tiempo de vida útil del proyecto de 4 años, tomando en cuenta el periodo de duración de los cargos de las autoridades de la EPN y si se realiza una evaluación del costo de mantenimiento del proyecto se observa lo siguiente.

[7] Inflación anual promedio BCE. 3 %

Años	Hardware y Software	Implementación Políticas y Procedimientos	Porcentaje Mantenimiento de Políticas y Procedimientos	Costo Mantenimiento Políticas	Costos Totales
0	150000	26646,90	0%	0,0	176646,9
1	0,0	0,0	0%	12822,72	12822,72
2	0,0	0,0	3%	13207,4016	13207,4016
3	0,0	0,0	3%	13603,6236	13603,6236
4	0,0	0,0	3%	14011,7324	14011,7324
					230292,37

Tabla 3.6: Costos estimados del proyecto en su vida útil.

Autor: Ing. Marco Santórum G.

3.4.4 IDENTIFICACIÓN DE BENEFICIOS

Una vez implantadas las Políticas de Seguridad de la Información en la EPN, se deberán observar los beneficios que estas generan, sin embargo resulta complicado cuantificarlos en todos los casos, puesto que no necesariamente todos los beneficios que se podría obtener serán perceptibles.

A continuación se detallan los beneficios que puede obtener la institución.

BENEFICIOS PARA LA INSTITUCION
Mejora de la calidad del servicio que prestan las dependencias hacia los usuarios de la EPN.
Beneficios ocasionados por sistemas mejorados en términos de la seguridad, precisión, velocidad y disponibilidad.
La Unidad de Gestión de la Información más eficaz y sobretodo más eficiente a la hora de atender los procedimientos de la institución cubiertos por las Políticas de Seguridad de la Información.
Políticas y procedimientos definidos.
Mejor uso y aprovechamiento de los recursos de TI de la institución.
Reducción de costos de los servicios de telecomunicaciones.
Ampliación de la disponibilidad de recursos usados en beneficio de actividades propias de la institución.
Respaldo legal y oficial a la hora de proceder en caso de violación a las políticas de seguridad de la Información por parte de los funcionarios de la Institución.
Mejora en la administración y control de los recursos de TI.
Mejor organización de los recursos de TI.
Reducción de los riesgos en los servicios de TI.
Concientización de los usuarios sobre el valor económico de los servicios de TI que recibe.
Contar con información precisa sobre la infraestructura y servicios de TI.
Gestión de la seguridad clara y estructurada.
Mejorar la imagen de institución a nivel interno y externo.

Tabla 3.7: Descripción de beneficios de la propuesta

Autor: Ing. Marco Santórum G.

Este conjunto de beneficios traen consigo sobretodo una mejora en el servicio, eficiencia y productividad de la institución es por esto que es tratará de cuantificarlos.

3.4.5 COSTO DE OPORTUNIDAD

La cuantificación de los beneficios resulta ser un tanto subjetiva puesto que se toma en cuenta posibilidades o probabilidades de que suceda un determinado escenario u otro.

La manera de cuantificar los beneficios por lo tanto se la hace tomando en cuenta la posibilidad de dejar de percibir los posibles beneficios si no se realiza una determinada inversión.

Por esto es necesario definir que es costo de oportunidad.

Si nos referimos a la gestión, el coste de oportunidad de una inversión, es el costo de la no realización de una inversión.

También se la puede definir como aquel costo en que se incurre al tomar una decisión y no otra. Aquel valor o utilidad que se sacrifica por elegir una alternativa A y despreciar una alternativa B. Tomar un camino significa que se renuncia al beneficio que ofrece el camino descartado. Valor que representa el desaprovechar una oportunidad.

3.4.6 CUANTIFICACIÓN DE BENEFICIOS

Para poder cuantificar los beneficios de la propuesta, será necesario establecer un estimado de valores en cuanto a: presupuesto anual de la institución, recursos necesarios para invertirlos en el soporte, mantenimiento y recuperación de servicios, adquisición de nueva tecnología, asesoramiento de seguridad, costo de los servicios

de telecomunicaciones, etc. Con estos valores se considerará un escenario muy conservador para que la propuesta no llegue a ser por demás optimista.

La Escuela Politécnica Nacional anualmente maneja un presupuesto aproximado de 40 millones de dólares anuales, de los cuales unos 15 millones de dólares se destinan al pago de sueldos y salarios.

Si se considera que el 40% de tiempo se destina al uso de TI, en una jornada diaria de 8 horas el 40 % equivale a 200 minutos. Si de las 3 horas 20 minutos de tiempo se logra mejorar la productividad en un 2 % de aquellas actividades no productivas tomando en cuenta el estudio de Kelly Services entonces se podrá cuantificar el siguiente valor.

Si de los 200 minutos consideramos el 2% de tiempo quiere decir que 4 minutos llegarán a ser productivos, si del presupuesto considerado de 15000000 por 160 horas, por los 4 minutos de costo de oportunidad se obtendría un valor de 375000 dólares anuales.

El presupuesto de la EPN obtiene ingresos por concepto de proyectos interinstitucionales por un valor de 4 millones de dólares. Si la imagen de la institución o el prestigio que proyecta la institución hacia afuera se ve afectada en un 1%, la EPN dejaría de percibir un valor de 40000 dólares anuales.

Estadísticamente se mostró que el 40 % del tráfico de una red organizacional no es destinado a actividades productivas, esto quiere decir que los recursos de la institución están siendo mal utilizados, por esto si el presupuesto anual que se requiere para el pago del proveedor de servicios de Internet es de 163258.32 dólares anuales y si se considera un aprovechamiento del servicio de Internet en un 2 % el costo de oportunidad anual sería: 3265 dólares.

En resumen, véase la tabla 3.6 que presenta un listado de beneficios cuantificados y totalizados de forma anual:

Factor de mejora	Beneficio anual estimado
Productividad de las TI	375000
Proyectos externos	40000
Conexión Internet	3265
TOTAL	**418265**

Tabla 3.8: Resumen de beneficios

Autor: Ing. Marco Santórum G.

Luego de cuantificar los beneficios, se puede determinar el beneficio anual estimado que es de **418265** dólares.

3.4.7 PROYECCIÓN DE BENEFICIOS DURANTE LA VIDA ÚTIL DEL PROYECTO

En base a los cálculos se esperarían beneficios de acuerdo a lo indicado en la tabla 3.7. Estos beneficios se estiman a lo largo de los 4 años de duración del proyecto.

Para esto siendo prudentes se considera una obtención progresiva de los beneficios esperados con una variación del 25% anual. Véase la tabla 3.8.

Año	Beneficios Esperados	Porcentaje alcanzado	Beneficios Reales
0	0	0%	0
1	418265	25%	104566,25
2	418265	50%	209132,5
3	418265	75%	313698,75
4	418265	100%	418265
		BENEFICIO TOTAL	1045662,5

Tabla 3.9: Beneficios estimados del proyecto a lo largo de su vida útil

Autor: Ing. Marco Santórum G.

3.4.8 CALCULO DE VARIABLES FINANCIERAS (VAN, TIR, PRI).

A continuación se presenta una proyección que permita visualizar de manera gráfica la relación del costo-beneficio a lo largo de la vida útil del proyecto. Véase el esquema costo beneficio en la *figura 3.8.*

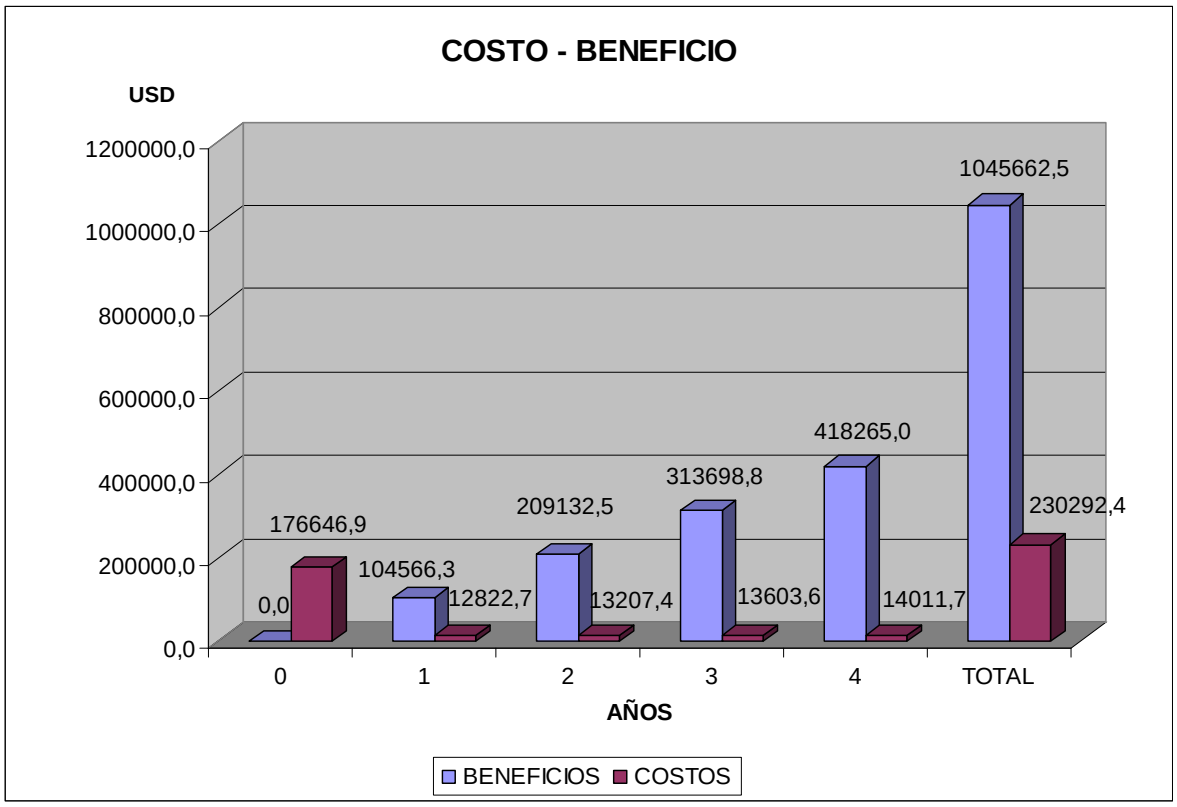

Figura 3.8: Relación Costos vs. Beneficios del Proyecto

Autor: Ing. Marco Santórum G.

El flujo de caja y la sumatoria correspondiente permite efectuar los cálculos de los indicadores financieros que permitirán concluir respecto a la factibilidad financiera del proyecto de políticas de seguridad de la información para la EPN:

Año	Costos	Beneficios	Flujo Neto de Caja (FNC)	Sumatoria FNC (SFNC)
0	208000	0	-208000	-208000
1	104566,3	20800	83766,25	-124233,75
2	209132,5	31200	177932,5	53698,75
3	313698,8	41600	272098,75	325797,5
4	418265	52000	366265	692062,5

Tabla 3.10: Flujo de caja del proyecto

Autor: Ing. Marco Santórum G.

El flujo neto de caja de cada período anual presentado en la tabla 3.10 permite realizar el cálculo de las variables financieras como el VAN, TIR usando la función VNA y TIR de Microsoft Excel con una tasa del 10.75%.[8]

VALOR ACTUAL NETO	$ 456.464,80
TASA INTERNA DE RETORNO	71%

Tabla 3.11: VAN – TIR

Autor: Ing. Marco Santórum G.

El costo ponderado del capital en el Ecuador es de 15,30%[9]. Este índice permite hacer una comparación con la tasa interna de retorno.

[8] Tasa BCE Febrero 2006: 10.50 %

[9] Fuente: ECON. CARLOS ARTIEDA C., MBA

El período de recuperación de la inversión de 1.7 años se calcula de la siguiente manera:

PRI = t1 + | SFNC1 | * (t2 –t1) / (| SFNC1 | + | SFNC2 |)

Donde t1 y t2 corresponden a los años en los que se produce el cambio de signo de la columna SFNC de la *tabla 3.8.*

PRI = 1 + (124233,75) * (2 – 1) / (124233,75+ 53698,75)
PRI = 1 + 124233,75/177932,5
PRI = 1 + 0.698
PRI = 1.70 años

La *figura 3.9* presenta de manera gráfica los resultados del periodo de recuperación de la inversión realizada:

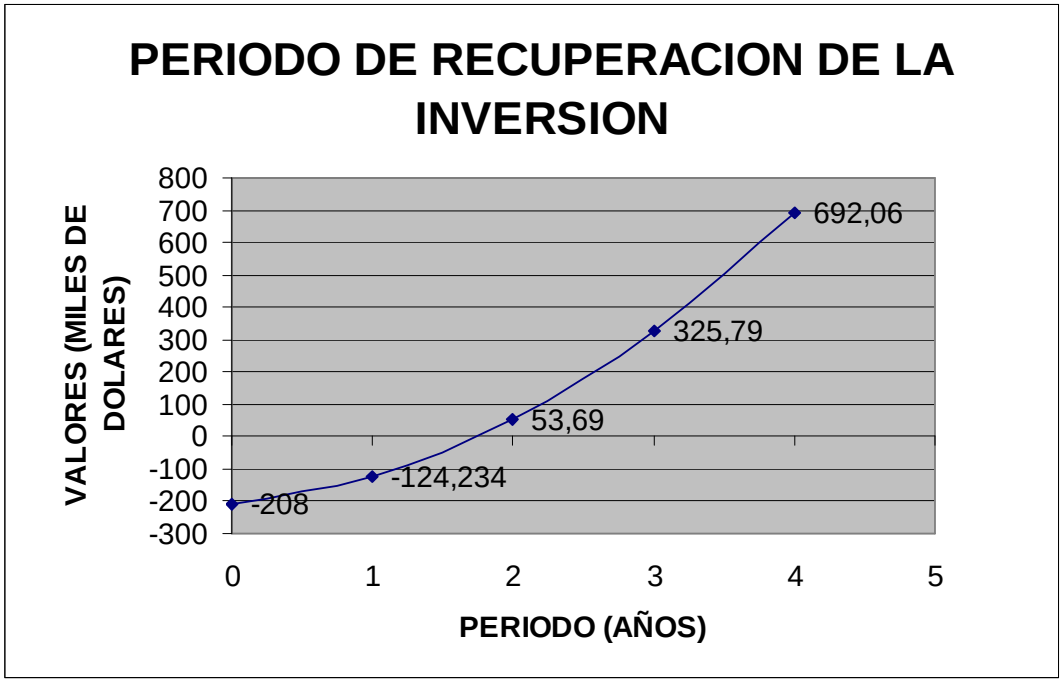

Figura 3.9: Gráfico del período de recuperación de la inversión

Autor: Ing. Marco Santórum G.

3.4.9 RESULTADOS DE LA FACTIBILIDAD ECONÓMICA

VALOR ACTUAL NETO (VAN)

El VAN se concibe como la ganancia obtenida en dólares a valor actual. El VAN es la cantidad de dinero que ganamos en términos netos.

Permite medir la riqueza que aporta el proyecto medida en dólares en el momento inicial.

La regla de decisión es la siguiente:

- Aceptar los proyectos con VAN>0 o rechazar los proyectos con VAN<0
- Es indiferente aceptar o rechazar los proyectos con VAN=0
- Entre dos proyectos alternativos, se debe seleccionar el que tenga mayor VAN.

El **Valor Actual Neto** resultante es de $ 456.464,80 dólares.

Si se usa la regla planteada el Proyecto garantiza la recuperación de la inversión en términos de dinero puesto que el valor VAN es mayor a cero y a más de esto permite recuperar la inversión y evitar gastos en los que se incurriría si no se ejecuta el proyecto.

De este valor se concluye que el proyecto es altamente recomendable y que de no hacerlo, se dejaría de percibir los beneficios planteados.

TASA INTERNA DE RETORNO (TIR)

La tasa interna de retorno puede definirse como el % de ganancia que obtienen los inversionistas por cada dólar invertido en el negocio o que desea poner como

inversión, por ejemplo si deseo invertir 1,000 dólares y la TIR resultante es 71%, entonces esto indica que cada dólar invertido ganará 71 centavos.

Mide la rentabilidad en términos porcentuales.

La regla de decisión es la siguiente:

- Aceptar los proyectos con TIR > r, siendo r la tasa de corte previamente definida.

La **Tasa Interna de Retorno** es del 71 % que es mayor a la tasa activa del BCE 10,75 %.

De este valor se concluye que el proyecto es altamente recomendable.

PERIODO DE RECUPERACION DE LA INVERSION PRI

Es el número de períodos en que un flujo de caja recupera el desembolso inicial o inversión hecha, por ejemplo si se invierte 1,000 y al cabo de un año se tiene 1,000, entonces se puede decir que se ha recuperado la inversión en un año, por tanto el PR sería igual a 1 año.

Por lo tanto permite medir la rentabilidad del proyecto en términos de tiempo.

La regla de decisión es la siguiente:

Aceptar los proyectos con PRI < p, siendo p el tiempo de vida del proyecto previamente definido.

El **Periodo de Recuperción de la inversión** es de 1.70 años, es decir, que casi al cumplir los dos años de vigencia del proyecto ya se habrá recuperado la inversión inicial.

CONCLUSIÓN

Los indicadores demuestran que el proyecto es altamente beneficioso pese a haber planteado un escenario muy prudente y sin ser optimistas.

3.5 ASPECTOS TÉCNICOS

Para evaluar la factibilidad del proyecto tomando en cuenta los aspectos técnicos a continuación se describe el proceso de adquisición de los equipos que permitirán gestionar la seguridad de la información de la institución.

Para este fin se nombró un comité de adquisición de los equipos de seguridad periférica.

Este comité debe seguir el siguiente proceso.

1. Diseño de un esquema de seguridad para cumplir con los requisitos de seguridad.
2. Determinación de las especificaciones técnicas de los equipos ha adquirir.
3. Determinación del presupuesto referencial para el proyecto.
4. Inicio del proceso de adquisición.

3.5.1 ESQUEMA DE SEGURIDAD BÁSICO INICIAL

El siguiente esquema de seguridad fue propuesto inicialmente para la adquisición de los equipos necesarios para el proyecto. Véase la figura 3.10.

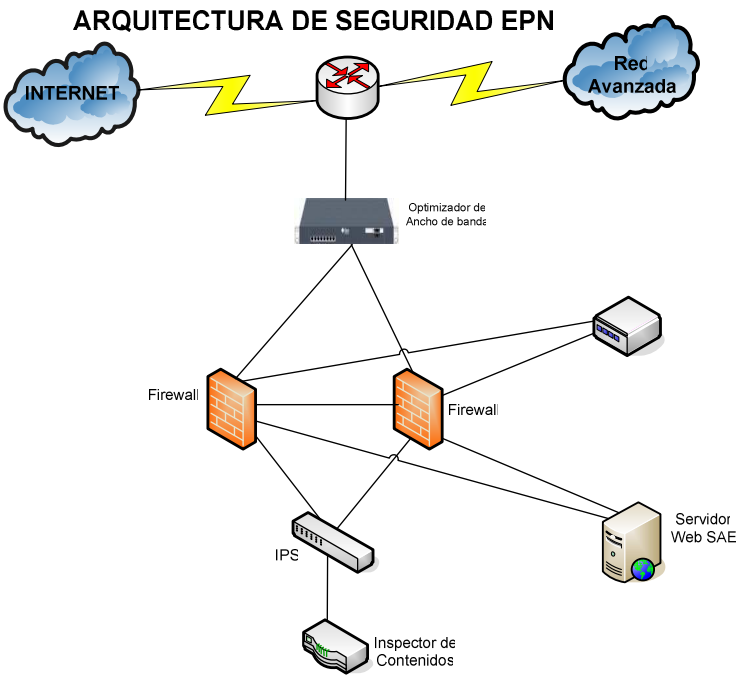

Figura 3.10: Arquitectura de seguridad de la EPN

Autores: Comité de adquisición

Actualmente el esquema de conexión de los dispositivos de seguridad a cambiado y será sometido a variación sin notificación de dichos cambios.

3.5.2 DEFINICION DE LAS ESPECIFICACIONES MÍNIMAS DE LOS EQUPOS DE SEGURIDAD

1. FIREWALL

- Firewalls
- Tipo appliance
- Certificación ICSA

- Capacidad de procesamiento de al menos 600Mbps y de al menos 300 Mbps de tráfico VPN
- Memoria 2048 MB
- Interfaces de Red 10/100/1000 y 1 interface 10/100 Mbps
- Alta disponibilidad en modo active/active con balanceo de carga entre los dos firewalls
- Alta disponibilidad active/active y active/standby
- Interface para operación Hot-Standby, fail-over
- 200000 conexiones simultáneas

2. IPS

- Performance 600Mbps
- Tipo appliance
- Sesiones Simultáneas 200000
- Interfaces de Red 10/100/1000 y 1 interface 10/100 Mbps
- 5000 nuevas conexiones TCP por segundo
- Capacidad de interoperar automáticamente con el firewall detallado en el item anterior, el inspector de contenido, servicios antivirus y el hardware de red de la EPN para realizar acciones proactivas sobre ataques detectados.
- Interfaz de línea de comando(consola)
- Administración centralizada, gráfica, remota y segura, desde la consola y el servidor de administración
- Administración basada en GUI integrada
-

3. INSPECTOR DE CONTENIDOS

- Hardware de tipo appliance
- Capacidad de integración con Firewalls que tengan certificación ICSA

- Interfaces 10/100/1000
- Capacidad de procesamiento de al menos 400 Mbps
- Operación en tiempo real
- Administración centralizada, gráfica, remota y segura, desde la consola y el servidor de administración
- Envío de alarmas por medio de snmp, syslog, consola
- Monitoreable (SNMP de preferencia SNMPv3 , MIB de preferncia MIB II)
- Reportes detallados y gerenciales

4. EQUIPO PARA AUTENTICAR USUARIOS

- Solución en Hardware y Software para Administrar y controlar accesos para mínimo 12000 usuarios
- Garantizar transacciones seguras
- Interfaces de red 10/100/1000
- Capacidad de integración con Firewalls que tengan certificación ICSA
- Soporte conexiones Inalámbricas, DialUP, LAN, VoIP y VPNs
- Integración con los equipos CISCO adquiridos para la Polired
- Monitoreo del comportamiento de los usuarios en la red
- Reportes del comportamiento de los usuarios en la red
- Protocolos 802.1X y EAP
- Manejo de ACLs y VLANs

5. OPTIMIZADOR DE ANCHO DE BANDA

- Throughput mínimo de 45 Mbps con capacidad de crecimiento a 100 Mbps full duplex
- Capacidad de integración con Firewalls que tengan certificación ICSA
- Número de clases soportadas: 1024
- Número de políticas soportadas: 1024

- Número de Hosts IP: 20000
- Número de Flujos IP: 150000
- 2 Interfaces de Red 10/100/1000 y 1 interface de red 10/100
- Soporte interfaz de hardware para failover con balanceo de carga
- Interface de Adminitración 10/100
- Puerto de Consola Serial/RJ45

6. CARACTERÍSTICAS MÍNIMAS DEL SOFTWARE DE ANTIVIRUS PARA LA EPN

- El antivirus debe tener certificación ICSA o haber pasado las pruebas de virus boletín, por lo menos en los siguientes sistemas operativos: Windows XP, Windows 2000 profesional, Windows 2000 server, Windows 2003 server.
- Cantidad de PCs: 1000
- Capacidad de integración con Firewalls que tengan certificación ICSA
- El antivirus deberá trabajar en las siguientes plataformas: Windows 98, Windows XP, Windows 2000 profesional, Windows 2000 server, Windows 2003 server, Windows Vista, Linux, Unix,
- El antivirus debe ser una Suite Integral, que cuente con una sola consola de administración central instalable sobre plataforma Windows Server 2000 o 2003 y/o Linux Red Hat Enterprise 4, que permita el control y monitoreo mediante números IP de las computadoras personales conectadas a la red.

3.5.3 PRESUPUESTO REFERENCIAL PARA LA ADQUISICION DE LOS EQUPOS DE SEGURIDAD

La Escuela Politécnica Nacional maneja un presupuesto de 40 millones anuales del cual se ha destinado un monto de 150000 dólares para la adquisición de los equipos mencionados anteriormente.

Cabe señalar que para la adquisición de estos equipos se han considerado los requerimientos planteados por la Ley de contratación pública del Ecuador.

Este presupuesto por lo tanto considera la adquisición de:

EQUIPOS	CANTIDAD
FIREWALL	DOS
ANTIVIRUS	UNO
IPS	DOS
OPTIMIZADOR DE ANCHO DE BANDA	DOS
INSPECTOR DE CONTENIDOS	UNO
AUTENTICADOR DE USUARIOS	UNO

Tabla 3.12: EQUIPOS DE SEGURIDAD

Autor: Ing. Marco Santórum G.

3.5.4 PROCESO DE ADQUISICIÓN

Una vez realizada la evaluación de los oferentes de los equipos se procedió a adquirir los equipos que entre otras cosas debieron cumplir con lo siguiente.

ESPECIFICACIONES GENERALES

Los equipos antes mencionados deben cumplir:

- Las versiones del sistema operativo de todos los equipos deben ser las últimas versiones liberadas por el fabricante a la fecha de compra.
- La solución de seguridad ofertada debe cumplir con las características mínimas descritas con anterioridad, y se debe garantizar compatibilidad, integración y operación entre los equipos ofertados con los equipos de comunicación de la Institución (switch cisco catalyst 4507, switch cisco 3560, router cisco 3845, router cisco 2611).

- La información confidencial (bases de datos de signatures, políticas de seguridad, eventos, logs, etc.) debe poder almacenarse en el servidor de administración de seguridades
- Todos los equipos deben ser capaces de enviar registros de eventos y alarmas al servidor de administración de seguridades o a la consola
- La comunicación entre los equipos, el servidor de administración de seguridad y la consola debe ser cifrada y autenticada.
- Los productos ofertados deben implementar syslog, agentes SNMP con las respectivas MIBs
- El sistema de seguridad debe minimizar la participación de los técnicos en el sistema, debe tomar acciones proactivas frente a ataques detectados. y además cumplir con por lo menos tres de las siguientes acciones:
- Reseteo de la conexión
- Deshabilitar puerto en el switch o router
- Reconfigurar ACLs y aplicar en el router, switch y/o firewall
- Bloqueo del Tráfico anómalo
- Poner automáticamente en una VLAN de cuarentena a los equipos en problema
- La propuesta deberá considerar actualización de software (security patches), IOS, Bdd de firmas de intrusiones y ataques, Bdd de firmas de virus, y demás Bdd que los equipos requieran para su normal desempeño por al menos un año.

CAPACITACIÓN

La capacitación debe ser realizada con equipos del oferente (Los equipos pueden no ser de la misma serie que los ofertados, pero si deben tener las funcionalidades solicitadas) y dictado por un instructor especializado en los equipos ofertados, en las

instalaciones del oferente, con un mínimo de 20 horas de capacitación por cada uno de los 5 requerimientos enumerados anteriormente, mínimo para tres personas.

INSTALACIÓN Y FUNCIONAMIENTO DE EQUIPOS

El oferente debe entregar los equipos en perfecto estado de funcionamiento, y configurarlos conjuntamente con el personal técnico del área de Redes de la Unidad de Gestión de la Información (UGI), y según los requerimientos de la Institución.

GARANTÍAS TÉCNICAS

La empresa oferente presentará por lo menos 1 año de garantía en las partes y piezas de los equipos, el soporte para los equipos debe ser 8X5.

La empresa oferente debe garantizar por un año las actualizaciones de: IOS, BDD y software que se requiera sin costo adicional, para que los diferentes equipos de seguridad puedan enfrentar los últimos ataques.

Los equipos deben ser nuevos, con certificación del fabricante de que no es reparado o reconstruido.

CAPITULO 4

CONCLUSIONES Y RECOMENDACIONES

Una vez concluida la etapa de creación de las Políticas de Seguridad de la Información, el presente documento se constituye en el entregable del proyecto que será entregado al Jefe de la Unidad de Gestión de la Información.

Esta propuesta deberá ser sometida a la etapa de revisión de ciclo de vida para que una vez revisada por parte del Comité de seguridad de la Información, el Jefe de la Unidad de Gestión de la Información oficialice la Propuesta ante Consejo Politécnico quienes serán los encargados de aprobar la propuesta para continuar con la Etapa de difusión.

4.1 CONCLUSIONES

- El primer paso a la hora de la creación de políticas de seguridad de la información implica identificar la necesidad de crear las mismas, por ejemplo debido a requerimientos legales, regulaciones técnicas, contractuales u operacionales de la Escuela Politécnica Nacional.

- La Escuela Politécnica Nacional es una institución pública del estado Ecuatoriano, la misma que debe cumplir con la legislación ecuatoriana vigente y los tratados internacionales a los cuales el Ecuador se ha suscrito. Esta base legal exige a las instituciones ecuatorianas a respetar e implementar las medidas necesarias para la vigencia de dichos tratados y leyes.

- Las Políticas de Seguridad de la Información se constituirán en los documentos oficiales de la institución a los cuales se deberá referirse

cualquier usuario de la Polired ante cualquier inquietud, controversia o ausencia de normatividad frente a procedimientos relacionados con la información.

- Las políticas requieren la participación de todos los estudiantes, profesores, empleados administrativos, autoridades y demás miembros de la comunidad politécnica, quienes deberán ser concienciados de la importancia y necesidad de cumplir con las mismas. Ninguna política, procedimiento o norma garantizará los principios de seguridad de la información si los usuarios directamente relacionados no están conscientes de la razón de ser de estas, caso contrario se constituirán en una medida represiva, objetivo, reto, etc., que un usuario buscará romper queriendo demostrar su inconformidad o capacidad de superarlo o violarlo.

- Las Políticas de Seguridad de la Información de la Escuela Politécnica Nacional presentan la posición oficial de la institución y se han elaborado con el fin de que tengan una aplicación a largo plazo y para salvaguardar la integridad de todos los componentes informáticos.

- El Instituto SANS provee “Templates” o “Plantillas” que han sido construidas en base a mejores prácticas organizacionales y por profesionales con amplia experiencia en el campo, sin embargo estas han sido planteadas con una orientación comercial por lo que no representan la posición de una institución pública que no tiene fines de lucro y menos aún con fines educativos. Por lo tanto es necesario realizar el análisis correspondiente con el fin de redactar políticas adecuadas a la realidad de la Escuela Politécnica Nacional.

- El Proyecto de definición e implantación de las Políticas de Seguridad de la Información de la Escuela Politécnica es sustentable desde el punto de vista organizacional, rentable desde el punto de vista financiero, es necesario y

obligatorio desde el punto de vista legal y factible desde el punto de vista operacional y técnico.

- Los beneficios identificados en este proyecto de tesis se sustentan en el concepto de costo de oportunidad, concepto que permite cuantificar aquellos beneficios no perceptibles o beneficios que no se generarían en el caso que el proyecto no se realice.

- Un marco de referencia permite seguir aquellas mejores prácticas de las organizaciones a nivel mundial de manera que garanticen el cumplimiento exitoso de los objetivos. Por lo tanto se constituyen en una herramienta sumamente útil a la hora de generar una propuesta sin embargo como en el presente caso requieren de una adaptación a la realidad del caso de estudio que se aplica.

- El ciclo de vida del proyecto como su nombre lo dice se constituye en el camino a seguir del proyecto y se añade además las iteraciones que se deberán tomar en cuenta para que el proyecto constantemente sea retroalimentado para conseguir que durante las iteraciones se vaya corrigiendo, puliendo y fortaleciendo.

4.2 RECOMENDACIONES

- A la hora de realizar una propuesta de gestión se puede tomar en cuenta muchos marcos de referencia utilizados en el mercado, no se debe limitarse a aquellos bien conocidos o estudiados durante la maestría puesto que a pesar de ser sobradamente excelentes quizá se podría hallar otros que con la misma base conceptual se aproximen mas a la realidad requerida.

- Se requiere asignar lo más pronto posible el encargado del proyecto de manera formal considerando dentro de su carga de trabajo la realización del proyecto para de esta manera dar inicio a las siguientes etapas del proyecto.

- Ninguna propuesta por mas bien fundamentada o realizada que no cuente con el apoyo, aprobación y puesta en marcha por parte de las autoridades funcionará por lo tanto se recomienda concretar el objetivo macro del proyecto que es cumplir con todas las etapas del proyecto.

- La propuesta generada debe servir como una base sobre la cual distintos profesionales agrupados en un comité de seguridad de la información realicen las observaciones pertinentes para que estas políticas puedan tener éxito y sean implementadas.

- Sería conveniente estudiar una materia que estudien aspectos legales, de manera que permitan conocer la legislación vigente y necesaria para la gestión de tecnologías de la información.

BIBLIOGRAFIA

[1] THE SANS SECURITY POLICY PROJECT, Introduction to the SANS Security Policy Project. http://www.sans.org/resources/policies/, año 2008.

[2] PATRICK D. HOWARD, Guía para elaboración de políticas de seguridad. http:/www.unal.edu.co/seguridad/documentos/guia_para_elaborar_politicas_v1_0.pdf

[3] SECRETARIA EJECUTIVA NACIONAL CNNA, Plan Nacional para combatir la trata, explotación sexual, laboral y otros medios de explotación de personas, en particular mujeres, niños, niñas y adolescentes. http://www.cnna.gov.ec/archivos/plan_nacional_trata.pdf, Diciembre 2006.

[4] NORMATIVA LEGAL ECUATORIANA, http://www.dlh.lahora.com.ec/paginas/judicial/PAGINAS/Pjudicial2.7.htm

[5] FITES, PHILIP AND MARTIN P.J. KRATZ. Information Systems Security: A Practitioner's Reference, London: International Thomson Computer Press, 1996.

[6] SEBASTIAN SEELIGMANN, Política de Información Universitaria. http://www.sans.org/resources/policies/, Año 1998.

[7] HUTT, ARTHUR E., SEYMOUR BOSWORTH, AND DOUGLAS B. HOYT. Computer Security Handbook, 3rd, John Wiley & Sons, New York, 1995.

[8] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, October 1995.

[9] PELTIER, THOMAS R., Information Security Policies and Procedures: A Practitioner's Reference, Auerbach Publications, New York, 1999.

ANEXOS

[1] COMITE DE SEGURIDAD DE LA INFORMACIÓN, Diagrama de Arquitectura de Seguridad de la Escuela Politécnica Nacional

[2] COMITE DE SEGURIDAD DE LA INFORMACIÓN, Bases proyecto de Seguridad Perimetral EPN.

[3] COMITE DE SEGURIDAD DE LA INFORMACIÓN, Características mínimas del software de antivirus para la EPN

[4] SHELDON BORKIN, The HIPAA Final Security Standards and ISO/IEC 17799

ANEXO 4: GLOSARIO

Cifrado

El cifrado es el proceso de convertir el texto plano en un galimatías ilegible, denominado texto cifrado o criptograma. Por lo general, la aplicación concreta del algoritmo de cifrado (también llamado cifra) se basa en la existencia de una clave: información secreta que adapta el algoritmo de cifrado para cada uso distinto.

SPAM

Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera al receptor. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

Malware

Malware malicious software, es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano hasta un spyware.

Virus

Un virus informático es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Aunque popularmente se incluye al "malware" dentro de los virus, en el sentido estricto de esta ciencia los virus son programas que se replican y ejecutan por sí mismos.

Antivirus

Los antivirus son programas cuya función es detectar y eliminar Virus informáticos y otros programas maliciosos (a veces denominados malware).

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos (también conocidos como firmas o vacunas) de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como Heurística) o la verificación contra virus en redes de computadoras.

Información sensible

Información sensible es el nombre que recibe la información personal privada de un individuo, por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos. Aunque lo más común es usar este término para designar datos privados relacionados con Internet o la informática, sobre todo contraseñas, tanto de correo electrónico, conexión a Internet, IP privada, sesiones del PC, etc. Los crackers utilizan la llamada Ingeniería social (ciencias políticas) para intentar hacerse con este tipo de información.

Hash

En informática, Hash se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un **hash** es el resultado de dicha función o algoritmo.

LDAP

LDAP (Lightweight Directory Access Protocol) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

DMZ

Una DMZ (del inglés Demilitarized zone) o Zona DesMilitarizada. En seguridad informática, una zona desmilitarizada (DMZ) o red perimetral es una red local (una subred) que se ubica entre la red interna de una institución y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

ACL

Una Lista de Control de Acceso o ACL (del inglés, Access Control List) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Internet

Internet es un método de interconexión descentralizada de redes de computadoras implementado en un conjunto de protocolos denominado TCP/IP y garantiza que redes físicas heterogéneas funcionen como una red lógica única, de alcance mundial.

Intranet

Una Intranet es una red de computadoras dentro de una red de área local (LAN) privada, empresarial o educativa que proporciona herramientas de Internet.

Extranet

Una extranet (extended intranet) es una red privada virtual que utiliza protocolos de Internet, protocolos de comunicación y probablemente infraestructura pública de comunicación para compartir de forma segura parte de la información u operación propia de una organización con proveedores, compradores, socios, usuarios o cualquier otro negocio u organización.

DoS

En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de ordenadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Firewall

Un cortafuegos, es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

Autenticación

Autenticación es el acto de establecimiento o confirmación de algo (o alguien) como auténtico, es decir que reclama hecho por, o sobre la cosa son verdadero. La autenticación de un objeto puede significar (pensar) la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad. La autenticación depende de uno o varios factores de autenticación.

Módem

Un módem es un equipo que sirve para modular y demodular (en amplitud, frecuencia, fase u otro sistema) una señal llamada portadora mediante otra señal de entrada llamada moduladora.

ADSL

ADSL son las siglas de Asymmetric Digital Subscriber Line ("Línea de Abonado Digital Asimétrica"). ADSL es un tipo de línea DSL. Consiste en una línea digital de alta velocidad, apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando el alcance no supere los 5,5 km. medidos desde la Central Telefónica.

Spyware

Los programas espías o spywares son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software.

Dirección MAC

En redes de computadoras la dirección MAC (Media Access Control address o dirección de control de acceso al medio) es un identificador hexadecimal de 48 bits que corresponde de forma única a una tarjeta o interfaz de red.

Ancho de Banda

Es común denominar ancho de banda digital a la cantidad de datos que se pueden transmitir en una unidad de tiempo. Por ejemplo, una línea ADSL de 256 kbps puede, teóricamente, enviar 256000 bits (no bytes) por segundo. Esto es en realidad la tasa de transferencia máxima permitida por el sistema, que depende del ancho de banda analógico, de la potencia de la señal, de la potencia de ruido y de la codificación de canal.

Dial-in

Conexión a Internet que se establece a través de un módem y una línea telefónica. A cada usuario se le asigna un número IP dinámico, válido **sólo** durante la comunicación

Dial-up

Una conexión por línea conmutada es una forma barata de acceso a Internet en la que el usuario utiliza un módem para llamar a través de la Red Telefónica Conmutada (RTC) al nodo del ISP, un servidor de acceso (por ejemplo PPP) y el protocolo TCP/IP para establecer un enlace módem-a-módem, que permite entonces que se enrute a Internet

VPN

La Red Privada Virtual (RPV), en inglés Virtual Private Network (VPN), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.