ACCIONES Y POLÍTICAS PARA LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC).

UNIVERISAD PEDAGÓGICA NACIONAL DEL ESTADO DE CHIHUAHUA

DEPARTAMENTO DE SISTEMAS

ACCIONES Y POLÍTICAS PARA LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC), DE LA UNIVERISAD PEDAGÓGICA NACIONAL DEL ESTADO DE CHIHUAHUA.

INTRODUCCIÓN

En base La Estrategia Digital Nacional (EDN) que se despliega en el marco de la Cuarta Transformación del Gobierno, el presente documento tiene por objetivo definir acciones y políticas para las Tecnologías de la Información y Comunicación de la Universidad Pedagógica Nacional del Estado de Chihuahua.

Con el fin de lograr un desarrollo de servicios informáticos y de comunicación con alto grado de funcionalidad, confidencialidad, eficiencia, integridad y disponibilidad de la información generada y utilizada por el personal y alumnos de la UPNECH, se requiere implementar acciones y procedimientos.

CAMPO DE APLICACIÓN

La aplicación de estas acciones y políticas va dirigida a todas las Unidades y Rectoria pertenecientes a la "UPNECH" y se aplicaran a todos los procesos y actividades referentes a Tecnologías de Información y comunicación.

PRINCIPIOS BASADOS EN LA ESTRATEGIA DIGITAL NACIONAL 2021-2024

Los principios de la EDN se refieren a un conjunto de conceptos que guían y respaldan las diferentes acciones y decisiones de la política tecnológica del Gobierno de México en todas las circunstancias. Se aplican a todas las iniciativas de proyectos y uso de TIC en el gobierno y a todas las relaciones con las partes involucradas que apoyan una cultura de colaboración, intercambio y optimización de recursos disponibles.

Basada en los principios de la EDN, la UPNECH da prioridad en buscar una adecuada administración tecnológica, la mejora de los servicios digitales y la optimización de los procesos, enmarcando dicha prioridad en los 4 siguientes principios descritos en el Diario Oficial de la Federación y los cuales se describen a continuación:

1. Principio de Austeridad.

Principio de bien común, relativo a lograr servicios de alta calidad con el máximo aprovechamiento de recursos y disminución de gasto.

2. Principio de Combate a la corrupción

Acabar con prácticas injustas, desleales, leoninas y perversas que benefician a intereses particulares perjudicando al Estado o a sus integrantes.

3. Principio de eficiencia en los procesos Digitales

Implica la simplificación operativa y atención focalizada de los procedimientos.

4. Principio de Seguridad de la Información

Concepto que hace referencia a la estabilidad, protección y certidumbre de la información generada o resguardada en sistemas o plataformas digitales.

Al igual que la EDN, la UPNECH busca promover e impulsar que los Estudiantes, Administrativos y Docentes usen y se beneficien del acceso a las tecnologías de la información y comunicación; así como de los servicios de Internet y su potencial.

Con base en lo anterior se presentan las siguientes acciones y políticas.

ACCIONES Y POLÍTICAS PARA LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC) EN LA UPNECH.

Las políticas y acciones aquí expuestas son aplicables a todo el personal que labore y que se encuentre dentro de las instalaciones de la UPNECH

1. EQUIPOS DE CÓMPUTO Y SISTEMAS DE INFORMACIÓN.

Los equipos de cómputo y sistemas de información son fundamentales para cualquier institución y deben ser protegidos; estos incluyen todos los datos tanto del usuario como de la institución.

La seguridad informática consiste en garantizar que los bienes y los servicios informáticos de una organización se usen únicamente para los propósitos para los que fueron creados o adquiridos y dentro del marco previsto.

Generalmente la seguridad informática se resume en cinco objetivos principales:

- Integridad: Garantizar que los datos sean los que se supone que son, es decir, que sean los correctos o no estén corruptos.
- Confidencialidad: Asegurar que solo los individuos autorizados tengan acceso a los recursos que se intercambian.
- Disponibilidad: Garantizar el correcto funcionamiento de los sistemas de información, así como de las tecnologías de comunicación.
- Evitar el rechazo: garantizar la no negación de una operación o acceso ya concedidos.
- Autenticación: asegurar que los individuos que pretenden tener acceso a los recursos, sean quienes deben ser.

Además de los objetivos anteriores, la seguridad informática también planea e implementa todas las Políticas de Uso de Equipo de Cómputo y Servicios Tecnológicos de la UPNECH, medidas necesarias para salvaguardar la información de vital importancia, así como evitar los accesos no autorizados a los equipos personales y principalmente a los servidores. Dentro de las medidas definidas se encuentran las siguientes:

- Preparar procedimientos acordes a las necesidades de las áreas principales y al centro de datos.
- Preparar y dar a conocer las políticas de seguridad.
- Concientizar, tanto a los administradores como a los usuarios, de la importancia del tema. Mejorar en forma continua la seguridad.
- Ofrecer asesoría, a manera de sugerencia.
- Registrar y dar seguimiento a los incidentes de seguridad, entre otros.

2. USO DE LOS BIENES INFORMATICOS

1.1 La UPNECH cuenta con 2 Centros de Datos (espacios donde se concentran los recursos necesarios para el acceso y procesamiento de la información) para atender las necesidades de las Unidades y Rectoria (ubicados en el área de Sistemas en Rectoria y en un servidor privado virtual, con el fin de asegurar y optimizar el aprovechamiento eficiente de los servidores de cómputo, equipos de comunicaciones y servicios compartidos.

1.2 En el caso de los usuarios, para fomentar el ahorro de energía, los equipos no deberán mantenerse encendidos una vez terminado el horario laboral (impresoras, computadoras, monitores, bocinas, etc.).

1.3 Toda la información generada, guardada y registrada en el equipo de cómputo es propiedad de la UPNECH y es responsabilidad del resguardante el uso que se le dé, así como de su conservación.

Respecto al software:

1.4 Se prohíbe la instalación de Software, Programas y/o Aplicaciones que no cuenten con licencia o autorización otorgada por parte del personal de Sistemas de la UPNECH.

1.5 Se prohíbe la instalación de Software, Programas y/o Aplicaciones Shareware, Freeware y Trial, que comprometan el uso eficiente de la red y los equipos de cómputo o que resulten ajenos a los fines relacionados con el desempeño de sus actividades.

1.6 Es responsabilidad del resguardante, el buen uso del software instalado en su equipo.

Respecto al Hardware e información

1.7 El personal que solicite o tenga a resguardo una computadora de escritorio, estación de trabajo, portátil, servidor, impresora, etc., se compromete a subsanar el daño ocasionado por robo, pérdida, maltrato o mal manejo del mismo o alguno de sus componentes.

1.8 Cada Área de la UPNECH a través del jefe de departamento y con la debida autorización de la respectiva Dirección Administrativa, podrá solicitar reubicar el equipo según lo considere conveniente,

para su mejor uso y aprovechamiento con la debida justificación, pero solo personal de Sistemas tendrá la facultad de administrar, controlar, auditar, desarmar, y reubicar dicho equipo.

1.9 Se prohíbe almacenar cualquier tipo de información ajena al trabajo (por ejemplo: archivos de música, imágenes, videos, etc.). En caso de que el personal autorizado localice este tipo de archivos tendrá la facultad de eliminarlos sin la necesidad de consultar al usuario.

Respecto a la impresión

1.10 Las impresoras son de uso común y no personal.

1.11 Se prohíbe la impresión total o parcial de información ajena a las actividades de la UPNECH.

1.12 Para fomentar el ahorro de papel y otros recursos, se imprimirá sólo el documento original, las copias de éste se deberán enviar a través de un archivo digital a los interesados, vía correo electrónico o, depositarlo en el repositorio o medio de almacenamiento en la nube.

1.13 Tratar de utilizar en medida de lo posible hojas de recicle para impresiones que no requieran hojas nuevas (por ejemplo: reportes, memos, hojas de servicio, etc.).

1.14 Solo se tendrá acceso a la impresora asignada a su área de trabajo, en caso de necesitar acceso a alguna otra impresora se hará se realizará la solicitud correspondiente al área de Sistemas.

3. SOPORTE TÉCNICO

2.1 Únicamente el personal de Soporte Técnico está autorizado para abrir, revisar, evaluar o reparar el equipo de cómputo. Por ningún motivo podrá hacerlo personal ajeno.

2.2 El mantenimiento Correctivo y/o Preventivo de Hardware y Software será única y exclusivamente para el equipo propiedad de la UPNECH y realizado por el personal de Soporte Técnico.

2.3 Los equipos que no son propiedad de la UPNECH no recibirán soporte, salvo con la autorización explícita mediante un oficio por parte de la Secretaría Administrativa de la UPNECH, justificando la solicitud.

2.4 El personal de Soporte Técnico tiene la facultad de revisar y evaluar periódicamente el equipo de cómputo en el momento que lo considere necesario y siempre en presencia del usuario.

2.5 Se establecerá un calendario de mantenimiento preventivo a los bienes informáticos de todas las áreas de la Institución, en este sentido se prevé realizar un mínimo de 2 revisiones al año, por el personal de Soporte Técnico.

2.6 El equipo que requiera de mantenimiento correctivo de software o hardware será trasladado al área dedicada a estas actividades, este movimiento se realizará previa evaluación del personal autorizado.

2.7 Solo el personal autorizado para evaluar las fallas del equipo deberá emitir un diagnóstico y tomar la decisión pertinente para la solución del problema.

2.8. En caso de requerirse la compra de hardware o software para la solución de una falla de equipo, el personal de soporte técnico deberá hacer la solicitud al departamento correspondiente previa autorización del jefe de Sistemas.

2.9 Todo hardware que sea ajeno al equipo y que se pretenda incorporar a éste, deberá ser previamente autorizado por parte del personal de Soporte Técnico.

2.10 Todo el equipo de cómputo contará con sello de seguridad para evitar la abertura del mismo, si por alguna circunstancia este sello es violado por personas ajenas al personal de Soporte Técnico, se procederá a levantar un acta para deslindar responsabilidades.

2.11 Solo personal de soporte técnico estará facultado para realizar movimientos de equipos tecnológicos (computadoras, monitores, impresoras, scanner, etc.), esto previa solicitud y autorización por parte de la Secretaría Administrativa de la UPNECH.

4. USO DE LA RED DE CÓMPUTO

3.1 Sólo el personal de Sistemas, está autorizado para cambiar la configuración física y lógica de la red alámbrica e inalámbrica, es decir cables, rosetas, antenas, access point, direcciones IP, configuración de las impresoras compartidas en red, tipo de red, etc. Así como para asistir a los usuarios en problemas de comunicación.

3.2 Todo equipo que lo requiera, deberá conectarse a la roseta de red con “cable de parcheo” certificado.

3.3 El usuario no está autorizado para instalar o desinstalar cables o dispositivos de red. En caso de ser requerido cualquier tipo de dispositivo de comunicaciones (tarjeta de red, Modem, Switch, Ruteador, etc) el personal de Sistemas hará la instalación correspondiente con previa autorización por parte de la Secretaría Administrativa de la UPNECH

3.4 Será responsabilidad total del usuario el uso de la información en su equipo u otros recursos al compartirlos en la red. Todo recurso compartido deberá tener contraseña o determinar que usuarios tendrán acceso, así como el tipo de permisos asignados.

3.5 En caso de requerir un mayor número de máquinas instaladas en un lugar donde sólo existe un nodo de red:

Solamente el personal de Sistemas está autorizado a instalar switches y Access point, previo estudio de factibilidad.

Todas las máquinas deberán quedar conectadas al switch con “cable de parcheo” certificado; en el caso de Access point, con tarjetas de red inalámbricas que cumplan con los estándares internacionales de seguridad.

3.6 Está prohibida la instalación de programas ajenos a la UPNECH que utilicen los recursos de la red a menos que sean autorizados por el personal de Sistemas.

3.7 Está prohibido el acceso a los “Sites” ya que son áreas de equipamiento de redes, en los cuales se encuentra el cableado y el equipo de comunicación.

3.8 Los daños ocasionados al cableado y/o roseta de la red por negligencia del usuario serán directamente responsabilidad del mismo, comprometiéndose a cubrir el costo por la reparación de dichos daños.

3.9 En el caso de los servidores:

El uso de los servidores es estrictamente para labores propias de la UPNECH, por lo cual los usuarios que tengan acceso a ellos no deberán utilizar sus recursos para fines personales (tales como almacenamiento de archivos, ejecución de programas, etc.).

Solamente el Jefe del departamento de Sistemas, por medio de un oficio podrá hacer la petición del uso de los servicios para el personal que labore en su departamento, debiendo indicar los siguientes puntos.

- Servidor que será accesado.
- Nombre del personal autorizado.
- Recurso a accesar y justificación del mismo.
- Privilegios a asignar.

3.10 Los servidores llevan un registro detallado de las operaciones ejecutadas en ellos, por lo cual el usuario será responsable totalmente del buen o mal uso de dichos recursos, así como pérdidas o cambios de información como resultados de errores de operación.

3.11 A cada servidor se le realiza un respaldo los días lunes, el cual es resguardado por un periodo de tres meses de operación, siendo responsabilidad del personal de Sistemas dicho respaldo. En caso de requerir que el respaldo se realice con una frecuencia diferente o se requiera un periodo mayor de almacenamiento, deberá solicitarse por escrito al personal de Sistemas.

3.12 El personal de Sistemas es responsable de la integridad de los datos que los usuarios depositen en los servidores, sin embargo, no será responsable por penalizaciones civiles o legales derivadas de la información resguardada.

3.13 En caso de requerir el respaldo de información específica que no esté contemplada dentro de los servidores, el usuario tendrá la obligación de notificarlo al personal de Sistemas a través de un oficio signado por jefe de departamento o la Secretaría Administrativa de la UPNECH, indicando la periodicidad de dicho respaldo, a fin de que se incluya en el compendio de información a resguardar los servidores asignados a esta función.

5. USUARIOS, CONTRASEÑAS, DATOS Y ACCESO A LA RED

4.1 Las claves de acceso a la red constan de dos partes: una es la cuenta de usuario y la otra es la contraseña, por lo que las cuentas serán personales.

4.2 Todo usuario registrado en la red será responsable de proteger su nombre de usuario, contraseña y datos de cualquier acceso no autorizado.

4.3 Las cuentas de usuario registradas en la red son de carácter estándar, únicamente el personal de Sistemas, tiene los privilegios de modificar la configuración e instalación de aplicaciones adicionales a los equipos de cómputo.

4.4 Las claves de acceso serán habilitadas únicamente por el personal de Sistemas.

4.5 El usuario es responsable de su clave de acceso. Ninguna contraseña debe ser divulgada, escrita, enviada por correo electrónico y compartida por cualquier otra persona ajena al usuario, ya que esto se considera una violación a la seguridad y si es detectado, se suspenderá la cuenta y se enviará un oficio informativo al titular del área a la cual está adscrito el usuario.

4.6 El usuario es responsable por las acciones que se lleven a cabo con su cuenta personal, es decir, las modificaciones a las bases de datos, archivos recibidos o enviados por correo electrónico, uso indebido de los recursos de la red, etc.

4.7 Queda estrictamente prohibido el uso de un nombre de usuario distinto al propio, aun con el consentimiento del usuario original.

4.8 Aquellos usuarios que tengan a su cargo información de carácter “importante” en su equipo de cómputo, tendrán acceso a una unidad de red en la cual se respaldaran dichos archivos en un periodo determinado en conjunto el personal de Sistemas con el usuario en cuestión.

6. ADMINISTRACIÓN DE LA RED

5.1 La seguridad en la red estará a cargo del personal de Sistemas, el cual utilizará diferentes tipos de Hardware o Software para controlar los accesos a Internet y servidores que proporcionen los accesos a la red interna y administrar los recursos.

5.2 Personal de Sistemas no ejerce control sobre el contenido de la información que circula a través de la red, del origen y destino, esta queda bajo la responsabilidad del usuario. No obstante, lo anterior, el personal de Sistemas tiene en funcionamiento permanente herramientas de monitoreo y control que posibilitan analizar y detectar usos indebidos; por lo tanto, se advierte que el contenido de la información que circula por la red, es monitoreada y sujeta a controles y reportes sobre su uso.

5.3 Corre por cuenta o riesgo del usuario cualquier información obtenida por medio del servicio de Internet.

5.4 incurrir en el incumplimiento de los siguientes puntos por primera vez, ameritará amonestación por escrito al usuario de la cuenta con copia al jefe del departamento. En caso de reincidir se procederá a la cancelación de la cuenta y sólo podrá reactivarse con previa autorización del jefe del departamento.

- Transmisión y circulación de materiales con derechos de propiedad intelectual, amenazantes u obscenos, ya sea en forma individual o masiva.
- Acceso a páginas de Internet para obtener información no relacionada con el área de trabajo del usuario. Esto incluye sitios de pornografía, deportes, juegos, música, video, chistes, piratería informática, etc.
- Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricas de redes y sistemas.
- Monopolizar los recursos en perjuicio de los otros usuarios, incluyendo: el envío de mensajes masivos a todos los usuarios de la red, inicio o continuación de cadenas, creación de procesos innecesarios, generar impresiones voluminosas, uso de recursos de impresión no autorizado.
- Exhibición de material pornográfico en cualquier lugar de la Institución utilizando el equipo de cómputo y/o los servicios de comunicación de la institución.

5.5 Cualquier usuario de la UPNECH que modifique la configuración de conectividad de red (IP, Gateway, DNS, etc.) se considerará como una amenaza a la seguridad de la información institucional. El personal de Sistemas suspenderá inmediatamente la cuenta de acceso a la red institucional y enviará un oficio informativo a la Dirección General o Ejecutiva correspondiente.

5.6 El personal de Sistemas atenderá a todos los usuarios que reporten un mal funcionamiento de su equipo de cómputo y de los servicios de red, Internet y correo electrónico, y presentará alternativas de apoyo al usuario.

7. APLICABLES A CORREO ELECTRÓNICO, PLATAFORMA EDUCATIVA Y SISTEMA INTEGRAL UNIVERSITARIO (SIU).

6.1 El usuario es responsable de respetar la Ley Federal de Derechos de Autor, no abusando de los recursos institucionales de cómputo, red, correo electrónico y plataforma educativa para distribuir o copiar de forma ilegal software licenciado o reproducir información sin conocimiento del autor.

6.2 El incumplimiento por parte del usuario del buen uso de su cuenta institucional puede ocasionar la suspensión de la misma.

6.3 Todo personal adscrito a la UPNECH que sea previamente autorizado por la por parte de la Secretaría Administrativa de la UPNECH, poseerá una cuenta de correo electrónico. La autorización deberá solicitarse por escrito al jefe de departamento de Sistemas.

6.4 La información enviada o recibida en el correo electrónico será responsabilidad total del usuario de la cuenta, dejando a la UPNECH fuera de cualquier responsabilidad penal o civil en la cual incurriera.

6.5 La información enviada a través de plataforma y correo electrónico, serán de la completa responsabilidad del usuario que lo emite, y deberá basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dicha información podrá emplearse en contra de los intereses de personas físicas, así como de la UPNECH ni de cualquier otra institución local o federal.

6.6 Los nombres de las cuentas de correo para trabajadores estarán conformadas por la primera letra del nombre y seguida por el primer apellido, en caso de que ya exista se utilizarán variantes con el nombre o usando el apellido materno. La clave o password será definida por el usuario una vez que el personal de sistemas le haya proporcionado la clave default.

6.7 Todo alumno inscrito de manera formal a la UPNECH, contará con una cuenta institucional con la cuál podrá hacer uso de los servicios digitales que brinda la Universidad (Correo electrónico, Plataforma Educativa y Sistema integral Universitario).

6.8 Los nombres de las cuentas de correo para alumnos estarán conformadas por la matricula asignada por el sistema de control escolar (SIGAA) . La clave o password institucional será definida por dicho sistema y no podrá ser modificada por el alumno.

6.9 Aquella persona que sea sorprendida haciendo mal uso de los servicios digitales para emprender ataques a sitios externos, será sancionada de acuerdo a las normas y leyes vigentes en la materia.

6.10 Cualquier abuso o problema con el buen uso y manejo de las cuentas deberá ser reportado al departamento de Sistemas en Rectoria.

6.11 Esta estrictamente prohibido el envío o publicación de información confidencial de la UPNECH a través de los servicios digitales que brinda la UPNECH.

6.12 Esta estrictamente prohibido el envío de correos “cadena”.

6.13 Evitar abrir los correos en los que exista duda de su procedencia o no solicitados.

6.14 Queda estrictamente prohibido el envío a través del correo electrónico de información encriptada a menos que sea autorizado por el área de Sistemas.

6.15 En caso de que el usuario no realice una consulta de su correo en un periodo no mayor a 90 días hábiles a partir de la última fecha de consulta de su correo, su cuenta será suspendida y todos los mensajes serán eliminados en forma automática y permanente del servidor de correo.

6.16 El espacio de almacenamiento disponible en el servidor-mail es limitado, motivo por el cual se recomienda que el usuario con cuenta de correo, consulte diariamente de su correo (de esta forma el usuario descarga el correo almacenándolo a su equipo de cómputo mediante el archivo de correo correspondiente).

6.17 El tamaño máximo para envío de correo será de 10 MB y el tamaño máximo para recibir correos será de 20 MB o menor de acuerdo al límite de espacio libre del servidor. (Esto es vigente para todas las áreas).

6.18 Es deber de todo usuario de correo electrónico, la buena administración del espacio asignado a su cuenta de correo y por lo tanto, es su responsabilidad, cualquier anomalía que se presente, derivada de la mala administración del espacio asignado para su cuenta.

6.19 Se recomienda crear carpetas para la mejor administración del correo y mantener la bandeja de entrada con la menor cantidad de mensajes.

6.20 Se recomienda no mantener almacenados en el correo archivos que ocupen demasiado espacio. Si éstos son necesarios para el usuario deberá almacenarlos en el equipo de cómputo.

6.21 El usuario será responsable del perjuicio que pueda ocasionarle el no poder recibir o enviar más correos en caso de que se agote el espacio que tiene asignado.

6.22 Es obligación de cada usuario, mantener su recipiente de elementos eliminados continuamente vacío, ya que esto representa espacio de correo utilizado innecesariamente, debido a que implica la saturación de la capacidad de almacenamiento del servidor o el equipo de cómputo.

6.23 En el caso de que un usuario desee enviar o recibir un correo electrónico cuyo tamaño sea mayor a 10MB, se deberá dirigir al personal de Informática, donde se le presentará alguna alternativa. Es preciso aclarar que este tipo de requerimientos serán considerados sólo si el correo a enviar o recibir será utilizado para fines laborales.

6.24 El personal de Sistemas se reservará el derecho de monitorear las cuentas que presenten un comportamiento sospechoso para la seguridad de la información institucional, detección de intrusos, propagación de virus, seguridad de la red de la UPNECH e inclusive podrá ir al lugar del usuario a verificar en su PC el uso que le esté dando a su correo institucional.

NOTA: El envío de mensajes masivos de correo electrónico deberá ser validado por el personal de Sistemas esto con el fin de asegurar que cumplan con las reglas establecidas para el buen uso del correo electrónico. Los mensajes masivos no deberán ni podrán ser enviados desde una cuenta estándar o ajena a la institución, ya que esto pone en riesgo la seguridad.

8. APLICABLES A INTERNET

7.1 Todo el personal de estructura de la UPNECH tendrá acceso al servicio de Internet (salvo aquellas personas que dadas sus labores no requieran de este servicio).

7.2 Cuando las necesidades del servicio así lo requieran, el jefe de departamento deberá solicitar por escrito al personal de Sistemas la habilitación del servicio de Internet para personal temporal.

7.3 A continuación se detallan algunos programas y acciones que no deben ser usados para el buen desempeño del servicio de Internet:

- Cualquier programa destinado a realizar enlaces de voz y video, que no tengan relación directamente con las tareas académicas o administrativas en la UPNECH.
- Descargas de gran tamaño (mayores a 200 Mb) o uso de archivos de audio y multimedia.
- Sitios de interacción social (redes sociales), páginas personales o aquellas que no tengan relación directamente con las tareas académicas o administrativas en la UPNECH.

También se restringe el acceso a las páginas del tipo:

- Dedicadas a proveer juegos en línea.
- Con información que no sea relevante al trabajo del departamento.
- Con material para adultos.
- Dedicados a la difusión personal (Redes Sociales).
- Servidores de almacenamiento masivo.

9. MEJORES PRÁCTICAS EL USO DE LOS BIENES Y SERVICIOS INFORMÁTICOS

1. MEJORES PRÁCTICAS PARA EL CORREO ELECTRÓNICO

- No enviar mensajes que violen los derechos de los destinatarios o de terceras personas.
- Al elaborar un correo electrónico se deberá hacer uso de un lenguaje apropiado.
- Revisar el buzón de su correo con frecuencia, especialmente si está suscrito a listas de interés. No intercambiar grandes volúmenes de información, a través de este servicio.
- Eliminar de su buzón de correo aquellos mensajes que no necesite mantener almacenados. No enviar mensajes con juegos, pornografía, obscenidades, virus, etc.
- No iniciar ni continuar una cadena de mensajes.

Cuidado con los ataques de phishing (robo de identidad), evite enviar cualquier tipo de información personal como: información de identidad, información sobre cuentas bancarias, nip o usuarios y claves de accesos. Esta información generalmente es solicitada con uso fraudulento por un atacante, nunca será solicitada por una empresa, institución o banco. La omisión a esta recomendación puede poner en riesgo su seguridad personal, familiar y su patrimonio.

2. MEJORES PRÁCTICAS ANTE LAS AMENAZAS A TRAVÉS DE LA WEB

- El uso global de Internet facilita de manera extraordinaria comunicaciones, sin embargo, esto lo convierte en una fuente de vulnerabilidad de nuestra información personal e institucional. Por esto se recomienda cautela en el manejo de los servicios e información que existe en esta red.
- Cuando en una página de un sitio web detecte alguna amenaza, como virus, gusanos, troyanos, addware, etc., que no pueda ser removido o eliminado por completo, notifique inmediatamente al personal de Sistemas. Nunca confirme una solicitud de estas páginas.
- El usuario debe verificar periódicamente (se sugiere cada semana) su computadora personal.

- Cada usuario es responsable y debe tomar medidas para evitar el contagio de virus, troyanos, gusanos, etc., en los archivos adjuntos que envía.
- El usuario queda eximido de cualquier responsabilidad cuando su cuenta de correo sea afectada por la actividad de un virus, troyano o gusano, el cual envíe mensajes a nombre del usuario, siempre y cuando se compruebe que el usuario es ajeno a la intromisión del virus en la red institucional de la UPNECH, puesto que el virus utiliza de manera aleatoria las cuentas de usuarios para propagarse a otros equipos, esto puede ocurrir antes de que las versiones actualizadas de los antivirus detecten su presencia en la red.

**Cualquier punto no establecido será evaluado y añadido a estas políticas por el jefe del departamento de Sistemas de la UPNECH.*