POLITICA DE SEGURIDAD INFORMATICA

2017

FUNDACION UNVERSITARIA NAVARRA
UNINAVARRA

Realizado por:	Revisado por:	Aprobado por:
_____	_____	_____
Cargo:	Cargo:	Cargo:

"Recuerda reciclar todo el material reutilizable que se genere para la realización del presente procedimiento"

FUNDACIÓN UNIVERSITARIA NAVARRA® UNINAVARRA	**POLITICA DE SEGURIDAD INFORMATICA**

CONTENIDO

INTRODUCCION

La fundación Universitaria Navarra – Uninavarra, en su crecimiento ha adquirido tecnología informática de punta, que permite tener centralizado sus datos. Aplicaciones de comunicación, administrativas (software), así como servidores de alto rendimiento, computadores e impresoras en las sedes (Hardware), los cuales ya no son herramientas de unos pocos, si no que por el contrario se han convertido en una necesidad para cumplir con las labores asignadas.

Entre más usuarios accedan al sistema de información, mayor será el riesgo en cuanto a la seguridad informática se refiere, de ahí que sea preciso adoptar directrices para el buen uso y custodia de las herramientas informáticas disponibles en la institución. El presente documento establece los lineamientos que permita fomentar la cultura de la seguridad y calidad de los datos y la información.

1. OBJETIVO

1.1. Objetivo General

- Establecer las reglas del buen uso de las herramientas informáticas de la Fundación Universitaria Navarra - Uninavarra, así como posibles sanciones por su desacato.

1.2. Objetivos Específicos.

- Generar una cultura institucional que incluya normas de "urbanidad" durante el uso y las expresiones de comunicación por los diferentes medios electrónicos.
- Establecer los parámetros de Uso y manejo de los equipos y herramientas informáticas por parte de todas las personas que tengan acceso al sistema de información.

2. ALCANCE

Las reglas y sanciones dispuestas en este manual aplican para las diferentes áreas y unidades funcionales que utilicen herramientas informáticas (computadores, impresoras, tabletas, Smartphone, accesspoint, memorias USB, CD, etc.) y que de alguna u otra forma se integren al sistema de información de la Fundación Universitaria Navarra - Uninavarra

3. DEFINICIONES

USUARIO DE LA RED INFORMÁTICA: Este concepto cobija a todos los clientes internos, estudiantes que utilicen la red de la institución o un computador externo previamente autorizado por escrito para ser conectado dentro de las instalaciones de la Universidad por un periodo determinado.

BACKUP: En tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

LAN: Local área network o red de área local, es la interconexión de una o varias computadoras y periféricos.

WAN: Wide área network o red de área amplia, es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes. Es cualquier red que une varias redes locales (LAN).

TIC: tecnologías de la información y la comunicación.

USB: El Universal Serial Bus (USB) (bus universal en serie BUS) es un estándar industrial desarrollado en los años 1990 que define los cables, conectores y protocolos usados en un bus para conectar, comunicar y proveer de alimentación eléctrica entre ordenadores y periféricos y dispositivos electrónicos.

VPN: Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

CPUS: Central Processing Unit (CPU/Unidad Central de Procesamiento) también llamado microprocesador o simplemente procesador, es el componente principal del ordenador y otros dispositivos programables, que interpreta las instrucciones contenidas en los programas y procesa los datos.

SPAM: Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

4. CONDICIONES DEL BUEN USO DE LA TECNOLOGÍA

4.1. Cumplimiento Ley 603 de 2000

Es iniciativa de la Universidad informar y educar sobre los beneficios que trae la legalidad para el país, la economía y la productividad de las empresas, recuerda que la defraudación a los Derechos Patrimoniales de Autor es un delito que tiene sanciones, pero es la responsabilidad de cada representante Legal el cumplimiento de la Ley 603 de 2000.

Las leyes que protegen en Colombia el Derecho de Autor, se encuentran el artículo 271 del Código Penal, que protege los Derechos Patrimoniales de Autor, y el 272, que sanciona la violación a los mecanismos de seguridad que protegen al software. Particularmente para el caso del software, es necesario que las empresas proveedores de servicios dentro de la Fundación Universitaria y que cuentan con PC instalados dentro de la Red (LAN o WAN) anexen a sus contratos la declaración del estado de cumplimiento en la materia, se aseguren que todos los programas instalados en la compañías que representan y que se encuentran al servicio de la Fundación Universitaria cuentan con las respectivas licencias, legalmente adquiridas y debidamente certificadas.

El compromiso de cada usuario es el compromiso de toda la institución. Por lo tanto, cualquier instalación de software dentro de la Fundación Universitaria debe ser aprobada por el área de TICS.

4.2. Buen manejo del insumo informático

Cada usuario debe conocer este documento y la correspondiente responsabilidad por sus acciones, al utilizar un insumo informático como PC, Servidor, Impresora, etc., dentro de las instalaciones de la Fundación Universitaria, acceder a la red o al Internet, a través de la infraestructura tecnológica construida exclusivamente para los servicios administrativos y asistenciales que se ofrecen. Para el buen uso de estos insumos se define:

- Realizar una limpieza diaria de los equipos informáticos a su cargo (Teclado, Mouse, Pantalla) de acuerdo al manual de Limpieza y Desinfección de la Fundación Universitaria.
- No consumir alimentos en las áreas de trabajo para evitar daños en los equipos.
- Utilizar las impresoras para labores exclusivas del cargo y no para tareas personales.
- No acceder a páginas de ocio y pornografía en internet.
- Prevenir la infección de los equipos informáticos vacunando los dispositivos extraíbles cada vez que se utilicen (USB, CD, DVD, etc.).
- Apagar el computador cuando termine su jornada laboral.
- No instalar Software no autorizado por la dirección de TICS.
- No guardar o almacenar fotografías, música o videos en los servidores (Carpeta organización).
- No conectarse a la Red Inalámbrica o alámbrica de equipos o dispositivos no autorizados por el TICS.
- Cumplir con las directrices emitidas por la dirección TICS

- No prestar o ceder el ID y o contraseña asignado por la dirección TICS a otras personas.
- Velar y resguardar la confidencialidad de la información.

4.3. Reporte novedad ingreso/retiro usuarios/vacaciones

Al momento del ingreso o retiro de un usuario de la institución, el área de Talento Humano de la Fundación Universitaria debe notificar inmediatamente por medio de un ticket (vía Helpdesk) que cree, bloquee o cancele la cuenta y clave(s) que tiene asignada de acuerdo a la novedad. La seguridad de la información debe garantizarse con un proceso oportuno de reporte de ingreso y retiro de usuarios en la red y/o aplicativos institucionales.

4.4. Control de impresión y racionalización del costo de impresión

Todo usuario tiene derecho a hacer uso de los servicios de impresión, siempre y cuando tenga relación con labores de la Fundación Universitaria, es decir, que el documento a imprimir esté relacionado con el objeto de las funciones a su cargo o de su contrato. La estrategia de reducción de costos de impresión es responsabilidad de cada usuario que tiene asignado un servicio de impresión garantizando impresión en baja calidad y solo de los documentos que ameriten para garantizar campañas de control de impresión.

4.5. Restricción al uso de dispositivos USB dentro de la Red

Los archivos externos y/o USB que traigan los usuarios infectados por virus son de responsabilidad del mismo, el usuario también es responsable de su información en la carpeta que tiene asignada. Es política de La Fundación Universitaria Navarra – Uninavarra restringir el uso de USB para minimizar el riesgo de proliferación de virus. restringe acceso a USB a los siguientes cargos

4.6. Asignación de recursos informáticos a terceros

La Fundación Universitaria Navarra – Uninavarra podrá conceder el uso de la tecnología, por ejemplo licencias de red, licencias de antivirus, licencias de aplicativos y herramientas de Office, uso de servicios de impresión, uso de puntos de switches, acceso a Internet, correo electrónico institucional entre otros, a terceras personas, siempre y cuando sea orden expresa de la rectoría.

4.7. Asignación antivirus al 100% servidores y PC

La Fundación Universitaria Navarra – Uninavarra no podrá tener dentro de la red institucional computadores que no estén cubiertos por su servidor de antivirus, esto para garantizar que no van a ocurrir problemas de virus o de seguridad. Así, cualquier computador de un proveedor o tercero que se conecte a la red debe garantizar el uso de software antivirus para proteger la red. También se incluyen las conexiones VPN.

4.8. Permisos para VPN

Los permisos para el acceso por VPN se brindarán solamente al siguiente personal:

- Directivo estratégico.
- Personal la Dirección TIC.

La solicitud de permisos para el personal diferente al descrito anteriormente deberá ser sustentada por el jefe inmediato quien deberá ser uno de los directores teniendo en cuenta la responsabilidad y las implicaciones de la custodia de la información.

4.9. Creación y conexión centros de cableado

Los nuevos centros de cableado que requieran conectarse al centro de cableado principal deben realizarse con fibra óptica. En las áreas asistenciales se trabajará siempre con cableado blindado.

4.10. Reporte por mal uso de recursos informáticos

Es deber de todo usuario reportar anomalías en el cuidado de equipos e impresoras; por ejemplo si derraman un líquido o algún alimento, clip o demás elementos sobre algún equipo de cómputo o impresora, se debe desconectar el equipo, llamar inmediatamente a la oficina de TIC y generar ticket al área de TIC para que quede como soporte del hallazgo.

5. RESPONSABILIDADES DEL USUARIO

5.1. Garantizar USB libres de virus

Verificar que los archivos, programas y medios de almacenamiento como USB que emplea para el transporte de información estén libres de virus informáticos, esto haciendo un uso adecuado del antivirus, teniendo presente el estado físico de estos medios y sus etiquetas. Garantizando que no utiliza USB que provengan de sitios de alto porcentaje de virus como son universidades, cafés Internet y el Hogar donde no existen unas políticas claras y precisas de Antivirus. La habilitación de la funcionalidad de las USB se hará por escrito/correo electrónico a la oficina de TIC previo análisis con el jefe respectivo.

5.2. Clave personal e intransferible

El Usuario y Contraseña de la Red es personal e Intransferible, igualmente el usuario y la contraseña del Sistema de Información y el correo es personal e Intransferible. Es responsabilidad de cada usuario proteger su(s) clave(s), genera sanción el compartir las claves o publicarlas en lugares visibles lo que afecta la seguridad de la red y el Sistema de Información de la institución.

5.3. Custodia de insumos informáticos y control de energía de monitores y computadores

Es responsabilidad de cada usuario proteger los insumos informáticos asignados bajo su custodia para el desempeño de sus funciones. Mientras el usuario está haciendo uso del equipo, es completamente responsable del mismo. En caso de cualquier falla o desperfecto, debe reportarlo de inmediato al personal encargado de TIC. El usuario no debe abandonar, ni alejarse físicamente del computador sin antes bloquear el computador o apagarlo físicamente. Se solicita bloquear el computador cuando se retire de su puesto de trabajo por más de una (1) hora si su puesto de trabajo está en un lugar de alto tráfico de usuarios y/o pacientes.

5.4. Custodia insumos informáticos para uso exclusivo de actividades laborales

Es responsabilidad de cada usuario proteger los insumos informáticos asignados bajo su custodia para el desempeño de sus funciones. Por lo tanto, el uso de la red, el correo y el disco duro de la estación de trabajo es laboral o del ámbito de la salud. No se permite acceder a páginas de Internet que no tienen ámbito laboral, descargar en su estación de trabajo música, juegos, archivos personales y/o académicos, fotos o software free no autorizado por la oficina de TIC. Se informa a los usuarios que la Fundación Universitaria cuenta con herramientas de gestión de monitoreo automatizadas en línea para el cumplimiento de esta política lo que reporta el uso de Internet de los usuarios. Por lo tanto, cualquier uso no autorizado será notificado directamente por el personal TIC a la Dirección de Talento Humano.

5.5. Garantizar Legalidad del Software en el equipo asignado

El software disponible en cada computador es propiedad de la Fundación Universitaria cada usuario es responsable del computador y debe firmar la aceptación de lo instalado en su equipo, si aparece instalado software que no pertenece a la Fundación Universitaria debe reportarlo inmediatamente a sistemas, el usuario es responsable de la legalidad del mismo ante las directivas la Fundación Universitaria y ante las autoridades externas que realicen la inspección. Si el computador es compartido todos los usuarios del mismo son responsables de él, sin importar quien realizó una instalación indebida.

5.6. No atentar contra insumo informático

En caso que algún usuario dañe o atente contra el buen funcionamiento de algún equipo voluntariamente, tendrá la obligación de cubrir el costo de la reparación, o bien encargarse personalmente de la reparación del insumo informático.

5.7. Responsabilidad de las Copias de Seguridad

El área de TIC es responsable de los backup de las unidades de almacenamiento asignadas a cada usuario, la información local de cada equipo es responsabilidad del usuario. Como las cuotas de espacio duro en disco son limitadas, el backup que se envía al servidor corresponde a documentos estrictamente requeridos como un backup especial.

Es responsabilidad del usuario realizar backup en CD de otra información de los archivos de las herramientas de trabajo de Office que no se guarde en el servidor como también depurar periódicamente la carpeta definida para el backup para no entorpecer las labores de backup institucionales.

6. ACTIVIDADES NO AUTORIZADAS AL USUARIO

6.1. Manipulación de información

En la Fundación Universitaria no está autorizado al usuario agregar, suprimir o modificar información en carpetas ajenas sin el consentimiento del propietario o el Jefe Inmediato responsable de la información.

6.2. Mensajes públicos

En La Fundación Universitaria Navarra – Uninavarra no está autorizado al usuario el uso de lenguaje inapropiado u ofensivo, en mensajes privados o públicos.

6.3. Recursos informáticos para actividades personales

En la Fundación Universitaria no está autorizado al usuario el uso de los servicios de tecnología para negocios particulares o para actividades no relacionadas con la salud o labores administrativas, ni para el beneficio particular de terceras personas o de instituciones que no tengan autorización o acuerdos con la institución. En la Fundación Universitaria no está autorizado al usuario el uso del computador para grabar, ver u obtener archivos de videos de páginas pornográficas o delictivas o para bajar o grabar música, realizar conexión a páginas no autorizadas, o instalar programas para un fin personal.

6.4. Red Exclusiva para propósitos laborales

En la Fundación Universitaria no está autorizado al usuario prestar su estación de trabajo o punto de red a terceros no autorizados para utilización de los servicios de la red para propósitos no laborales o usarlos para propósitos fraudulentos, comerciales o publicitarios. No está autorizado prestar su punto de red para conectar un PC de un tercero no autorizado por el área de TIC o para la conexión de PC personales para bajar información de la red o para realización de actividades personales con portátiles no matriculados como autorizados para conectarse a la Red interna.

6.5. Ingreso Personal no autorizado a los centros de computo

En la Fundación Universitaria no está autorizado el ingreso a los centros de computo a menos con este con permiso por escrito por parte del director TIC

6.6. Cambio Configuración estación de trabajo

En la Fundación Universitaria no está autorizado al usuario modificar la configuración de los equipos, adicionar o cambiar puertos, modificar configuraciones, cambiar papel tapiz, descansa pantallas o cualquier otro ítem de configuración sin el consentimiento del personal de soporte técnico de TIC.

6.7. Mover físicamente los insumos informáticos del puesto de trabajo

En la Fundación Universitaria no está autorizado al usuario el mover físicamente los equipos de cómputo, impresoras, equipos de red, servidores. Las actividades de movimiento y/o traslado de insumos de informático son labores exclusivas del área TICS, cualquier otra persona que lo haga sin la autorización pertinente será directamente responsable de la integridad de los equipos transportados.

6.8. Uso de recursos informáticos en horario no laboral según el cargo

En la Fundación Universitaria no está autorizado al usuario el acceso a los servicios informáticos en horario diferente al laboral de lunes a domingo para realizar trabajos diferentes a los asignados al cargo.

6.9. Uso de objetos no acordes a la función del insumo informático

En la Fundación Universitaria no está autorizado al usuario poner encima o tener cerca del equipo líquidos, alimentos, papelería pasada, u obstruir la ventilación de los equipos con cualquier objeto, o colocar los insumos de cómputo en el piso donde exista la posibilidad de golpes o maltrato por obstaculizar el paso.

6.10. Intercambio de insumos informáticos que alteren el Inventario de Hardware

En la Fundación Universitaria no está autorizado al usuario o al jefe del usuario intercambiar teclados, CPUS, monitores, reguladores, UPS o impresoras sin la autorización de personal de TICS y el personal de Activos Fijos de la Fundación Universitaria, estos movimientos alteran el inventario de hardware.

7. REGLAMENTACIÓN PARA NO USUARIOS DE LA FUNDACION UNIVERSITARIA.

Se deja de ser usuario de los servicios informáticos automáticamente en los siguientes casos:

- Empleados retirados voluntaria e involuntariamente.
- Al terminar el convenio o prácticas en la institución.
- Al terminar Outsourcing u ofertas mercantil de servicios con terceros.
- Por alguna sanción o investigación
- Por terminación de cualquier vínculo con la Fundación Universitaria.

8. FALTAS CON TRÁMITE DISCIPLINARIO

- Todo aquel usuario que use una cuenta o use una clave que no le corresponde.
- Facilitar, prestar, alquilar o vender a otra persona su clave(s) personal (password).
- Apoderarse de claves de acceso de otros usuarios, acceder y/o modificar archivos de otro usuario, grabar o copiar información en carpetas de otros usuarios sin el consentimiento del dueño de la información.
- Perturbar el trabajo de los demás enviando mensajes continuos que impidan en normal funcionamiento del trabajo.
- Violar o intentar violar los sistemas de seguridad de los equipos internos o externos para dañar u obtener información confidencial.
- Jaquear, escuchar o decodificar el tráfico de la red interna o externa o cualquier intento de obtención de información confidencial que se transmita a través de la misma.
- Realizar labores propias de los administradores del sistema sin permiso escrito del personal de sistemas.
- Por ninguna causa se permitirá que los usuarios destapen o traten de reparar los equipos.
- La instalación de tarjetas y otros elementos, así como la reparación de anomalías son llevadas a cabo por personal de sistemas o terceros autorizados, o personal de mantenimiento autorizado por la oficina de TICS.
- Por ninguna causa se permitirá el ingreso de PC personales de contratistas, empleados de la Fundación Universitaria para que sean revisados, formateados o configurados por personal de soporte de TIC.

9. RESPONSABILIDAD DEL PROVEEDOR DE OUTSOURCING DE TECNOLOGIA DE LA INFORMACION (TI)

El proveedor de Outsourcing de TI es responsable de velar el cumplimiento del presente documento, cualquier falta u omisión de notificación genera sanción al proveedor de Outsourcing.

10. SANCIONES

Las sanciones acerca del incumplimiento de este documento sobre el uso de tecnología se realizan según el vínculo de trabajo que se tenga con la persona que realiza la sanción.

10.1. Funcionarios

Se notificará a la oficina de Talento Humano para que se realice la respectiva investigación y descargos a los que haya lugar.

10.2. Contratistas

La notificación de la sanción es reportada al interventor del contrato.

10.3. Docentes y estudiantes

La falta al cumplimiento de este reglamento será notificada al director del Programa Educativo, y se llevara a comité Docencia servicio.