UNIVERSIDAD NACIONAL DE EDUCACIÓN
Enrique Guzmán y Valle
"Alma Máter del Magisterio Nacional"

RECTORADO

RESOLUCIÓN N° 1947-2017-R-UNE

Chosica, 06 de julio del 2017

VISTO el Oficio N° 327-2017-DIGA-UNE, del 28 de junio del 2017, de la Dirección General de Administración de la Universidad Nacional de Educación Enrique Guzmán y Valle.

CONSIDERANDO:

Que con Resolución Ministerial N° 004-2016-PCM, aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de Seguridad de la Información, Requisitos 2da. Edición", en todas las entidades integrantes del Sistema Nacional de Informática;

Que siendo la Dirección de la Oficina de Informática responsable de la implementación del dispositivo señalado en el párrafo precedente, eleva mediante el Oficio N° 068-2017-ORC-OI, del 17 de mayo del 2017, a la Oficina de Organización y Procesos adscrita a la Oficina de Planificación y Desarrollo Institucional, el proyecto del Plan de Seguridad de la Información de la UNE, por corresponder;

Que el referido documento tiene como objetivo asegurar una adecuada protección de la información de la UNE, así como brindar apoyo y orientación con respecto a la seguridad de la información de conformidad a las normas pertinentes;

Que con Oficio N° 290-2017-OOyP/OCPyDI-UNE, el Jefe de la Oficina de Organización y Procesos, envía al Director de la Oficina Central de Planificación y Desarrollo Institucional, quien a su vez, eleva mediante el Oficio N° 196-2017-DCPyDI-UNE, del 26 de junio del 2017, a la Dirección General de Administración el proyecto del Plan de Seguridad de la Información de la UNE, a fin de que efectivice el trámite correspondiente;

Que mediante el documento del visto, la Directora General de Administración envía al Rector el expediente en mención que ha sido evaluado en su oportunidad, para su aprobación correspondiente;

Estando a lo dispuesto por la autoridad universitaria; y,

En uso de las atribuciones conferidas por los artículos 59° y 60° de la Ley N° 30220 - Ley Universitaria, concordante con los artículos 19°, 20° y 23° del Estatuto de la UNE y los alcances de la Resolución N° 1518-2016-R-UNE, con cargo a dar cuenta al Consejo Universitario;

SE RESUELVE:

ARTÍCULO 1°.- APROBAR el Plan de Seguridad de la Información de la Universidad Nacional de Educación Enrique Guzmán y Valle, conforme se detalla en el anexo que consta de treinta y uno (31) folios.

ARTÍCULO 2°.- DISPONER que las dependencias correspondientes se encarguen de dar cumplimiento a lo dispuesto en la presente resolución.

ARTÍCULO 3°.- ENCARGAR a la Oficina de Informática la supervisión y cumplimiento de las políticas establecidas en el presente dispositivo.

Regístrese, comuníquese y cúmplase.

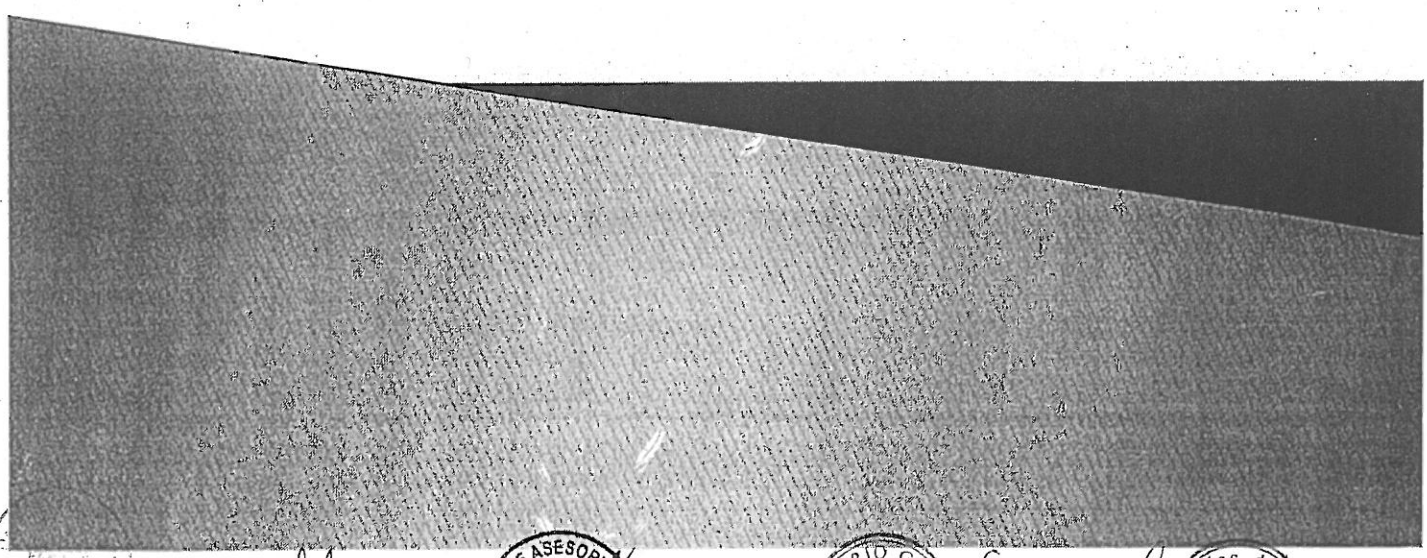
Dr. Segundo Emilio Rojas Saenz
Secretario General

Dr. Luis Alberto Rodríguez De Los Ríos
Rector

SERS.anst.

UNIVERSIDAD NACIONAL DE EDUCACIÓN
ENRIQUE GUZMÁN Y VALLE
ALMA MÁTER DEL MAGISTERIO NACIONAL

PLAN DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE (OFICINA DE INFORMÁTICA)



PLAN DE SEGURIDAD DE LA INFORMACIÓN

Introducción

Las Políticas de Seguridad de la Información surgen como una herramienta institucional para sensibilizar a cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la UNE sobre la importancia y sensibilidad de la información y servicios críticos, de tal forma que le permitan desarrollar adecuadamente sus labores y cumplir con su propósito misional.

El Plan de Seguridad Informática constituye el documento fundamental para el control y la seguridad de la información de la UNE y rige la operación de los activos informáticos que se encuentran distribuidos en sus diferentes dependencias, considerando que el acceso tanto a la Red como a Internet se hará solamente por los usuarios autorizados.

Teniendo en cuenta que el Sistema Informático de la UNE es el conjunto de hardware, software utilizado y la información generada o procesada en el mismo, las medidas que se establecen en el Plan de Seguridad Informática son de obligatorio cumplimiento para todo el personal de la UNE que haga uso de las tecnologías instaladas.

1. Objetivo

a. Definir las pautas de propósito general para asegurar una adecuada protección de la información de la UNE.
b. Brindar apoyo y orientación a la Alta Dirección con respecto a la seguridad de la información, de acuerdo con los requisitos, reglamentos y las leyes pertinentes.
c. Implementar el Sistema de Gestión de Seguridad de la Información en conformidad con la norma NTP ISO/IEC 27001:2014

2. Alcance

El presente documento es de aplicación y cumplimiento obligatorio del servidor civil que labora en la Oficina de Informática, y las demás dependencias administrativas que están en relación directa con la gestión financiera, contable y presupuestal de la Institución.

3. Responsabilidad

El Director de la Oficina de Informática es el responsable de la implementación de este dispositivo.

El Personal encargado de la Oficina de Informática es el responsable de supervisar y coordinar las acciones para que se apliquen y cumplan las políticas establecidas en el presente documento.

Los usuarios y operadores de las dependencias de la Oficina de Informática son los responsables de ejecutar los procedimientos en los cuales estén involucrados para el cumplimiento y aplicación de los procedimientos establecidos en el presente documento.

4. Vigencia

El Plan de Seguridad de la Información entrará en vigencia al día siguiente de su aprobación mediante Resolución Rectoral.

5. Base Legal

a. Constitución Política del Perú
b. Ley N° 30220, Ley Universitaria.
c. Ley N° 28740: Ley del Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa.
d. Decreto Supremo 018-2007-ED: Reglamento de la Ley N° 28740.
e. Decreto Supremo N°016-2015-MINEDU: Política de aseguramiento de la calidad de la educación superior universitaria.
f. Resolución N° 0377-2015-R-UNE, su modificatoria la Resolución Nº 009-2016-AU-UNE, Estatuto de la Universidad Nacional de Educación Enrique Guzmán y Valle.
g. Resolución N° 2663-2016-R-UNE, Reglamento General de la Universidad Nacional de Educación Enrique Guzmán y Valle.
h. Ley N° 27444, Ley del Procedimiento Administrativo General y establece la publicación de diversos dispositivos legales en el portal del Estado peruano y en portales Institucionales.
i. Decreto Legislativo N° 1246, Decreto Legislativo que aprueba diversas medidas de simplificación administrativa.
j. Resolución Ministerial Nº 004-2016-PCM. Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
k. Directiva Nº 008-95-INEI/SJI. "Recomendaciones Técnicas para la Protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública".
l. Directiva Nº 010-95-INEI/SJI. "Recomendaciones Técnicas para la Organización y Gestión de los Servicios Informáticos para la Administración Publica".

Of. de Organización y Procesos - UNE
OFICINA DE INFORMÁTICA FOLIO
OFICINA DE ASESORÍA LEGAL V°B° JEFATURA
SECRETARIO GENERAL UNE
RECTOR

m. Directiva Nº 016-2002-INEI/DTNP "Normas Técnicas para el Almacenamiento y Respaldo de la Información Procesada por las Entidades de la Administración Pública".
n. R.D. Nº 320-2006-CG: Aprueban las "Normas de Control Interno".

PLAN DE SEGURIDAD DE LA INFORMACIÓN

1. Política de clasificación de la información.

Objetivo:

Asegurar que la información reciba el nivel de protección apropiado de acuerdo con el tipo de clasificación establecido por la UNE.

Aplicabilidad:

Estas políticas se aplican a la Alta Dirección, funcionarios y demás directores y jefes de las diferentes dependencias de la UNE.

Directrices:

Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere la UNE como, por ejemplo:

a. Formularios / comprobantes propios o de terceros.
b. Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
c. Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
d. Información transmitida vía oral o por cualquier otro medio de comunicación.

Los usuarios responsables de la información de la UNE deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que esta información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como *Valiosa* para la UNE. Independiente del tipo de activo, se deben considerar las siguientes características.

a. El activo de información es reconocido como valioso para la UNE.
b. No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
c. Forma parte de la identidad de la organización y sin el cual la UNE puede estar en algún nivel de riesgo.

d. Los niveles de clasificación de la información que se ha establecido son: INFORMACIÓN PÚBLICA RESERVADA, INFORMACIÓN PÚBLICA CLASIFICADA (PRIVADA Y SEMIPRIVADA) e INFORMACIÓN PÚBLICA.

2. Políticas de seguridad para los recursos humanos.

Objetivo:

Asegurar que los funcionarios, directores, jefes, docentes y servidores civiles de la UNE entiendan sus responsabilidades y las funciones de sus roles y usuarios, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

Aplicabilidad:

Estas son políticas que aplican a la Alta Dirección, directores, jefes de Oficina, jefes de Área y en general a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

Se debe asegurar que los funcionarios, directores, jefes y demás colaboradores de la UNE entiendan sus responsabilidades en relación con las políticas de seguridad de la información de la UNE y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información.

3. Políticas específicas para usuarios de la UNE.

Objetivo:

Definir las pautas generales para asegurar una adecuada protección de la información de la UNE por parte de los usuarios de la entidad.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, directores, jefes de Oficina, jefes de Área y en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. La UNE suministra una cuota de almacenamiento de la información en un servidor de archivos con los permisos necesarios para que cada usuario guarde la información que crea importante y sobre ella se garantizará la disponibilidad en caso de un daño en el equipo asignado. Esta información será guardada durante un máximo de 2 años. Es de aclarar que el usuario final deberá copiar la información necesaria en la carpeta destinada para este fin la cual se encuentra asignada automáticamente como unidad U:\.

2. La UNE instalará copia de los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades requeridas para cubrir las necesidades. El uso de programas sin la respectiva licencia y autorización de la Oficina de Informática (imágenes, videos, software o música), obtenidos a partir de otras fuentes (Internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para la entidad, por lo que esta práctica no está autorizada.
3. Todo el software usado en la plataforma tecnológica de la UNE debe tener su respectiva licencia y estar acorde con los derechos de autor.
4. La UNE no se hace responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus funcionarios o demás servidores.
5. El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.) pueden ocasionalmente generar riesgos para la entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar dispositivos de almacenamiento externo, se debe obtener aprobación formal e individual de la Oficina de Informática de la UNE, previa solicitud escrita por parte del jefe inmediato.
6. Los programas instalados en los equipos son de propiedad de la UNE. La copia no autorizada de programas o de su documentación implica una violación a la política general de la UNE. Aquellos funcionarios, directores, jefes o demás servidores que utilicen copias no autorizadas de programas o su respectiva documentación quedarán sujetos a las acciones disciplinarias establecidas por la UNE o las sanciones que especifique la ley.
7. La UNE se reserva el derecho de proteger su buen nombre y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas de propiedad de la entidad. Estos controles pueden incluir valoraciones periódicas del uso de los programas y las auditorías anunciadas y no anunciadas.
8. Los recursos tecnológicos y de software asignados a los funcionarios de la UNE son responsabilidad de cada funcionario.
9. Los usuarios son los responsables de la información que administran en sus equipos personales y deben abstenerse de almacenar en ellos información no institucional.
10. Los usuarios solo tendrán acceso a los datos y recursos autorizados por la Oficina de Informática, y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.
11. Es responsabilidad de cada usuario proteger la información que está contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos informáticos; adicionalmente se deben proteger los datos de entrada de estos procesos.
12. Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la entidad.

Of. de Organización y Procesos - UNE -

OFICINA DE INFORMATICA FOLIO N°

OFICINA DE ASESORIA LEGAL V°B° JEFATURA

SECRETARIO GENERAL - UNE -

Universidad Nacional del Santa - RECTOR -

13. Cualquier evento o posible incidente que afecte la seguridad de la información, debe ser reportado inmediatamente a la Oficina de Informática de la UNE.
14. Los jefes de las diferentes dependencias de la UNE, en conjunto con la Oficina de Informática, propiciarán actividades para concientizar al personal sobre las precauciones necesarias que deben realizar los usuarios finales, para evitar revelar información confidencial cuando se hace una llamada telefónica, que pueda ser interceptada mediante acceso físico a la línea o al auricular o ser escuchada por personas que se encuentren cerca. Lo anterior se debe aplicar también cuando el funcionario, director, jefe o demás servidores se encuentren en sitios públicos como restaurantes, transporte público, ascensores, etc.
15. Los datos de los sistemas de información y aplicaciones no deben intercambiarse utilizando archivos compartidos en los computadores, discos virtuales, CD, DVD, medios removibles; deben usarse los mismos servicios del sistema de información, los cuales están controlados y auditados.

4. Políticas específicas para funcionarios y Servidores civiles de la Oficina de Informática.

Objetivo:

Definir las pautas generales para asegurar una adecuada protección de la información de la UNE por parte de los funcionarios y servidores civiles de la Oficina de Informática de la entidad.

Aplicabilidad:

Estas políticas se aplican todos los funcionarios, servidores civiles y colaboradores de la Oficina de Informática y a terceros que se encuentren encargados de cualquier sistema de información.

Directrices:

1. El personal de la Oficina de Informática de la UNE no debe dar a conocer su clave de usuario a terceros sin previa autorización del director de la Oficina de Informática.
2. Los usuarios y claves de los administradores de sistemas y del personal de la Oficina de Informática son de uso personal e intransferible.
3. El personal de la Oficina de Informática debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo con el rol asignado.
4. Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimientos de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el director de la Oficina de Informática y los jefes de las oficinas dependientes de la Dirección.

5. Los documentos y en general la información de procedimientos, seriales, software, etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.
6. Para el cambio o retiro de equipos de funcionarios, se deben seguir políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo con el al software disponible en la entidad. Ej.: formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos.
7. Los funcionarios encargados de realizar la instalación o distribución de software solo instalarán productos con licencia y software autorizado.
8. Los funcionarios de la Oficina de Informática no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del director de la Oficina de Informática y su respectivo registro.
9. Los funcionarios de la Oficina de Informática se obligan a no revelar a terceras personas la información a la que tengan acceso en el ejercicio de sus funciones de acuerdo con sus niveles de seguridad. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.
10. Los funcionarios de la Oficina de Informática no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.
11. Toda licencia de software o aplicativo informático y sus medios se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.
12. Las copias licenciadas y registradas del software adquirido deben ser únicamente instaladas en los equipos y servidores de la entidad. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la entidad.
13. La copia de programas o documentación requiere tener la aprobación escrita de la Dirección de la Oficina de Informática y del proveedor si este lo exige.
14. El personal de la Oficina de Informática debe velar porque se cumpla con el registro en la bitácora de acceso al datacenter de las personas que ingresen y que hayan sido autorizadas previamente por la Oficina de Redes y Comunicaciones.
15. Por defecto, deben ser bloqueados, todos los protocolos y servicios que no se requieran en los servidores; no se debe permitir ninguno de ellos, a menos que sea solicitado y aprobado oficialmente por la Alta Dirección de la UNE a través de la Oficina de Informática.
16. Aquellos servicios y actividades que no son esenciales para el normal funcionamiento de los sistemas de información deben ser aprobados oficialmente por la entidad, a través de la Oficina de Informática y deben ser asegurados mediante controles que permitan la preservación de la seguridad de la información.
17. El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.

18. Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.
19. Las pruebas de laboratorio o piloto deben ser autorizadas por el director de la Oficina de Informática, para sistemas de información, de software tipo freeware o shareware o de sistemas que necesiten conexión a internet. Estas pruebas estas deben ser realizadas sin conexión a la red LAN de la entidad y con una conexión separada de Internet o en su defecto con una dirección IP diferente a las direcciones públicas de producción.

5. Políticas específicas para Webmaster.

Objetivo:

Proteger la integridad de las páginas Web institucionales, el software y la información contenida.

Aplicabilidad:

Estas políticas se aplican a todos los funcionarios, jefes y servidores civiles de la UNE y a terceros que se encuentren desempeñando el rol de Webmaster.

Directrices:

1. Los responsables de los contenidos de las páginas Web (webmasters), deben preparar y depurar la información de su Área o dependencia y reportar a la jefatura los requerimientos de actualización de la versión del software; deben disponer de un archivo actualizado con la información de la página inicial del sitio; y deben registrar la autorización de publicación por parte del funcionario autorizado y coordinar con la Dirección los lineamientos del sitio.
2. Se deberá seguir una política que permita auditar la publicación o modificación de información oficial en las páginas web.
3. Las claves de acceso de el/los responsable(s) de los contenidos de las páginas Web (webmasters) son estrictamente confidenciales, personales e intransferibles.

6. Política de Tercerización u *Outsourcing*

Objetivo:

Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

Aplicabilidad:

Estas son políticas que se aplican a contratistas, proveedores de outsourcing, consultores y contratistas externos, personal temporal y, en general, a todos los usuarios de la información que realicen estas tareas en la UNE.

Directrices:

1. Selección de *outsourcing*

   Se deben establecer criterios de selección que contemplen la historia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.

2. Análisis de riesgos

   Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas a la UNE. El resultado del análisis de riesgos será la base para el establecimiento de los controles y debe ser presentado a la O0ficina de Informática antes de firmar el contrato de *outsourcing*.

3. Acuerdos con terceras partes

   Con el fin de proteger la información de ambas partes, se debe formalizar un acuerdo de confidencialidad. El acuerdo deberá definir claramente el tipo de información que intercambiarán las partes, los medios, la frecuencia y los procedimientos a seguir.

   Si la información intercambiada lo amerita, teniendo en cuenta la calificación de la información de acuerdo con sus niveles de seguridad, se debe preparar y legalizar un acuerdo de confidencialidad entre la entidad y el *outsourcing* de acuerdo con el objetivo y el alcance del contrato; lo cual debe quedar firmado por ambas partes. En todos los casos, deben firmarse acuerdos de niveles de servicio que permitan cumplir con las políticas de seguridad de la información y con los objetivos de la UNE.

7. Política de retención y archivo de datos.

Objetivo:

Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

Aplicabilidad:

Estas políticas se aplican a la Alta Dirección, directores, jefes de Oficina, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. La política de retención de archivos debe establecer cuánto tiempo se deben mantener almacenados los archivos en la UNE de acuerdo con la norma archivística vigente.

2. Las reglas y los principios generales que regulan la función archivística del Estado se encuentran definidos por la Ley, la cual es aplicable a la administración pública en sus diferentes niveles producidos en función de su misión y naturaleza.
3. La ley prevé el uso de las Tecnologías de la Información y las Comunicaciones en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos.

8. Política de disposición de información, medios y equipos.

Objetivo:

Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y propender por su recuperación oportuna.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, jefes de Oficina, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas que permitan su monitoreo y correcto estado de funcionamiento; para ello, se debe realizar los mantenimientos preventivos y correctivos que se requieran.

9. Política de respaldo y restauración de información.

Objetivo:

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software se pueda recuperar después de una falla.

Aplicabilidad:

Esta política será aplicada por los administradores de tecnología, encargados de sistemas de información y jefaturas de área que decidan sobre la disponibilidad e integridad de los datos.

Directrices:

1. La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento como cinta, cartucho, CD, DVD, etc.
2. Los administradores de los servidores, los sistemas de información o los equipos de comunicaciones son los responsables de definir la frecuencia de respaldo y los requerimientos de seguridad de la información (codificación) y el administrador del sistema de respaldo es el responsable de realizar los respaldos periódicos.

3. Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.
4. Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.
5. Un plan de emergencia debe ser desarrollado para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.
6. Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación de los usuarios finales realizar las copias en las carpetas destinadas para este fin.
7. Deben existir al menos una copia de la información de los discos de red, la cual deberá permanecer fuera de las instalaciones de la UNE.
8. Semanalmente, la Dirección de la Oficina de Informática verificará la correcta ejecución de los procesos de backup, suministrará las cintas requeridas para cada trabajo y controlará la vida útil de cada cinta o medio empleado.
9. La Oficina de Informática debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas de la UNE.
10. Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.
11. Es responsabilidad de cada dependencia mantener depurada la información de las carpetas virtuales para la optimización del uso de los recursos de almacenamiento que entrega la Oficina de Informática a los usuarios.
12. La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.
13. Las Unidades de Almacenamiento de respaldo serán verificadas semanalmente para comprobar su correcto estado y de ser necesario se cambiará de acuerdo con la tecnología de almacenamiento vigente.

Periodicidad sugerida del procedimiento de respaldo:

14. Las Copias de Seguridad de las Bases de Datos de los Servidores principales se realizarán todos los días de la semana automáticamente 2 veces al día, 1 copia a las 12:30 p.m. y otra a las 11:00 p.m. para no interrumpir el normal desempeño de las labores diarias.
15. La copia de Seguridad de las máquinas virtuales se realizará diariamente. Dicho proceso se realizará en horas de la madrugada para no interrumpir el normal desempeño de las labores diarias; dicho backup puede ser incremental o total.
16. Las Copias de Seguridad de los códigos fuente de los aplicativos se respaldarán cada vez que se realicen actualizaciones e implementaciones de cada aplicativo, a juicio de los programadores.
17. Las Copias de Seguridad (backup) de los archivos de Ofimática (Word, Excel, Power Point, Open Office, Acrobat, etc.), Dibujos CAD y Base de Datos,

almacenados en las computadoras personales, se realizarán según criterio del usuario, se recomienda evaluar el volumen y/o nivel de importancia de la información.

10. Política de gestión de activos de información.

Objetivo:

Establecer la forma en que se logra y mantiene la protección adecuada de los activos de información.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, jefes de Oficina, servidores civiles y en general a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. Inventario de activos de información

   La Oficina de Informática mantendrá un inventario o registro actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información.

   Una parte de los activos de información se mantendrá en una base de datos bajo la responsabilidad de la Oficina de Informática (Base de datos de gestión de configuraciones - Configuration Management Database CMDB).

2. Propietarios de los activos de información

   La UNE es propietaria de los activos de información y los administradores de estos activos son los funcionarios, jefes o demás colaboradores de la UNE (denominados "usuarios") que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de tecnología de información y comunicaciones (TIC).

11. Política de uso de los activos.

Objetivo:

Mantener la protección adecuada de los activos de información mediante la asignación de estos a los usuarios finales que deban administrarlos de acuerdo con sus roles y funciones.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, jefes de Oficina, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. Los activos de información pertenecen a la UNE y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.
2. Los usuarios deberán utilizar únicamente los programas y equipos autorizados por la Oficina de Informática.
3. La UNE proporcionará al usuario los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de la UNE; los funcionarios o los servidores civiles solo podrán realizar backup de sus archivos personales o de información pública. Para copiar cualquier tipo de información clasificada o reservada, debe pedir autorización a su jefe inmediato, de acuerdo con las normas sobre clasificación de la información según los niveles de seguridad establecidos por la UNE. Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución serán sancionados de acuerdo con las normas y legislación vigentes.
4. Periódicamente, la Oficina de Informática efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o el uso de aplicativos o programas informáticos no autorizados será considerada como una violación a las Políticas de Seguridad de la Información de la UNE.
5. Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados a través la Oficina de Informática con su correspondiente justificación para su respectiva viabilidad.
6. Estarán bajo custodia de la Oficina de Informática los medios magnéticos/electrónicos (discos, CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en Internet y los passwords de administración de los equipos informáticos, sistemas de información o aplicativos.
7. En caso de ser necesario y previa autorización de la Oficina de Informática de la UNE, los funcionarios podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de Internet o de cualquier otra red o medio, en los equipos informáticos a su cargo.
8. Los recursos informáticos de la UNE no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.
9. Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos. Estos actos incluyen, pero no se limitan a: envió de correo electrónico masivo con fines no institucionales y práctica de juegos en línea.
10. Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización de la Oficina de Informática:
    a. Instalar software en cualquier equipo de la UNE.

b. Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de la UNE.
c. Modificar, revisar, transformar o adaptar cualquier software de propiedad de la UNE.
d. Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la UNE.
e. Copiar o distribuir cualquier software de propiedad de la UNE.

11. El usuario deberá informar al jefe inmediato de cualquier violación de las políticas de seguridad o uso indebido que tenga conocimiento.
12. El usuario será responsable de todas las transacciones o acciones efectuadas con su "cuenta de usuario".
13. Ningún usuario deberá acceder a la red o a los servicios TIC de la UNE, utilizando una cuenta de usuario o clave de otro usuario.
14. Cada usuario es responsable de asegurar que el uso de redes externas, tal como Internet, no comprometa la seguridad de los recursos informáticos de la UNE. La Oficina de Informática de la UNE (Oficina de Redes y Comunicaciones) es el área responsable de realizar el aseguramiento de los accesos a Internet, acceso a redes de terceros y a las redes de la entidad. Esta responsabilidad incluye prevenir que intrusos tengan acceso a los recursos informáticos y prevenir también la introducción y propagación de virus.
15. Todo archivo o material recibido a través de medio magnético/electrónico o descarga de Internet o de cualquier red externa deberá ser revisado para detección de virus y otros programas destructivos antes de ser instalados en la infraestructura informática de la UNE.
16. Todos los archivos provenientes de equipos externos a la UNE deben ser revisados para detección de virus antes de su utilización dentro de la red de la UNE.
17. Todo cambio en la infraestructura informática deberá estar controlado y será realizado de acuerdo con los procedimientos de gestión de cambios de la Oficina de Informática de la UNE.
18. La información de la UNE debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los que se pueda garantizar que la información esté segura y puede ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.

12. Política de uso de estaciones cliente.

Objetivo:

Garantizar que la seguridad es parte integral de los activos de información y que son bien utilizados por los usuarios finales.

Aplicabilidad:

Estas son políticas que aplican a la Alta Dirección, directores, jefes de Oficina, funcionarios, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. La instalación de software en los computadores suministrados por la UNE es una función exclusiva de la Oficina de Informática. Se mantendrá una lista actualizada del software autorizado para instalar en los computadores.
2. Se definirán dos (2) perfiles de Administradores locales:
   - Desarrolladores de aplicaciones.
   - Usuarios que necesitan utilizar software específico, que por su naturaleza requieren permisos de administrador local para su ejecución.
3. Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red archivos de vídeo, música y fotos que no sean de carácter institucional.
4. En el Disco C:\ de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a estos archivos.
5. El préstamo de equipos de cómputo, computadores portátiles y vídeo proyectores se debe tramitar a través de la Oficina de Informática con anticipación y se proveerá de acuerdo con la disponibilidad.
6. Los equipos que ingresan temporalmente a la UNE que son de propiedad de terceros: deben ser registrados en las porterías de la entidad para poder realizar su retiro sin problemas; la UNE no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones.
7. La Oficina de Informática no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo de información) a equipos que no sean de la UNE.

13. Política de uso de Internet.

Objetivo:

Establecer unos lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, directores, jefes de Oficina, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.
2. No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de la UNE o que representen peligro para la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por la UNE.
3. El acceso a este tipo de contenidos con propósitos de estudio, de seguridad o de investigación debe contar con la autorización expresa de la Oficina de Informática.
4. La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio de Internet/Intranet. En forma específica, el usuario debe cumplir los requerimientos de la política de uso de Internet descrita en este documento.
5. Niveles de Usuarios
   Se tienen los siguientes niveles:
   a. Nivel 0: Libre acceso
   b. Nivel 1: Navegación + facebook + youtube
   c. Nivel 2: Navegación + youtube
   d. Nivel 3: Navegación – redes sociales
   e. Nivel 4: Páginas extensión .gob

8. Si el sistema proxy usado para prevenir en caso, que los usuarios hagan visitas a lugares inapropiados, páginas pornográficas o de sitios web peligrosos detecta alguno de estos hechos por parte de algún usuario, este será bloqueado e informado a su jefe inmediato superior para que tome las medidas disciplinarias del caso, según sea la gravedad del hecho. Este mismo sistema no requerirá un ID de inicio de sesión adicional y el uso de Active Directory de Windows Server servirá para identificar a los usuarios de Internet. El sistema será capaz de registrar el tiempo de actividad en Internet, la duración de la actividad, los sitios web visitados, todos los datos descargados y el tipo de datos descargados. La Oficina de Informática realizará un monitoreo permanente, mediante las herramientas con las que cuenta, para determinar el cumplimiento de estas políticas y aplicará en mérito a sus funciones las restricciones que crean convenientes.

14. Política de uso de mensajería instantánea y redes sociales.

Objetivo:

Definir las pautas generales para asegurar una adecuada protección de la información de la UNE, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, directores, jefes de Oficina, funcionarios, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con otras instituciones. La totalidad del personal de la UNE solo utilizará el sistema Lync o Skype Empresarial como medio de comunicación en línea entre usuarios de la UNE.
2. No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.
3. La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, trabajador o colaborador de la UNE, que sea creado a nombre personal, como redes sociales, twitter®, facebook®, youtube® linkedIn® o blogs, se considera fuera del alcance del Plan de Seguridad de la Información y, por lo tanto, su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

15. Política de uso de discos de red o carpetas virtuales.

Objetivo:

Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, directores, jefes de Oficina, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. Para que los usuarios tengan acceso a la información ubicada en los discos de red, se debe registrar la solicitud a través de servicios compartidos especificando el acceso y permisos, correspondientes al rol y funciones a desempeñar por la Oficina de Informática de la UNE. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.
2. La información institucional que se trabaje en las estaciones cliente de cada usuario debe ser trasladada periódicamente a los discos de red por ser información institucional.

3. La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.
4. Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tablets, celulares inteligentes, etc. o en los discos de red.
5. Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización de su jefe inmediato.
6. Se prohíbe el uso de la información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.
7. La responsabilidad de generar las copias de respaldo de la información de los discos de red está a cargo de la Oficina de Informática.
8. La responsabilidad de custodiar la información en copias de respaldo controladas, fuera de las instalaciones de la UNE, está a cargo de la Oficina de Informática.

16. Política de uso de impresoras y del servicio de Impresión.

Objetivo:

Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, directores, jefes de Oficina, funcionarios, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. Los documentos que se impriman en las impresoras de la UNE deben ser de carácter institucional.
2. Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.
3. Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar a la Oficina de Informática.

17. Política de uso de puntos de red de datos (red de área local – LAN).

Objetivo:

Asegurar la operación correcta y segura de los puntos de red

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, directores, jefes de Oficina, funcionarios, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. Los usuarios deberán emplear los puntos de red para la conexión de equipos informáticos estándar. Los equipos de uso personal, que no son de propiedad de la UNE, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por la Oficina de Informática.
2. La instalación, activación y gestión de los puntos de red es responsabilidad de la Oficina de Informática (Oficina de Redes y Comunicaciones).

18. Políticas de seguridad del centro de datos y centros de cableado.

Objetivo:

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

Aplicabilidad:

Estas políticas se aplican a los funcionarios, servidores civiles, usuarios de la UNE actuales o por ingresar y a terceros que estén encargados de cualquier parte o sistema de la plataforma informática.

Directrices:

1. No se permite el ingreso al centro de datos al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos debe disponerse de una planilla para el registro, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.
2. La Oficina de Informática debe garantizar que el control de acceso al centro de datos de la UNE cuenta con dispositivos electrónicos de autenticación o sistema de control biométrico.
3. La Oficina de Informática deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía
4. La limpieza y el aseo del centro de datos estará a cargo del Área Administrativa y debe efectuarse en presencia de un servidor civil de la Oficina de Informática. El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.
5. En las instalaciones del centro de datos o centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así

como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.

6. El centro de datos debe estar provisto de:
   a. Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
   b. Pisos elaborados con materiales no combustibles.
   c. Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.
   d. Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
   e. Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo con las recomendaciones del fabricante o al menos una vez cada seis meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.
   f. Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.
7. El cableado de la red debe ser protegido de interferencias, por ejemplo usando canaletas.
8. Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
9. La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizada por la Oficina de Informática y exclusivamente con fines institucionales.
10. Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario o trabajador autorizado de la Oficina de Informática.
11. Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro de datos.
12. Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.
13. Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
14. Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

19. Políticas de seguridad de los Equipos

Objetivo:

Asegurar la protección de la información en los equipos.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, directores, jefes de Oficina, funcionarios, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. Protecciones en el suministro de energía
   A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, pantallas; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por el área Administrativa.
2. Seguridad del cableado
   a. Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
   b. Deben existir planos que describan las conexiones del cableado.
   c. El acceso a los centros de cableado (racks) debe estar protegido.
3. Mantenimiento de los Equipos
   a. La UNE debe mantener contratos de soporte y mantenimiento de los equipos críticos.
   b. Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento.
   c. Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas.
   d. Los equipos que requieran salir de las instalaciones de la UNE para reparación o mantenimiento deben estar debidamente autorizados y se debe garantizar que en dichos elementos no se encuentra información establecida como crítica en la clasificación de la información de acuerdo con los niveles de clasificación de la información.
   e. Para que los equipos puedan salir de las instalaciones, se debe suministrar un nivel mínimo de seguridad, que al menos cumpla con los requerimientos internos, teniendo en cuenta los diferentes riesgos de trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior de la UNE.
   f. Cuando un dispositivo vaya a ser reasignado o retirado de servicio, debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando herramientas para realizar sobre-escrituras en la información existente o la presencia de campos magnéticos de alta intensidad. Este proceso puede además incluir, una vez realizado el proceso anterior, la destrucción física del medio, utilizando impacto, fuerzas o condiciones extremas.
4. Ingreso y retiro de activos de información de terceros.
   a. El retiro e ingreso de todo activo de información de propiedad de los usuarios de la UNE, utilizados para fines personales, se realizará mediante los procedimientos establecidos por la Oficina de Control

Patrimonial y Seguridad. La UNE no se hace responsable de los bienes o los problemas que se presenten al conectarse a la red eléctrica de la UNE.

b. El retiro e ingreso de todo activo de información de los visitantes que presten servicios a la UNE (consultores, practicantes, visitantes, etc.) será registrado y controlado en las porterías de la UNE. El personal de vigilancia verificará y registrará las características de identificación del activo de información.
c. El traslado entre dependencias de la UNE de todo activo de información está a cargo de la Oficina de Control Patrimonial y Seguridad para el control de inventarios.

20. Política de escritorio y pantalla limpia.

Objetivo:

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, directores, jefes de Oficina, funcionarios, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. El personal de la UNE debe conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
2. El personal de la UNE debe bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
3. Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.
4. No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

21. Política de uso de correo electrónico.

Objetivo:

Definir las pautas generales para asegurar una adecuada protección de la información de la UNE, en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, directores, secretarios, jefes de Oficina, funcionarios, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. Esta política define y distingue el uso de correo electrónico aceptable/apropiado e inaceptable/inapropiado y establece las directrices para el uso seguro del servicio.
2. Servicio de correo electrónico:

   Permite a los usuarios de la UNE, el intercambio de mensajes, a través de una cuenta de correo electrónico institucional, que facilita el desarrollo de sus funciones.

   Principios guía:

   a. Los usuarios del correo electrónico institucional son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.

   b. Los servicios de correo electrónico institucional se emplean para servir a una finalidad operativa y administrativa en relación con la entidad. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC de la UNE se consideran bajo el control de la entidad.

3. Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la UNE y no debe utilizarse para ningún otro fin.
4. El envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red, no está autorizado.
5. No está autorizado el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad.
6. Condiciones de uso del servicio:
   a. Cuando un funcionario, trabajador o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire de la UNE, su cuenta de correo será desactivada.
   b. Los correos electrónicos deben contener la siguiente nota respecto al manejo del contenido:

   "El contenido de este mensaje y sus anexos son propiedad de la UNE, es únicamente para el uso del destinatario ya que puede contener información pública reservada o información pública clasificada (privada o semiprivada), las cuales no son de carácter público. Si usted no es el destinatario, se le informa que cualquier uso, difusión, distribución o copiado de esta comunicación están prohibidos. Cualquier revisión, retransmisión, diseminación o uso del mismo, así como cualquier acción que se tome respecto de la información contenida, por personas o entidades diferentes al propósito original de la misma, es ilegal. Si usted es el destinatario, le solicitamos dar un manejo adecuado a la

información; de presentarse cualquier suceso anómalo, por favor informarlo al correo redes@une.edu.pe."

c. El tamaño del buzón de correo electrónico estará determinado por el rol desempeñado por el usuario en la UNE.
d. Cada área deberá solicitar la creación de las cuentas electrónicas, sin embargo, las Oficinas de Personal y de Contrataciones son las responsables de solicitar la modificación o cancelación de las cuentas electrónicas a la Oficina de Informática (Oficina de Redes y Comunicaciones)
e. Las cuentas de correo electrónico son propiedad de la UNE, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con la entidad, ya sea como personal nombrado, contratado o CAS, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la Entidad y no debe utilizarse para ningún otro fin.
f. Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo con la clasificación de la información establecida por la UNE.
g. Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la Entidad.
h. Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y, por lo tanto, asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos, no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe reenviar el correo a la cuenta redes@une.edu.pe con la frase "correo sospechoso" en el asunto.
i. El único servicio de correo electrónico autorizado en la entidad es el asignado por la Oficina de Informática.

22. Política de control de acceso.

Objetivo:

Definir las pautas generales para asegurar un acceso controlado, físico o lógico, a la información de la plataforma informática de la UNE, así como el uso de medios de computación móvil.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, directores, jefes de Oficina, funcionarios, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. La UNE proporcionará a los funcionarios y personal contratado (personas naturales) todos los recursos tecnológicos necesarios con el fin de que puedan desempeñar las funciones para las cuales fueron contratados; por tal

motivo, no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como computadores portátiles, tablets, enrutadores, agendas electrónicas, celulares inteligentes, access point, que no sean autorizados por la Oficina de Informática.

2. La UNE suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados. Estas claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se les dé a las claves asignadas.
3. Solo usuarios designados por la Oficina de Informática estarán autorizados para instalar software o hardware en los equipos, servidores e infraestructura de telecomunicaciones de la UNE.
4. Todo trabajo que utilice los servidores de la UNE con información de la entidad, sus funcionarios o servidores civiles, se debe realizar en sus instalaciones, no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación de la Oficina de Informática.
5. La conexión remota a la red de área local de la UNE debe ser hecha a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada.

23. Política de establecimiento, uso y protección de claves de acceso.

Objetivo:

Controlar el acceso a la información.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, directores, secretarios, jefes de Oficina, funcionarios, servidores civiles y en general a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. Se debe concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.
2. Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la Entidad.
3. Los usuarios deben tener en cuenta los siguientes aspectos:
   a. No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo, almacenadas en un macro o en una clave de función.
   b. El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta o su jefe inmediato.
   c. Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.

d. Se bloqueará el acceso a todo usuario que haya intentado el ingreso, sin éxito, a un equipo o sistema informático, en forma consecutiva por tres veces.
e. La clave de acceso será desbloqueada solo por la Oficina de Redes y Comunicaciones, luego de la solicitud formal por parte del responsable de la cuenta. Para todas las cuentas especiales, la reactivación debe ser documentada y comunicada a la Oficina de Informática.

Las claves o contraseñas deben:

f. Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
g. Tener mínimo seis caracteres alfanuméricos.
   Complejidad mínima: no incluir palabras de diccionario. Las contraseñas deben utilizar tres de los siguientes cuatro tipos de caracteres:
   1. Minúsculas
   2. Mayúsculas
   3. Números
   4. Caracteres especiales como !¡@#$%A&*(){}[] ¿?-_*
h. Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.
i. Cambiarse obligatoriamente cada 60 días, o cuando lo establezca la Oficina de Informática.
j. Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.
k. Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
l. No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.
m. No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.
n. No ser reveladas a ninguna persona, incluyendo al personal de la Oficina de Informática.
o. No registrarlas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento esté aprobado.

24. Política de adquisición, desarrollo y mantenimiento de sistemas de información.

Objetivo:

Garantizar que la seguridad es parte integral de los sistemas de información.

Aplicabilidad:

Estas son políticas que se aplican a los jefes de Oficina, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. Asegurar que los sistemas de información o aplicativos informáticos incluyen controles de seguridad y cumplen con las políticas de seguridad de la información.
2. En caso de desarrollos propios de la entidad, se debe verificar que están completamente documentados, que las diferentes versiones se preservan adecuadamente en varios medios y se guarda copia de respaldo externa a la entidad.
3. Desarrollar estrategias para analizar la seguridad en los sistemas de información.
4. Todo nuevo hardware y software que se vaya a adquirir y conectar a la plataforma tecnológica de la UNE, por cualquier dependencia o proyecto de la Universidad, deberá ser gestionado por la Oficina de Informática para su correcto funcionamiento.
5. La compra de una licencia de un programa permitirá a la UNE realizar una copia de seguridad (a no ser que esté estipulado de manera distinta), para ser utilizada en caso de que el medio se averíe.
6. Cualquier otra copia del programa original será considerada como no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.
7. La Oficina de Informática será la única dependencia autorizada para realizar copia de seguridad del software original.
8. La instalación del software en las máquinas de la UNE se realizará únicamente a través de la Oficina de Informática (Unidad de Soporte Técnico).
9. El software proporcionado por la UNE no puede ser copiado o suministrado a terceros.
10. En los equipos de la UNE se podrá utilizar el software licenciado por la Oficina de Informática y el adquirido o licenciado por los proyectos o programas que se encuentran en la UNE.
11. Para la adquisición y actualización de software, es necesario efectuar la solicitud a la Oficina de Informática con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.
12. El software que se adquiera a través de los proyectos o programas debe quedar a nombre de la UNE.
13. Se encuentra prohibido el uso e instalación de juegos en los computadores de la UNE.
14. Se presentarán para dar de baja el software de acuerdo con los lineamientos dados por la Entidad.

25. Política de uso de dispositivos móviles

Objetivo:

Establecer las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes (smart phones), tablets, entre otros) de la entidad.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, directores, secretarios, jefes de Oficina, funcionarios, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE que tengan asignado un dispositivo.

Directrices:

1. Los dispositivos móviles (teléfonos móviles, teléfonos inteligentes-smart phones, tablets, entre otros) son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones de los usuarios de la entidad.
2. Los dispositivos móviles deben estar integrados a una plataforma de administración controlada por la Oficina de Informática.
3. Los usuarios deben tener instaladas únicamente las aplicaciones distribuidas y autorizadas por el administrador de la plataforma.
4. En el caso del nivel directivo, se autoriza el uso de aplicaciones de redes sociales.
5. Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo.
6. Los dispositivos móviles deben tener únicamente la tarjeta sim asignada por la entidad, de igual forma la tarjeta sim únicamente debe instalarse en los equipos asignados por la entidad.
7. Ante la pérdida del equipo, ya sea por sustracción o extravío, deberá dar cuenta en forma inmediata a la Oficina de Informática.
8. Los teléfonos móviles y/o teléfonos inteligentes deben permanecer encendidos y cargados durante las horas laborales o de acuerdo con la responsabilidad y requerimientos propios del cargo.
9. Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por la UNE con el fin de realizar actividades propias de su cargo o funciones asignadas en la entidad.
10. En caso de requerir instalación de aplicaciones adicionales en el dispositivo móvil, se debe solicitar a la Oficina de Informática para su aprobación.

26. Política para realización de copias en estaciones de trabajo de usuario final.

Objetivo:

Asegurar la operación de realización de copias de información en estaciones de trabajo de usuario final.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, directores, jefes de Oficina, funcionarios, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE.

Directrices:

1. Sobre las obras creadas por los empleados y funcionarios en virtud de su vinculación con la UNE, son de propiedad de la Universidad con las excepciones que la ley señale.
2. En el evento de retiro de un funcionario o traslado de dependencia, previa notificación de la Oficina Central de Personal, de la Oficina de Informática generará una copia de la información contenida en el equipo asignado al perfil del usuario a una unidad de almacenamiento.
3. Una vez esta información se encuentre ubicada en la unidad de almacenamiento, se le realiza copia de seguridad mensual en cinta magnética, la cual es enviada al custodio de medios magnéticos, para conservar esta información en el tiempo.
4. Si el jefe de la dependencia de la cual se retira el usuario requiere copia de esta información, debe realizar solicitud a la Oficina de Informática, quien evaluará la pertinencia de la copia.
5. Se debe seguir el procedimiento de Borrado Seguro para equipos Final, a fin de garantizar la copia de la información para la entidad y la eliminación de la información almacenada en el disco local.
6. Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información, excepto aquellos que se encuentren habilitados los privilegios de escritura por puertos USB.
7. En caso de presentarse alguna falla en los equipos de cómputo, se debe reportar a la Oficina de Informática (Unidad de Soporte Técnico), en caso de requerirse copia de la información, esta se realizará de manera temporal durante las diferentes labores de reparación o mantenimiento.

27. Política para Comunicaciones unificadas.

Objetivo:

Definir las pautas de uso de las comunicaciones por parte de los usuarios autorizados de la UNE.

Aplicabilidad:

Estas son políticas que se aplican a la Alta Dirección, directores, secretarios, jefes de Oficina, funcionarios, servidores civiles y, en general, a todos los usuarios de la información que cumplan con los propósitos generales de la UNE y que utilizan estos servicios.

Directrices:

1. Las comunicaciones unificadas (Lync o Skype Empresarial) deben ser usadas de forma austera y no se permite el envío de mensajes con contenido que atente contra la integridad de las personas o las instituciones.
2. Antes de enviar cualquier contenido, se debe verificar que no contenga malware (virus, código malicioso, etc.), mediante el uso del antivirus instalado por la Oficina de Informática en los equipos institucionales.
3. La información que se publique o divulgue debe guardar las medidas de seguridad exigibles de acuerdo con el tipo de calificación que se le haya dado a dicha información y debe corresponder al entorno laboral.
4. Cada usuario será responsable por el adecuado uso que dé a las herramientas. Los daños y perjuicios que puedan llegar a causar serán de completa responsabilidad de la persona que los haya generado.
5. Los usuarios de los sistemas de comunicaciones unificadas deben firmar el acta de compromiso y reserva previa entrega de los equipos y/o asignación de usuario a la Oficina de Informática.