UNIVERSIDAD NACIONAL DE EDUCACIÓN

RESOLUCIÓN No.- UNAE-R-2019-013

PhD. Freddy Javier Álvarez González
RECTOR
UNIVERSIDAD NACIONAL DE EDUCACIÓN

CONSIDERANDO:

Que, la Constitución de la República del Ecuador en su Art. 347 dispone: *"Será responsabilidad del Estado: (...) 7. Erradicar el analfabetismo puro, funcional y digital, y apoyar los procesos de post-alfabetización y educación permanente para personas adultas, y la superación del rezago educativo. 8. Incorporar las tecnologías de la información y comunicación en el proceso educativo y propiciar el enlace de la enseñanza con las actividades productivas o sociales."*;

Que, el inciso primero del artículo 355 de la Constitución de la República del Ecuador, dispone que: "El Estado reconocerá *a las universidades y escuelas politécnicas autonomía académica, administrativa, financiera y orgánica, acorde con los objetivos del régimen de desarrollo y los principios establecidos en la Constitución.";*

Que, el artículo 17 de la LOES prescribe: *"Reconocimiento de la autonomía responsable.- El Estado reconoce a las universidades y escuelas politécnicas autonomía académica, administrativa, financiera y orgánica, acorde con los principios establecidos en la Constitución de la República. En el ejercicio de autonomía responsable, las universidades y escuelas politécnicas mantendrán relaciones de reciprocidad y cooperación entre ellas y de estas con el Estado y la sociedad; además observarán los principios de justicia, equidad, solidaridad, participación ciudadana, responsabilidad social y rendición de cuentas. Se reconoce y garantiza la naturaleza jurídica propia y la especificidad de todas las universidades y escuelas politécnicas.";*

Que, el artículo 18 de la Ley Orgánica de Educación Superior, dispone: *"Ejercicio de la autonomía responsable.- La autonomía responsable que ejercen las instituciones de educación superior consiste en: (...) e) La libertad para gestionar sus procesos internos; (...)"*;

Que, la Ley Orgánica de Educación Superior, en su artículo 124 dispone: *"Formación en valores y derechos.- Es responsabilidad de las instituciones de educación superior proporcionar a quienes egresen de cualquiera de las carreras o programas, el conocimiento efectivo de sus deberes y derechos ciudadanos y de la realidad socioeconómica, cultural y ecológica del país; el dominio de una lengua diferente a la materna y el manejo efectivo de herramientas informáticas."*;

Que, el artículo 39 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, señala: *"Acceso universal, libre y seguro al conocimiento en entornos digitales.- El acceso al conocimiento libre y seguro en entornos digitales e informáticos, mediante las tecnologías de la información y comunicaciones desarrolladas en plataformas compatibles entre sí; así como el despliegue en infraestructura de telecomunicaciones, el desarrollo de contenidos y aplicaciones digitales y la apropiación de tecnologías, constituyen un elemento transversal de la economía social de los conocimientos, la creatividad y la innovación y es indispensable para lograr la satisfacción de necesidades y el efectivo goce de derechos. El acceso universal, libre y seguro al conocimiento en entornos digitales es un derecho de las y los ciudadanos. El Estado generará las condiciones necesarias para garantizar progresivamente la universalización del acceso a las tecnologías de la información y comunicación, priorizando el uso de*

Parroquia Javier Loyola
(Chuquipata)
Azogues, Ecuador
TELF 07 370-1200
info@unae.edu.ec

tecnologías libres, bajo los principios de: soberanía tecnológica, seguridad, neutralidad de la red, acceso libre y sin restricciones a la información y precautelando la privacidad. Estas condiciones serán respetadas sin perjuicio del proveedor del servicio. Los organismos de control competentes vigilarán que se cumplan con estas condiciones. El Estado dirigirá y ejecutará las acciones correspondientes para precautelar la naturaleza colaborativa y participativa de las tecnologías de la información y comunicación, así como fomentar el desarrollo de redes comunitarias; y, potenciar la pluralidad y diversidad de sus usuarios.";

Que, el artículo 268 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, establece que no se consideran invenciones: *"(...) 9. El software o el soporte lógico, como tal; (...)";*

Que, el Código Orgánico Integral Penal – COIP, en su artículo 178 prescribe: *"Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. (...)";*

Que, el Código Orgánico Integral Penal – COIP, en su artículo 229 establece: *"Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. (...)";*

Que, el Código Orgánico Integral Penal – COIP, en su artículo 232 dispone: *"Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. (...)";*

Que, mediante Ley publicada en Segundo Suplemento del Registro Oficial Nro. 147, de fecha 19 de diciembre del 2013 y reformada mediante Ley No. 0, publicada en Registro Oficial Suplemento 297 de 2 de Agosto del 2018, se crea la Universidad Nacional de Educación UNAE, como una institución de educación superior de derecho público, sin fines de lucro, con personería jurídica propia, con autonomía académica, administrativa, financiera y orgánica, acorde con lo establecido en la Constitución de la República y la Ley Orgánica de Educación Superior;

Que, el inciso tercero y cuarto de la Disposición Transitoria Primera de la Ley de Creación de la Universidad Nacional de Educación UNAE señala que: *"(...) La Comisión Gestora, hasta el 31 de diciembre de 2020, actuará como máxima autoridad de la Universidad Nacional de Educación UNAE, y desempeñará las funciones académicas, administrativas, financieras y regulatorias requeridas, con las funciones propias de autoridad universitaria, encargándose de planificar, administrar, conformar, normar y ejecutar las acciones necesarias para el inicio y desarrollo de las actividades de la institución. El Ministro de la Autoridad Nacional de Educación o su delegado, formará parte de la Comisión Gestora. Quien presida la Comisión Gestora, representará jurídicamente a la Universidad Nacional de m Educación UNAE mientras dure el período de transición. (...)";*

Parroquia Javier Loyola
(Chuquipata)
Azogues, Ecuador
TELF 07 370-1200
info@unae.edu.ec

Que, mediante Decreto Ejecutivo N° 555, de 08 de noviembre de 2018, el Presidente Constitucional de la República, Lenin Moreno Garcés, delegó al Secretario de Educación Superior, Ciencia y Tecnología e Innovación la facultad de designar y remover, previa evaluación de desempeño a los miembros de las comisiones gestoras de la Universidad Amazónica Ikiam, Universidad de Investigación de Tecnología Experimental Yachay, Universidad de la Artes y Universidad Nacional de Educación UNAE;

Que, mediante Acuerdo N° SENESCYT, 2018-012, de 23 de febrero de 2018, el Secretario de Educación Superior Ciencia Tecnología e Innovación Designó como miembros de la Comisión Gestora de la Universidad Nacional de Educación UNAE, a las siguientes personas en calidad de miembros internos: PhD Freddy Álvarez González, PhD María Nelsy Rodríguez Lozano, PhD Rebeca Castellanos Gómez y Mgs. Verónica del Pilar Moreno quien actuará como Secretaria de la Comisión, en calidad de miembros externos: PhD Magdalena Herdoiza Mera, Mgs Juan Fernando Samaniego Froment y el Ministro de Educación o su delegado permanente;

Que, mediante Acuerdo N° SENESCYT, 2018-093, de 30 de noviembre de 2018, el Secretario de Educación Superior Ciencia Tecnología e Innovación, acordó aceptar la renuncia voluntariamente aceptada por la miembro de la Comisión Gestora de la UNAE, PhD. Rebeca Castellanos Gómez y designó en como miembro interno de la Comisión Gestora de la Universidad Nacional de Educación, al PhD. Stefos Efstathios en su calidad de Vicerrector Académico de la UNAE;

Que, mediante RESOLUCIÓN-SO-002-No.-013-CG-UNAE-R-2018, de 05 de marzo de 2018, la Comisión Gestora de la UNAE, ratificó como Presidente - Rector de la Universidad Nacional de Educación, al PhD. Freddy Javier Álvarez González, a quien se le otorga la representación legal, judicial y extrajudicial, de esta Institución de Educación Superior mientras dure el período de transición establecido en la Ley; a la vez que, convalida todas sus actuaciones, realizadas en calidad de Rector, durante el período comprendido entre el 23 de febrero al 05 de marzo de 2018;

Que, mediante RESOLUCIÓN-SO-003-No-017-CG-UNAE-R-2018, de 03 de abril de 2018, la Comisión Gestora, expidió el *"REGLAMENTO DE FUNCIONAMIENTO DE LA COMISIÓN GESTORA DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN – UNAE"*, el cual en sus literales a) y f) del Artículo 8 denominado *"Deberes y atribuciones de/la Presidente/a Rector/a"*, establecen lo siguiente: *"a) Ejerce la representación legal, judicial y extrajudicial de la Universidad; (...) g) Ejecutar las directrices de la Comisión Gestora";*

Que, el literal g) del artículo 26 del Estatuto de la Universidad Nacional de Educación establece como una de las atribuciones y responsabilidades de Rector: *"Emitir lineamientos de gestión institucional";*

Que, mediante memorando Nro. UNAE-TICS-2019-0054-M, de 22 de febrero de 2019, el Director de Soporte Tecnológico, (S), remite al Rector de la UNAE, los archivos correspondientes a las políticas de seguridad de la información que el Departamento de Soporte Tecnológico desea implementar, y solicita, designar a quién corresponda para que se evalúe y valide estas políticas para que las mismas puedan entrar en vigencia;

Que, mediante sumilla inserta en el memorando Nro. UNAE-TICS-2019-0054-M, de 22 de febrero de 2019, el Rector de la UNAE, remite a Procuraduría para revisión y emisión del instrumento legal correspondiente; y,

Parroquia Javier Loyola
(Chuquipata)
Azogues, Ecuador
TELF 07 370-1200
info@unae.edu.ec

UNIVERSIDAD NACIONAL DE EDUCACIÓN

En ejercicio de las atribuciones que confiere la Ley Orgánica de Educación Superior, la Ley de Creación de la Universidad Nacional de Educación UNAE, el Estatuto de la UNAE y las Resoluciones de la Comisión Gestora referidas en los antecedentes:

RESUELVE

Artículo 1.- Aprobar las siguientes Políticas de Seguridad de la Información de la Universidad Nacional de Educación:

a) Políticas de uso de laboratorios;
b) Políticas de soporte técnico;
c) Políticas de respaldo de información de servidores;
d) Políticas de respaldo de información para usuarios;
e) Políticas de equipos;
f) Políticas de gestión de contraseñas;
g) Políticas de seguridad data center;
h) Políticas capacitación de servicios institucionales;
i) Políticas de uso de internet;
j) Políticas del servicio de gestión académica
k) Políticas correo electrónico;
l) Políticas del servicio sistema de gestión documental;

Estas son parte integrante de la presente Resolución.

DISPOSICIONES GENERALES

PRIMERA: De la Ejecución de la presente Resolución encárguese a la Dirección de Soporte Tecnológico.

SEGUNDA: De la difusión de la presente Resolución, encárguese a la Secretaría General.

DISPOSICIÓN FINAL

La presente Resolución entrará en vigencia a partir de la fecha de su suscripción.

COMUNÍQUESE Y CÚMPLASE.-

Dado y suscrito en la ciudad de Azogues, provincia del Cañar, a primero (07) de mayo de 2019.

PhD. Freddy Javier Álvarez González
RECTOR
UNIVERSIDAD NACIONAL DE EDUCACIÓN

GESTIÓN/ACTIVIDAD	NOMBRES Y APELLIDOS	CARGO FUNCIÓN	FIRMA
ELABORADO POR:	GUILLERMO VERDUGO SANTANDER	ESPECIALISTA DE NORMATIVA	
REVISADO Y APROBADO POR:	VERÓNICA MORENO GARCÍA	PROCURADORA	

Parroquia Javier Loyola
(Chuquipata)
Azogues, Ecuador
TELF 07 370-1200
info@unae.edu.ec

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN

1. Introducción.

Como lo dice en su misión la Universidad Nacional de Educación tiene como misión contribuir a la formación de educadores y pedagogos que con sus modos de hacer, de pensar y de investigar transformen el Sistema Nacional Educativo a fin de construir una sociedad justa, equitativa, libre y democrática generando modelos educativos, pedagógicos y didácticos de excelencia caracterizados por su rigor científico, enfoque de derechos y de interculturalidad, por lo tanto la Universidad Nacional de Educación considera a la información generada como un elemento fundamental para el cumplimiento de la misma.

Entendiendo que la información institucional es un activo que, como otros activos de la institución es esencial que sea protegido adecuadamente; la Universidad Nacional de Educación está comprometida con la protección de la información crítica asociada a los servicios y procesos de enseñanza, aprendizaje y de investigación y con la información generada por los departamentos administrativos de la Universidad.

El objetivo de la seguridad de la información es la de garantizar la calidad de la misma, buscando mantener la confidencialidad, la disponibilidad y la integridad de los datos generando estrategias que deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Es importante que el sistema de gestión de seguridad de la información forme parte y esté integrado con los procesos de la organ6ización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles.

2. Objetivos

Controlar el uso correcto de los equipos institucionales asignados.

Elaborar el programa de mantenimiento preventivo anual para el equipo de cómputo de la Universidad Nacional de Educación.

Políticas de Equipos

1. Infraestructura de Hardware
    a. La Dirección de Soporte Tecnológico tiene la responsabilidad de controlar y llevar un inventario detallado de la infraestructura de hardware de la Universidad Nacional de Educación.
    b. La Dirección de Soporte Tecnológico es el ente autorizado para definir los estándares a considerar en la adquisición de activos informáticos.
2. Mantenimientos Equipos
    a. El mantenimiento técnico preventivo de todos los activos de infraestructura de tecnología, deberá ser realizado y/o gestionado por la Dirección de Soporte Tecnológico, considerando su vigencia tecnológica
    b. El mantenimiento técnico correctivo de todos los activos de infraestructura de tecnología de información de la Universidad Nacional de Educación, debe ser realizado de acuerdo los siguientes niveles:
        i. El nivel de help-desk, el mismo que se constituye en un soporte inicial vía telefónica directamente al usuario en dificultad.
        ii. El apoyo en el sitio del personal de soporte del área de informática al usuario en dificultad
    c. La Dirección de Soporte Tecnológico comunicará el programa de mantenimiento preventivo a las diferentes Direcciones de la Universidad Nacional de Educación, informando a los usuarios la fecha de visita de cada uno de los mantenimientos de los equipos con al menos dos días de anticipación.
    d. Las actividades deberán ser programadas en fechas que no afecte el desarrollo normal de las laboren de los usuarios.
    e. El mantenimiento preventivo a los equipos de cómputo e impresoras, se ejecutará de acuerdo a lo establecido en el plan de mantenimiento. Este se realizará en las instalaciones físicas de la institución según la programación establecida
    f. En caso de no poder cumplir los mantenimientos programados por cualquier eventualidad, se deberá programar nueva fecha y deberá informarse por escrito y con anterioridad, los cambios a los directamente implicados.
    g. En caso de que algún equipo requiera ser enviado por "garantía", el departamento de Soporte Tecnológico elaborará los informes respectivos para el envío de los mismos a los proveedores correspondientes e informará mediante correo electrónico institucional a la Dirección Administrativa el movimiento del equipo para fines pertinentes.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN

1. Introducción.

Como lo dice en su misión la Universidad Nacional de Educación tiene como misión contribuir a la formación de educadores y pedagogos que con sus modos de hacer, de pensar y de investigar transformen el Sistema Nacional Educativo a fin de construir una sociedad justa, equitativa, libre y democrática generando modelos educativos, pedagógicos y didácticos de excelencia caracterizados por su rigor científico, enfoque de derechos y de interculturalidad, por lo tanto la Universidad Nacional de Educación considera a la información generada como un elemento fundamental para el cumplimiento de la misma.

Entendiendo que la información institucional es un activo que, como otros activos de la institución es esencial que sea protegido adecuadamente; la Universidad Nacional de Educación está comprometida con la protección de la información crítica asociada a los servicios y procesos de enseñanza, aprendizaje y de investigación y con la información generada por los departamentos administrativos de la Universidad.

El objetivo de la seguridad de la información es la de garantizar la calidad de la misma, buscando mantener la confidencialidad, la disponibilidad y la integridad de los datos generando estrategias que deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Es importante que el sistema de gestión de seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles.

2. Objetivos

Garantizar una política de contraseñas que precautele la seguridad de cada uno de las cuentas de usuario creadas

Implementar seguridades mediante contraseñas seguras, las cuales cumplen normas internacionales para su creación y modificación.

Conocer los procesos de creación, y desactivación de cuentas

Política de Gestión de Contraseñas.

1. Uso de contraseñas
    a. Todos los servicios implementados por la Dirección de Soporte Tecnológico tienen por defecto la creación de contraseñas para cada uno de los usuarios.
2. Directiva de contraseñas
    a. Todos los servicios implementados por la Dirección de soporte Tecnológico poseerán la siguiente restricción de contraseñas exigiéndose 3 de los 4 requisitos de los valores permitidos en el punto II :
        i. 8 caracteres como mínimo y 16 caracteres como máximo.
        ii. Valores permitidos:
            1. A-Z
            2. a-z
            3. 0-9
            4. ! @ # $ % ^ & * - _ + = [ ] { } | \ : ‘ , . ? / ` ~ “ < > ( ) ;
            5. Caracteres UNICODE no permitidos
            6. No puede contener el alias del nombre del usuario (la parte previa al símbolo @).
    b. De forma predeterminada, la fecha de expiración de la contraseña está habilitada. Si se habilita, los usuarios tendrán que cambiar obligatoriamente sus contraseñas después de 90 días.
    c. Los usuarios que estén registrados en el Servicio de Directorio recibirán la notificación de expiración de la contraseña.
3. Historial de contraseñas
    a. No se podrá utilizar la última contraseña otra vez
    b. La contraseña no podrá contener ni nombres ni apellidos del usuario.
    c. No deben usarse contraseñas que sean idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
    d. Los usuarios no deberán almacenar la contraseña en la computadora. Algunos cuadros de diálogo presentan una opción para guardar o recordar la contraseña; no debe seleccionarse esa opción.
4. Bloqueo de cuenta
    a. Después de 10 intentos de inicio de sesión (ingreso de clave incorrecta), el usuario tendrá que resolver un diálogo de CAPTCHA como parte del inicio de sesión.
    b. La Dirección de Soporte Tecnológico tendrá la potestad de bloquear cuentas de usuario según lo considere necesario.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN

1. Introducción.

Como lo dice en su misión la Universidad Nacional de Educación tiene como misión contribuir a la formación de educadores y pedagogos que con sus modos de hacer, de pensar y de investigar transformen el Sistema Nacional Educativo a fin de construir una sociedad justa, equitativa, libre y democrática generando modelos educativos, pedagógicos y didácticos de excelencia caracterizados por su rigor científico, enfoque de derechos y de interculturalidad, por lo tanto la Universidad Nacional de Educación considera a la información generada como un elemento fundamental para el cumplimiento de la misma.

Entendiendo que la información institucional es un activo que, como otros activos de la institución es esencial que sea protegido adecuadamente; la Universidad Nacional de Educación está comprometida con la protección de la información crítica asociada a los servicios y procesos de enseñanza, aprendizaje y de investigación y con la información generada por los departamentos administrativos de la Universidad.

El objetivo de la seguridad de la información es la de garantizar la calidad de la misma, buscando mantener la confidencialidad, la disponibilidad y la integridad de los datos generando estrategias que deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Es importante que el sistema de gestión de seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles.

2. Objetivos

Crear políticas que regulen los accesos al datacenter.

Garantizar el buen estado de los equipos del datacenter mediante herramientas de monitoreo.

Política Data Center

1. Política de Uso Data Center
    a. El único personal autorizado para el acceso al data center es el personal de la Dirección de Soporte Tecnológico
    b. Todo acceso de personal ajeno a la Dirección de Soporte Tecnológico deberá ser autorizado previamente.
    c. Es responsabilidad del Especialista de Infraestructura Informática el asignar los permisos de acceso al Data Center, de acuerdo a la autorización por parte del Director de Soporte Tecnológico
    d. El único medio de acceso para el ingreso al Data Center es la huella dactilar o clave de acceso.
    e. Materiales inflamables o peligrosos (como por ejemplo cartón, cajas, papel o cualquier otro material similar), no podrán ser almacenados dentro de ningún espacio del Data Center.
    f. No se permiten comidas ni bebidas en el Data Center.
    g. Se prohíbe fumar dentro del Data Center.
    h. No se permite tomar fotos ni el uso de cámaras fotográficas o cámaras de video.
    i. No arrastrar equipo sobre el piso falso del Data Center.
    j. No pueden introducir ni utilizar ninguno de los siguientes materiales en el Data Center:
        i. Productos derivados del Tabaco
        ii. Explosivos
        iii. Armas
        iv. Químicos
        v. Drogas ilegales
        vi. Artículos electromagnéticos
        vii. Materiales radioactivos
        viii. Cámaras fotográficas o de video
    k. La Dirección de Soporte Tecnológico se reserva el derecho de inspeccionar todos los objetos que entran o salen del Data Center.
    l. Dentro del equipamiento de seguridad que el Data Center debe tener se especifica lo siguiente:
        i. Puerta blindada de seguridad.
        ii. Control de acceso
        iii. CCTV interno
        iv. Sistema de enfriamiento
        v. Sistema contra incendios
        vi. Piso falso

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN

1. Introducción.

Como lo dice en su misión la Universidad Nacional de Educación tiene como misión contribuir a la formación de educadores y pedagogos que con sus modos de hacer, de pensar y de investigar transformen el Sistema Nacional Educativo a fin de construir una sociedad justa, equitativa, libre y democrática generando modelos educativos, pedagógicos y didácticos de excelencia caracterizados por su rigor científico, enfoque de derechos y de interculturalidad, por lo tanto la Universidad Nacional de Educación considera a la información generada como un elemento fundamental para el cumplimiento de la misma.

Entendiendo que la información institucional es un activo que, como otros activos de la institución es esencial que sea protegido adecuadamente; la Universidad Nacional de Educación está comprometida con la protección de la información crítica asociada a los servicios y procesos de enseñanza, aprendizaje y de investigación y con la información generada por los departamentos administrativos de la Universidad.

El objetivo de la seguridad de la información es la de garantizar la calidad de la misma, buscando mantener la confidencialidad, la disponibilidad y la integridad de los datos generando estrategias que deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Es importante que el sistema de gestión de seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles.

2. Objetivos

Garantizar la capacitación del personal docente y/o administrativo sobre los servicios implementados por la dirección de Soporte Tecnológico.

Crear planes de capacitaciones para el personal docente, administrativo y a los estudiantes.

Establecer sesiones para retroalimentar al personal de Tics sobre los avances de los sistemas implementados por la dirección de Soporte Tecnológico

Políticas de capacitación de servicios institucionales

1. Es obligación de la Dirección de Soporte Tecnológico capacitar a los usuarios sobre el funcionamiento correcto de los servicios implementados.
    a. Para el personal administrativo vinculado, el mismo será capacitado en el momento de la entrega de las credenciales de accesos a los diversos servicios implementados por la Dirección de Soporte Tecnológico
    b. Para el personal académico vinculado, el mismo será capacitado siguiendo el plan de capacitación de la Coordinación de Gestión Académica de Grado, se incluye también la capacitación al momento de entregar las credenciales de uso para cada docente.
    c. Para la capacitación a los estudiantes de la Universidad Nacional de Educación, la misma dependerá del plan de inducción que elabore la dirección de Bienestar Universitario.
2. Es obligación de la Dirección de Soporte Tecnológico coordinar capacitaciones internas sobre los avances en cada uno de los servicios implementados.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN

1. Introducción.

Como lo dice en su misión la Universidad Nacional de Educación tiene como misión contribuir a la formación de educadores y pedagogos que con sus modos de hacer, de pensar y de investigar transformen el Sistema Nacional Educativo a fin de construir una sociedad justa, equitativa, libre y democrática generando modelos educativos, pedagógicos y didácticos de excelencia caracterizados por su rigor científico, enfoque de derechos y de interculturalidad, por lo tanto la Universidad Nacional de Educación considera a la información generada como un elemento fundamental para el cumplimiento de la misma.

Entendiendo que la información institucional es un activo que, como otros activos de la institución es esencial que sea protegido adecuadamente; la Universidad Nacional de Educación está comprometida con la protección de la información crítica asociada a los servicios y procesos de enseñanza, aprendizaje y de investigación y con la información generada por los departamentos administrativos de la Universidad.

El objetivo de la seguridad de la información es la de garantizar la calidad de la misma, buscando mantener la confidencialidad, la disponibilidad y la integridad de los datos generando estrategias que deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Es importante que el sistema de gestión de seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles.

2. Objetivos

Crear conciencia en los usuarios sobre el buen uso del internet

Conocer los posibles problemas que pueden tener los usuarios en el momento de manejar información personal en webs no seguras

Conocer las medidas que se van a tomar para evitar la visualización de páginas no autorizadas como la descarga de software ilegal.

Políticas de Uso de Internet

1. Dirección de Soporte Tecnológico
    a. La Dirección de Soporte Tecnológico debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
    b. La Dirección de Soporte Tecnológico debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
    c. La Dirección de Soporte Tecnológico debe monitorear continuamente el canal o canales del servicio de Internet.
    d. La Dirección de Soporte Tecnológico debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
    e. La Dirección de Soporte Tecnológico debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.
    f. El área encargada para realizar los filtros web es Infraestructura de Redes.
2. Usuarios
    a. No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, aplicativos de descarga P2P (torrents) hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.
3. Bloqueo de Páginas Web
    a. Las páginas web serán bloquedas desde el firewall institucional.
    b. Se bloquearán las páginas que no sean inherentes a temas académicos o institucionales.
    c. Para el desbloqueo de alguna página web específica se deberá solicitar y justificar la razón del mismo; el Director de cada departamento deberá enviar la solicitud por el Sistema de Gestión Documental al Director de Soporte Tecnológico.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN

1. Introducción.

Como lo dice en su misión la Universidad Nacional de Educación tiene como misión contribuir a la formación de educadores y pedagogos que con sus modos de hacer, de pensar y de investigar transformen el Sistema Nacional Educativo a fin de construir una sociedad justa, equitativa, libre y democrática generando modelos educativos, pedagógicos y didácticos de excelencia caracterizados por su rigor científico, enfoque de derechos y de interculturalidad, por lo tanto la Universidad Nacional de Educación considera a la información generada como un elemento fundamental para el cumplimiento de la misma.

Entendiendo que la información institucional es un activo que, como otros activos de la institución es esencial que sea protegido adecuadamente; la Universidad Nacional de Educación está comprometida con la protección de la información crítica asociada a los servicios y procesos de enseñanza, aprendizaje y de investigación y con la información generada por los departamentos administrativos de la Universidad.

El objetivo de la seguridad de la información es la de garantizar la calidad de la misma, buscando mantener la confidencialidad, la disponibilidad y la integridad de los datos generando estrategias que deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Es importante que el sistema de gestión de seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles.

2. Objetivos

Conocer sobre el buen uso del sistema de gestión académica (creación, edición, desactivación usuarios).

Política del servicio Sistema de Gestión Académica

1. Uso del Sistema de Gestión Académica
    a. Solo el personal vinculado laboralmente en la Universidad Nacional de Educación es el autorizado para hacer uso del Sistema de Gestión Académica
    b. Solo los estudiantes que estén matriculadas en la Universidad Nacional de Educación podrán hacer uso del Sistema de Gestión Académica.
    c. Para cualquiera de los dos casos anteriores, el servicio del Sistema de Gestión Académica debe ser utilizado exclusivamente en el ámbito académico y/o administrativo.
    d. Los usuarios estarán sujetos a revisiones por parte de la Dirección de Soporte tecnológico en cuanto al tráfico y manejo seguro de la información enviada, cuando esta sea solicitada por la autoridad competente.
2. Creación de cuentas del Sistema de Gestión Académica
    a. La creación de cuentas del Sistema de Gestión Académica para el personal administrativo y/o académico será realizado por el departamento de Talento Humano en el momento de confirmar la contratación del personal para laborar en la Universidad Nacional de Educación.
    b. La creación de cuentas del Sistema de Gestión Académica para los estudiantes se realizará automáticamente en el momento de postulación del mismo.
    c. Secretaría General validará las cuentas de los estudiantes en el momento en que se encuentren debidamente matriculados en la Universidad Nacional de Educación.
3. Responsabilidad en el uso de la cuenta
    a. Es responsabilidad absoluta del propietario de una cuenta del Sistema de Gestión Académica el manejo de la misma, así como el resguardo de su usuario y contraseña de acceso a la cuenta.
4. Desactivación de cuentas del Sistema de Gestión Académica.
    a. Las cuentas del Sistema de Gestión Académica serán desactivadas por la dirección de Talento humano, en el momento en el que un funcionario sea este académico y/o administrativo termine su relación laboral con la Universidad Nacional de Educación.
    b. Las cuentas del Sistema de Gestión Académica serán desactivadas por la Secretaría General, de conformidad con el Reglamento de Régimen Académico.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN

1. Introducción.

Como lo dice en su misión la Universidad Nacional de Educación tiene como misión contribuir a la formación de educadores y pedagogos que con sus modos de hacer, de pensar y de investigar transformen el Sistema Nacional Educativo a fin de construir una sociedad justa, equitativa, libre y democrática generando modelos educativos, pedagógicos y didácticos de excelencia caracterizados por su rigor científico, enfoque de derechos y de interculturalidad, por lo tanto la Universidad Nacional de Educación considera a la información generada como un elemento fundamental para el cumplimiento de la misma.

Entendiendo que la información institucional es un activo que, como otros activos de la institución es esencial que sea protegido adecuadamente; la Universidad Nacional de Educación está comprometida con la protección de la información crítica asociada a los servicios y procesos de enseñanza, aprendizaje y de investigación y con la información generada por los departamentos administrativos de la Universidad.

El objetivo de la seguridad de la información es la de garantizar la calidad de la misma, buscando mantener la confidencialidad, la disponibilidad y la integridad de los datos generando estrategias que deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Es importante que el sistema de gestión de seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles.

2. Objetivos

Establecer normas y procedimientos para el correcto funcionamiento del servicio de correo electrónico implementado por la Dirección de Soporte Tecnológico.

Prevenir y evitar el mal uso de la información y minimizar el impacto de amenazas reales tales como saturación del sistema, accesos no autorizados, daños por virus, conducta ilegal, acoso o fraude.

Asegurar que todo el personal de la institución conozca las responsabilidades y obligaciones que tiene al ser calificado como usuario del correo electrónico interno de la institución.

Política Correo Electrónico

1. Uso del Correo Electrónico Institucional
    a. Todo personal que se encuentre vinculado a la Universidad Nacional de Educación a través de contrato o con nombramiento son los autorizados para hacer uso del correo electrónico institucional.
    b. Solo las personas que estén matriculadas en la Universidad Nacional de Educación podrán hacer uso del correo electrónico institucional.
    c. Para cualquiera de los dos casos anteriores, el servicio de correo electrónico debe ser utilizado exclusivamente en el ámbito educativo, académico y administrativo relacionado a la Universidad Nacional de Educación.
    d. Los usuarios estarán sujetos a revisiones por parte de la Dirección de Soporte tecnológico en cuanto al tráfico y manejo seguro de la información enviada, cuando esta sea solicitada por la autoridad competente
    e. No se permite el envío de archivos adjuntos que contengan extensión .exe

2. Creación del Correo Electrónico
    a. La creación de los correos electrónicos institucionales serán solicitados por la / el Director de Talento Humano de Talento Humano o su delegado en el momento de confirmar el ingreso o vinculación del personal académico y/o administrativo en la Universidad Nacional de Educación
    b. La creación de los correos electrónicos institucionales serán solicitados por la / el Secretario General en el momento en el que se confirme que los estudiantes se encuentren debidamente matriculados en la Universidad Nacional de Educación.
    c. Para cualquiera de los dos casos anteriores, las solicitudes de creación de correos electrónicos deberán ser enviados por correo institucional dirigido al Director de Soporte Tecnológico, para la creación y asignación de sus respectivas licencias.
    d. El Director de Soporte Tecnológico asignará la tarea de creación de usuarios a las áreas de Soporte y/o Infraestructura para la activación de correos electrónicos institucionales.
    e. La creación de correos electrónicos departamentales lo solicitará el responsable de cada una de los departamentos por medio del Sistema de Gestión Documental, dirigido al Director de Soporte Tecnológico.
    f. El Departamento de Soporte Tecnológico deberá contar con una cuenta de correo electrónico para la recopilación de soportes, dudas, etc.
3. Mensajes Masivos
    a. El envió de mensajes a grupos o listas de destinatarios, sean estos destinatarios internos o externos de forma "personal" se encuentra prohibido. Se incluye en esta prohibición, el envío de mensajes conocidos como "cadenas".

b. El envío de mensajes a grupos o listas de destinatarios internos se permite únicamente para los correos electrónicos departamentales.
c. Está prohibido que los usuarios envíen alertas de seguridad. Si algún usuario recibe una alerta proveniente de dominios externos al correo electrónico institucional, deberá comunicarlo de manera inmediata a las cuentas de la Dirección de Soporte Tecnológico, o ingresar a la mesa de ayuda e indicar el inconveniente.
d. Se prohíbe expresamente para todo usuario autorizado el uso de técnicas de ataque a sistemas de correo electrónico como mail SPAM, mail Bombing, mail Spoofing o mail Relay. Del mismo modo será responsabilidad de la Dirección de Soporte Tecnológico la habilitación y/o mitigación de mecanismos tecnológicos para prevenir los mismos.
e. Se encuentra expresamente prohibido difundir la dirección de correos electrónicos en páginas de dudosa procedencia, o páginas fuera del ámbito educativo o administrativo.

4. Información del Remitente
    a. Para facilitar las comunicaciones, cada mensaje electrónico debe incluir, el nombre y apellido del remitente, su cargo, el área de trabajo a la que pertenece.
    b. Los datos que se visualizarán como información del remitente (firma) en cada uno de los correos electrónicos del personal académico y administrativo serán enviados por la Dirección de Talento Humano.
    c. Para realizar algún cambio en los datos de destinatario, será la Dirección de Talento Humano el encargado de actualizar los mismos y enviar dicha actualización por medio de correo electrónico a la Dirección de Soporte Tecnológico.

5. Responsabilidad en el uso de la cuenta de correo institucional
    a. Es responsabilidad absoluta del propietario de una cuenta de correo electrónico institucional el manejo de la misma, así como el resguardo de su usuario y contraseña de acceso a la cuenta.

6. Restricciones al contenido de los mensajes
    a. Está prohibido enviar o reenviar mensajes, imágenes o videos que incluyan contenidos sexuales o que se consideren ofensivos o discriminatorios.
    b. Está prohibido el enviar o reenviar mensajes en cadena.
    c. Está prohibido propagar en forma intencional, todo tipo de virus o código malicioso en general, a través del correo.

7. Privacidad de los Mensajes Electrónicos
    a. Los usuarios deben tratar los mensajes electrónicos como de uso institucional.

b. Está prohibido enviar, en cualquier parte del correo o en archivos adjuntos, información institucional a personas no autorizadas a conocerla o poseerla.
c. El correo electrónico, debe considerarse como de dominio público o de mensajería insegura. Esto significa que no se debe incluir números de tarjetas de crédito, cuentas bancarias, contraseñas u otra información confidencial. La Universidad no se responsabiliza por problemas que ocasionen el incumplimiento de esta política.

8. Desactivación y Eliminación de Correos Electrónicos
   a. La información de las cuentas de correo electrónico a ser desactivadas serán solicitadas por la Dirección de Talento humano, en el momento en el que un funcionario sea este académico y/o administrativo termine su relación laboral con la Universidad Nacional de Educación, esta información deberá ser enviada por medio del Sistema de Gestión Documental y dirigido a la Dirección de Soporte Tecnológico.
   b. La información de cuentas de correo electrónico a ser desactivadas serán solicitadas por Secretaría General, en el momento en el que un estudiante termine su carrera académica y/o se retire de la Universidad Nacional de Educación, esta información deberá ser enviada por medio del Sistema de Gestión Documental y dirigido a la Dirección de Soporte tecnológico.
   c. El Director de Soporte Tecnológico asignará la tarea de desactivación de usuarios a las áreas de Soporte y/o Infraestructura para la desactivación de los mismos.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN

1. Introducción.

Como lo dice en su misión la Universidad Nacional de Educación tiene como misión contribuir a la formación de educadores y pedagogos que con sus modos de hacer, de pensar y de investigar transformen el Sistema Nacional Educativo a fin de construir una sociedad justa, equitativa, libre y democrática generando modelos educativos, pedagógicos y didácticos de excelencia caracterizados por su rigor científico, enfoque de derechos y de interculturalidad, por lo tanto la Universidad Nacional de Educación considera a la información generada como un elemento fundamental para el cumplimiento de la misma.

Entendiendo que la información institucional es un activo que, como otros activos de la institución es esencial que sea protegido adecuadamente; la Universidad Nacional de Educación está comprometida con la protección de la información crítica asociada a los servicios y procesos de enseñanza, aprendizaje y de investigación y con la información generada por los departamentos administrativos de la Universidad.

El objetivo de la seguridad de la información es la de garantizar la calidad de la misma, buscando mantener la confidencialidad, la disponibilidad y la integridad de los datos generando estrategias que deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Es importante que el sistema de gestión de seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles.

2. Objetivos

Implementar mecanismos para que los usuarios puedan respaldar en los servidores institucionales la información generada diariamente

Crear políticas de respaldos para usuarios

Políticas de Respaldo de información para Usuarios.

1. Uso de medios de almacenamiento.
    a. Es responsabilidad de la Dirección de Soporte Tecnológico asegurar que el acceso a la red (inalámbricas y físicas) para el uso de recursos compartidos cuente con métodos de validación de acceso implementados
    b. Todos los usuarios deberán obtener los accesos a la o las carpetas compartidas para guardar información en los servidores institucionales.
        i. El personal de Soporte Tecnológico será el encargado de la creación de los recursos compartidos en cada una de las máquinas institucionales y/o estaciones de trabajo hacia el servidor.
    c. Es obligación y responsabilidad de parte de los usuarios el respaldar diariamente la información sensible que se encuentre en sus computadoras institucionales o estaciones de trabajo institucional. El usuario es responsable de los respaldos de la información generada en las maquinas institucionales asignadas.
        i. Los usuarios deberán realizar los respaldos en las carpetas compartidas, las mismas estarán habilitadas en cada una de las máquinas institucionales de los usuarios; cabe recalcar que toda la información almacenada en las carpetas compartidas se almacenará en el FileServer institucional, el mismo que consta como servidor crítico y su respaldo se lo realiza diariamente y con un máximo de 3 días para la recuperación de información perdida y/o eliminada.
        ii. Únicamente el personal del departamento o área con el acceso a la carpeta compartida será quien tenga los permisos para acceder, crear, modificar, eliminar la información existente en los recursos compartidos respectivos.
    d. En caso de que por el volumen de información se requiera algún respaldo en CD o en unidad de Disco Duro externo, este servicio de respaldo deberá solicitarse por escrito a la Dirección de Soporte Tecnológico y con la firma del Director del área correspondiente.
    e. No es permitido guardar o intercambiar archivos de audio en cualquier formato (Wav, Mp3, etc.) para fines personales.
    f. No es permitido guardar o intercambiar archivos de videos y/o fotografías personales en cualquier formato.
    g. No es permitido compartir o almacenar información de la Universidad Nacional de Educación en medios públicos de almacenamiento en la nube no autorizados por la institución.
    h. Es responsabilidad del usuario final solicitar el respaldo de sus cuentas de correo electrónico y del Sistema de Gestión Documental antes de terminar con la relación laboral con la Universidad Nacional de Educación.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN

1. Introducción.

Como lo dice en su misión la Universidad Nacional de Educación tiene como misión contribuir a la formación de educadores y pedagogos que con sus modos de hacer, de pensar y de investigar transformen el Sistema Nacional Educativo a fin de construir una sociedad justa, equitativa, libre y democrática generando modelos educativos, pedagógicos y didácticos de excelencia caracterizados por su rigor científico, enfoque de derechos y de interculturalidad, por lo tanto la Universidad Nacional de Educación considera a la información generada como un elemento fundamental para el cumplimiento de la misma.

Entendiendo que la información institucional es un activo que, como otros activos de la institución es esencial que sea protegido adecuadamente; la Universidad Nacional de Educación está comprometida con la protección de la información crítica asociada a los servicios y procesos de enseñanza, aprendizaje y de investigación y con la información generada por los departamentos administrativos de la Universidad.

El objetivo de la seguridad de la información es la de garantizar la calidad de la misma, buscando mantener la confidencialidad, la disponibilidad y la integridad de los datos generando estrategias que deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Es importante que el sistema de gestión de seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles.

2. Objetivos

Crear políticas de uso del Sistema de Gestión Documental para garantizar la correcta administración de los documentos creados, enviados, recibidos por parte del personal administrativo y académico de la Universidad Nacional de Educación.

Conocer los procedimientos de creación y asignación de usuarios.

Establecer las restricciones que tienen los usuarios al momento de usar el sistema.

Política del servicio Sistema de Gestión Documental

1. Uso del Sistema de Gestión Documental
    a. Solo personal que se encuentre vinculado laboralmente a la Universidad Nacional de Educación son los autorizados para hacer uso del Sistema de Gestión Documental
    b. Los usuarios estarán sujetos a revisiones por parte de la Dirección de Soporte tecnológico en cuanto al tráfico y manejo seguro de la información enviada, cuando esta sea solicitada por la autoridad competente.
2. Creación de cuentas del Sistema de Gestión Documental
    a. La creación de cuentas del Sistema de Gestión Documental institucional será solicitados por la Dirección de Talento Humano en el momento de confirmar la vinculación del personal académico o administrativo que ingrese a laborar en la Universidad Nacional de Educación, el mismo se creará conjuntamente con el servicio de correo electrónico.
    b. El Director de Soporte Tecnológico asignará la tarea de creación de usuarios en el servicio de directorio a las áreas de Soporte y/o Infraestructura para la activación y/o creación de las cuentas del SGD.
3. Información del Remitente
    a. Para facilitar las comunicaciones, cada cuenta del servicio del Sistema de Gestión Documental debe incluir, el nombre y apellido del remitente, su cargo, el área de trabajo a la que pertenece, el título académico y el estado civil.
    b. Los datos que se visualizarán como información del remitente en cada una de las cuentas del Sistema de Gestión Documental del personal académico y administrativo serán enviados por la Dirección de Talento Humano.
    c. Para realizar algún cambio en los datos de destinatario, será la Dirección de Talento Humano el encargado de actualizar los mismos y enviar dicha actualización por medio de correo electrónico a la Dirección de Soporte Tecnológico.
4. Prohibición de usar Cuentas Ajenas
    a. Los usuarios tienen prohibido enviar o recibir mensajes, usando la identidad de otro usuario.
5. Restricciones al contenido de los mensajes
    a. Está prohibido enviar o reenviar mensajes, imágenes o videos que incluyan contenidos sexuales o que se consideren ofensivos o discriminatorios.
    b. Está prohibido el enviar o reenviar mensajes en cadena.
    c. Está prohibido propagar en forma intencional, todo tipo de virus o código malicioso en general, a través del Servicio de Gestión Documental.
6. Privacidad de los Mensajes del Sistema de Gestión Documental
    a. Los usuarios deben tratar los mensajes del Sistema de Gestión Documental como de uso interno. Si se desea que sea tratado como información privada entre el remitente y el destinatario, se debe explicitar en el mismo como RESERVADA o CONFIDENCIAL

b. El Sistema de Gestión Documental, debe considerarse como de dominio público o de mensajería insegura. Esto significa que no se debe incluir números de tarjetas de crédito, cuentas bancarias, contraseñas u otra información confidencial.

7. Desactivación de cuentas del Sistema de Gestión Documental.
   a. La información de las cuentas del Sistema de Gestión Documental a ser desactivadas serán solicitadas por la Dirección de Talento humano, en el momento en el que un funcionario sea este académico o administrativo termine su relación laboral con la Universidad Nacional de Educación, esta información deberá ser enviada por medio del mismo Sistema de Gestión Documental y dirigido a la Dirección de Soporte tecnológico.
   b. El Director de Soporte Tecnológico asignará la tarea de desactivación de usuarios en el Sistema de Gestión Documental a las áreas de Soporte y/o Infraestructura para la desactivación de los mismos.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN

1. Introducción.

Como lo dice en su misión la Universidad Nacional de Educación tiene como misión contribuir a la formación de educadores y pedagogos que con sus modos de hacer, de pensar y de investigar transformen el Sistema Nacional Educativo a fin de construir una sociedad justa, equitativa, libre y democrática generando modelos educativos, pedagógicos y didácticos de excelencia caracterizados por su rigor científico, enfoque de derechos y de interculturalidad, por lo tanto la Universidad Nacional de Educación considera a la información generada como un elemento fundamental para el cumplimiento de la misma.

Entendiendo que la información institucional es un activo que, como otros activos de la institución es esencial que sea protegido adecuadamente; la Universidad Nacional de Educación está comprometida con la protección de la información crítica asociada a los servicios y procesos de enseñanza, aprendizaje y de investigación y con la información generada por los departamentos administrativos de la Universidad.

El objetivo de la seguridad de la información es la de garantizar la calidad de la misma, buscando mantener la confidencialidad, la disponibilidad y la integridad de los datos generando estrategias que deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Es importante que el sistema de gestión de seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles.

2. Objetivos

Crear políticas para el buen uso de la información generada por la institución.

Conocer qué tipo de respaldos se ejecutan en el momento de realizar los backups de información.

Crear planes de creación de backups para el respaldo de la información generada por la Universidad Nacional de Educación

Políticas de Respaldo de información de Servidores.

1. Almacenamiento
    a. La información almacenada en los servidores, deber ser periódicamente respaldada en medios adecuados.
    b. Los trabajos relacionados con la restauración de información o la ejecución de labores de mantenimiento son responsabilidad de la Dirección de Soporte Tecnológico.
    c. Todas las solicitudes de recuperación de cualquier información respaldada deberá ser previamente aprobada por el Director del área requirente y la misma petición ser enviada mediante el Sistema de Gestión Documental al Director de Soporte Tecnológico.
    d. El área encargada de planificar, monitorear, realizar y recuperar los respaldos ejecutados es la de Infraestructura Informática.
    e. La restauración de las máquinas virtuales tendrán como mínimo 3 puntos de recovery para las máquinas catalogadas como críticas y 1 punto semanal como mínimo para las otras máquinas virtuales.
        i. Las máquinas virtuales catalogadas como críticas son: FileServer, Sistema de Gestión Documental, Sistema de Gestión Académica, Koha, Dominio, Moodles.
    f. El medio de respaldo serán servidores físicos o NAS, los mismos que permitan asegurar la información en el tiempo.
    g. Los respaldos deberán ser ubicados en un edificio diferente de donde se encuentra la información original, y deberá contener medidas de seguridad y acceso.
    h. Es responsabilidad del usuario final guardar la información a respaldar dentro de las diferentes carpetas compartidas del servidor de archivos.
    i. Todos los respaldos se realizarán de forma completa e incremental.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN

1. Introducción.

Como lo dice en su misión la Universidad Nacional de Educación tiene como misión contribuir a la formación de educadores y pedagogos que con sus modos de hacer, de pensar y de investigar transformen el Sistema Nacional Educativo a fin de construir una sociedad justa, equitativa, libre y democrática generando modelos educativos, pedagógicos y didácticos de excelencia caracterizados por su rigor científico, enfoque de derechos y de interculturalidad, por lo tanto la Universidad Nacional de Educación considera a la información generada como un elemento fundamental para el cumplimiento de la misma.

Entendiendo que la información institucional es un activo que, como otros activos de la institución es esencial que sea protegido adecuadamente; la Universidad Nacional de Educación está comprometida con la protección de la información crítica asociada a los servicios y procesos de enseñanza, aprendizaje y de investigación y con la información generada por los departamentos administrativos de la Universidad.

El objetivo de la seguridad de la información es la de garantizar la calidad de la misma, buscando mantener la confidencialidad, la disponibilidad y la integridad de los datos generando estrategias que deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Es importante que el sistema de gestión de seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles.

2. Objetivos

Conocer sobre la opción "mesa de ayuda" implementada por la dirección de Soporte Tecnológico

Conocer la forma de ingreso y las opciones que nos brinda la mesa de ayuda

Evaluar todas las incidencias y requerimientos reportados en la mesa de ayuda

Política de Soporte Técnico

1. Mesa de Ayuda. GLPI
    a. La creación de los usuarios administrativos y académicos para el acceso a la plataforma de soporte será responsabilidad de la Dirección de Soporte Tecnológico.
    b. Las credenciales de acceso a la plataforma soporte.unae.edu.ec, serán las mismas que la del correo institucional.
    c. Todas las solicitudes de soporte técnico deberán ser registradas en la plataforma soporte.unae.edu.ec, la misma se recibirá y resolverá oportunamente.
    d. Sólo se atenderán solicitudes que se refieran al software y hardware de máquinas institucionales, es decir que cuenten con el número de inventario correspondiente a la Universidad Nacional de Educación.
    e. A través de las solicitudes registradas en la plataforma de servicio soporte.unae.edu.ec se cuantificará el servicio prestado y permitirá establecer programas de capacitación y/o adiestramiento enfocados a áreas o temas específicos, sustitución de equipo, etc.
    f. En cada uno de los soportes se dará prioridad a todos los requerimientos y/o incidencias registradas en la plataforma soporte.unae.edu.ec.
    g. Los tiempos de respuesta variarán dependiendo del número de soportes que se tengan en cola de atención.
    h. Se deberá especificar puntualmente el problema, sea este por requerimiento o por incidencia, como también especificar la ubicación del equipo a realizar el soporte.
    i. Antes de realizar cualquier apertura de casos de soporte mediante la plataforma, el usuario deberá asegurarse que él equipo no se encuentra apagado y/o desconectado.
2. Reservas
    a. La plataforma soporte.unae.edu.ec también ayudará a las reservas de:
        i. Auditorios
        ii. Laboratorios
        iii. Salas de Reunión
        iv. Y otros espacios que en el futuro se consideren reservables
    b. Las reservas pueden realizarse cuando el espacio reservable se encuentre disponible.
    c. La plataforma soporte.unae.edu.ec permite cancelaciones de reservas, las mismas que deberán ser realizadas por la persona que realizó dicha reserva.
    d. Las reservas se las podrán realizar de manera diaria, semanal, mensual.
    e. Todo caso creado y tratado dentro de la plataforma soporte.unae.edu.ec, enviará un registro de dicha actividad a los correos institucionales

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN

1. Introducción.

Como lo dice en su misión la Universidad Nacional de Educación tiene como misión contribuir a la formación de educadores y pedagogos que con sus modos de hacer, de pensar y de investigar transformen el Sistema Nacional Educativo a fin de construir una sociedad justa, equitativa, libre y democrática generando modelos educativos, pedagógicos y didácticos de excelencia caracterizados por su rigor científico, enfoque de derechos y de interculturalidad, por lo tanto la Universidad Nacional de Educación considera a la información generada como un elemento fundamental para el cumplimiento de la misma.

Entendiendo que la información institucional es un activo que, como otros activos de la institución es esencial que sea protegido adecuadamente; la Universidad Nacional de Educación está comprometida con la protección de la información crítica asociada a los servicios y procesos de enseñanza, aprendizaje y de investigación y con la información generada por los departamentos administrativos de la Universidad.

El objetivo de la seguridad de la información es la de garantizar la calidad de la misma, buscando mantener la confidencialidad, la disponibilidad y la integridad de los datos generando estrategias que deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Es importante que el sistema de gestión de seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles.

2. Objetivos

Garantizar el buen uso de los laboratorios mediante políticas que regulen el uso de los mismos.

Informar y asignar responsabilidades del cuidado de los laboratorios a los estudiantes, docentes y administrativos en el momento de reservar los mismos.

Política Uso laboratorios.

1. Uso de laboratorio
    a. Los Laboratorios de cómputo son para uso exclusivo de los estudiantes, personal académico y administrativo.
    b. Los laboratorios de cómputo tienen la capacidad de treinta (30) participantes.
    c. El usuario tendrá acceso al paquete de software y aplicaciones que estén disponible o instaladas en los equipos de cómputo en cada laboratorio
    d. El usuario debe preservar el orden y aseo del área en el cual este durante el servicio del laboratorio de computo.
    e. El uso de los laboratorios se regirá a los procesos de reservas de cada uno, el mismo que se lo realizara mediante la plataforma soporte.unae.edu.ec
    f. La plataforma para reservar los laboratorios se encontrará disponible las 24 horas los 365 días del año (soporte.unae.edu.ec).
    g. En referencia a préstamos de los laboratorios a instituciones públicas y/o privadas, estas deberán enviar la solicitud a la UNAE en la dirección Parroquia Javier Loyola (sector Chuquipata), Azogues en la provincia de Cañar, Ecuador para ser autorizadas por la máxima autoridad de la Universidad, y comunicar por medio del Sistema de Gestión Documental al Director Administrativo con copia a la Dirección de Soporte Tecnológico una vez aprobada la solicitud.
    h. Los usuarios (docentes, estudiantes, administrativos) deberán reportar cualquier anomalía a la Dirección de Soporte Tecnológico, en caso de no ser reportada el usuario que haya reservado el laboratorio será responsable de la anomalía que se presente.
    i. Queda totalmente prohibido:
        i. El ingreso a los Laboratorios con cualquier tipo de alimentos y bebidas.
        ii. Dejar cualquier tipo de basura.
        iii. Usar software indebido u ocasionar cualquier daño o modificación al existente.
        iv. Cambiar de lugar o modificar la conexión de cualquier dispositivo.
        v. Cualquier comportamiento que atente contra la integridad de los usuarios y elementos del laboratorio.
        vi. Utilizar el equipo de cómputo por más de dos usuarios.
    j. El equipo de cómputo es exclusiva responsabilidad del usuario, una vez que él se encuentre utilizándolo.
    k. Queda estrictamente prohibida la perturbación del ambiente del laboratorio por medios de altavoces o bocinas, siempre deberá ser con audífonos y a un volumen moderado.
    l. Es obligación del usuario al finalizar su jornada de trabajo apagar el CPU del equipo mediante el sistema operativo y el monitor mediante el botón de "Encendido".

m. Queda totalmente prohibido consultar páginas web que difundan contenido inapropiado o no académico (páginas con contenido pornográfico o de alta violencia, entre otras).
n. Es responsabilidad del usuario el manejo de información personal o confidencial, así como de sus cuentas y contraseñas usadas dentro del laboratorio.
o. Todos los laboratorios de la Universidad Nacional de Educación deberán contar con cámaras de monitoreo.

2. Responsabilidad del Usuario
   a. La Dirección de Soporte Tecnológico no se hace responsable por la pérdida de información o archivos que se guarden en los discos duros de las computadoras de los laboratorios, ya que éstas borran todos los cambios efectuados al apagar el equipo, y no existe forma de recuperar la información.
   b. La Dirección de Soporte Tecnológico no se hace responsable por la pérdida de dispositivos como memorias flash, cds, tablets, discos duros o cualquier otro artículo dejado en el laboratorio.
      i. La Dirección Administrativa será la responsable con la cual deberá comunicarse el usuario por artículos extraviados.
   c. El usuario que cause daño físico a la infraestructura de los Laboratorios de la Unidad de Informática, deberá realizar la sustitución o reparación correspondiente.
   d. Está prohibido mover o cambiar cualquier equipo, monitor o periférico de lugar.
   e. El uso de laptops en los laboratorios de cómputo queda a discreción del docente, los mismos deberán conectarse a internet mediante la red inalámbrica institucional.
3. Uso del Laboratorio para Clases
   a. Los docentes que deseen utilizar los Laboratorios de la Universidad Nacional de Educación deberán realizar la correspondiente reservación con no menos de 24 hrs. de antelación o de manera programada o calendarizada por medio de la plataforma soporte.unae.edu.ec
   b. Es responsabilidad del docente terminar la cátedra y retirar a los alumnos de los laboratorios una vez que finalice el horario asignado.
   c. El docente DEBERÁ permanecer en los Laboratorios mientras sus alumnos se encuentren dentro de las instalaciones.
   d. Los docentes serán responsables del comportamiento de los alumnos a su cargo.