POLÍTICA DE USO DE LA INFORMACIÓN, ACTIVOS DE INFORMACIÓN INSTITUCIONAL Y SEGURIDAD INFORMÁTICA

Aprobación: 20 de mayo de 2021 – Resolución RCP-152-2021.

Resolución Nro. RCP-152-2021

El Consejo Politécnico de la Escuela Politécnica Nacional

Considerando

Que el artículo 16 de la Constitución de la República del Ecuador reconoce como derecho de las personas, ejercidos en forma individual o colectiva, entre otros: "(…) 2. El acceso universal a las tecnologías de información y comunicación. (…)";

Que la Carta Fundamental del Estado determina, en su artículo 17: "El Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto: (…) 2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada (…)";

Que el artículo 18 de la Norma Suprema del Estado prescribe: "Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior. 2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información";

Que el artículo 66 de la Constitución de la República establece que se reconoce y garantiza a las personas, entre otros derechos: "(…) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley (…)";

Que el artículo 226 de la Constitución de la República prescribe: "Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución";

Que la Carta Fundamental del Estado reconoce, en su artículo 355, la autonomía de las universidades y escuelas politécnicas, que debe ser ejercida y comprendida de manera solidaria y responsable, garantizando esta el ejercicio de la libertad académica y el derecho a la búsqueda de la verdad, sin restricciones, el gobierno y gestión de sí mismas, en consonancia con los principios de alternancia, transparencia y los derechos políticos, así como la producción de ciencia, tecnología, cultura y arte;

Que el artículo 39 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconoce el acceso universal, libre y seguro a entornos digitales, al señalar: "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 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 40 del Código en referencia establece: "El Estado garantizará el acceso universal al servicio público de internet en los términos previstos en la Constitución de la República (…). Las universidades y escuelas politécnicas deberán poner a disposición acceso a internet inalámbrico libre y gratuito en toda el área de sus sedes y extensiones. (…)";

Que el artículo 1 de la Ley Orgánica de Transparencia y Acceso a la Información Pública reconoce el principio de publicidad de la información pública, al establecer: "El acceso a la información pública es un derecho de las personas que garantiza el Estado. Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONGs), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley";

Que el artículo 5 de la referida Ley establece: "Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado";

Que el artículo 6 de la Ley ibídem determina: "Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República. El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes (…)";

Que el artículo 10 de la Ley Orgánica de Transparencia y Acceso a la Información Pública establece: "Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y

documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción. Quienes administren, manejen, archiven o conserven información pública, serán personalmente responsables, solidariamente con la autoridad de la dependencia a la que pertenece dicha información y/o documentación, por las consecuencias civiles, administrativas o penales a que pudiera haber lugar, por sus acciones u omisiones, en la ocultación, alteración, pérdida y/o desmembración de documentación e información pública. Los documentos originales deberán permanecer en las dependencias a las que pertenezcan, hasta que sean transferidas a los archivos generales o Archivo Nacional (…)";

Que el segundo inciso del artículo 9 de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos determina: "La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente";

Que la Disposición Transitoria Novena de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, con respecto a los datos personales, establece: "son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley";

Que el apartado 410-04 de las Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos establece: "La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria. La Unidad de Tecnología de Información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran. Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales, además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información (…)";

Que el apartado 410-10 de las Normas ibídem determina: "La Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas: 1. Ubicación adecuada y control de acceso físico a la Unidad de Tecnología de Información y en especial a las áreas de: servidores, desarrollo y bibliotecas. 2. Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado. 3. En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación. 4. Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización. 5. Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados. 6. Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire controlado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros; 7. Consideración y disposición de sitios de procesamiento alternativos. 8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana";

Que el artículo 19 del Estatuto de la Escuela Politécnica Nacional prescribe que el Consejo Politécnico es el órgano colegiado superior de la Escuela Politécnica Nacional y se constituye en la máxima autoridad de esta institución de educación superior;

Que conforme lo establece el artículo 21 del Estatuto de esta Escuela Politécnica, son funciones y atribuciones del Consejo Politécnico, entre otras: "e) Dictar, reformar, derogar e interpretar los reglamentos generales y especiales, así como tomar las resoluciones que creen o extingan derechos y obligaciones en el ámbito institucional";

Que a través de Resolución Administrativa No. 218-2013, de 07 de noviembre de 2013, se aprobó el Instructivo General de Seguridad y Uso adecuado de las Tecnologías de la Información y Comunicación;

Que mediante Memorando EPN-DGIP-2016-885-M, del 15 de agosto de 2016, el Director de Gestión de la Información y Procesos, en la referida fecha, remitió al Director de Asesoría Jurídica de ese entonces el Acta de Constitución del Proyecto de Centro de Respuesta a Incidentes de Seguridad Informáticos (CSIRT-EPN);

Que el Consejo Politécnico conoció la propuesta de "Política de uso de la información, activos de información institucional y seguridad informática", remitida por la Dirección de Gestión de la Información y Procesos, en las sesiones ordinarias efectuadas el 03 de octubre y el 23 de noviembre de 2018;

Que en las sesiones referidas en el considerando que antecede, los miembros de Consejo Politécnico solicitaron que la mencionada propuesta sea revisada por profesores de esta Institución de Educación Superior relacionados con su temática y que esta se actualice, previo a la adopción de una resolución;

Que mediante Memorando EPN-DGIP-2019-0039-M, de 16 de enero de 2019, el Director de Gestión de Información y Procesos, considerando lo solicitado por Consejo Politécnico, en las sesiones ordinarias efectuadas el 03 de octubre y 23 de noviembre de 2018, solicitó a los profesores Ph.D. Jenny Torres y M.Sc. Gabriel López lo siguiente: "(...) revisar y sugerir los cambios que consideren necesarios para mejorar la Política de Uso de la Información, Activos de Información Institucional y Seguridad Informática, la misma que es para beneficio de toda la Institución y que deberá ser acatada por toda la Comunidad Politécnica";

Que a través de Memorando EPN-DGIP-2020-0452-M, de 29 de mayo de 2020, el Director de Gestión de Información y Procesos solicitó a la Directora de Asesoría Jurídica la emisión de un criterio jurídico con respecto al "Proyecto de Política de Uso de la Información, Activos de Información Institucional y Seguridad Informática", previa aprobación por parte del Consejo Politécnico, considerando que se han solventado las observaciones y se han incluido las recomendaciones realizadas por los profesores encargados de su revisión;

Que mediante Memorando EPN-DAJ-2020-0308-M, de 15 de junio de 2020, la Directora de Asesoría Jurídica remitió el informe relativo al Proyecto referido en el considerando que precede;

Que a través de Memorando EPN-DAJ-2020-0712-M, de 14 de diciembre de 2020, la Directora de Asesoría Jurídica corroboró las observaciones que no habían sido estimadas y se mantenían en el Proyecto aludido en considerandos que preceden;

Que a través de Memorando EPN-DGIP-2021-0001-M, de 04 de enero de 2021, el Director de Gestión de Información y Procesos, en lo principal, comunicó a la Directora de Asesoría Jurídica: "(...) se han insertado las recomendaciones brindadas por la Dirección Jurídica, para su revisión final, previo el envío de la política, para la aprobación por Consejo Politécnico";

Que mediante Memorando EPN-DAJ-2021-0031-M, de 15 de enero de 2021, la Directora de Asesoría Jurídica remitió, para conocimiento del Director de Gestión de Información y Procesos, el "Informe emitido sobre la revisión de Política de uso de la Información, activos de información institucional y seguridad informática";

Que a través de Memorando EPN-DGIP-2021-0198-M, de 10 de marzo de 2021, el Director de Gestión de Información y Procesos comunicó a la Directora de Asesoría Jurídica lo siguiente: "(...) adjunto encuentre Usted el documento actualizado de la "POLÍTICA DE USO DE LA INFORMACIÓN, ACTIVOS DE INFORMACIÓN INSTITUCIONAL Y SEGURIDAD INFORMÁTICA" una vez que se han insertado las recomendaciones brindadas por la DAJ en cuanto a los considerandos y se han solventado las observaciones finales emitidas por los docentes encargados de la revisión (...)";

Que mediante Memorando EPN-DAJ-2021-0195-M, de 28 de marzo de 2021 la Directora de Asesoría Jurídica emitió el informe sobre la revisión del proyecto de la Política de uso de la Información, activos de información institucional y seguridad informática, en el cual, en lo principal, se concluye: "(...) el Proyecto de Política establece los lineamientos de actuación de la Comunidad Politécnica en relación con los recursos, servicios, y seguridad de información, como componentes que permitan el aseguramiento de la calidad y la consecución de los objetivos y misión institucionales, en tanto guarden conformidad con las disposiciones legales, reglamentarias vigentes. Es menester indicar que la presente revisión se limita al contexto legal del proyecto, por lo que el contenido

de índole técnico, es responsabilidad exclusiva de la unidad requirente (…)";

Que a través de Memorando EPN-DGIP-2021-0269-M, de 06 de abril de 2021, el Director de Gestión de Información y Procesos de la Escuela Politécnica Nacional remitió, para conocimiento de Consejo Politécnico, el Informe Motivado para la Revisión y Aprobación del proyecto de "Política de Uso de la Información, Activos de Información Institucional y Seguridad Informática", el cual fue expuesto a tal Órgano en la sesión desarrollada el 22 de abril de 2021;

Que mediante Acuerdo ACP-041-2021, de 22 de abril de 2021, el Consejo Politécnico decidió: "Dar por conocida la presentación realizada por el Director de Gestión de la Información y Procesos, relativa al proyecto de Política de Uso de la Información, Activos de Información Institucional y Seguridad Informática. En una siguiente sesión se tratará la aprobación del Proyecto de Política que se ha puesto en conocimiento de este Consejo. Los miembros de Consejo Politécnico podrán realizar observaciones al referido Proyecto hasta el 18 de mayo de 2021, las cuales serán enviadas a Secretaría General, con copia a la Dirección de Gestión de la Información y Procesos. El documento que contiene la Política en referencia es parte integrante de este Acuerdo";

Que una vez receptadas las observaciones al Proyecto de Política de Uso de la Información, Activos de Información Institucional y Seguridad Informática, el Consejo Politécnico conoció y analizó los numerales sobre los cuales se plantearon observaciones;

Que tras conocerse las observaciones realizadas por los miembros del Consejo Politécnico al Proyecto aludido, estas se procesaron y se concilió su texto definitivo;

Que la modernidad exige a las entidades, privadas y públicas, resguardar su patrimonio, bienes y activos, incluyendo su información institucional y datos informáticos;

Que es necesario que la Escuela Politécnica cuente con una política de uso de la información, activos de información institucional y seguridad informática, que propenda a prevenir el uso indebido de tales activos de información, así como proteger, resguardar y asegurar su adecuada disponibilidad, integridad y confidencialidad; y,

en ejercicio de sus facultades y atribuciones, establecidas en la normativa vigente, **expide la siguiente**:

POLÍTICA DE USO DE LA INFORMACIÓN, ACTIVOS DE INFORMACIÓN INSTITUCIONAL Y SEGURIDAD INFORMÁTICA

1.- DECLARACIÓN DE LA POLÍTICA

La Escuela Politécnica Nacional – EPN declara como política el diseñar, implementar, mantener, mejorar y cumplir, de manera continua, con un Sistema de Gestión de Seguridad de la Información propio (SGSI), acorde a la realidad institucional y apegado a estándares como la NTE INEN-ISO/IEC 27001:2013, preservando la confidencialidad, integridad y disponibilidad de la información, realizando actividades de formación y concientización en materia de los procesos de seguridad de la información y monitoreo de los cambios significativos de los riesgos que puedan afectar la información frente a las amenazas más importantes.

2.- OBJETIVO

Disponer de una política de seguridad y uso adecuado de Tecnologías de la Información y Comunicación (TIC), a fin de prevenir el uso inadecuado de los activos de información, así como proteger, resguardar y asegurar la disponibilidad, integridad y confidencialidad de estos y lo que en ellos se genera, como apoyo a los objetivos estratégicos de la Institución.

3.- DEL ÁMBITO DE APLICACIÓN:

Esta política será de aplicación para todos los miembros de la comunidad politécnica, incluyendo usuarios externos y público en general que, por algún motivo justificado, manejen o accedan a los activos de información institucionales.

La seguridad de la información demanda la participación y el apoyo de autoridades, personal académico, personal de apoyo académico, servidores, trabajadores y estudiantes de la EPN, quienes interactúan con los activos de información institucionales.

4.- DEFINICIONES:

Para la aplicación de esta Política, se considerarán las siguientes definiciones:

Activos de Información Crítica: Son los activos de información indispensables para la operación de la Institución (como, por ejemplo: información de

configuraciones sobre sistemas operativos, software de bases de datos, código fuente y aplicaciones sensibles de los activos).

Activos de información Institucional: Un activo de información es todo lo que procesa, genera o almacena información relacionada a los distintos procesos de la EPN, como pueden ser hardware, software, documentos físicos, documentos electrónicos, entre otros.

Aplicaciones Institucionales: Software desarrollado o adquirido por la EPN con el fin de prestar un servicio y apoyar las actividades de la Institución.

Cifrado: Transformación criptográfica de datos (denominada "texto sin formato") en una forma diferente (llamada "texto cifrado") que oculta el significado original de los datos y evita que la forma original de estos sea usada. El proceso inverso correspondiente es el “descifrado", que representa una transformación que restaura los datos cifrados a su forma original. [1]

Comunidad politécnica: Son todas las autoridades, miembros del personal académico, personal de apoyo académico, servidores, trabajadores y estudiantes de la EPN.

Confidencialidad: Propiedad que implica que la información no está disponible o no es divulgada a personas, entidades o procesos no autorizados. [6]

Credenciales institucionales: Es la cuenta creada en un sistema de información de la Institución que posibilita realizar o ejecutar un determinado proceso, función o actividad. Esta puede ser asignada a un usuario, un área o un servicio.

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de los establecido en la Ley de Comercio Electrónico, Firmas y Mensajes de Datos. [3]

Disponibilidad: Propiedad de estar disponible y utilizable en el momento que sea requerido por una entidad autorizada. [6]

Dispositivo tecnológico: Cualquier objeto o sistema que tenga la funcionalidad de procesar datos electrónicos o conectarse a redes informáticas, tales como: servidores físicos o virtuales, computadoras de escritorio, tabletas, dispositivos móviles, entre otros.

Hardware: Componentes físicos de un sistema de información. [1]

Información confidencial: Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución de la República. [2]

La información que afecte a la intimidad de la persona o cuyo uso indebido genere discriminación, revele su origen étnico, su vida afectiva y familiar, creencias religiosas, filiación o pensamiento político, condición migratoria, su vida sexual o reproductiva, su orientación sexual, identidad de género, datos biométricos, cuyo uso público atente contra los derechos humanos consagrados en la Constitución de la República e Instrumentos Internacionales, se considera información confidencial.

Información Crítica: Es la información que se considera indispensable para la operación de la Institución (ejemplo: datos personales, información académica, entre otros).

Información Institucional: Se considera información institucional todo documento, en cualquier formato, físico y/o digital, generado en los activos de información institucional o por los miembros de la comunidad politécnica, en el ámbito de su competencia, como parte de la EPN.

Información oficial: Se considera información oficial de la EPN toda aquella información o anuncio emitido únicamente desde los canales oficiales institucionales.

Integridad: Propiedad de proteger la precisión y completitud de los activos. [6]

Mensaje de datos: Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio.

Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, fax e intercambio electrónico de datos. [3]

Protección de datos: El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de tal carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información, requerirán la autorización del titular o el mandato de la ley. [4]

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. [6]

Sistemas de Información: Conjunto organizado de recursos y procedimientos de computación y comunicación; es decir, equipos y servicios, junto con su infraestructura, instalaciones y personal de apoyo, que crean, recopilan, registran, procesan, almacenan, transportan, recuperan, exhiben, difunden, controlan o proporcionan información para realizar un conjunto de funciones. [1]

Software: Programas de computadora (que se almacenan y se ejecutan en el hardware de la computadora) y datos asociados (que también se almacenan en el hardware) que se pueden escribir o modificar dinámicamente durante la ejecución. [1]

Software Malicioso: Hardware, firmware o software que se incluye intencionalmente o se inserta en un sistema para un propósito dañino. Un programa que se inserta en un sistema, generalmente de forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o sistema operativo de la víctima, o de molestar o interrumpir a la víctima. [1][5]

Usuarios de los activos de información: Se considera usuario interno de la información a todo miembro de la comunidad politécnica.

Usuarios Externos: Se consideran usuarios externos de los activos de información a quienes no forman parte de la comunidad politécnica y que requieren acceso a los activos de información de la Institución, amparados en la ejecución de actividades de gestión, académicas, de investigación, vinculación y actividades de auditoría, evaluación y control.

Virus: Sección auto replicante (y generalmente oculta) de software (generalmente lógica maliciosa) que se propaga al infectar; es decir, al insertar una copia de sí mismo en otro programa y convertirse en parte de este. Un virus no puede correr solo, requiere que su programa host se ejecute para activarse. [1]

DEL USO DE LA INFORMACIÓN Y LOS ACTIVOS DE INFORMACIÓN INSTITUCIONAL:

5.- PROPIEDAD Y USO:

Toda la información generada y/o contenida en los activos de información institucionales, excluyendo la información personal de los miembros de la comunidad politécnica, es propiedad de la EPN.

Toda la información generada en activos de información que no son institucionales, producto del ámbito de competencia de los miembros de la comunidad politécnica, es propiedad de la EPN.

Toda información y activo de información institucional, se utilizará y estará, en forma exclusiva, al servicio de los intereses de la EPN y de sus dependencias.

Es responsabilidad de los miembros de la comunidad politécnica el uso adecuado de la información, así como de los activos de información institucionales.

La Dirección de Gestión de Información y Procesos (DGIP) podrá definir las características técnicas generales que sirven como línea base para la adquisición de activos de información institucional.

La DGIP podrá presentar directrices y/o procedimientos para que los activos de información se encuentren actualizados y asegurados.

El Centro de Respuesta a Incidentes de Seguridad Informáticos (CSIRT-EPN) podrá gestionar mecanismos para la protección de los activos de información institucionales.

El CSIRT-EPN podrá realizar evaluaciones técnicas en los activos de información de propiedad de la EPN e informará al Rector y/o Vicerrectores sobre actividades consideradas no permitidas con respecto a tales activos.

El uso o divulgación ilegal o inadecuada de información personal o activos de información institucional dará lugar a las acciones legales y disciplinarias pertinentes.

No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el

ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas. [2]

6.- RESPALDOS DE INFORMACIÓN:

La DGIP generará y gestionará los respaldos de los activos de información críticos, así como de la información crítica institucional de las diferentes Unidades Académicas y Administrativas de la EPN.

Los respaldos de los activos de información críticos, así como de la información crítica institucional de las diferentes Unidades Académicas y Administrativas de la EPN, deben almacenarse de manera cifrada, fuera de la Institución, de acuerdo a la Directriz de Cifrado Aceptable de la EPN.

Es responsabilidad de cada miembro de la comunidad politécnica realizar respaldos de la información que genera, inherente a las actividades institucionales.

La DGIP deberá generar y podrá actualizar el procedimiento para "Generar y Gestionar los respaldos de los activos de información críticos e información crítica institucional"

7.- DESTRUCCIÓN DE INFORMACIÓN:

Los respaldos de los activos de información críticos, así como la información crítica institucional de las diferentes Unidades Académicas y Administrativas de la EPN que se encuentren desactualizados y no sean necesarios serán destruidos.

Las autoridades académicas y administrativas autorizarán la destrucción de los respaldos de los activos de información críticos, así como de la información crítica institucional de las diferentes Unidades Académicas y Administrativas de la EPN, con base en el procedimiento "Destrucción de respaldos de los activos de información críticos e información crítica institucional", generado y actualizado por la DGIP.

8.- ACUERDOS DE CONFIDENCIALIDAD Y NO DIVULGACIÓN:

La DGIP gestionará los acuerdos de confidencialidad y no divulgación de la Información con los miembros de la comunidad politécnica.

La DGIP gestionará los acuerdos de confidencialidad y no divulgación de la Información con los proveedores contratados u otras instituciones públicas o

privadas que requieren acceso a los activos de información o información institucional.

9.- USO DE ANTIVIRUS:

Todos los dispositivos tecnológicos de propiedad de la EPN tendrán instalado el antivirus proporcionado por la DGIP.

Todos los dispositivos tecnológicos que no son de propiedad de la Institución que se conecten a la red de la EPN tendrán instalado un antivirus, si estos dispositivos tecnológicos no cuentan con un antivirus, el dueño de la misma debe informar aquello a la DGIP, para que se tomen las respectivas medidas de contención.

La DGIP podrá desconectar los dispositivos tecnológicos de la red, cuando encuentre en estos virus o software malicioso, producto de la omisión o falta de uso de un antivirus.

La DGIP deberá generar y podrá actualizar procedimientos para el uso del antivirus institucional, tendientes a la regulación y control de este.

10.- CONTROL DE ACCESO

Todos los sistemas de información que adquiera y/o desarrolle la EPN deben contar con mecanismos de control y autenticación cifrados para el acceso a los mismos, como, por ejemplo: uso de cuentas de usuarios, contraseñas, doble autenticación, registro de acceso, permisos, entre otros mecanismos, la creación de la contraseña con base a la "Directriz de Manejo de contraseñas".

La DGIP, conjuntamente con el CSIRT-EPN, deberán generar y podrán actualizar las directrices que consideren adecuadas para realizar el respectivo control de acceso, como, por ejemplo: la "Directriz de Control de Acceso a los Servicios y Aplicaciones de TI de la EPN", la "Directrices de clasificación y acceso a la información", instructivos y protocolos derivados.

11.- USO DEL CORREO ELECTRÓNICO INSTITUCIONAL:

Las cuentas de correo electrónico institucional son generadas por la DGIP, con el empleo de dominios válidos autorizados por la EPN.

Las cuentas de correo electrónico institucional deben ser utilizadas con el fin de enviar y recibir mensajes de datos inherentes a las actividades institucionales.

Las cuentas de correo electrónico institucional no deben ser usadas para esparcir contenidos discriminatorios, despectivos, difamatorios, acosadores o violentos.

La DGIP deberá generar y podrá actualizar la directriz para el "Uso del Servicio de Correo Electrónico Institucional", la cual incluye normas de desactivación de cuentas, entre otros.

El contenido de los correos electrónicos es personal y no podrá ser accedido o entregado a otra persona (no titular), incluso por disposición del Rector de la EPN, salvo los casos solicitados con orden judicial.

Los usuarios de las cuentas de correo electrónico son los responsables del contenido emitido y enviado en los mensajes electrónicos, así como de la información adjunta que se remita.

12.- USO DEL INTERNET:

El internet debe estar disponible para todos los miembros de la comunidad politécnica.

El uso del internet de la EPN se destina a fines académicos, de investigación, administrativos y de vinculación.

El uso de blogs, redes sociales, contenedores de video, entre otros, por parte de los miembros de la comunidad politécnica, está limitado según el perfil de los usuarios y, en forma ocasional, fuera de horario de trabajo, para que tal uso no interfiera en las labores diarias de estos.

El buen uso de los recursos referidos, para actividades académicas, no está restringido.

Los usuarios del servicio de internet provisto por la EPN deben conocer y cumplir con la "Directriz de Uso de Internet".

Queda prohibido el esparcir o difundir contenidos discriminatorios, despectivos, difamatorios o acosadores, así como cualquier otro contrario a la legalidad o la ética, así como el envío de mensajes no relacionados con los objetivos de la Institución, empleando la infraestructura de la EPN.

13.- INSTALACIÓN DE SOFTWARE:

El software y aplicaciones que se instalan en los dispositivos tecnológicos que pertenecen a la EPN deben ser licenciados.

No está permitida la instalación de software o aplicaciones piratas o de dudosa procedencia.

La DGIP podrá desinstalar todo software y/o aplicación pirata o de dudosa procedencia que se haya configurado en los dispositivos tecnológicos de la Institución.

14.- INFORMACIÓN CONFIDENCIAL:

La DGIP deberá generar y podrá actualizar procedimientos para que se apliquen criterios de confidencialidad en los sistemas de información.

Los datos personales de los miembros de la comunidad politécnica son confidenciales y podrán ser utilizados solamente para fines de gestión, investigación, docencia y vinculación de la EPN, previa autorización de sus titulares, conforme lo dispone la normativa legal vigente.

El CSIRT-EPN implementará y difundirá buenas prácticas de seguridad que contemplen la sensibilización en los temas de información confidencial a la comunidad politécnica.

15.- CREDENCIALES DE ACCESO A LOS ACTIVOS DE INFORMACIÓN INSTITUCIONAL:

Las credenciales de acceso a los activos de información son personales e intransferibles y no deben ser expuestas en sitios visibles.

La DGIP notificará a la Dirección de Talento Humano en caso de detectar que cualquier autoridad, miembro del personal académico, personal de apoyo académico, servidores y trabajadores, utiliza inadecuadamente sus credenciales de acceso entregándolas a cualquier persona, sea ésta de la Comunidad Politécnica o un usuario externo, como lo establece el acuerdo de confidencialidad del empleado.

Es responsabilidad de cada miembro de la comunidad politécnica acatar y cumplir todas las disposiciones y procedimientos establecidos, para mantener la confidencialidad en el uso de credenciales institucionales de acceso a los

activos de información.

16.- PROPIEDAD INTELECTUAL:

Toda la obra científica, de investigación, de trabajo de titulación, de software, bases de datos, entre otros, generados con los recursos institucionales y por algún miembro de la comunidad politécnica, con base en sus actividades institucionales, debe registrarse, según sea el caso, de acuerdo con la normativa legal vigente referente a propiedad intelectual.

17.- SEGURIDADES DE REDES LAN E INALÁMBRICA:

La DGIP podrá implementar filtros para todo el tráfico entre el Internet y la red LAN e inalámbrica de la EPN, utilizando para el efecto herramientas especializadas.

La DGIP podrá activar el cifrado, autenticación y autorización en las redes LAN e inalámbricas para mantener limitado el acceso a estas.

18.- SEGURIDADES DE REDES PRIVADAS VIRTUALES (VPN):

Toda conexión a la red de la EPN mediante el uso de VPN será autorizada y monitoreada por la DGIP.

19.- REDES INALÁMBRICAS NO AUTORIZADAS:

Está prohibida la instalación en la red de la EPN de todo dispositivo (puntos de acceso, routers inalámbricos, entre otros) que no haya sido verificado y validado por la DGIP.

La DGIP podrá, mediante informe técnico, retirar y desinstalar el servicio prestado por dispositivos no autorizados.

20.- AUDITORÍA Y EVALUACIÓN DE VULNERABILIDADES:

El CSIRT-EPN verificará el cumplimiento de la normativa interna relacionada con seguridad informática, así como el seguimiento a las recomendaciones emitidas en informes ante los incidentes de seguridad informática que se han gestionado.

El CSIRT-EPN podrá realizar auditorías y/o revisiones de seguridad informática, con periodicidad anual.

El CSIRT-EPN podrá analizar, dar soporte y coordinar la respuesta a los incidentes de seguridad informática que se presenten con los activos de información institucionales.

El CSIRT-EPN podrá gestionar las vulnerabilidades detectadas en los activos de información institucional.

Los resultados de las evaluaciones y auditorias de seguridad informática podrán ser comunicados por el CSIRT-EPN, al Director de Gestión de Información y Procesos y al Rector de la Institución.

ÁMBITO DE SANCIONES

21.- MEDIDAS CORRECTIVAS O DISCIPLINARIAS:

La DGIP deberá notificar el incumplimiento de lo establecido en la presente Política al Rector y a los Vicerrectores, para establecer las medidas correctivas o disciplinarias a las que hubiere lugar, de conformidad con el artículo 207 de la Ley Orgánica de Educación Superior, artículo 43 de la Ley Orgánica del Servicio Público, artículo 80 del Reglamento General a la Ley Orgánica del Servicio Público, artículo 46 del Código del Trabajo, conjuntamente con el Reglamento Interno de Trabajo de la Escuela Politécnica Nacional y su Estatuto, además de lo indicado en el numeral 6.2 de la Directriz General Cumplimiento de Regulaciones de Seguridad de la Información e Infracciones, aplicable para autoridades, personal académico, personal de apoyo académico, servidores, trabajadores y estudiantes.

DISPOSICIONES GENERALES

PRIMERA.- En todo lo no previsto en esta Política, de acuerdo a la naturaleza de control y administración de bienes y normativa que la regula, se aplicarán, según corresponda, las leyes y reglamentos vigentes y demás instrumentos jurídicos que tengan relación con los mismos.

SEGUNDA.- Para la aplicación de la presente Política, se considerarán incorporadas todas las Directrices, Procedimientos y normativa en general relacionada con la Seguridad Informática y las Tecnologías de Información y Comunicación generadas por la DGIP.

TERCERA.- Encárguese al Director de la DGIP la actualización, de ser el caso, de las Directrices, Procedimientos y demás normativa relacionada con las Tecnologías de Información y Comunicación.

CUARTA.- Encárguese al Oficial de Seguridad de la Información (OSI) la actualización, de ser el caso, de toda la normativa de seguridad informática y de información relacionada.

QUINTA.- Encárguese al OSI la difusión, socialización, implementación y ejecución de la presente Política.

SEXTA.- Desagréguese la estructura y funcionalidad del CSIRT-EPN de la DGIP.

SEPTIMA.- La presente Política entra en vigencia a partir de su aprobación.

OCTAVA.- Se encarga al OSI la generación de una directriz para la gestión de la información no crítica.

DISPOSICIÓN DEROGATORIA

Se deroga el "Instructivo General de Seguridad y Uso Adecuado de las Tecnologías de la Información y Comunicación", así como las demás normas de igual o menor jerarquía emitidas con anterioridad, que se opongan a la presente Política.

REFERENCIAS DE LA POLÍTICA

[1] IETF RFC 4949 Ver 2. Internet Security Glossary, páginas 119, 140, 153, 288, 185 y 333, https://www.rfc-editor.org/rfc/pdfrfc/rfc4949.txt.pdf
[2] Ley Orgánica de acceso y Transparencia a la información Pública, Art. 6
[3] Ley de Comercio Electrónico, Firmas y Mensajes de Datos, Disposición general novena.
[4] Constitución de la República., Art. 66 numeral 19.
[5] NIST SP 800-61 Rev. 1, página 60, Computer Security Incident Handling Guide.
[6] NTE INEN-ISO/IEC 27000:2012, páginas 2 y 3, sección 2, Términos y definiciones.

DISPOSICIÓN FINAL

La presente Política fue aprobada por el Consejo Politécnico, en su Décima Sesión Ordinaria, efectuada el 20 de mayo de 2021, a través de Resolución RCP-152-2021.

Firmado electrónicamente por:
FERNANDO JAVIER
CALDERON ORDONEZ

Ab. Fernando Calderón Ordóñez
SECRETARIO GENERAL EPN