2026

ESCUELA DE ARTES PLÁSTICAS Y DISEÑO

Manual de Políticas de la Oficina de Tecnología

Realizado por: Sr. Roldan Roldán, Oficial Principal de Informática

TABLA DE CONTENIDO

Política de Seguridad de la Información

Propósito

Esta política establece los lineamientos para proteger la confidencialidad, integridad y disponibilidad de la información institucional de la EAPD durante el año académico 2025-2026 y en adelante.

Alcance

Aplica a todo el personal administrativo, académico, estudiantes y contratistas que utilicen los sistemas de información y redes de la institución.

Disposiciones de la Política

1. ***Protección de la información institucional:*** Toda información generada, recibida, almacenada o transmitida por la institución deberá ser protegida contra accesos no autorizados, alteración, divulgación indebida o destrucción.
2. ***Clasificación y manejo de la información***: La información institucional deberá clasificarse de acuerdo con su nivel de sensibilidad (pública, interna, confidencial o restringida) y su manejo deberá realizarse conforme a los controles establecidos para cada nivel.
3. ***Almacenamiento y transmisión de los datos:*** Los datos sensibles (académicos, financieros, de investigación y personales) deben almacenarse y transmitirse mediante cifrado aprobado (AES-256, TLS 1.2 o superior).
4. ***Cumplimiento con leyes y reglamentos aplicables:*** La gestión de la información deberá cumplir con las leyes, reglamentos y normativas aplicables relacionadas con privacidad, protección de datos y acceso a la información pública. Esto incluye la prohibición de utilizar dispositivos no autorizados para acceder a la red de la institución.
5. ***Revisión y actualización de la política:*** Esta política será revisada periódicamente para garantizar su vigencia y alineación con los cambios tecnológicos, operacionales y regulatorios. Adicionalmente, la Oficina de Tecnología realizará auditorías periódicas de seguridad para validar cumplimiento.

Definiciones de Términos

Datos Sensibles: Información académica, financiera, personal, de salud, investigativa o cualquier dato que requiera regulación y/o protección por ley.

Dispositivo No Autorizado: Equipo tecnológico personal o externo que no haya sido aprobado por la Oficina de Tecnología para acceder a los sistemas institucionales.

Información Institucional: Toda información, documento, archivo, comunicación, dato o material digital creado, procesado, recibido o almacenado utilizando computadoras, cuentas, sistemas, redes o servicios en la nube provistos por la EAPD.

Sistema Institucional: Cualquier computadora, servidor, red, aplicación, plataforma en la nube o recurso tecnológico propiedad de la EAPD o administrado en su nombre.

Usuario: Cualquier empleado, facultad, estudiante, contratista o tercero autorizado a utilizar los sistemas institucionales.

Responsabilidades

A. **La institución a través de la Oficina de Tecnología**:
La EAPD, a través de la Oficina de Tecnología, será responsable de establecer, implementar y mantener las medidas necesarias para proteger la seguridad, confidencialidad, integridad y disponibilidad de la información institucional. Entre sus responsabilidades se incluyen, pero no se limitan a:
    - Desarrollar, implementar y mantener políticas, normas y procedimientos relacionados con la seguridad de la información y el uso seguro de los recursos tecnológicos de la institución.
    - Administrar y proteger la infraestructura tecnológica de la institución.
    - Establecer controles de acceso a los sistemas y recursos tecnológicos.
    - Gestionar copias de seguridad y mecanismos de recuperación de la información institucional para garantizar la continuidad de las operaciones en caso de incidentes o fallas tecnológicas.
    - Monitorear el uso de los sistemas tecnológicos institucionales conforme a las leyes y reglamentos aplicables, con el propósito de identificar riesgos, incidentes de seguridad o uso indebido de los recursos.
    - Atender y gestionar incidentes de seguridad de la información, incluyendo la investigación, documentación y mitigación de riesgos asociados.
    - Proveer orientación y capacitación a toda la comunidad universitaria autorizada al uso de los recursos tecnológicos sobre las mejores prácticas para la protección de la información y el uso seguro de la tecnología.
    - Velar por el cumplimiento de las leyes, reglamentos y normativas aplicables en materia de seguridad de la información.

B. **Usuarios**:
Todos los usuarios de los sistemas y recursos tecnológicos institucionales, incluyendo estudiantes, empleados, facultad, contratista y cualquier persona autorizada, tendrá las siguientes responsabilidades:
    - Utilizar los recursos tecnológicos de manera responsable y para fines legítimos, relacionados con funciones académicas, administrativas o institucionales autorizadas.
    - Proteger sus credenciales de acceso

- Cumplir con las políticas, normas y procedimientos institucionales relacionados con la seguridad de la información y el uso de los recursos tecnológicos.
- Proteger la información institucional de la cual tenga acceso evitando comprometer la seguridad de la información.
- Evitar la instalación o uso de programas “software” no autorizados en los equipos o sistemas institucionales.
- Reportar inmediatamente a la Oficina de Tecnología cualquier situación, incidente de seguridad, pérdida de equipo o intento de acceso no autorizado que pueda comprometer la seguridad de la información.

Cumplimiento / Sanciones

El incumplimiento de esta política puede conllevar sanciones administrativas según establecidas en las Normas de Conducta y Medidas Correctivas Aplicables a Empleados y Funcionarios de la Escuela de Artes Plásticas y Diseño de Puerto Rico.

Referencias

- PRITS – Política de Seguridad de la Información del Gobierno de Puerto Rico.
- NIST SP 800-53 – “Security and Privacy Controls for Federal Information Systems”
- ISO/IEC 27001:2013 – Sistemas de Gestión de Seguridad de la Información.

Certificación y aprobación

Esta política ha sido revisada y aprobada conforme a las disposiciones institucionales vigentes y entrará en vigor a partir de la fecha de su firma.

Nombre y firma de la Autoridad Nominadora:

Dra. Ileana Muñoz Landrón

Dra. Ileana Muñoz Landrón (Mar 18, 2026 14:39:04 EDT)

Fecha: 18/03/2026

Política de Uso Aceptable de Tecnología

Propósito

El propósito de esta política es establecer normas para el uso correcto de los recursos tecnológicos de la EAPD, incluyendo computadoras, redes, impresoras, dispositivos móviles, correo electrónico institucional y acceso a internet.

Alcance

Aplica a todo el personal administrativo, académico, estudiantes y contratistas con acceso a los sistemas.

Disposiciones de la Política

1. Los recursos tecnológicos se utilizarán exclusivamente para fines académicos, administrativos y de investigación autorizados por la EAPD.
2. Se prohíbe el acceso, almacenamiento o distribución de material ilegal, ofensivo o que atente contra la seguridad (ej. pornografía explícita, apuestas, "malware").
3. Está prohibido instalar programas "software" no autorizado o sin licencia.
4. Los usuarios deberán respetar la privacidad y propiedad intelectual de terceros.
5. El uso de la red institucional será monitoreado conforme a las regulaciones aplicables para garantizar la seguridad y el cumplimiento de las políticas.
6. Toda información, documento, archivo, comunicación o dato creado, procesado o almacenado en computadoras, cuentas institucionales, sistemas, servidores o servicios en la nube provistos por la EAPD es propiedad exclusiva de la institución. Los usuarios reconocen que la institución puede acceder a esta información para fines operacionales, auditorías, investigaciones de incidentes, cumplimiento regulatorio o continuidad de servicios.

Definiciones de Términos

Correo Electrónico Institucional: Las cuentas de correo electrónico provistas y administradas por la EAPD para toda comunicación oficial de las áreas administrativas, académicas y estudiantiles.

Fines Académicos, Administrativos y de Investigación Autorizados: Cualquier actividad o tarea directamente relacionada con la misión, funciones y responsabilidades oficiales del usuario

dentro de la EAPD (enseñanza, aprendizaje, administración de la institución, investigación académica o institucional, etc.).

Institución: La entidad propietaria y administradora de los recursos tecnológicos y de esta Política, en este caso la Escuela de Artes Plásticas y Diseño de Puerto Rico (EAPD).

Material Ilegal, Ofensivo o que Atente contra la Seguridad: Cualquier contenido, archivo o dato que viole leyes aplicables, sea difamatorio, acosador, discriminatorio, o que represente una amenaza a la integridad o disponibilidad de los sistemas de la EAPD. Ejemplos explícitos: pornografía, contenido relacionado con apuestas, software malicioso (malware).

- Material Ilegal: acceso, almacenamiento o distribución de pornografía en cualquiera de sus manifestaciones, descarga o distribución de material que infrinja derechos de autor, la promoción y uso de sustancias controladas. Material con contenido amenazante directo hacia una persona o la institución.
- Material Ofensivo: acceso, creación, almacenamiento o distribución de contenido con lenguaje obsceno, vulgar o de índole sexual que no esté relacionado con fines académicos autorizados. Contenido que promueva discurso de odio por razones de raza, sexo, política, religión, discapacidad, entre otros. Contenido que incluya acoso, hostigamiento e intimidación. Imágenes o mensajes degradantes hacia individuos o grupos. Contenido que promueva violencia gráfica sin justificación académica.
- Material que Atente contra la Seguridad: instalación o distribución de virus, "malware" o programas "software" no autorizados. Uso de herramientas de "hacking" sin autorización formal. Compartir cuentas institucionales con terceros. Manipulación o alteración no autorizada de sistemas, archivos o configuraciones. Divulgación de información confidencial sin autorización.

Programas "Software" no Autorizado: Cualquier programa de aplicación o sistema instalado en un recurso tecnológico de la EAPD que no haya sido aprobado expresamente por la Oficina de Tecnología o que carezca de la licencia de uso legal correspondiente.

Recursos Tecnológicos: Todo equipo, sistema, servicio o infraestructura de tecnología de la información provisto o administrado por la EAPD. Incluye, sin limitarse a: computadoras, "laptops", impresoras, dispositivos móviles, servidores, cuentas de correo electrónico institucional, acceso a internet, redes cableadas (LAN) e inalámbricas (Wi-Fi), y servicios en la nube (cloud services).

Usuarios: Toda persona a la que se le ha concedido acceso a los recursos tecnológicos de la EAPD. Incluye a: personal administrativo, facultad, estudiantes y contratistas.

Responsabilidades

A. **Institución a través de la Oficina de Tecnología**
   - Comunicar periódicamente esta política.
   - Establecer los mecanismos razonables de supervisión y control para asegurar el cumplimiento de esta política por parte de los usuarios.

- Atender e investigar alegadas violaciones a esta política conforme a los procedimientos institucionales aplicables.
- Recomendar las medidas correctivas o sanciones aplicables según la magnitud de la violación a esta política una vez se tenga el resultado de la investigación.
- Revisar y actualizar periódicamente esta política, según sea necesario, para atender cambios tecnológicos o regulatorios.

B. **Usuario**

- Utilizar los recursos tecnológicos únicamente para fines legítimos, académicos, administrativos o institucionales autorizados.
- Cumplir con lo establecido en esta política.
- Respetar la integridad de los equipos, redes y plataformas institucionales.
- Reportar cualquier uso indebido, vulnerabilidad o incidente relacionado con el uso de los recursos tecnológicos institucionales.

Cumplimiento /Sanciones

El incumplimiento de esta política puede conllevar sanciones administrativas según establecidas en las Normas de Conducta y Medidas Correctivas Aplicables a Empleados y Funcionarios de la Escuela de Artes Plásticas y Diseño de Puerto Rico.

Referencias

- PRITS – Políticas de Uso Aceptable y Ciberseguridad del Gobierno de Puerto Rico.
- NIST SP 800-12 – Introducción a la Seguridad en las Computadoras
- ISO/IEC 27002:2013 – Código de Prácticas para Controles de Seguridad de la Información.

Certificación y aprobación

Esta política ha sido revisada y aprobada conforme a las disposiciones institucionales vigentes y entrará en vigor a partir de la fecha de su firma.

Nombre y firma de la Autoridad
Nominadora:

Dra. Ileana Muñoz Landrón

Dra. Ileana Muñoz Landrón (Mar 18, 2026 14:39:04 EDT)

Fecha: 18/03/2026

Política de Contraseñas y Autenticación

Propósito

El propósito de esta política es establecer los requisitos mínimos para la creación, uso, administración y protección de contraseñas en los sistemas tecnológicos de la EAPD.

Alcance

Aplica a todo el personal administrativo, académico, estudiantes y contratistas que accedan a los recursos institucionales.

Disposiciones de la Política

1. Todas las cuentas de usuario deben estar protegidas con una contraseña única y personal.
2. Las contraseñas deben cumplir con los siguientes requisitos mínimos:
    - Longitud minima: 12 caracteres.
    - Uso de mayúsculas, minúsculas, números y caracteres especiales.
    - No contener información personal evidente (nombre, fecha de nacimiento, etc.).
3. Las contraseñas deben cambiarse al menos cada **90 días** o antes si existe sospecha de compromiso.
4. Está prohibido compartir contraseñas o anotarlas en lugares accesibles.
5. Se implementará **autenticación multifactor (MFA)** en sistemas críticos (correo institucional, almacenamiento en la nube, servidores y sistemas administrativos).
6. Los accesos inactivos por más de 90 días deben ser deshabilitados automáticamente.

Definiciones de Términos

Autenticación: El proceso mediante el cual se verifica la identidad de un Usuario que intenta acceder a un sistema.

Autenticación Multifactor (MFA): Un método de seguridad en sistemas tecnológicos que requiere que el usuario presente dos o más formas diferentes de verificación para confirmar su identidad antes de permitir el acceso a una cuenta, sistema o aplicación. Incluyen:

- algo que el usuario sabe: contraseña, pin o respuesta a preguntas de seguridad

- algo que el usuario tiene: código enviado al celular por SMS, “token”, o tarjeta inteligente.
- algo que el usuario es: huella digital o biometría, reconocimiento facial, entre otros.

Compromiso de Contraseña (Sospecha de Compromiso): Cualquier evento o circunstancia en la que la confidencialidad de una contraseña haya sido violada, ya sea por conocimiento no autorizado, exposición pública o sospecha de ataque.

Contraseña / Credencial: Una cadena secreta de caracteres (letras, números y/o símbolos) utilizada para verificar la identidad de un usuario y garantizar el acceso a un sistema o recurso tecnológico.

Cuentas de Usuario: Los identificadores personales y únicos asignados a cada individuo (personal administrativo, académico, estudiantes, contratistas) que permiten el acceso a los recursos tecnológicos de la institución.

Requisitos Mínimos de Contraseña: El conjunto de reglas de complejidad y longitud (mínimo 12 caracteres, uso de mayúsculas, minúsculas, números y caracteres especiales) que un sistema debe imponer para la creación de una contraseña aceptable.

Sistemas Críticos: Aquellos recursos tecnológicos y sistemas cuya confidencialidad, integridad o disponibilidad son esenciales para las operaciones de la institución, y cuyo compromiso podría tener un impacto grave. Ejemplos en la política: correo institucional, almacenamiento en la nube, servidores y sistemas administrativos.

Responsabilidades

A. **Institución a través de la Oficina de Tecnología**:
   - Establecer y mantener los estándares de seguridad para la creación, uso y manejo de contraseñas en los sistemas de la institución.
   - Configuración de los controles tecnológicos que se requieran en el cumplimiento de esta política.
   - Implementación de los mecanismos de autenticación segura a través de la autenticación multifactor (MFA).
   - Administrar el acceso a los sistemas institucionales.
   - Proteger la confidencialidad de las credenciales de acceso.
   - Monitorear actividades inusuales o intentos de acceso no autorizado a los sistemas de la institución.
   - Restablecer contraseñas o desbloquear cuentas.
   - Evaluar y actualizar periódicamente los controles de autenticación.

B. **Responsabilidades de los Usuarios**

- Crear contraseñas seguras que cumplan con los requisitos establecidos por la institución.
- Mantener la confidencialidad de su contraseña evitando compartirla o escribirla en lugares accesibles o visibles.
- Cambiar la contraseña cuando el sistema lo requiera.
- Cerrar sesión o bloquear el equipo cuando se deje desatendido.
- Notificar inmediatamente a la Oficina de Tecnología cualquier actividad sospechosa.
- Utilizar las credenciales de acceso únicamente para fines autorizados.

Cumplimiento / Sanciones

El incumplimiento de esta política puede conllevar sanciones administrativas según establecidas en las Normas de Conducta y Medidas Correctivas Aplicables a Empleados y Funcionarios de la Escuela de Artes Plásticas y Diseño de Puerto Rico.

Referencias

- PRITS – Guía de Ciberseguridad y Control de Accesos.
- NIST SP 800-63B – Digital Identity Guidelines (Authentication and Lifecycle Management).
- ISO/IEC 27001 – Control de accesos.

Certificación y aprobación

Esta política ha sido revisada y aprobada conforme a las disposiciones institucionales vigentes y entrará en vigor a partir de la fecha de su firma.

Nombre y firma de la Autoridad Nominadora:

Dra. Ileana Muñoz Landrón

Dra. Ileana Muñoz Landrón (Mar 18, 2026 14:39:04 EDT)

Fecha: 18/03/2026

Política de Inventario y Control de Activos Tecnológicos

Propósito

El propósito de esta política es establecer los lineamientos y controles para la identificación, registro, manejo, custodia, uso y disposición de los activos tecnológicos de la institución con el fin de asegurar el uso, administración y protección de forma eficiente.

Alcance

Esta política aplica a todos los activos tecnológicos propiedad de la institución, así como los recursos tecnológicos asignados para el uso de empleados, facultad, estudiantes y personal autorizado. El alcance de la misma incluye, pero no se limita a:

- Computadoras de escritorios y portátiles.
- Servidores y equipos de red.
- Monitores, impresoras y escáneres
- Equipo audiovisual y de laboratorio digital.
- Sistemas de almacenamiento de datos.
- Pantallas inteligentes
- Equipos periféricos y accesorios tecnológicos.
- Programas “software” institucionales licenciados.

Disposiciones de la Política

La institución mantendrá un sistema formal de inventario y control de todos los activos tecnológicos con el fin de garantizar su adecuada administración, seguridad, mantenimiento y uso responsable.

1. Todos los activos tecnológicos propiedad de la institución deberán ser registrados en el inventario oficial de la escuela, así como en un inventario administrado por la Oficina de Tecnología.
2. Cada equipo deberá contar con una identificación o etiqueta institucional que permita su reconocimiento y seguimiento dentro del inventario institucional.
3. El inventario incluirá:

    - Tipo de equipo o activo

- Marca, modelo y número de serie
- Ubicación física
- Unidad administrativa responsable
- Usuario asignado (cuando aplique)
- Fecha de adquisición
- Número de propiedad o identificación institucional

4. Cualquier traslado o cambio de ubicación de un activo tecnológico debe ser notificado y autorizado por la Oficina de Tecnología.
5. Se realizará verificaciones o auditorias periódicas del inventario tecnológico para asegurar la exactitud de los registros y el cumplimiento con esta política.

Definiciones de Términos

Activo Tecnológico / Equipo Tecnológico: Se define como cualquier dispositivo físico, equipo o programa "software" licenciado, propiedad de la EAPD, que se utiliza para procesar, almacenar o transmitir información, o para soportar la infraestructura de red institucional.

Auditoría de Inventario: Es el procedimiento periódico y obligatorio, realizado al menos una vez al año, que tiene como finalidad verificar físicamente la existencia de los activos tecnológicos y confirmar la exactitud de los datos registrados en el inventario oficial.

Disposición de Activos Tecnológicos: Es el proceso mediante el cual la institución determina el retiro, reemplazo, transferencia, reciclaje o eliminación de un activo tecnológico que ha llegado al final de su vida útil o que ya no cumple con las necesidades institucionales.

Inventario Tecnológico: Es el registro oficial que documenta y mantiene actualizada la información relacionada con los activos tecnológicos de la institución, incluyendo su identificación, ubicación, estado, usuario asignado y demás datos relevantes para su debido control y administración. Este inventario recae en la Oficina de Tecnología.

Movimiento / Reasignación: Se refiere a cualquier cambio en la ubicación física o en el usuario asignado de un activo tecnológico, el cual debe ser autorizado previamente y actualizado de inmediato en el inventario oficial.

Número de Identificación Único (Número de Propiedad): Es el código alfanumérico o etiqueta física de rotulación asignada individualmente a cada activo tecnológico con el propósito de garantizar su seguimiento, identificación única y correlación dentro del inventario oficial.

Oficina de Tecnología (OT): Es la unidad institucional responsable de la administración de los sistemas de información, el mantenimiento del inventario oficial de activos tecnológicos, la configuración de los activos y la gestión de la baja o reasignación de los equipos, asegurando así el cumplimiento de esta política.

Usuario Asignado: Persona o unidad administrativa responsable del uso y custodia de un activo tecnológico específico que le ha sido formalmente asignado para el desempeño de sus funciones institucionales.

Usuario Autorizado: Es la persona ya sea empleado, facultad o estudiante que ha sido autorizada para acceder, utilizar o administrar sistemas, equipos o recursos tecnológicos institucionales, conforme a las funciones académicas o administrativas que desempeñan.

Responsabilidades

A. Institución a través de la Oficina de Tecnología

La institución, a través de la Oficina de Tecnología, será responsable de establecer, administrar y supervisar los mecanismos necesarios para el adecuado inventario, control, uso y disposición de los activos tecnológicos institucionales. Entre sus responsabilidades se incluyen, pero no se limitan a:

- Establecer y mantener un inventario actualizado de todos los activos tecnológicos de la institución, incluyendo computadoras, servidores, dispositivos móviles, equipos periféricos, equipos de red, licencias de software y otros recursos tecnológicos.
- Asignar un identificador único o número de inventario a cada activo tecnológico para facilitar su control, rastreo y administración durante todo su ciclo de vida.
- Registrar y documentar la asignación de activos tecnológicos a empleados, oficinas o dependencias institucionales, manteniendo evidencia de dicha asignación.
- Implementar procedimientos para la adquisición, registro, traslado, préstamo, mantenimiento y disposición final de los activos tecnológicos conforme a las normativas institucionales y gubernamentales aplicables.
- Realizar verificaciones periódicas del inventario tecnológico para garantizar la exactitud de los registros y la localización de los equipos.
- Coordinar el mantenimiento preventivo y correctivo de los activos tecnológicos institucionales para garantizar su funcionamiento adecuado.
- Establecer controles para la instalación y uso de software autorizado, asegurando el cumplimiento con licencias y derechos de uso.
- Coordinar el retiro, reutilización o disposición final de equipos tecnológicos que hayan llegado al final de su vida útil, conforme a las normas institucionales y ambientales aplicables.
- Mantener documentación y registros relacionados con los activos tecnológicos, incluyendo historial de mantenimiento, asignación y movimientos de equipos.
- Proveer orientación a los usuarios sobre el uso adecuado, manejo y cuidado de los activos tecnológicos asignados.

1. Usuarios

Todos los usuarios a quienes se les asigne o autorice el uso de activos tecnológicos institucionales tendrán las siguientes responsabilidades:

- Utilizar los activos tecnológicos exclusivamente para fines institucionales, académicos o administrativos autorizados.
- Custodiar y proteger los equipos tecnológicos asignados**, e**vitand**o** daños, pérdida, robo o uso indebido de los mismos.
- No transferir, prestar, reubicar o permitir el uso de los activos tecnológicos asignados a terceros sin la autorización previa de la Oficina de Tecnología o de la autoridad correspondiente.
- Notificar inmediatamente a la Oficina de Tecnología y a su supervisor en caso de pérdida, daño, robo o mal funcionamiento de cualquier activo tecnológico asignado.
- Permitir la verificación o inspección de los activos tecnológicos asignados cuando sea requerido para fines de inventario o control institucional.
- Utilizar los equipos de forma responsable y conforme a las políticas institucionales de tecnología y seguridad de la información.
- Devolver los activos tecnológicos asignados cuando así sea requerido por la institución, incluyendo en casos de traslado de oficina, cambio de funciones o cese de empleo o relación institucional.

Cumplimiento / Sanciones

El incumplimiento de esta política puede conllevar sanciones administrativas según establecidas en las Normas de Conducta y Medidas Correctivas Aplicables a Empleados y Funcionarios de la Escuela de Artes Plásticas y Diseño de Puerto Rico.

Referencias

- PRITS – Normas de Gestión de Activos Tecnológicos del Gobierno de Puerto Rico.
- NIST SP 1800-5 – “IT Asset Management”
- ISO/IEC 19770 – Gestión de activos de “software” y “hardware”.

Certificación y aprobación

Esta política ha sido revisada y aprobada conforme a las disposiciones institucionales vigentes y entrará en vigor a partir de la fecha de su firma

Nombre y firma de la Autoridad Nominadora:

Dra. Ileana Muñoz Landrón

Fecha: 18/03/2026

Política de Respaldos “Backups” y Plan de Recuperación ante Desastres (DRP)

Propósito

El propósito de esta política es garantizar la continuidad de las operaciones académicas y administrativas de la Escuela de Artes Plásticas y Diseño de Puerto Rico (EAPD) mediante la protección de la información crítica.

Alcance

Esta política aplica a todos los sistemas de información, bases de datos, servidores, aplicaciones institucionales, equipos tecnológicos y repositorios digitales que almacenan o procesan información institucional de la EAPD. Adicional a todos los empleados, estudiantes, facultad, contratistas y usuarios autorizados.

Disposiciones de la Política

1. **Implementación de mecanismos de respaldos**: Todos los sistemas de información identificados como críticos para las operaciones institucionales deberán contar con mecanismos de respaldo automatizados. Estos mecanismos deberán ser monitoreados y verificados periódicamente para asegurar su correcto funcionamiento.

2. **Alcance de la información respaldada:** Las copias de seguridad deberán incluir, como mínimo, la siguiente información institucional esencial:
   - Archivos académicos y administrativos de carácter crítico.
   - Bases de datos relacionadas con estudiantes, empleados, operaciones financieras y otros sistemas institucionales.
   - Configuraciones de servidores, sistemas operativos, aplicaciones institucionales y equipos de red.

3. **Frecuencia de los respaldos:** La institución deberá establecer un programa de respaldos que incluya, al menos, las siguientes frecuencias:
   - **Respaldos diarios:** archivos y bases de datos considerados críticos.
   - **Respaldos semanales:** copias completas de sistemas o aplicaciones institucionales.

- **Respaldos mensuales:** copias completas almacenadas en una ubicación alterna o externa.

4. Ub**icación de las copias de seguridad:** Con el propósito de reducir riesgos de pérdida de información, las copias de respaldo deberán almacenarse en al menos dos ubicaciones distintas, que incluyan:
   - Un almacenamiento seguro dentro de la infraestructura institucional.
   - Un almacenamiento externo o en servicios de nube autorizados por la institución.

5. **Protección y cifrado de los respaldos:** Todas las copias de seguridad deberán estar protegidas mediante mecanismos de cifrado que cumplan con estándares de seguridad reconocidos, tales como **AES-256**, **TLS 1.2** o versiones superiores, u otros estándares equivalentes aprobados por la institución.

6. **Pruebas de restauración de información:** La Oficina de Tecnología deberá realizar pruebas periódicas de restauración de datos, al menos cada seis (6) meses, con el fin de validar la integridad de los respaldos y la efectividad de los procedimientos de recuperación.

7. **Plan de Recuperación ante Desastres:** La institución deberá mantener un Plan de Recuperación ante Desastres (DRP, por sus siglas en inglés) debidamente documentado, aprobado y actualizado, el cual contemple procedimientos para la restauración de sistemas y datos ante eventos que puedan afectar la continuidad de las operaciones institucionales, tales como:
   - fenómenos naturales (por ejemplo, huracanes, terremotos o incendios),
   - fallas eléctricas prolongadas o interrupciones de infraestructura tecnológica, y
   - incidentes de ciberseguridad, incluyendo ataques cibernéticos.

8. **Conservación de respaldos:** La institución deberá establecer periodos de retención para las copias de seguridad, conforme a la naturaleza de la información y a las normativas institucionales y legales aplicables.

Definiciones de Términos

Cifrado / Encriptación: Es el proceso de aplicar algoritmos criptográficos a los datos de Respaldo para hacerlos ilegibles a cualquier parte no autorizada, utilizando estándares de seguridad aprobados como AES-256 o TLS 1.2 o superior.

Información Crítica: Comprende todos los datos, archivos y configuraciones cuya pérdida o falta de disponibilidad afectaría severamente la misión de la institución, incluyendo archivos académicos, bases de datos de estudiantes, facultad, empleados y configuraciones esenciales de servidores.

Plan de Recuperación de Desastres (DRP): Es el conjunto documentado y aprobado de procedimientos y recursos que describen las acciones a seguir para restaurar los Sistemas Críticos y reanudar las operaciones de la Universidad después de un evento disruptivo mayor o desastre.

Restauración / Pruebas de Restauración: La restauración es el proceso de copiar los datos de un respaldo a un sistema en funcionamiento. Las pruebas de restauración son los ejercicios periódicos y formales que realiza la Oficina de Tecnología para verificar que los respaldos son recuperables, completos y funcionales.

Sistemas Críticos: Son aquellos sistemas, bases de datos o servicios cuya operación es esencial para la ejecución de las funciones académicas, administrativas y de investigación de la Universidad, y cuya interrupción o pérdida de datos causaría un impacto operativo significativo.

Ubicación de Almacenamiento Externa (Sitio Alterno): Se refiere a un lugar físico o servicio de almacenamiento remoto (incluida la nube) geográficamente separado del sitio principal de operación de la Universidad, utilizado para almacenar copias de Respaldo para protección contra desastres locales.

Responsabilidades

A. Institución, a través de la Oficina de Tecnología

La institución, a través de la Oficina de Informática, será responsable de establecer, implementar y mantener los mecanismos necesarios para garantizar la protección, respaldo y recuperación de la información institucional. Entre sus responsabilidades se incluyen, pero no se limitan a:

- Desarrollar y mantener procedimientos de respaldo de la información institucional, asegurando que los sistemas críticos cuenten con copias de seguridad conforme a las disposiciones establecidas en esta política.
- Identificar y clasificar los sistemas y datos críticos para las operaciones académicas, administrativas y financieras de la institución, con el fin de priorizar su respaldo y recuperación.
- Implementar y administrar soluciones tecnológicas de respaldo automatizado**,** garantizando la integridad, disponibilidad y seguridad de las copias de seguridad.
- Establecer y mantener mecanismos seguros de almacenamiento de respaldos**,** incluyendo ubicaciones alternas o servicios externos autorizados para reducir el riesgo de pérdida de información.
- Desarrollar, documentar y mantener actualizado el Plan de Recuperación ante Desastres (Disaster Recovery Plan – DRP)**,** el cual deberá incluir los procedimientos necesarios para la restauración de sistemas y datos en caso de incidentes mayores.
- Realizar pruebas periódicas de restauración y recuperación de información, con el propósito de validar la efectividad de los respaldos y del plan de recuperación.
- Monitorear y verificar regularmente la ejecución de los respaldos**,** asegurando que estos se completen correctamente y que los datos puedan ser restaurados cuando sea necesario.

- Mantener controles de acceso adecuados a los sistemas de respaldo, limitando su acceso únicamente al personal autorizado.
- Documentar incidentes relacionados con pérdida de información o activación del plan de recuperación**, i**ncluyendo las acciones tomadas para restaurar los servicios y prevenir recurrencias.
- Proveer orientación y capacitación a los usuarios sobre las buenas prácticas para la protección y manejo adecuado de la información institucional.

B. Usuarios

Todos los empleados, estudiantes y usuarios autorizados que utilicen sistemas o recursos tecnológicos institucionales tendrán las siguientes responsabilidades:

- Utilizar los sistemas institucionales de manera responsable, conforme a las políticas y normas de tecnología establecidas por la institución.
- Guardar y almacenar la información institucional en los sistemas, servidores o repositorios autorizados por la institución**,** para asegurar que dicha información sea incluida en los procesos de respaldo.
- Evitar almacenar información institucional crítica exclusivamente en dispositivos personales o medios no autorizados**,** que no formen parte de los mecanismos institucionales de respaldo.
- Notificar oportunamente a la Oficina de Tecnología cualquier incidente que pueda afectar la integridad o disponibilidad de la información institucional, incluyendo pérdida de archivos, fallas de sistemas o sospechas de incidentes de seguridad.
- Cumplir con las políticas institucionales relacionadas con seguridad de la información, uso aceptable de la tecnología y protección de datos.
- Cooperar con la Oficina de Tecnología durante procesos de recuperación de información, cuando sea necesario para restaurar sistemas o datos institucionales.

Cumplimiento / Sanciones

El incumplimiento de esta política puede conllevar sanciones administrativas según establecidas en las Normas de Conducta y Medidas Correctivas Aplicables a Empleados y Funcionarios de la Escuela de Artes Plásticas y Diseño de Puerto Rico.

Referencias

- PRITS – Políticas de Continuidad de Negocio y Ciberseguridad
- NIST SP 800-34 Rev.1 – “Contingency Planning Guide for Federal Information Systems”
- ISO/IEC 27031 – Directrices para la continuidad de negocio en Tecnología de la Informática

Certificación y aprobación

Esta política ha sido revisada y aprobada conforme a las disposiciones institucionales vigentes y entrará en vigor a partir de la fecha de su firma.

Nombre y firma de la Autoridad Nominadora:

Dra. Ileana Muñoz Landrón

Dra. Ileana Muñoz Landrón (Mar 18, 2026 14:39:04 EDT)

Fecha: 18/03/2026

Política de Mantenimiento Preventivo y Correctivo de Equipos Tecnológicos

Propósito

El propósito de esta política es garantizar la disponibilidad y confiabilidad de los equipos y sistemas tecnológicos de la Escuela de Artes Plásticas y Diseño de Puerto Rico (EAPD) mediante un mantenimiento programado y la pronta atención de fallas.

Alcance

Esta política aplica a todos los equipos y activos tecnológicos propiedad de la institución o utilizados para el desempeño de funciones académicas, administrativas u operacionales dentro de la institución. El alcance de esta política incluye, pero no se limita a:

1. Equipos de cómputo institucionales, tales como computadoras de escritorio, computadoras portátiles, estaciones de trabajo y dispositivos móviles asignados para uso institucional.
2. Servidores, sistemas de almacenamiento y equipos de infraestructura tecnológica**,** incluyendo equipos de red, enrutadores, conmutadores, puntos de acceso inalámbrico y otros componentes de la red institucional.
3. Equipos periféricos y dispositivos tecnológicos complementarios, tales como impresoras, escáneres, proyectores, dispositivos de almacenamiento externo y otros equipos utilizados para apoyar las operaciones institucionales.
4. Software institucional y sistemas operativos instalados en los equipos tecnológicos**,** incluyendo actualizaciones, parches de seguridad y mantenimiento de aplicaciones.
5. Los empleados, estudiantes, contratistas y usuarios autorizados que utilicen equipos tecnológicos institucionales o tengan responsabilidad sobre su manejo o custodia.
6. Las actividades de mantenimiento preventivo y correctivo realizadas por la Oficina de Tecnología o personal autorizado, incluyendo inspección, limpieza, actualización de software, reparación, reemplazo de componentes y otras acciones destinadas a garantizar el funcionamiento adecuado de los equipos.

Esta política aplica a los equipos tecnológicos ubicados dentro de las instalaciones institucionales, así como a aquellos que hayan sido asignados para uso institucional fuera de las instalaciones, cuando corresponda.

Disposiciones de la Política

1. **Mantenimiento preventivo de equipos tecnológicos**
   Todos los equipos tecnológicos institucionales deberán recibir mantenimiento preventivo de forma periódica, de acuerdo con su tipo, función y nivel de criticidad para las operaciones institucionales. Como referencia general se establecen las siguientes frecuencias mínimas:
   - Computadoras de escritorio y portátiles**:** revisión trimestral que incluya limpieza física del equipo, verificación de componentes y mantenimiento de software.
   - Impresoras y equipos periféricos**:** revisión preventiva al menos cada seis (6) meses.
   - Servidores, conmutadores "switches" y equipos de red**:** monitoreo continuo de funcionamiento y mantenimiento preventivo programado al menos cada seis (6) meses.

2. **Mantenimiento correctivo**
   Todo equipo tecnológico que presente fallas, deterioro o funcionamiento inadecuado deberá ser atendido mediante mantenimiento correctivo a la mayor brevedad posible. La atención de incidentes deberá priorizar aquellos sistemas o equipos que sean esenciales para las operaciones académicas, administrativas o institucionales.

3. **Registro de mantenimiento**
   La Oficina de Tecnología deberá mantener un registro actualizado y detallado de todas las intervenciones de mantenimiento preventivo y correctivo realizadas a los equipos tecnológicos institucionales. Dicho registro deberá incluir, al menos:
   - Fecha de la intervención o servicio realizado.
   - Descripción del mantenimiento o reparación efectuada.
   - Condición o estado del equipo luego de la intervención.
   - Nombre o identificación del personal responsable de realizar el mantenimiento.

4. **Procedimientos estandarizados de mantenimiento**
   Todas las actividades de mantenimiento deberán realizarse conforme a procedimientos técnicos estandarizados establecidos por la Oficina de Tecnología, con el propósito de garantizar la integridad de los equipos, la seguridad de la información y la continuidad de los servicios tecnológicos institucionales.

5. **Disposición de equipos no reparables**
   Aquellos equipos tecnológicos que, luego de su evaluación técnica, se determine que no pueden ser reparados o que han alcanzado el final de su vida útil, deberán ser gestionados conforme a lo establecido en la Política de Inventario y Control de Activos Tecnológicos, asegurando que su baja, reemplazo o disposición final quede debidamente documentada.

Definiciones de Términos

Baja Documentada: Es la acción final y formal de retirar un equipo tecnológico irreparable del servicio, proceso que debe ser registrado en el inventario oficial de la institución conforme a la Política de Inventario y Control de Activos Tecnológicos.

Equipos Tecnológicos / Activo Tecnológico Institucional: Se define como cualquier dispositivo físico, hardware o componente de infraestructura de tecnología, propiedad de la institución, que requiere atención y cuidado periódico para su correcto funcionamiento.

Mantenimiento Correctivo: Es la actividad de servicio técnico no planificada que se realiza para reparar un equipo tecnológico que ya ha presentado una falla o avería, con el objetivo de restablecer su funcionalidad lo más pronto posible.

Mantenimiento Preventivo: Es la actividad de servicio técnico planificada y periódica que se realiza sobre un equipo tecnológico en un estado funcional, con el objetivo de prevenir la aparición de fallas, preservar su vida útil y garantizar su disponibilidad y rendimiento óptimo.

Procedimientos Estandarizados: Se refiere a los métodos, pasos y herramientas aprobados y documentados por la Oficina de Tecnología que deben seguirse para ejecutar el mantenimiento físico y de software, garantizando la seguridad de los datos y la consistencia en el servicio.

Registro Detallado de Mantenimiento: Es el documento formal administrado por la Oficina de Tecnología que consolida el historial completo de las intervenciones de mantenimiento preventivo y correctivo, incluyendo la fecha, la descripción del trabajo realizado y el responsable.

Sistemas Críticos: Son aquellos equipos (tales como servidores, equipos de red o infraestructura principal) cuya interrupción o falla tiene un impacto inmediato y grave en las operaciones académicas o administrativas esenciales de la institución requiriendo la máxima prioridad de atención correctiva.

Responsabilidades

A. Institución a través de la Oficina de Tecnología:

La EAPD, a través de la Oficina de Tecnología será la responsable de:

- Establecer y ejecutar un programa de mantenimiento preventivo para los equipos tecnológicos institucionales, conforme a la criticidad, tipo de equipo y mejores prácticas de la industria.
- Realizar inspecciones periódicas, actualizaciones de software, parchos de seguridad, limpieza física y optimización del rendimiento de los equipos tecnológicos institucionales.
- Atender y gestionar el mantenimiento correctivo de los equipos que presenten fallas o interrupciones en su funcionamiento, ya sea mediante personal interno o proveedores autorizados.
- Mantener un registro actualizado de mantenimiento, reparaciones, reemplazos y diagnósticos realizados a los equipos tecnológicos.

- Evaluar periódicamente el estado y ciclo de vida de los equipos, con el fin de recomendar su reparación, actualización o reemplazo cuando sea necesario.
- Coordinar con suplidores o técnicos especializados los servicios de mantenimiento que requieran intervención externa o garantía del fabricante.
- Establecer mecanismos oficiales para la notificación de fallas o incidentes tecnológicos, asegurando una respuesta oportuna.
- Velar por que los equipos tecnológicos cumplan con los estándares institucionales de seguridad, funcionamiento y protección de la información.

B. Usuarios

Todo usuario de equipos tecnológicos institucionales tendrá las siguientes responsabilidades:

- Utilizar los equipos tecnológicos de manera adecuada y conforme a las políticas institucionales vigentes.
- Notificar oportunamente a la Oficina de Tecnología cualquier falla, daño o funcionamiento irregular en los equipos asignados o utilizados.
- Evitar la manipulación, reparación, modificación o instalación de componentes de hardware o software sin la autorización de la Oficina de Tecnología.
- Permitir el acceso al equipo cuando sea requerido para fines de mantenimiento preventivo, correctivo o inspección técnica.
- Proteger los equipos bajo su uso o custodia contra daños, uso indebido, negligencia o pérdida.
- No trasladar equipos tecnológicos de su ubicación asignada sin la autorización correspondiente de la Oficina de Tecnología.
- Cooperar con los procesos de mantenimiento programado**,** incluyendo apagado, reinicio o entrega temporal del equipo cuando sea requerido.

Cumplimiento / Sanciones

El incumplimiento de esta política puede conllevar sanciones administrativas según establecidas en las Normas de Conducta y Medidas Correctivas Aplicables a Empleados y Funcionarios de la Escuela de Artes Plásticas y Diseño de Puerto Rico.

Referencias

- PRITS – Políticas de Gestión de Activos y Mantenimiento Tecnológico
- NIST SP 800-53 – Control de Operaciones y Mantenimiento de Sistemas
- ISO/IEC 27002 – Controles de seguridad física y ambiental

Certificación y aprobación

Esta política ha sido revisada y aprobada conforme a las disposiciones institucionales vigentes y entrará en vigor a partir de la fecha de su firma.

Nombre y firma de la Autoridad Nominadora:

Dra. Ileana Muñoz Landrón

Dra. Ileana Muñoz Landrón (Mar 18, 2026 14:39:04 EDT)

Fecha: 18/03/2026

Política de Gestión de Incidentes de Seguridad

Propósito

El propósito de esta política es garantizar la detección, reporte, análisis y resolución de incidentes de seguridad informática en la Escuela de Artes Plásticas y Diseño de Puerto Rico (EAPD), minimizando impactos sobre la información, sistemas y operaciones.

Alcance

Aplica a todo el personal administrativo, académico, estudiantes y contratistas que utilicen los sistemas institucionales.

Disposiciones de la Política

1. **Obligatoriedad del Reporte**
   Todo evento que comprometa o amenace la seguridad de la información debe ser notificado de manera inmediata y obligatoria a la Oficina de Tecnología. La omisión o demora en el reporte de un incidente conocido será considerada una falta a las normas de seguridad institucional.

2. **Clasificación de Incidentes**
   Se define como incidente de seguridad cualquier evento adverso que afecte la confidencialidad, integridad o disponibilidad de los activos de información. Sin limitarse a estos, se incluyen:
   - **Intrusiones:** Accesos no autorizados a sistemas, aplicaciones o infraestructura de red.
   - **Código Malicioso:** Detección de "malware", "ransomware", troyanos o cualquier "software" hostil.
   - **Filtración de Datos:** Pérdida, robo, alteración o exposición accidental de datos sensibles o regulados.
   - **Disrupción Tecnológica:** Fallas críticas en servicios esenciales, servidores o infraestructura de soporte.

3. **Registro y Trazabilidad**
   La Oficina de Tecnología mantendrá una Bitácora Oficial de Incidentes, la cual servirá como registro histórico y evidencia técnica. Cada entrada deberá contener, de forma mínima, los siguientes metadatos:
   - Sello de tiempo (fecha y hora exacta del suceso y del reporte).

- Identificación del activo o usuario afectado.
- Naturaleza y descripción técnica del evento.
- Protocolo de respuesta y acciones correctivas ejecutadas.
- Personal técnico responsable del manejo del caso.

4. **Ciclo de Respuesta y Resolución**
   Todo incidente reportado será sujeto a un proceso de investigación, contención y resolución. El tiempo de respuesta estará sujeto a la matriz de criticidad establecida, garantizando que los eventos de alto impacto reciban atención prioritaria para minimizar el daño operativo.

5. **Mejora Continua y Mitigación**
   Tras la resolución de un incidente, se realizará un análisis de causa raíz para identificar vulnerabilidades. Los hallazgos se utilizarán para implementar medidas preventivas y correctivas que fortalezcan la postura de seguridad y reduzcan la probabilidad de recurrencia.

6. **Protocolo de Escalación y Notificación Externa**
   En casos de incidentes de alta severidad o impacto sistémico, la Oficina de Tecnología elevará el informe al Rector (a). Asimismo, se cumplirá con el deber de notificación a entidades externas como PRITS (Puerto Rico Innovation and Technology Service**)** y agencias de ley y orden pertinentes, conforme a la normativa vigente.

Definiciones de Términos

Acciones Correctivas: Son las medidas técnicas o administrativas implementadas por la Oficina de Tecnología con el objetivo de contener, erradicar y recuperar un sistema afectado por un Incidente de Seguridad, devolviéndolo a un estado operativo seguro.

Bitácora Oficial de Incidentes: Es el registro formal y centralizado mantenido por la Oficina de Tecnología que documenta cada Incidente de Seguridad, incluyendo detalles como fecha, hora, descripción de los hechos, el impacto potencial y todas las acciones tomadas para la resolución.

Criticidad del Incidente: Es la clasificación de la severidad del incidente de seguridad, la cual se basa en el impacto potencial sobre las operaciones institucionales, la información sensible y el tiempo requerido para su resolución.

Incidente de Seguridad Informática: Se define como cualquier evento adverso, confirmado o sospechoso, que representa una violación de las políticas de seguridad de la información, una amenaza a la integridad, confidencialidad o disponibilidad de los sistemas, o un fallo crítico en la infraestructura tecnológica.

Información Sensible: Se refiere a todo dato, archivo o comunicación que, si es expuesto, alterado o perdido, podría resultar en un daño a la reputación, legal, administrativo o financiero significativo para la institución o sus miembros.

PRITS: Se define como la Oficina de Innovación y Servicios de Tecnología del Gobierno de Puerto Rico, la entidad gubernamental a la cual se debe reportar incidentes graves según la normativa aplicable en el territorio.

Reporte Inmediato: Es la obligación que tiene todo usuario de notificar a la Oficina de Tecnología de la institución, sin dilación y tan pronto tenga conocimiento, sobre cualquier evento que pueda constituir un incidente de seguridad.

Responsabilidades

A. Institución a través de la Oficina de Tecnología

La institución, a través de la Oficina de Tecnología, será responsable de establecer, coordinar e implementar las acciones necesarias para la adecuada gestión de incidentes de seguridad de la información. Entre sus responsabilidades se incluyen:

- Establecer y mantener procedimientos formales para la identificación, reporte, clasificación, manejo y resolución de incidentes de seguridad de la información que puedan afectar los sistemas, redes, aplicaciones o datos institucionales.
- Monitorear continuamente la infraestructura tecnológica institucional, incluyendo redes, servidores, sistemas y dispositivos, con el propósito de detectar actividades inusuales, vulnerabilidades o posibles incidentes de seguridad.
- Evaluar y clasificar los incidentes reportados, determinando su nivel de impacto, criticidad y las acciones necesarias para su contención y mitigación.
- Coordinar la respuesta técnica ante incidentes de seguridad, incluyendo la contención, análisis, mitigación y recuperación de los sistemas o servicios afectados.
- Documentar y mantener registros de los incidentes de seguridad, incluyendo la naturaleza del incidente, fecha de detección, acciones tomadas, impacto y medidas correctivas implementadas.
- Notificar a las autoridades institucionales correspondientes cuando un incidente represente un riesgo significativo para la seguridad de la información, la continuidad de las operaciones o el cumplimiento de disposiciones legales o regulatorias.
- Preservar la evidencia digital cuando sea necesario para procesos de investigación, auditoría o acciones disciplinarias o legales.
- Implementar medidas correctivas y preventivas para reducir la probabilidad de recurrencia de incidentes de seguridad.
- Coordinar la restauración segura de los sistemas, servicios o datos afectados, asegurando la continuidad de las operaciones institucionales en la medida posible.
- Promover la capacitación y concienciación en seguridad de la información dirigida a los usuarios institucionales, con el fin de fortalecer la prevención y el manejo adecuado de incidentes.
- Revisar y actualizar periódicamente los procedimientos de gestión de incidentes, conforme a las mejores prácticas de seguridad de la información y a las necesidades institucionales.

B. Usuarios

Todos los usuarios de los sistemas, redes, equipos y recursos tecnológicos institucionales tienen la responsabilidad de contribuir a la protección de la seguridad de la información y de reportar oportunamente cualquier incidente o situación que pueda representar un riesgo para la institución. Entre sus responsabilidades se incluyen:

- Reportar de manera inmediata a la Oficina de Tecnología cualquier incidente de seguridad, sospecha de incidente o actividad inusual que pueda afectar los sistemas, equipos, redes o información institucional.
- Notificar situaciones tales como, entre otras: accesos no autorizados, pérdida o robo de equipos institucionales, correos electrónicos sospechosos, presencia de virus o software malicioso, fallas inusuales en los sistemas, o divulgación accidental de información confidencial.
- Proveer información precisa y completa al momento de reportar un incidente, incluyendo una descripción de lo ocurrido, fecha y hora aproximada, sistema o equipo afectado y cualquier otra información relevante que facilite la investigación.
- No intentar resolver, investigar o manipular por cuenta propia un posible incidente de seguridad que pueda comprometer sistemas, equipos o evidencias digitales.
- Cooperar con la Oficina de Tecnología durante los procesos de investigación, análisis y resolución de incidentes de seguridad, cuando sea requerido.
- Proteger sus credenciales de acceso, evitando compartir contraseñas o permitir el uso de sus cuentas por terceros, ya que cada usuario es responsable del uso de sus accesos institucionales.
- Cumplir con las políticas, normas y procedimientos institucionales de seguridad de la información, incluyendo aquellas relacionadas con el uso aceptable de la tecnología, contraseñas, manejo de datos y protección de activos tecnológicos.
- Participar en las actividades de orientación o capacitación relacionadas con seguridad de la información que sean promovidas por la institución.

Cumplimiento / Sanciones

El incumplimiento de esta política puede conllevar sanciones administrativas según establecidas en las Normas de Conducta y Medidas Correctivas Aplicables a Empleados y Funcionarios de la Escuela de Artes Plásticas y Diseño de Puerto Rico.

Referencias

- PRITS – Guía de Gestión de Incidentes de Ciberseguridad
- NIST SP 800-61 Rev. 2 – “Computer Security Incident Handling Guide”
- ISO/IEC 27035 – Gestión de incidentes de seguridad de la información

Certificación y aprobación

Esta política ha sido revisada y aprobada conforme a las disposiciones institucionales vigentes y entrará en vigor a partir de la fecha de su firma.

Nombre y firma de la Autoridad Nominadora:

Dra. Ileana Muñoz Landrón

Dra. Ileana Muñoz Landrón (Mar 18, 2026 14:39:04 EDT)

Fecha: 18/03/2026

Política de Compras y Contratación de Servicios de Tecnología

Propósito

Esta política tiene como propósito establecer los lineamientos y criterios institucionales que regirán la adquisición de equipos tecnológicos, programas informáticos, sistemas, licencias, infraestructura tecnológica y la contratación de servicios relacionados con tecnología de la información. De igual forma, busca asegurar que toda compra o contratación de servicios tecnológicos en la institución se realice de manera planificada, transparente, segura y alineada con las necesidades operacionales, académicas y administrativas**,** garantizando la compatibilidad con la infraestructura tecnológica existente, el cumplimiento con los estándares de seguridad de la información, y el uso eficiente de los recursos institucionales.

Finalmente, con esta política se procura que las decisiones relacionadas con la adquisición de tecnología se realicen con la evaluación técnica correspondiente por parte de la Oficina de Tecnología, de manera que se promueva la sostenibilidad, interoperabilidad, mantenimiento adecuado y protección de los activos tecnológicos institucionales.

Alcance

Esta política aplica a todos los empleados, unidades administrativas, departamentos académicos, programas, proyectos institucionales y cualquier otra dependencia que solicite, gestione o participe en procesos de compra o contratación de equipos, sistemas, licencias o servicios tecnológicos para uso institucional.

El alcance de esta política incluye, pero no se limita a:

- Compra de computadoras, laptops, tabletas y otros dispositivos tecnológicos.
- Adquisición de servidores, equipos de red, almacenamiento y componentes de infraestructura tecnológica.
- Compra o suscripción de programas informáticos, aplicaciones, sistemas institucionales y licencias de software.

- Contratación de servicios tecnológicos externos tales como mantenimiento, soporte técnico, desarrollo de sistemas, servicios en la nube, seguridad informática, hospedaje de sistemas o consultoría tecnológica.
- Renovación, actualización o ampliación de servicios o sistemas tecnológicos existentes.

Esta política deberá cumplirse en conjunto con las normativas gubernamentales de compras, contratación, seguridad de la información, manejo de activos tecnológicos y cualquier otra reglamentación aplicable**,** incluyendo normativas federales.

Disposiciones de esta Política

1. Toda adquisición de equipos tecnológicos, programas informáticos o contratación de servicios relacionados con tecnología deberá estar debidamente justificada, autorizada conforme a los procesos institucionales establecidos y registrada en los sistemas administrativos correspondientes.

2. Previo a la adquisición de cualquier equipo, sistema o servicio tecnológico, deberá realizarse un análisis de necesidad que considere, entre otros aspectos:

    - La funcionalidad y los requerimientos operacionales del área solicitante.
    - La compatibilidad e integración con la infraestructura tecnológica institucional existente.
    - Los posibles riesgos de seguridad de la información asociados al equipo, sistema o software a adquirir.

3. En los procesos de adquisición y contratación se favorecerán proveedores autorizados o certificados, que cumplan con los estándares aplicables de seguridad de la información, licenciamiento, soporte técnico y cumplimiento normativo.

4. Todo contrato, acuerdo de servicio o licencia de software relacionado con tecnología deberá ser evaluado y contar con el aval del Oficial Principal de Informática, previo a su formalización, firma o implementación, con el fin de asegurar su viabilidad técnica y cumplimiento con los estándares institucionales.

5. La Oficina de Tecnología o unidad designada mantendrá un registro actualizado de todas las adquisiciones y contratos tecnológicos, el cual deberá incluir, entre otros, la siguiente información:

    - Tipo de adquisición o servicio contratado.
    - Nombre del proveedor.
    - Fecha de compra, vigencia del contrato o período de servicio.
    - Unidad o persona responsable de la gestión o administración del recurso.

6. Toda modificación, renovación, extensión o cancelación de contratos o licencias tecnológicas deberá ser debidamente documentada y contar con las aprobaciones institucionales correspondientes.

7. Los procesos de compra y contratación de tecnología deberán cumplir con las leyes y reglamentaciones aplicables del Gobierno de Puerto Rico, así como con las políticas y directrices emitidas por la Puerto Rico Innovation and Technology Service (PRITS). Asimismo, estos procesos estarán sujetos a las disposiciones y supervisión de la Administración de Servicios Generales de Puerto Rico (ASG) y de la Oficina de Gerencia y Presupuesto (OGP), según corresponda.

   De igual manera, podrán ser objeto de evaluación, fiscalización o auditoría por parte de la Oficina del Contralor de Puerto Rico y de la Oficina del Inspector General de Puerto Rico, conforme a la normativa vigente.

Definiciones de Términos

Adquisiciones Tecnológicas / Compras: Se refiere a la obtención por parte de la institución de cualquier equipo de hardware, licencia de "software" o servicio que involucre tecnología de la información para uso institucional.

Análisis de Necesidad: Es la evaluación preliminar obligatoria que se realiza antes de iniciar cualquier adquisición, con el objetivo de justificar el requerimiento, determinar su compatibilidad con la infraestructura existente y evaluar los riesgos de seguridad asociados.

Contratación de Servicios de Tecnología: Se define como el proceso formal para establecer acuerdos contractuales con proveedores externos para la provisión de servicios relacionados con la tecnología, tales como consultoría, mantenimiento especializado o servicios en la nube.

Infraestructura Existente: Se refiere al conjunto de hardware, software, sistemas de red y servicios tecnológicos que ya están operando dentro de la institución y con los cuales debe integrarse cualquier nueva adquisición.

Oficial Principal de Informática (OPI): Es la persona cuya responsabilidad es la dirección de la Oficina de Tecnología de la EAPD, así como de establecer la estrategia tecnológica y con la autoridad de revisar y recomendar contratos, licencias y adquisiciones.

Proveedores Certificados: Son aquellas empresas o individuos que demuestran tener las credenciales, licencias y cumplimiento de estándares requeridos por PRITS y el Gobierno de Puerto Rico para la entrega de bienes y servicios tecnológicos.

Registro de Compras y Contratos: Es el documento oficial mantenido por la Oficina de Tecnología que detalla los datos relevantes de cada adquisición y contratación, incluyendo el proveedor, la vigencia, la justificación y el responsable de su gestión.

Responsabilidades

A. Institución a través de la Oficina de Tecnología

La institución, a través de la Oficina de Tecnología, será responsable de establecer los criterios técnicos y administrativos que aseguren que las compras y contrataciones de tecnología se realicen de manera planificada, segura y alineada con las necesidades institucionales. Entre sus responsabilidades se incluyen:

- Evaluar técnicamente las solicitudes de adquisición o contratación de servicios tecnológicos, con el fin de determinar su viabilidad, pertinencia y alineación con la infraestructura tecnológica institucional.
- Asesorar a las unidades administrativas y académicas en la identificación de soluciones tecnológicas adecuadas que respondan a sus necesidades operacionales y funcionales.
- Verificar la compatibilidad e integración de los equipos, sistemas, programas o servicios a adquirir con la infraestructura tecnológica existente en la institución.
- Evaluar los aspectos de seguridad de la información, incluyendo riesgos asociados al uso de equipos, aplicaciones o servicios tecnológicos, antes de recomendar su adquisición o implementación.
- Revisar y emitir recomendaciones técnicas relacionadas con contratos, acuerdos de servicio, licencias de software y otros documentos vinculados a la adquisición o contratación de tecnología.
- Mantener un registro actualizado de las adquisiciones tecnológicas**,** incluyendo equipos, licencias, servicios contratados y sus respectivos períodos de vigencia.
- Coordinar la instalación, configuración e integración inicial de los equipos o sistemas tecnológicos adquiridos cuando corresponda.
- Promover el cumplimiento de las políticas institucionales de tecnología, así como de las normas y reglamentaciones aplicables del Gobierno de Puerto Rico relacionadas con compras y servicios tecnológicos.
- Identificar necesidades institucionales de actualización o renovación tecnológica**,** con el fin de apoyar la planificación estratégica y la sostenibilidad de la infraestructura tecnológica.

B. Responsabilidades de los Usuarios

Los usuarios que soliciten o gestionen la adquisición de equipos tecnológicos, programas o servicios relacionados con tecnología tendrán las siguientes responsabilidades:

- Justificar adecuadamente la necesidad de la adquisición o contratación**,** describiendo el propósito, uso institucional y beneficios esperados para las funciones académicas o administrativas.
- Canalizar las solicitudes de compra o contratación de tecnología a través de los procesos institucionales establecidos**,** incluyendo la evaluación técnica por parte de la Oficina de Tecnología.

- No realizar compras directas de equipos, software o servicios tecnológicos para uso institucional sin la debida evaluación y aprobación conforme a esta política y a los procedimientos administrativos vigentes.
- Proveer información completa y precisa sobre los requerimientos funcionales o técnicos relacionados con el equipo, sistema o servicio solicitado.
- Utilizar los equipos, sistemas o servicios tecnológicos adquiridos exclusivamente para fines institucionales**,** en cumplimiento con las políticas y normas aplicables.
- Colaborar con la Oficina de Tecnología en los procesos de instalación, configuración, evaluación o implementación de los recursos tecnológicos adquiridos.
- Notificar oportunamente cualquier problema, deficiencia o incumplimiento relacionado con equipos o servicios tecnológicos adquiridos mediante contratos o compras institucionales.

Cumplimiento / Sanciones

El incumplimiento de esta política puede conllevar sanciones administrativas según establecidas en las Normas de Conducta y Medidas Correctivas Aplicables a Empleados y Funcionarios de la Escuela de Artes Plásticas y Diseño de Puerto Rico.

Referencias

- PRITS – Normas de Adquisiciones y Contratación de Tecnología.
- NIST SP 800-53 – Controles de Adquisición y Gestión de Activos.
- ISO/IEC 19770 – Gestión de activos de “software” y “hardware”.

Certificación y aprobación

Esta política ha sido revisada y aprobada conforme a las disposiciones institucionales vigentes y entrará en vigor a partir de la fecha de su firma.

Nombre y firma de la Autoridad Nominadora:

Dra. Ileana Muñoz Landrón

Dra. Ileana Muñoz Landrón (Mar 18, 2026 14:39:04 EDT)

Fecha: 18/03/2026

Política de Programas “Software” y Licenciamiento

Propósito

Esta política tiene como propósito establecer los lineamientos institucionales para la adquisición, instalación, uso, gestión y control del software utilizado en los equipos y sistemas tecnológicos de la Escuela de Artes Plásticas y Diseño de Puerto Rico**,** garantizando el cumplimiento con las leyes de propiedad intelectual, los acuerdos de licenciamiento y las normas aplicables.

Alcance

Esta política aplica a todos los empleados, docentes, personal administrativo, contratistas, estudiantes y cualquier otra persona que utilice equipos, sistemas o recursos tecnológicos institucionales.

El alcance de esta política incluye, pero no se limita a:

- Todo programa “software” instalado en computadoras de escritorio, laptops, servidores y otros dispositivos tecnológicos propiedad de la institución.
- Programas informáticos, aplicaciones, sistemas institucionales, utilidades y herramientas tecnológicas utilizadas para fines académicos o administrativos.
- Programas “software” adquirido mediante licencias institucionales, suscripciones, licencias individuales o acuerdos con proveedores.
- Aplicaciones instaladas localmente en los equipos o utilizadas mediante plataformas en la nube o servicios en línea autorizados por la institución.
- Todo proceso relacionado con la instalación, uso, actualización, mantenimiento y control de licencias de programas “software” dentro de la institución.

El cumplimiento de esta política es obligatorio y deberá observarse en conjunto con otras políticas institucionales relacionadas con el uso de la tecnología, la seguridad de la información, el manejo de activos tecnológicos y los procesos de adquisición de tecnología.

Disposiciones de esta Política

1. Todo programa “software” utilizado en la institución deberá contar con una licencia válida y vigente, conforme a los términos establecidos por el proveedor o fabricante, o tratarse de software libre o de código abierto previamente evaluado y autorizado por la Oficina de Tecnología.
2. No se permitirá la instalación de software no autorizado en los equipos tecnológicos institucionales. Toda instalación deberá realizarse o contar con la aprobación de la Oficina de Tecnología.
3. Los usuarios no podrán modificar, reproducir, copiar, compartir o distribuir programas “software” instalado en los equipos institucionales sin la autorización expresa de la Oficina de Tecnología y sin cumplir con los términos del acuerdo de licenciamiento correspondiente.
4. Antes de autorizar el uso o la implementación de un programa “software “gratuito o de código abierto (por ejemplo, herramientas como GIMP o Photopea), la Oficina de Tecnología realizará una evaluación que considere, entre otros aspectos:
    - Los niveles de seguridad del programa y las vulnerabilidades conocidas.
    - La compatibilidad con la infraestructura tecnológica institucional.
    - El posible impacto sobre la privacidad y la protección de los datos institucionales.
5. La Oficina de Tecnología mantendrá un inventario actualizado de todas las licencias de programas “software” institucionales, el cual deberá incluir, entre otros, la siguiente información:
    - Nombre del software.
    - Tipo de licencia o modalidad de suscripción.
    - Fecha de adquisición y fecha de vencimiento de la licencia.
    - Unidad o persona responsable de su administración o gestión.
6. Las actualizaciones, parches de seguridad y renovaciones de licencias deberán gestionarse de manera oportuna por la Oficina de Tecnología, con el propósito de garantizar el cumplimiento con los acuerdos de licenciamiento, mantener la seguridad de los sistemas y asegurar el funcionamiento adecuado del software institucional.

Definiciones de Términos

Actualizaciones, Parches y Renovaciones: Son las actividades periódicas de gestión que se realizan para instalar correcciones de seguridad, mejoras de funcionalidad o para extender la vigencia legal del uso de un programa “software”, asegurando el cumplimiento y la protección contra vulnerabilidades.

Inventario de Licencias: Es el registro formal y centralizado mantenido por la Oficina de Tecnología que documenta todos los detalles clave de las licencias de programas “software” institucionales, incluyendo el tipo, la fecha de adquisición, la fecha de vencimiento y los términos de uso.

Licencia Válida: Es el permiso legal formal y documentado, adquirido por la institución, que autoriza el uso, la instalación y la copia de un programa "software" bajo términos y condiciones específicos, cumpliendo con las leyes de propiedad intelectual.

Programas "software": Se define como el conjunto de programas, procedimientos, reglas e instrucciones que permiten a las computadoras realizar tareas específicas, incluyendo sistemas operativos, aplicaciones, herramientas y "firmware".

Programas "software" Libres / Código Abierto (Open Source): Es aquel programa "software" cuyas licencias permiten a los Usuarios ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el programa libremente, pero cuya implementación requiere una evaluación formal de seguridad y compatibilidad por parte de la Oficina de Tecnología.

Programas "software" no Autorizado: Se refiere a cualquier programa instalado o utilizado en equipos institucionales que no cuenta con una licencia válida que no ha sido aprobado expresamente por la Oficina de Tecnología de la institución

Propiedad Intelectual: Son los derechos legales exclusivos concedidos al creador o propietario de una obra (en este caso, el programa "software" que prohíben su modificación, copia o distribución sin la autorización expresa del titular de la licencia.

Responsabilidades

A. Institución a través de la Oficina de Tecnología

La institución, a través de la Oficina de Tecnología, será responsable de establecer y administrar los mecanismos necesarios para asegurar el uso legal, seguro y adecuado de los programas "software" en los equipos y sistemas institucionales. Entre sus responsabilidades se incluyen:

- Establecer y administrar los procedimientos para la adquisición, instalación, actualización y control del "software" institucional, conforme a las necesidades académicas y administrativas de la institución.
- Evaluar y autorizar la instalación de "software" en los equipos institucionales, verificando su compatibilidad con la infraestructura tecnológica y su cumplimiento con los requisitos de seguridad de la información.
- Velar por el cumplimiento de las leyes de propiedad intelectual y de los acuerdos de licenciamiento aplicables al software utilizado en la institución.
- Mantener un inventario actualizado de las licencias de "software" institucionales, incluyendo información sobre tipo de licencia, número de licencias disponibles, fechas de adquisición y vigencia.
- Gestionar la instalación, configuración, actualización y aplicación de parches de seguridad del "software" institucional, con el fin de garantizar el funcionamiento adecuado de los sistemas y la protección de la información.

- Evaluar la utilización de “software” gratuito o de código abierto antes de su implementación en los equipos institucionales, considerando aspectos de seguridad, compatibilidad y protección de los datos institucionales.
- Realizar revisiones periódicas del “software” instalado en los equipos institucionales, con el propósito de verificar el cumplimiento de esta política y de los acuerdos de licenciamiento.
- Orientar y ofrecer asesoramiento técnico a las unidades administrativas y académicas sobre la selección y uso adecuado de programas y aplicaciones informáticas.
- Tomar las medidas necesarias para la remoción o sustitución de software no autorizado, obsoleto o que represente un riesgo para la seguridad de la información o la infraestructura tecnológica.

B. Usuarios

Todos los usuarios de los equipos, sistemas y recursos tecnológicos institucionales tienen la responsabilidad de cumplir con las disposiciones establecidas en esta política. Entre sus responsabilidades se incluyen:

- Utilizar únicamente el “software” autorizado e instalado en los equipos institucionales, conforme a los términos de licenciamiento establecidos por el proveedor.
- No instalar, copiar, descargar o utilizar “software” en los equipos institucionales sin la autorización previa de la Oficina de Tecnología.
- No reproducir, compartir, transferir o distribuir “software” institucional en violación de los acuerdos de licenciamiento o de las leyes de propiedad intelectual.
- Utilizar el “software” institucional exclusivamente para fines académicos, administrativos o institucionales, según corresponda.
- Notificar a la Oficina de Tecnología cualquier problema, irregularidad o mal funcionamiento relacionado con el “software” instalado en los equipos institucionales.
- Colaborar con la Oficina de Tecnología durante procesos de actualización, mantenimiento o verificación del “software” instalado en los equipos institucionales.
- Cumplir con las políticas institucionales relacionadas con el uso de la tecnología y la seguridad de la información, así como con las disposiciones establecidas en esta política.

Cumplimiento / Sanciones

El incumplimiento de esta política puede conllevar sanciones administrativas según establecidas en las Normas de Conducta y Medidas Correctivas Aplicables a Empleados y Funcionarios de la Escuela de Artes Plásticas y Diseño de Puerto Rico.

.

Referencias

- PRITS – Guía de Licenciamiento y Seguridad de “Software”.
- NIST SP 800-53 – Controles de Gestión de” Software” y Vulnerabilidades.
- ISO/IEC 19770 – Gestión de Activos de “Software”.

Certificación y aprobación

Esta política ha sido revisada y aprobada conforme a las disposiciones institucionales vigentes y entrará en vigor a partir de la fecha de su firma.

Nombre y firma de la Autoridad Nominadora:

Dra. Ileana Muñoz Landrón

Dra. Ileana Muñoz Landrón (Mar 18, 2026 14:39:04 EDT)

Fecha: 18/03/2026

Política de Capacitación y Concienciación Tecnológica

Propósito
El propósito de esta política es establecer las directrices para el desarrollo de competencias digitales y la creación de una cultura de seguridad en el uso de la tecnología. Busca asegurar que todo el personal:

- **Optimice el uso de las herramientas:** Reducir la brecha digital para mejorar la eficiencia operativa.
- **Mitigue riesgos de seguridad:** Capacitar a los empleados para identificar amenazas (como "*phishing*" o "*malware"*) y actuar como la primera línea de defensa de la organización.
- **Fomente la responsabilidad:** Garantizar que los usuarios comprendan sus obligaciones legales y éticas al manejar activos tecnológicos y datos sensibles.
- **Garantice la continuidad:** Mantener al equipo actualizado ante los cambios constantes del entorno tecnológico.

Alcance

Esta política aplica a todos los empleados, facultad, estudiantes, contratistas y proveedores autorizados con acceso a los sistemas, redes o datos de la institución. Así como activos tecnológicos como: el uso de computadoras, dispositivos móviles, "software" institucional, servicios en la nube y cualquier otro recurso digital propiedad de la institución utilizado para fines laborales.

Disposiciones de la Política

La institución implementará programas periódicos de capacitación y concienciación tecnológica, dirigidos a fortalecer las competencias de los usuarios en materia de:

- Ciberseguridad y buenas prácticas en el uso de la tecnología.
- Uso seguro del correo electrónico, aplicaciones y sistemas institucionales.
- Protección de datos personales, confidenciales e institucionales.
- Prevención de incidentes de seguridad, incluyendo, entre otros, "phishing", "malware" y "ransomware".

Todo usuario deberá participar, como mínimo una vez al año, en actividades de capacitación o concienciación en temas de tecnología y seguridad de la información, conforme a lo establecido por la institución.

La institución desarrollará y pondrá a disposición de los usuarios materiales de apoyo y recursos educativos, tales como manuales, guías prácticas, tutoriales y contenido audiovisual, accesibles a través de los medios institucionales.

La Oficina de Tecnología será responsable de evaluar la efectividad de los programas de capacitación, mediante mecanismos tales como encuestas, evaluaciones de conocimiento y el análisis de métricas relacionadas con incidentes de seguridad reportados.

La participación en procesos de capacitación en seguridad de la información será requisito obligatorio para empleados, docentes y contratistas de nuevo ingreso, previo a la asignación de credenciales o acceso a los sistemas institucionales.

Definiciones de Términos

Buenas Prácticas Digitales: Son los métodos y comportamientos recomendados que los Usuarios deben aplicar en el manejo de los sistemas y la información (tales como la gestión de contraseñas o el uso seguro del correo electrónico) para minimizar riesgos de seguridad y operativos.

Capacitación y Concienciación Tecnológica: Se define como el conjunto de actividades educativas y programas de formación diseñados para instruir a los usuarios sobre el uso seguro, ético y eficiente de los recursos tecnológicos y para fomentar una cultura de seguridad dentro de la institución.

Ciberseguridad: Es la práctica de proteger los sistemas, redes y programas de ataques digitales maliciosos que buscan acceder, modificar o destruir información sensible, o interrumpir los procesos operacionales.

Métricas de Incidentes Reportados: Son los datos cuantitativos utilizados por la Oficina de Tecnología para evaluar la efectividad de los programas de capacitación, midiendo el cambio en el número y la calidad de los reportes de incidentes por parte de los usuarios.

“Phishing”, “Malware” y “Ransomware”: Son tipos específicos de amenazas de seguridad que se utilizan en la capacitación:

- “Phishing”: Intentos de fraude para obtener información sensible mediante la suplantación de identidad en comunicaciones electrónicas.
- “Malware”: Programas “software” malicioso diseñado para dañar, deshabilitar o tomar el control de un sistema.
- Ransomware: Un tipo de” malware” que cifra los datos del usuario y exige un pago para su restauración.

Usuarios: Toda persona (personal administrativo, académico, estudiantes y contratistas) que utiliza los sistemas y recursos tecnológicos de la institución y que está obligada a participar en los programas de capacitación y concienciación.

Responsabilidades

A. Institución a través de la Oficina de Tecnología

- Diseñar, implementar y actualizar un programa continuo de capacitación y concienciación tecnológica dirigido a todos los usuarios institucionales.
- Ofrecer adiestramientos periódicos sobre temas de ciberseguridad, uso seguro de sistemas, protección de datos y manejo responsable de la información institucional.
- Establecer la frecuencia mínima de las capacitaciones, asegurando que estas se realicen al menos una vez al año o según los riesgos emergentes identificados.
- Desarrollar materiales educativos, guías, campañas informativas y recursos digitales que promuevan buenas prácticas en el uso de la tecnología.
- Mantener registros de participación, cumplimiento y aprovechamiento de las actividades de capacitación.
- Evaluar periódicamente la efectividad de los programas de capacitación mediante métricas, encuestas u otros mecanismos de medición.
- Notificar oportunamente a los usuarios sobre nuevas amenazas, vulnerabilidades o cambios en las políticas y procedimientos tecnológicos.
- Fomentar una cultura institucional de seguridad de la información y uso responsable de los recursos tecnológicos.
- Coordinar, cuando sea necesario, con otras dependencias institucionales la integración de la capacitación tecnológica en procesos académicos y administrativos.

B. Usuarios

- Participar activamente en las actividades de capacitación y concienciación tecnológica requeridas por la Institución.
- Completar los adiestramientos dentro de los periodos establecidos y cumplir con los requisitos de actualización periódica.
- Aplicar en su quehacer diario las buenas prácticas de seguridad y uso adecuado de la tecnología adquiridas durante las capacitaciones.
- Mantenerse informados sobre las políticas, normas y procedimientos tecnológicos vigentes.
- Reportar a la Oficina de Tecnología cualquier incidente de seguridad, intento de fraude o actividad sospechosa.
- Proteger sus credenciales de acceso y no compartirlas con terceros.
- Utilizar los recursos tecnológicos institucionales de manera responsable, ética y conforme a las normativas establecidas.
- Colaborar con la Institución en los procesos de evaluación y mejora de los programas de capacitación, cuando así se requiera.

Cumplimiento / Sanciones

El incumplimiento de esta política puede conllevar sanciones administrativas según establecidas en las Normas de Conducta y Medidas Correctivas Aplicables a Empleados y Funcionarios de la Escuela de Artes Plásticas y Diseño de Puerto Rico.

Referencias

- PRITS – Guía de Concienciación en Ciberseguridad
- NIST SP 800-50 – "Building an Information Technology Security Awareness and Training Program"
- ISO/IEC 27002 – Controles de Concienciación y Formación en Seguridad de la Información

Certificación y aprobación

Esta política ha sido revisada y aprobada conforme a las disposiciones institucionales vigentes y entrará en vigor a partir de la fecha de su firma.

Nombre y firma de la Autoridad Nominadora:

Dra. Ileana Muñoz Landrón

Dra. Ileana Muñoz Landrón (Mar 18, 2026 14:39:04 EDT)

Fecha: 18/03/2026

Política de Uso del Correo Electrónico y Comunicaciones Digitales

Propósito

Esta política tiene como propósito establecer las normas y directrices que regulan el uso adecuado, seguro y responsable del correo electrónico institucional y de los medios de comunicación digitales de la Institución. Asimismo, busca garantizar la protección de la información institucional, la confidencialidad de los datos, la integridad de las comunicaciones y la disponibilidad de los sistemas tecnológicos, minimizando riesgos asociados a incidentes de seguridad como accesos no autorizados, pérdida de información, fraude electrónico, "phishing" y otras amenazas cibernéticas.

Alcance

Esta política aplica a todos los miembros de la comunidad institucional, incluyendo, pero sin limitarse a, empleados, docentes, estudiantes, contratistas, consultores y cualquier otra persona autorizada a utilizar los sistemas tecnológicos de la Institución.

Disposiciones de la Política

1. Todo usuario deberá utilizar exclusivamente el correo electrónico institucional para la gestión de comunicaciones relacionadas con asuntos académicos, administrativos, oficiales o de investigación.
2. Se prohíbe el envío, reenvío, almacenamiento o distribución de correos electrónicos que contengan material ilegal, ofensivo, discriminatorio, difamatorio o que pueda comprometer la seguridad de la información o la reputación institucional.
3. Los usuarios deberán ejercer precaución ante correos electrónicos sospechosos y estarán obligados a reportar de inmediato a la Oficina de Tecnología cualquier intento de "phishing", "malware", fraude digital u otra actividad maliciosa.
4. Se prohíbe el uso del correo electrónico institucional para fines personales, comerciales o ajenos a la gestión institucional, salvo autorización expresa de la Institución.
5. La Oficina de Tecnología implementará y mantendrá mecanismos de seguridad, tales como filtros de contenido, antivirus, sistemas de detección de amenazas y otras herramientas, con el fin de proteger la infraestructura tecnológica y a sus usuarios.
6. Toda comunicación oficial deberá cumplir con las políticas institucionales de privacidad, confidencialidad y protección de datos aplicables.

7. Los usuarios deberán conservar los correos electrónicos institucionales que constituyan documentos oficiales, conforme a las normas institucionales de retención y disposición de documentos.
8. El correo electrónico institucional es propiedad de la Institución, por lo que podrá ser monitoreado, auditado o revisado conforme a las leyes y normativas aplicables, respetando los principios de confidencialidad y debido proceso.
9. Se prohíbe el uso del correo electrónico institucional para el envío masivo de mensajes no autorizados (spam), cadenas, propaganda o contenido no relacionado con las funciones institucionales.
10. Los usuarios deberán proteger sus credenciales de acceso al correo electrónico y no compartirlas con terceros bajo ninguna circunstancia.
11. Toda comunicación emitida desde el correo institucional deberá mantener un lenguaje profesional, respetuoso y acorde con los valores y normas de la Institución.
12. El uso del correo electrónico institucional desde dispositivos personales deberá cumplir con los controles de seguridad establecidos por la Institución.

Definiciones de Términos

Comunicaciones Digitales Oficiales: Son todos los mensajes, transmisiones y archivos intercambiados a través de las plataformas de mensajería y sistemas electrónicos autorizados por la EAPD, incluyendo el correo electrónico institucional.

Contenido Ilegal, Ofensivo o que Ponga en Riesgo la Seguridad: Se refiere a cualquier mensaje o archivo que viole las leyes aplicables, sea de naturaleza difamatoria, acosadora o discriminatoria, o que contenga enlaces y archivos que introduzcan “malware”, “phishing” o amenazas a los sistemas.

Correo Electrónico Institucional: Se define como la cuenta de mensajería electrónica provista y administrada por la EAPD a los usuarios, destinada exclusivamente para la comunicación de actividades académicas, administrativas y de investigación relacionadas con la institución.

Correo Sospechoso: Es cualquier mensaje de correo electrónico que parezca ser un intento de fraude, suplantación de identidad (phishing), o que contenga archivos adjuntos o enlaces inesperados que puedan comprometer la seguridad del Usuario o de la red institucional.

Filtros y Controles: Son las herramientas y configuraciones de seguridad implementadas por la Oficina de Tecnología en los servidores de correo, con el propósito de inspeccionar, bloquear o marcar automáticamente los mensajes maliciosos o no deseados (spam).

Fines Personales o Comerciales no Autorizados: Se refiere al uso del correo electrónico institucional para actividades no relacionadas con las funciones y responsabilidades del usuario dentro de la EAPD, incluyendo, pero no limitándose a, el envío masivo de publicidad, la gestión de negocios personales o el ocio.

Normas de Retención de Documentos y Registros: Son las regulaciones internas de la EAPD que dictan el periodo de tiempo mínimo y la manera en que ciertos correos electrónicos institucionales que contienen información oficial deben ser conservados.

Responsabilidades

1. **Institución a través de la Oficina de Tecnología**

   La Institución, a través de la Oficina de Tecnología, será responsable de:

   - Administrar, mantener y asegurar el funcionamiento adecuado de los servicios de correo electrónico institucional y plataformas de comunicación digital.
   - Implementar controles de seguridad, incluyendo filtros de contenido, sistemas antivirus, detección de amenazas y mecanismos de protección contra phishing, malware y otras vulnerabilidades.
   - Establecer, divulgar y mantener actualizadas las normas, procedimientos y guías relacionadas con el uso del correo electrónico y las comunicaciones digitales.
   - Proveer orientación y capacitación a los usuarios sobre el uso seguro, responsable y eficiente de estas herramientas.
   - Monitorear el uso de los sistemas de correo electrónico institucional conforme a las leyes y normativas aplicables, garantizando la protección de la información y el cumplimiento institucional.
   - Atender y responder a incidentes de seguridad relacionados con el correo electrónico y las comunicaciones digitales, implementando las medidas correctivas necesarias.
   - Mantener mecanismos de respaldo, recuperación y continuidad del servicio para proteger la información institucional.
   - Gestionar las cuentas de correo institucional, incluyendo su creación, modificación, suspensión o eliminación, según corresponda.
   - Velar por el cumplimiento de las políticas institucionales de privacidad, confidencialidad y protección de datos en el uso de las comunicaciones digitales.

2. **Usuarios**

   Todos los usuarios de los sistemas de correo electrónico y comunicaciones digitales institucionales serán responsables de:

   - Utilizar el correo electrónico institucional y las herramientas digitales únicamente para fines oficiales, académicos, administrativos o de investigación.
   - Cumplir con todas las políticas, normas y procedimientos institucionales relacionados con el uso de la tecnología y la seguridad de la información.
   - Proteger sus credenciales de acceso y evitar compartirlas con terceros.
   - Mantener la confidencialidad de la información transmitida o recibida mediante los sistemas institucionales.
   - Ejercer precaución al abrir correos electrónicos, enlaces o archivos adjuntos, especialmente cuando provengan de fuentes desconocidas o sospechosas.

- Reportar de inmediato a la Oficina de Tecnología cualquier incidente de seguridad, intento de fraude o actividad inusual relacionada con el correo electrónico.
- Utilizar un lenguaje profesional, respetuoso y acorde con los valores institucionales en todas las comunicaciones digitales.
- Cumplir con las disposiciones sobre retención, manejo y disposición de correos electrónicos que constituyan documentos oficiales.
- Evitar el uso indebido del correo electrónico institucional, incluyendo el envío de contenido no autorizado, ofensivo o ajeno a las funciones institucionales.

Cumplimiento / Sanciones

El incumplimiento de esta política puede conllevar sanciones administrativas según establecidas en las Normas de Conducta y Medidas Correctivas Aplicables a Empleados y Funcionarios de la Escuela de Artes Plásticas y Diseño de Puerto Rico.

Referencias

- PRITS – Políticas de Seguridad y Buenas Prácticas en Comunicaciones Digitales
- NIST SP 800-45 Rev. 2 – “Guidelines on Electronic Mail Security”
- ISO/IEC 27002 – Controles de Comunicación y Operación Segura de Sistemas

Certificación y aprobación

Esta política ha sido revisada y aprobada conforme a las disposiciones institucionales vigentes y entrará en vigor a partir de la fecha de su firma.

Nombre y firma de la Autoridad Nominadora:

Dra. Ileana Muñoz Landrón

Dra. Ileana Muñoz Landrón (Mar 18, 2026 14:39:04 EDT)

Fecha: 18/03/2026

Política de Acceso a la Red y Segmentación de “VLANs”

Propósito

La presente política tiene como propósito establecer las directrices y controles para el acceso seguro, controlado y eficiente a la red institucional, así como para la adecuada segmentación de la infraestructura de red mediante el uso de Redes de Área Local Virtuales (VLANs). Asimismo, busca proteger la confidencialidad, integridad y disponibilidad de la información y de los recursos tecnológicos, mediante la segregación lógica del tráfico de red, la limitación de accesos no autorizados y la mitigación de riesgos asociados a incidentes de ciberseguridad.

De igual forma, esta política promueve una gestión estructurada de la red institucional que permita optimizar el rendimiento, fortalecer la seguridad y garantizar la continuidad de los servicios tecnológicos en apoyo a las funciones académicas, administrativas y de investigación.

Alcance

Esta política aplica a todos los componentes de la infraestructura de red institucional, incluyendo, pero sin limitarse a, redes cableadas e inalámbricas, servidores, equipos de telecomunicaciones, sistemas de seguridad perimetral, dispositivos finales y cualquier otro recurso conectado a la red institucional. Igualmente, aplica a todos los usuarios autorizados, incluyendo empleados, docentes, estudiantes, contratistas, consultores y terceros que accedan a la red institucional, ya sea desde las instalaciones físicas de la Institución o de manera remota. Regula el acceso a la red institucional, la asignación de privilegios, la autenticación de usuarios y dispositivos, así como la implementación y administración de “VLANs” para la segmentación del tráfico de red, conforme a criterios de seguridad, función organizacional y nivel de riesgo.

Su cumplimiento es obligatorio y abarca el uso de dispositivos institucionales y personales que se conecten a la red, así como todas las actividades realizadas a través de la misma.

Disposiciones de la Política

1. Toda conexión a la red institucional deberá estar debidamente autenticada y autorizada, conforme al rol del usuario, tipo de dispositivo y nivel de acceso requerido.

2. La red institucional estará segmentada mediante Redes de Área Local Virtuales (VLANs), con el propósito de separar el tráfico académico, administrativo, de voz, de invitados y de sistemas críticos, entre otros, conforme a criterios de seguridad y funcionalidad.
3. El acceso a cada "VLAN" estará restringido exclusivamente a los usuarios y dispositivos autorizados, minimizando el riesgo de accesos indebidos y la propagación de amenazas dentro de la red.
4. Los dispositivos críticos de la infraestructura de red, tales como switches, routers, firewalls y controladores inalámbricos, deberán estar debidamente protegidos, configurados de forma segura y sujetos a monitoreo continuo.
5. Se implementarán mecanismos de filtrado de contenido y control de navegación para restringir el acceso a sitios web maliciosos o inapropiados, tales como aquellos relacionados con malware, phishing, contenido ilegal u otros definidos por la normativa institucional y los estándares aplicables, incluyendo los de PRITS.
6. Todo cambio en la configuración de la red, incluyendo la creación, modificación o eliminación de "VLANs", deberá ser previamente autorizado, documentado y gestionado por la Oficina de Tecnología conforme a procedimientos establecidos.
7. Se realizarán auditorías periódicas de los accesos, configuraciones y tráfico de red, con el fin de verificar el cumplimiento de esta política, identificar vulnerabilidades y detectar actividades inusuales o incidentes de seguridad.
8. Todo dispositivo que se conecte a la red institucional deberá cumplir con los requisitos mínimos de seguridad establecidos por la Institución, incluyendo actualizaciones, antivirus y configuraciones seguras.
9. El acceso a la red inalámbrica institucional deberá estar segmentado y protegido mediante mecanismos de autenticación segura, diferenciando entre usuarios internos y visitantes (red de invitados).
10. Se implementarán controles de acceso a la red basados en políticas (por ejemplo, Network Access Control - NAC), que permitan validar la identidad y el estado de seguridad de los dispositivos antes de conceder acceso.
11. El tráfico entre "VLANs" deberá estar controlado mediante reglas de firewall o listas de control de acceso (ACLs), limitando la comunicación únicamente a lo estrictamente necesario.
12. Se deberán mantener registros (logs) de acceso y actividad en la red, los cuales serán resguardados conforme a las políticas institucionales de retención de información y podrán ser utilizados para fines de auditoría e investigación.
13. El acceso remoto a la red institucional deberá realizarse a través de mecanismos seguros, tales como redes privadas virtuales (VPN) u otras tecnologías autorizadas por la Institución.
14. Se prohíbe la instalación o conexión de dispositivos de red no autorizados, tales como "routers, switches" o puntos de acceso inalámbrico, que puedan comprometer la seguridad o segmentación de la red.
15. La Oficina de Tecnología deberá evaluar periódicamente la arquitectura de segmentación de la red (VLANs) para asegurar su efectividad, escalabilidad y alineación con las necesidades institucionales.

Definiciones de Términos

Auditoría Periódica de Accesos y Tráfico: Es la revisión sistemática y programada de los registros de conexión y del flujo de datos de la red institucional, realizada con el fin de verificar el cumplimiento de esta política y detectar cualquier actividad anómala o acceso no autorizado.

Autenticación: Es el proceso mediante el cual se verifica la identidad de un usuario o dispositivo conectado a la red institucional, garantizando que solo las entidades legítimas intentan obtener acceso.

Autorización: Es el proceso que determina los recursos de red específicos (como el acceso a determinadas "VLANs" o servidores) a los que un usuario o dispositivo ya autenticado tiene permiso para acceder, basándose en su rol.

Dispositivos de Red Críticos: Son los componentes de hardware esenciales para el funcionamiento de la red (tales como "switches", "routers" y "firewalls") cuya configuración, disponibilidad y protección son fundamentales para la continuidad del servicio y la seguridad de la red institucional.

Filtros de Contenido: Son las medidas de seguridad implementadas a nivel de red para inspeccionar y bloquear el acceso a sitios web, aplicaciones o contenidos que han sido clasificados como inapropiados, maliciosos o contrarios a las políticas institucionales.

Red Institucional / Infraestructura de Red: Se define como el conjunto interconectado de "hardware" (routers, switches, firewalls) y software que permite la comunicación y el acceso a los recursos tecnológicos y a internet dentro de la institución.

"VLAN" (Virtual Local Area Network) / Segmentación: Es una técnica de segmentación lógica que divide una única red física en múltiples redes virtuales independientes, con el propósito de separar y aislar el tráfico de datos por su tipo (académico, administrativo, invitados, voz) para mejorar la seguridad y el rendimiento.

Responsabilidades

A. Institución a través de la Oficina de Tecnología

La Institución, a través de la Oficina de Tecnología, será responsable de:

1. Diseñar, implementar y administrar la arquitectura de red institucional, incluyendo la segmentación mediante "VLANs" conforme a criterios de seguridad, funcionalidad y mejores prácticas.
2. Establecer y mantener controles de acceso a la red, asegurando que la autenticación y autorización de usuarios y dispositivos se realice de acuerdo con sus roles y niveles de privilegio.
3. Configurar, proteger y monitorear continuamente los dispositivos de red críticos, tales como "switches, routers, firewalls" y sistemas inalámbricos.

4. Implementar mecanismos de seguridad, incluyendo firewalls, listas de control de acceso (ACLs), sistemas de detección y prevención de intrusiones, filtrado de contenido y soluciones de “Network Access Control (NAC)”.
5. Administrar la creación, modificación y eliminación de “VLANs”, asegurando que todo cambio sea debidamente autorizado, documentado y controlado.
6. Monitorear el tráfico de red y mantener registros (logs) de actividad para fines de auditoría, cumplimiento y respuesta a incidentes.
7. Realizar evaluaciones periódicas de vulnerabilidades, auditorías de red y pruebas de seguridad para identificar riesgos y fortalecer la infraestructura.
8. Garantizar la implementación de mecanismos de acceso remoto seguro, tales como “VPN” u otras tecnologías autorizadas.
9. Proveer orientación y capacitación básica a los usuarios sobre el acceso seguro a la red institucional y el uso adecuado de los recursos tecnológicos.
10. Atender, investigar y responder a incidentes de seguridad relacionados con el acceso a la red, implementando las medidas correctivas necesarias.
11. Velar por el cumplimiento de las normativas, estándares aplicables (incluyendo PRITS) y políticas institucionales relacionadas con la seguridad de la red.

B. Usuarios:

Todos los usuarios de la red institucional serán responsables de:

- Acceder a la red institucional únicamente mediante los mecanismos de autenticación autorizados y utilizando credenciales válidas.
- Utilizar la red conforme a su rol y nivel de acceso asignado, absteniéndose de intentar acceder a recursos o segmentos (VLANs) no autorizados.
- Proteger sus credenciales de acceso y no compartirlas con terceros bajo ninguna circunstancia.
- Asegurar que los dispositivos que utilicen para conectarse a la red cumplan con los requisitos mínimos de seguridad establecidos por la Institución.
- Abstenerse de instalar, conectar o configurar dispositivos de red no autorizados, tales como “routers, switches” o puntos de acceso inalámbrico.
- Utilizar la red institucional de manera responsable, ética y conforme a las políticas de uso aceptable de la tecnología.
- Reportar de inmediato a la Oficina de Tecnología cualquier incidente de seguridad, anomalía o actividad sospechosa en la red.
- No intentar evadir los controles de seguridad implementados, tales como filtros de contenido, segmentación de red o mecanismos de autenticación.
- Cumplir con todas las políticas, normas y procedimientos institucionales relacionados con el acceso y uso de la red.

Cumplimiento / Sanciones

El incumplimiento de esta política puede conllevar sanciones administrativas según establecidas en las Normas de Conducta y Medidas Correctivas Aplicables a Empleados y Funcionarios de la Escuela de Artes Plásticas y Diseño de Puerto Rico.

Referencias

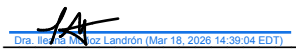
- PRITS – Guía de Seguridad de Redes y Segmentación de Sistemas
- NIST SP 800-53 – “Security and Privacy Controls for Information Systems”
- ISO/IEC 27002 – Controles de Comunicaciones y Operaciones de Seguridad

Certificación y aprobación

Esta política ha sido revisada y aprobada conforme a las disposiciones institucionales vigentes y entrará en vigor a partir de la fecha de su firma.

Nombre y firma de la Autoridad Nominadora:

Dra. Ileana Muñoz Landrón



Fecha: 18/03/2026

Política de Acceso a Información de Cuentas Deshabilitadas de Empleados

Propósito

Esta política tiene como propósito establecer los lineamientos y controles para el acceso, manejo y recuperación de la información contenida en cuentas institucionales deshabilitadas de empleados, garantizando la continuidad operacional de la Institución y la adecuada gestión de la información institucional. La misma, busca proteger la confidencialidad, integridad y disponibilidad de los datos, asegurando que el acceso a dicha información se realice de forma autorizada, justificada y conforme a las leyes, reglamentos y políticas institucionales aplicables.

De igual forma, esta política promueve la correcta administración de los activos de información ante la desvinculación, cambio de funciones o ausencia prolongada de un empleado, minimizando riesgos de pérdida de información crítica o interrupciones en los procesos institucionales.

Alcance

Esta política aplica a todas las cuentas institucionales de empleados que hayan sido deshabilitadas, suspendidas o inactivadas por motivo de renuncia, terminación de empleo, retiro, cambio de puesto, licencias prolongadas u otras circunstancias administrativas.

Incluye, pero no se limita a, cuentas de correo electrónico institucional, sistemas de información, plataformas digitales, almacenamiento en la nube y cualquier otro recurso tecnológico que contenga información institucional asociada al empleado.

Esta política aplica a la Oficina de Tecnología, Recursos Humanos, supervisores y cualquier otro personal autorizado que participe en el proceso de solicitud, evaluación, autorización y acceso a la información contenida en dichas cuentas. u cumplimiento es obligatorio y se extiende a todo el personal que, por la naturaleza de sus funciones, tenga intervención en la gestión o acceso a este tipo de información.

Disposiciones de la Política

1. Toda solicitud de acceso a cuentas deshabilitadas deberá realizarse exclusivamente mediante correo electrónico dirigido al Oficial Principal de Información (OPI).
2. El correo de solicitud deberá incluir la siguiente información obligatoria:

    - Nombre completo del peticionario.
    - Puesto o cargo del peticionario.
    - Tema o descripción breve de la petición.
    - Justificación de la necesidad de acceso.
    - Firma del peticionario (electrónica o escaneada).

3. El OPI evaluará la solicitud considerando criterios de confidencialidad, necesidad legítima y autorización jerárquica.
4. Si la solicitud es considerada válida, el OPI remitirá la petición a la autoridad nominadora de la Institución para su aprobación formal antes de proceder.
5. Una vez obtenida la aprobación por escrito de la autoridad nominadora, el OPI notificará al peticionario que el proceso será realizado, indicando el tiempo estimado de cumplimiento.
6. El custodio o encargado de las cuentas (seguridad de red o administrador de sistemas) será instruido formalmente por el OPI para habilitar temporalmente la cuenta solicitada, exclusivamente con el propósito de recuperar la información requerida.
7. Una vez completada la extracción o entrega de la información, el OPI notificará al solicitante sobre el cumplimiento del proceso y documentará la acción realizada.
8. La cuenta será deshabilitada nuevamente de inmediato, y la autoridad nominadora será notificada mediante correo electrónico confirmando que la cuenta ha sido cerrada y que no existen accesos activos.
9. Todo el proceso deberá ser documentado y archivado electrónicamente en el sistema de registros de la Oficina de Tecnología, por un período mínimo de cinco (5) años, garantizando trazabilidad y cumplimiento de auditorías.

Definiciones de Términos

Autoridad Nominadora: Rector(a) o Director(a) Ejecutivo(a) con poder formal de aprobación.

Cuenta deshabilitada: Perfil o credencial de usuario cuya autenticación ha sido bloqueada o revocada.

Custodio de Cuentas: Administrador de sistemas responsable de gestionar las credenciales y accesos.

Oficial Principal de Informática (OPI): Responsable de evaluar, autorizar y supervisar los procesos tecnológicos y de seguridad de la información institucional.

Peticionario: Persona que solicita acceso a la información.

Responsabilidades

A. Oficina de Tecnología / Oficial Principal de Informática

- Recibir, evaluar y gestionar todas las solicitudes de acceso a cuentas deshabilitadas, verificando necesidad legítima, confidencialidad y cumplimiento de la política.
- Coordinar con la autoridad nominadora la aprobación formal antes de conceder cualquier acceso temporal.
- Instruir formalmente al custodio de cuentas sobre la habilitación temporal y el alcance del acceso permitido.
- Monitorear y supervisar el acceso temporal, asegurando que se realice exclusivamente para fines institucionales autorizados.
- Documentar y archivar todo el proceso, incluyendo solicitudes, aprobaciones, acciones realizadas y cierre de cuentas, por un período mínimo de cinco (5) años.
- Notificar al solicitante y a la autoridad nominadora sobre el cumplimiento del proceso y el cierre definitivo de la cuenta.

B. Autoridad Nominadora

- Revisar y aprobar formalmente las solicitudes de acceso a cuentas deshabilitadas, asegurando que cada petición tenga justificación legítima y cumpla con las normas institucionales.
- Garantizar que el acceso temporal a la información se limite a fines institucionales y se realice bajo los controles de seguridad establecidos.
- Ser notificada por la Oficina de Tecnología/OPI sobre la finalización del acceso y el cierre definitivo de la cuenta.

C. Custodio de Cuentas (Administrador de Sistemas)

- Habilitar temporalmente las cuentas deshabilitadas únicamente siguiendo instrucciones formales del OPI.
- Asegurar que el acceso temporal cumpla con los límites establecidos (tiempo, finalidad, datos autorizados).
- Mantener la seguridad de la cuenta y prevenir accesos no autorizados durante el periodo temporal.
- Deshabilitar la cuenta inmediatamente después de completada la recuperación de información y notificar al OPI sobre el cierre.

D. Peticionario

- Solicitar acceso a cuentas deshabilitadas exclusivamente mediante los canales oficiales y con toda la información requerida (nombre, cargo, descripción de la solicitud, justificación y firma).
- Limitar el uso de la información recuperada a los fines institucionales autorizados.

- No intentar acceder a la cuenta por medios no autorizados ni compartir credenciales de terceros.
- Reportar inmediatamente cualquier incidente o irregularidad detectada durante el proceso de acceso temporal.

Cumplimiento / Sanciones

El incumplimiento de esta política puede conllevar sanciones administrativas según establecidas en las Normas de Conducta y Medidas Correctivas Aplicables a Empleados y Funcionarios de la Escuela de Artes Plásticas y Diseño de Puerto Rico.

Referencias

- **PRITS:** Política de Seguridad de la Información del Gobierno de Puerto Rico, sección de Acceso y Control de Cuentas
- **NIST SP 800-53 Rev. 5:** Controles AC-2 (Account Management), AC-3 (Access Enforcement), y AU-6 (Audit Review, Analysis, and Reporting)
- **NIST SP 800-171:** Protección de Información Institucional No Clasificada (CUI)
- **ISO/IEC 27002:** Control de Acceso y Gestión de Identidades

Certificación y aprobación

Esta política ha sido revisada y aprobada conforme a las disposiciones institucionales vigentes y entrará en vigor a partir de la fecha de su firma.

Nombre y firma de la Autoridad Nominadora:

Dra. Ileana Muñoz Landrón

Dra. Ileana Muñoz Landrón (Mar 18, 2026 14:39:04 EDT)

Fecha: 18/03/2026