CERTIFICACIÓN NÚMERO 16
2025-2026

Yo, Luz E. Maldonado Reyes, secretaria de la Junta de Retiro del Fideicomiso del Sistema de Retiro UPR, CERTIFICO:

La Junta de Retiro del Fideicomiso del Sistema de Retiro UPR, en reunión ordinaria celebrada el 17 de octubre de 2025, en virtud de la Ley Núm 219-2012, conocida como Ley de Fideicomisos y la Escritura Número 58, sobre Ratificación y Reconocimiento de Fideicomiso de 29 de junio de 2016, determinó aprobar lo siguiente:

"Política de Ciberseguridad del Fideicomiso del Sistema de Retiro UPR"

Y, PARA QUE ASÍ CONSTE, expido la presente Certificación, en San Juan, Puerto Rico, hoy 31 de octubre de 2025.

Luz E. Maldonado Reyes
Secretaria
Junta de Retiro UPR

Política de Ciberseguridad del Fideicomiso del Sistema de Retiro UPR

Certificación Núm. 16 (2025-2026)

INDICE **PÁGINA**

"Política de Ciberseguridad del Fideicomiso del Sistema de Retiro UPR"

ARTÍCULO I - TÍTULO

Este documento se conocerá como la "Política de Ciberseguridad del Fideicomiso del Sistema de Retiro UPR" (en adelante, la Política de Ciberseguridad).

ARTÍCULO II - RESUMEN EJECUTIVO

La presente Política de Ciberseguridad se promulga con el objetivo primordial de proteger los activos de información del Fideicomiso del Sistema de Retiro UPR (en adelante, el Fideicomiso) y la Junta de Retiro UPR (en adelante Junta) y asegurar la confidencialidad, integridad y disponibilidad de los datos que gestiona. En un entorno digital cada vez más complejo y con amenazas persistentes, el Fideicomiso y la Junta se comprometen a implementar un marco robusto de ciberseguridad que salvaguarde la información de sus participantes, jubilados(as), empleados, y fiduciarios, así como la infraestructura tecnológica que apoya sus operaciones críticas.

ARTICULO III. BASE LEGAL

La Junta de Retiro UPR lo adopta esta Política de Ciberseguridad en virtud de la autoridad que le confiere la Escritura Núm. 58, sobre Ratificación y Reconocimiento de Fideicomiso; la Ley Núm. 219 de 31 de agosto de 2012, según enmendada, conocida como Ley de Fideicomisos de Puerto Rico.

ARTÍCULO IV - PROPÓSITO Y ALCANCE

A**.** La Política de Ciberseguridad tiene los siguientes propósitos:

1. Establecer los principios, estándares y controles de ciberseguridad para proteger la información y los sistemas de información del Fideicomiso y la Junta contra accesos no autorizados, divulgación, alteración, destrucción o interrupción.
2. Definir las responsabilidades de los usuarios, el personal de la Oficina de Sistemas de Información (OSI), los contratistas y terceros en relación con la ciberseguridad.
3. Establecer un marco para la gestión de riesgos cibernéticos, la detección de incidentes, la respuesta y la recuperación.
4. Promover una cultura organizacional de concientización y responsabilidad en ciberseguridad en todos los niveles del Fideicomiso y la Junta.

B. Alcance: La Política de Ciberseguridad aplica a todos los activos de información, sistemas, redes, aplicaciones y dispositivos propiedad o bajo la custodia del Fideicomiso y la Junta, independientemente de su ubicación física o de quién los opere. Incluye a todos los usuarios, sean fiduciarios, empleados, participantes, jubilados, contratistas,

consultores, suplidores, visitantes o cualquier tercero autorizado con acceso a los recursos del Fideicomiso.

ARTÍCULO V - DEFINICIONES

Para fines de interpretación y aplicación de esta Política, los siguientes términos aquí utilizados tendrán el siguiente significado:

Las palabras y frases usadas en esta Política se interpretarán según el contexto y el significado aceptado por el uso común y consciente; las usadas en el tiempo presente incluyen el futuro; las usadas en el género masculino incluyen el femenino y el neutro, salvo en los casos en que tal interpretación resultare absurda. El singular incluye el plural y el singular.

A. ***Endpoints:*** dispositivo informático que se comunica a través de una red a la que está conectado**.** Normalmente se refiere a los dispositivos que utilizamos a diario como computadoras, *laptops*, teléfonos celulares, *tablets* o dispositivos de Internet.

B. Menor privilegio: principio que establece que cada usuario, sistema, aplicación o proceso debe tener únicamente los permisos mínimos necesarios para realizar sus funciones legítimas y nada más.

C. Necesidad de saber: principio que establece que una persona debe tener acceso únicamente a la información que necesita para cumplir con sus funciones o responsabilidades laborales, y nada más.

ARTÍCULO VI - PRINCIPIOS DE CIBERSEGURIDAD

La Ciberseguridad es la práctica de proteger sistemas, redes, datos y programas de ataques cibernéticos digitales maliciosos.

El Fideicomiso y la Junta se comprometen a regirse por los siguientes principios fundamentales de Ciberseguridad:

A. Confidencialidad: Proteger la información sensible y clasificada de ser divulgada a personas o entidades no autorizadas.

B. Integridad: Asegurar que la información no sea modificada o destruida de manera no autorizada, manteniendo su exactitud y completitud.

C. Disponibilidad: Garantizar que los usuarios autorizados tengan acceso a la información y a los sistemas cuando sea necesario.

D. Gestión de Riesgos: Identificar, evaluar, priorizar y mitigar los riesgos cibernéticos de manera continua, adoptando un enfoque proactivo.

E. Cumplimiento Legal y Regulatorio: Adherirse estrictamente a todas las leyes, reglamentos y políticas aplicables en materia de ciberseguridad y protección de datos.

F. Concientización y Capacitación: Educar y capacitar continuamente a todo el personal sobre las mejores prácticas de ciberseguridad y sus responsabilidades individuales.

G. Mejora Continua: Revisar y actualizar continuamente esta Política y sus controles asociados para adaptarse a la evolución de las amenazas y tecnologías.

ARTÍCULO VII - GESTIÓN DE RIESGOS CIBERNÉTICOS

A. Evaluación de Riesgos: La OSI realizará evaluaciones periódicas de riesgos cibernéticos para identificar vulnerabilidades, amenazas y el impacto potencial en sus activos de información. Estas evaluaciones se llevarán a cabo trimestralmente y tras cambios significativos en la infraestructura o los sistemas.

B. Mitigación de Riesgos: Se implementarán controles de seguridad técnicos, administrativos y físicos para mitigar los riesgos identificados a un nivel aceptable. Esto incluirá, pero no se limitará a, la implementación de cifrado, autenticación multifactorial, segmentación de red, y controles de acceso basados en roles.

C. Monitoreo Continuo: Se establecerán mecanismos de monitoreo continuo veinticuatro horas al día, los siete días de la semana (24/7) de la seguridad de la red y los sistemas para detectar y responder a actividades sospechosas o incidentes.

ARTÍCULO VIII - GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD

A. Detección y Notificación: Todos los usuarios tienen la responsabilidad de reportar cualquier incidente de ciberseguridad sospechoso o confirmado a la OSI de manera inmediata. La OSI es responsable de la detección y análisis inicial de incidentes.

B. Respuesta a Incidentes: La OSI establecerá un Plan de Respuesta a Incidentes de Ciberseguridad que detalle los procedimientos para contener, erradicar y recuperar los sistemas y datos afectados por un incidente. Este plan incluirá roles y responsabilidades claras, y se probará y actualizará regularmente.

C**.** Comunicación y Notificación Externa: En caso de un incidente cibernético que cumpla con los criterios de notificación del Plan de Respuesta, el Fideicomiso, a través de la OSI, la alta gerencia y la Junta, notificarán a las autoridades pertinentes (como el FBI, de ser necesario) en un plazo no mayor a 8 horas desde el descubrimiento del incidente. Se determinará la necesidad de notificar a individuos afectados según la magnitud del incidente y las leyes aplicables de protección de datos.

D. Análisis Post-Incidente: Se realizará un análisis exhaustivo después de cada incidente para identificar la causa raíz, las lecciones aprendidas y las acciones correctivas necesarias para prevenir futuras ocurrencias.

ARTÍCULO IX – IMPLEMENTACION DE CONTROLES DE SEGURIDAD

El Fideicomiso implementará, como mínimo, los siguientes controles de seguridad:

A. Control de Acceso:
   - Implementación del principio de "necesidad de saber" y "menor privilegio".
   - Uso de autenticación multifactorial (MFA) para accesos remotos y a sistemas críticos.
   - Gestión de identidades y accesos robusta, con revisiones periódicas de privilegios.

B. Seguridad de la Red:
   - Segmentación de redes para limitar el movimiento lateral en caso de una brecha.
   - Uso de *firewalls*, sistemas de detección/prevención de intrusiones (IDS/IPS).
   - Uso de Redes Privadas Virtuales (VPN) para acceso remoto seguro.

C. Protección de Endpoints:
   - Implementación de software antivirus/antimalware en todos los dispositivos.
   - Gestión de parches y actualizaciones de seguridad de manera regular.
   - Encriptación de datos en dispositivos portátiles y de almacenamiento.

D. Gestión de Vulnerabilidades:
   - Escaneos de vulnerabilidades periódicos y pruebas de penetración.
   - Proceso formal para la remediación de vulnerabilidades.

E. Protección de Datos:
   - Clasificación de la información según su sensibilidad y criticidad.
   - Cifrado de datos sensibles en reposo y en tránsito.
   - Implementación de políticas de retención y eliminación segura de datos.
   - Realización de copias de seguridad (backups) regulares y probadas para asegurar la recuperación de datos.

F. Adiestramientos y Capacitación en Ciberseguridad:
   - Programa de capacitación obligatorio anual para todos los usuarios.
   - Adiestramientos sobre amenazas actuales (phishing, ransomware, etc.).
   - Simulacros de phishing para evaluar la preparación de los usuarios.

G. Seguridad en la Adquisición y Desarrollo de Sistemas:
   - Integración de la seguridad desde las fases iniciales del ciclo de vida del desarrollo de software (SDLC).

- Revisión de seguridad y cumplimiento de proveedores externos antes de la contratación.

ARTÍCULO X - RESPONSABILIDADES

A. Junta de Retiro / Dirección Ejecutiva:
   - Aprobar y respaldar la Política de Ciberseguridad y asegurar los recursos necesarios para su implementación.
   - Revisar el estado de la ciberseguridad en el Fideicomiso periódicamente.

B. Oficina de Tecnología e Información (OTI) / Director de OTI:
   - Desarrollar, implementar y mantener esta Política y los procedimientos de ciberseguridad.
   - Supervisar la implementación de los controles de seguridad y la gestión de riesgos.
   - Dirigir la respuesta a incidentes de ciberseguridad.
   - Actualizarse con relación a las amenazas cibernéticas y las mejores prácticas adoptadas por la comunidad tecnológica.

C. Usuarios (Empleados, Participantes, Jubilados, Fiduciarios, Contratistas):
   - Cumplir con estas políticas y el Plan de Respuesta de Incidentes de Ciberseguridad del Fideicomiso.
   - Proteger las credenciales de acceso y dispositivos.
   - Reportar incidentes de seguridad o actividades sospechosas de manera inmediata.
   - Participar en los adiestramientos y concientización sobre ciberseguridad.

ARTÍCULO XI - CUMPLIMIENTO Y CONSECUENCIAS

A. Cumplimiento: El cumplimiento de esta Política es obligatorio para todos los usuarios. El desconocimiento de esta Política no exime de su cumplimiento.

B. Auditorías: El Fideicomiso realizará auditorías internas y/o externas periódicas para verificar el cumplimiento con esta Política y las regulaciones aplicables.

C. Consecuencias: Las violaciones a esta Política pueden resultar en acciones disciplinarias, incluyendo la terminación del empleo o contrato, y/o las acciones legales correspondientes, sin perjuicio de las sanciones civiles y penales establecidas por la Ley federal conocida como "Computer Fraud and Abuse Act" ("CFAA"), 18 U.S.C. § 1030.

ARTÍCULO XII - REVISIÓN Y MANTENIMIENTO

Esta Política de Ciberseguridad será revisada y actualizada semestralmente o cuando ocurran cambios significativos en el entorno regulatorio, tecnológico o de amenazas. Cualquier enmienda o derogación deberá ser aprobada por la Junta de Retiro UPR para asegurar la coherencia con la política tecnológica y de ciberseguridad.

ARTÍCULO XIII - SEPARABILIDAD

A. Las disposiciones de esta Política son separables entre sí, y la nulidad de cualquier artículo o sección no afectará la validez de los demás artículos o secciones.

B. Corresponderá a la Junta de Retiro UPR interpretar las disposiciones de esta Política y decidir cualquier controversia en relación con sus disposiciones o con situaciones no previstas en el mismo.

ARTÍCULO XIV – DEROGACION O ENMIENDA

Esta política podrá ser enmendada o derogada únicamente por la Junta de Retiro UPR.

ARTICULO XV- VIGENCIA

Esta Política entrará en vigor inmediatamente después de su aprobación.