



Universidad Interamericana de Puerto Rico

NORMAS SOBRE LA CONFIDENCIALIDAD DE LA INFORMACION

DOCUMENTO NORMATIVO I-1209-006

Introducción

La Universidad Interamericana de Puerto Rico, como parte de los procesos administrativos, maneja información de diversa índole. Esta información es, en su mayor parte, de carácter confidencial. La confidencialidad de la información se extiende a los procesos de recopilación, uso y divulgación, a través de diferentes medios, entre ellos documentos, sistemas electrónicos y medios de transferencia o almacenamiento de información.

Existen leyes que requieren que la información confidencial manejada por la Institución se mantenga protegida de accesos no autorizados. Por ello, es de suma importancia que se den a conocer a toda la comunidad universitaria y se implanten las normas aquí establecidas para el manejo de la información confidencial.

I. Base legal

Estas normas se establecen en virtud de la autoridad conferida al Presidente de la Universidad por la Junta de Síndicos en los Estatutos de la Universidad. Las mismas tienen su base en la política establecida por la Junta de Síndicos en los documentos Política Institucional para el Uso Apropiado de la Tecnología de Información, los Sistemas de Información Computadorizados y las Telecomunicaciones; la Reglamentación de la Universidad Interamericana de Puerto Rico sobre el Directorio de Estudiantes y Ex-Alumnos; y Guías, Normas y Procedimientos para la Protección de la Información del Consumidor.

Además, están en armonía con las leyes internacionales, federales y estatales aplicables que gobiernan la privacidad y confidencialidad de información, incluyendo el "Electronic Communications Privacy Act" de 1986, la Ley FERPA de 1974 (según enmendada), 20 U.S.C. 1232g, las regulaciones establecidas bajo 34 C.F.R., Parte 99, "Portability and Accountability Act" (HIPAA) y las reglamentaciones de la "Federal Communication Commission".

Oficina del Presidente


II. Propósito

Este documento tiene el propósito de definir cuál información es confidencial y de establecer las normas que deberá seguir la comunidad universitaria cuando maneje o reciba información catalogada de esta forma. Estas normas, además, se seguirán en todos los procedimientos que incluyen el manejo de información confidencial, entre ellos: la divulgación de información a terceros, de documentos digitales y las firmas digitales y firmas digitalizadas.

Estos procedimientos se establecen en documentos separados.

III. Alcance


Estas normas serán aplicables a todas las personas que por motivos de sus funciones tengan acceso a información confidencial de la Universidad. Estas personas incluyen, pero no necesariamente se limitan a:

- 
- 3.1 Empleados de los recintos y centros cibernéticos.
 - 3.2 Empleados de la Oficina Central del Sistema.
 - 3.3 Estudiantes de las unidades académicas, incluyendo aquellos matriculados en cursos a distancia y padres y/o custodios de estudiantes.
 - 3.4 Entidades externas con las que la Universidad intercambia información autorizada.
 - 3.5 Miembros de la Junta de Síndicos.
 - 3.6 Suplidores y contratistas

IV. Definiciones

Para propósitos de este documento, los siguientes términos tendrán el significado que se indica a continuación:

- 4.1 Centro de Informática y Telecomunicaciones – oficina en el nivel central o de una unidad que administra, mantiene y configura las aplicaciones, sistemas de información, redes, telecomunicaciones y las cuentas de los usuarios.
- 4.2 Comunidad Universitaria – conjunto de personas que trabaja o estudia en la Universidad.


- 
- 4.3 “Data Leak/Loss Prevention” (DLP) – herramienta que permite evitar la pérdida de información confidencial, así como también monitorear los accesos a estos datos en la red.
 - 4.4 Ejecutivo Principal – los rectores y los decanos de las escuelas profesionales.
 - 4.5 Información confidencial – información que al ser divulgada pueda causar daño o perjuicio a la persona. Esto incluye, pero no se limita a información sobre el seguro social, número de licencia de conducir, fecha de nacimiento, número de tarjeta de crédito, cuenta de banco o condiciones de salud y expedientes académicos. La información confidencial puede incluir secretos de negocio, planes de mercadeo y programas de desarrollo de la Universidad, entre otros.
 - 4.6 Información cifrada o en clave – información que se ha transformado utilizando un algoritmo o una clave para que no pueda ser leída por nadie, excepto el remitente autorizado.
 - 4.7 Junta de Síndicos – la Junta de Síndicos de la Universidad Interamericana de Puerto Rico, Inc.
 - 4.8 Presidente – el Presidente de la Universidad Interamericana de Puerto Rico.
 - 4.9 “Remote Authentication Dial-In User Server” (RADIUS) – protocolo de autenticación y autorización para aplicaciones de acceso a la red.
 - 4.10 Sistema de Control de Acceso del Controlador de Acceso a Terminales “Terminal Access Controller Access Control System” (TACACS) – protocolo de autenticación remota que se usa para gestionar el acceso a servidores y dispositivos de comunicaciones. Para lograr esto, proporciona servicios separados de autenticación, autorización y registro.
 - 4.11 Universidad o Institución – la Universidad Interamericana de Puerto Rico, Inc.

V. Privacidad y confidencialidad

- 5.1 La información a la que se accede en la Universidad se recibe de entidades externas, o es creada internamente. Esta información debe utilizarse con responsabilidad, a tenor con las leyes y reglamentos mencionados anteriormente, y está sujeta a las normas aquí establecidas.
 - 5.1.1 La confidencialidad de la información aplica tanto a la información electrónica como a los documentos en papel. Esto incluye, pero no

se limita a: expedientes académicos y otros expedientes propiedad de la Institución y reglamentación relacionada con la conservación de ciertos expedientes, según la política institucional o las leyes aplicables.

5.1.2 Las leyes de confidencialidad incluyen protección a expedientes, documentos e información relacionada directamente con las personas de la comunidad universitaria, que incluye pero no se limita a: transcripciones de créditos (y cualquier otro documento obtenido de la institución en la cual el estudiante haya estado previamente matriculado), información administrativa, académica y personal, directorio de información, al igual que la información de revisión y evaluación del personal.



5.2 La información utilizada por la Universidad puede encontrarse en diferentes medios. Esto incluye, pero no se limita necesariamente a lo siguiente: papel, diskettes, discos compactos, microfichas, cintas magnéticas, cartuchos, discos duros, "pen drives", vídeos (videocasetes) y DVD's, entre otros. También incluye información de diversa índole, como: textos, gráficos, videocintas y grabaciones de audio, entre otras.

VI. Disposiciones generales

- 6.1 La Universidad Interamericana se compromete a acatar las leyes que gobiernan la confidencialidad de la información y, a su vez, proteger esa información de una manera congruente con su clasificación y valor. La política de la Universidad sobre la divulgación de información académica de sus estudiantes se encuentra en los catálogos de la Universidad, y en los documentos normativos citados en la Sección I - Base legal, de este documento.
- 6.2 La Universidad evita la divulgación no autorizada de información, asegura el cumplimiento de las leyes y reglamentaciones vigentes y protege el valor y la reputación de su información, siendo ésta una de las más importantes normas de confidencialidad dentro de la Universidad.
- 6.3 La Universidad se compromete a trabajar de forma ética y legal al recopilar y utilizar la información de sus estudiantes y empleados. Esta información sólo será utilizada para propósitos educativos o de trabajo.
- 6.4 Para garantizar la confidencialidad de la información, los sistemas de información de la Universidad proveen módulos de rigurosa seguridad para el otorgamiento de contraseñas para limitar los accesos. Los permisos de acceso a los sistemas son aprobados o denegados por los supervisores de los empleados. De esta forma, se asegura de que sólo

aquellas personas cuyas funciones requieran acceder a cierta información puedan tener esa prerrogativa.

- 6.5 La Universidad tiene la obligación de asegurar que sus empleados observen los más altos estándares de conducta para mantener la confidencialidad de información y protegerla de fraude o uso inapropiado.
- 6.6 La Institución exige a las empresas externas, con las cuales realiza proyectos y trabajos especiales, que protejan en forma apropiada y mantengan la confidencialidad de la información personal que se comparte con ellas.
- 6.7 La Universidad respeta la privacidad de los usuarios de sus recursos tecnológicos, pero se reserva el derecho de inspeccionar el uso de tales recursos cuando haya una sospecha fundada de violaciones a las políticas y normas de la Universidad, a las leyes internacionales, federales y estatales, o cuando haya una situación de emergencia o una amenaza a la integridad o seguridad del sistema de computadoras.

VII. Manejo de la información confidencial


7.1 Categorías para clasificación

7.1.1 La clasificación de la información determinará cómo la información se asegura, maneja, retiene y dispone. La divulgación de información institucional a las fuentes externas se rige por la Ley FERPA de 1974 (según enmendada), 20 U.S.C. 1232g, y las regulaciones establecidas en ella bajo, 34 C.F.R., Parte 99. La información de la Universidad se clasificará en una de las siguientes categorías:


- 7.1.1.1 Información confidencial – información cuya pérdida, corrupción o divulgación desautorizada serían una violación de leyes federales o estatales, regulaciones o contratos de la Universidad.
- 7.1.1.2 Información para uso exclusivamente operacional – información cuya pérdida, corrupción o divulgación desautorizada no necesariamente producen alguna pérdida comercial, financiera o legal. No obstante, dicha información está disponible solamente a un custodio o a los usuarios autorizados.
- 7.1.1.3 Información privada – información cuya divulgación no produciría ninguna pérdida comercial, financiera o legal, pero involucra problemas de credibilidad personal, reputación u otros problemas de privacidad personal.

- 7.1.1.4 Información restringida – información cuya pérdida, corrupción o divulgación desautorizada tenderían a causar daño a la Universidad o a sus funciones de investigación o producirían alguna pérdida comercial, financiera o legal a la Institución.
- 7.1.1.5 Información no clasificada – información que no entra en ninguna de las otras clasificaciones de la información desglosadas anteriormente. Esta información está generalmente disponible, posiblemente sin la aprobación de un custodio específico de la información.

7.2 Proceso de clasificación

- 
- 7.2.1 Toda la información, no importa el medio o naturaleza, será clasificada por las personas correspondientes, Sección VIII - Responsabilidades y será identificada según las categorías anteriores (Sección 7.1.1).
- 7.2.2 Toda información será identificada en el nivel más seguro de la clasificación. Cuando exista información de clasificación mixta, se deberá clasificar en la categoría más segura. Si un empleado no está seguro de la clasificación de cierta información, debe consultar con su supervisor inmediato.
- 7.2.2.1 Cuando se trate de información contenida en un archivo o base de datos, la información será clasificada en el mismo nivel que el archivo o base de datos del cual fue extraída (operacional, privada, restringida o confidencial).
- 7.2.3 Toda información será:
- 7.2.3.1 Asegurada contra la creación, actualización y procesamiento por medios electrónicos y contra la divulgación no autorizada.
- 7.2.3.2 Apropiadamente asegurada y no accesible a los usuarios no autorizados cuando no esté en uso.
- 7.2.3.3 Dispuesta o destruida de manera apropiada, según estipulado en el Reglamento para la Administración de Documentos (incluye todo informe que contenga información operacional, privada, restringida o confidencial).
- Los informes en papel, microficha o película deberán triturarse y los discos blandos o unidades de disco duro deberán borrarse para que su información no pueda recobrase.

7.3 Accesos


- 
- 7.3.1 Sólo los usuarios autorizados tendrán el acceso a la información institucional clasificada. Las personas a cargo deberán otorgar códigos únicos de seguridad que identifiquen a los usuarios y sus contraseñas.
 - 7.3.2 La autorización de acceso a la información clasificada como privada, restricta o confidencial deberá basarse en la función del trabajo o en un requisito del curso académico, cuando aplique.
 - 7.3.3 El código de acceso no deberá compartirse con otros usuarios.
 - 7.3.4 Los usuarios autorizados deberán conocer el nivel de protección requerido de la información a la cual acceden.
 - 7.3.5 Los usuarios que entren a un sistema de información no deberán dejar la máquina desatendida y desbloqueada, para evitar que alguien no autorizado pueda acceder al sistema.
 - 7.3.6 La información confidencial deberá utilizarse exclusivamente durante el desempeño de las tareas de la Universidad y se prohíbe su uso para otros propósitos que estén fuera del interés de la Universidad.
 - 7.3.7 Ningún usuario deberá autorizar una conexión remota a su computadora de parte de un tercero, sin previa autorización de su supervisor.
 - 7.3.8 El acceso a la computadora concedido a un usuario autorizado se eliminará cuando éste se transfiera de una unidad departamental a otra o cuando termine o se retire de su empleo; en el caso de estudiantes, cuando se gradúen o cuando su cuenta de cortesía sea inactivada o innecesaria.
 - 7.3.9 Cuando el usuario autorizado cese en sus funciones en la Universidad, vendrá obligado a observar las normas de confidencialidad de la información con respecto a la divulgación de contenidos.

7.4 Protección de la información


- 7.4.1 La información institucional se protegerá de la manera que corresponda a su clasificación y valor. El costo de la seguridad de la información deberá corresponder al valor de la información asegurada.


- 7.4.2 La información institucional, no importa el medio o naturaleza, será divulgada por las oficinas oficialmente designadas por el Presidente o el Ejecutivo Principal de la unidad, en consulta con la Oficina de Asesoría Jurídica.
- 7.4.2 De ser requerido por ley o regulación, la Universidad informará de inmediato las violaciones de seguridad de información a las autoridades externas. Si no existe tal requisito, el Presidente, en coordinación con los administradores apropiados de las unidades académicas, sopesará el impacto de notificar la violación al medio externo, antes de informar estas violaciones. Representantes de la Oficina de Asesoría Jurídica deberán ayudar a las autoridades universitarias en su determinación del impacto de notificar el incidente.

VIII. Responsabilidades

- 
- 8.1 El Presidente y los Ejecutivos Principales de las unidades tendrán la responsabilidad de:
- 8.1.1 Definir a qué categorías de la información institucional pueden acceder y manejar los diversos grupos de personas de la Institución (por ejemplo, facultad a tiempo completo o a jornada parcial, empleados, estudiantes, socios financieros, otras instituciones educativas y público general, entre otros).
- 8.1.2 Determinar los departamentos que serán responsables de la seguridad de la información y de ejercer las siguientes funciones, que incluyen, pero no se limitan a:
- 8.1.2.1 supervisar e implantar las políticas, normas y procedimientos para la seguridad de la información.
- 8.1.2.2 coordinar o realizar las auditorías de la seguridad de la información y las investigaciones de incidentes cuando ocurra un problema de seguridad de información.
- 8.1.2.3 determinar qué unidades departamentales serán responsables de la autorización de firmas electrónicas y su documentación.
- 8.1.2.4 desarrollar un programa de adiestramientos para la concienciación de la seguridad de la información.
- 8.1.3 Establecer la frecuencia de monitorías para realizar cotejos de verificación y evaluar si se está cumpliendo con las normas de confidencialidad de la información.

- 8.2 Los custodios de la información designados en las unidades serán responsables de:
- 8.2.1 Conocer y entender la función de la información bajo su responsabilidad.
 - 8.2.1.1 Entender el impacto que las decisiones de acceso tienen sobre la información y determinar las necesidades operacionales y de equipo de los usuarios.
 - 8.2.1.2 Apoyar y facilitar los procesos para el manejo de la información institucional y para atender las necesidades operacionales y tecnológicas de su oficina.
 - 8.2.2 Conocer en detalle la información confidencial que recae bajo su responsabilidad. Al hacer este análisis, deberán evaluar cómo se verían afectadas las operaciones de la Institución, si esa información no estuviese disponible. También deberán evaluar los riesgos en caso de que esa información pudiera utilizarse ilegalmente o malintencionadamente, o si cae en manos de personal no autorizado.
 - 8.2.3 Asegurarse de que la información se haya clasificado apropiadamente, de acuerdo con las leyes del estado y las leyes federales, los requisitos de las agencias reguladoras y cualquier obligación contractual, las regulaciones universitarias y las normas de confidencialidad y sensibilidad de la información.
 - 8.2.4 Asegurarse de que la información clasificada como confidencial se identifique físicamente así. Esto puede hacerse con un sello físico o electrónico que diga "Información Confidencial" o "Información sólo para Uso Interno".
 - 8.2.4.1 Asegurarse de que se registren las entradas que se realicen de los datos relacionados con los accesos de información restringida y confidencial. Este registro debe incluir: nombre, firma de los usuarios, fecha y hora de los accesos.
 - 8.2.4.2 En algunos casos donde los usuarios de información confidencial o restringida hagan cambios autorizados, podría requerirse también conservar el contenido original de los datos. Esta información podría ser requerida por auditores internos o externos, o por entidades legales.
 - 8.2.5 Desarrollar, probar e implantar un plan de recuperación de la información, en caso de desastre.

- 
- 8.2.6 Evaluar periódicamente el nivel de riesgo de la información bajo su mando.
 - 8.2.7 Recomendar en qué medios y bajo qué condiciones estará disponible la información.
 - 8.2.8 Asegurarse de que se mantenga la exactitud de la información.
 - 8.2.9 Asegurarse de que sólo los usuarios autorizados tengan el acceso a la información y repasar periódicamente si es necesario hacer algún cambio.
- 8.3 La Oficina de Recursos Humanos de las unidades debe:
- 8.3.1 Designar, si fuese necesario, un administrador de seguridad que se haga responsable diariamente de las tareas relacionadas con la seguridad de la información (por ejemplo, mantener las tablas de acceso y desarrollar adiestramientos sobre el conocimiento de la seguridad, entre otros).
 - 8.3.2 Notificar al Centro de Informática y Telecomunicaciones cuando un empleado cese funciones con la Universidad solicitando la cancelación de los accesos.
- 8.4 El personal del Centro de Informática y Telecomunicaciones del nivel central tendrá la responsabilidad de:
- 8.4.1 Asesorar al personal de las unidades del Sistema en todo lo relacionado con la confidencialidad de la información, cuando sea necesario.
 - 8.4.2 Velar porque los sistemas de información cumplan con las leyes de confidencialidad y, a su vez, sean protegidos de accesos no autorizados.
 - 8.4.3 Asegurarse de que se registren en los sistemas, según corresponda, los datos relacionados con los accesos de información restringida y confidencial que se realicen. El registro debe incluir: código de los usuarios, fecha y hora de los accesos. En algunos casos, podría requerirse conservar también el contenido original de los datos cambiados por los usuarios. Esta información podría ser requerida por auditores internos o externos o por entidades legales.
 - 8.4.4 Desarrollar, probar e implantar un plan de recuperación de la información en caso de desastres.

- 
- 8.4.5 Evaluar, al menos cada seis meses el nivel de riesgo de la información bajo su mando.
 - 8.4.6 Evaluar periódicamente los cambios en sistemas de información que puedan afectar la accesibilidad y seguridad de la información y tomar las medidas necesarias para mantener la seguridad de la información.
 - 8.4.7 Recomendar en qué medios y bajo qué condiciones estará disponible la información.
 - 8.4.8 Asegurarse de que se hayan inactivado o eliminado todos los códigos de acceso a los sistemas universitarios de las personas que hayan terminado el empleo o se hayan transferido a otra unidad.
 - 8.4.9 Evaluar la adquisición de una solución DLP que permita prever pérdida de información confidencial, así como también monitorear los accesos a datos confidenciales en la red. Al evaluar esta solución, se deberá tener en consideración lo siguiente:
 - 8.4.9.1 Identificar cuál es la información confidencial que requiere monitoreo. Para eso, se debe analizar cómo se afecta la Universidad al tener que cumplir con leyes aplicables y al tener que proteger su propiedad intelectual.
 - 8.4.9.2 Definir las prioridades a trabajarse dentro de la solución DLP, enfocándose primero en las áreas más propensas a pérdida de información confidencial.

8.5 Los usuarios serán responsables de:

- 8.5.1 Custodiar toda la información que utilicen, sin importar el medio.
- 8.5.2 Asegurarse de que la información autorizada a la que tienen acceso, esté protegida contra la destrucción o la divulgación.
- 8.5.3 Asegurar bajo llave cualquier documento confidencial, cuando abandonen su área de trabajo.
- 8.5.4 Salir del sistema de información de la computadora institucional, si no acceden a la información durante un tiempo extendido.
- 8.5.5 Renovar los datos de información transmitidos para asegurarse de que estén trabajando con la información exacta y actualizada.

IX. Accesos a áreas restringidas

- 9.1 Los visitantes a las áreas en donde se utiliza información confidencial deberán estar supervisados por personal de la Universidad y nunca deberán dejarse desatendidos.
- 9.2 La entrada a lugares donde se trabaje con información sensible deberá contar con la seguridad apropiada.
- 9.3 Ningún usuario estará autorizado a prestar sus tarjetas de acceso a otras personas.
- 9.4 Cuando las tarjetas de acceso a las instalaciones físicas de la Universidad se pierdan o sean robadas, el usuario deberá reportar esta situación de inmediato a la persona responsable de otorgar las mismas.
- 9.5 Habrá cámaras de seguridad ubicadas en los lugares estratégicos de la Universidad. Esto incluye al Centro de Informática y Telecomunicaciones donde deberán instalarse cámaras de seguridad que detecten cualquier persona que intente acceder a los diferentes servidores, incluyendo aquellos donde se guarde información confidencial.
- 9.6 Todo visitante a un área donde se trabaja con información confidencial deberá firmar un registro de entrada al área y obtener una tarjeta que lo identifique como visitante.


X. Manejo de equipos

- 10.1 Nunca, los equipos, ni ninguna instalación física, deberán dejarse desatendidos.
- 10.2 Aquellos equipos que se quieran decomisar deberán manejarse siguiendo el procedimiento establecido por la Vicepresidencia de Gerencia, Finanzas y Servicios Sistémicos.
- 10.3 Las máquinas que contengan información confidencial deberán ser previamente identificadas y atendidas sólo por el personal técnico autorizado a estos fines.
- 10.4 Los equipos que contengan información altamente confidencial deberán tener una dirección "Mac Address" que pueda ser rastreada, de ser necesario.
- 10.5 Ningún equipo, propiedad de la Universidad, incluyendo computadoras portátiles o "laptops", podrá sacarse fuera de las instalaciones físicas sin un documento que así lo autorice.

XI. Información a ser compartida con terceros

- 11.1 Los vendedores, contratistas, consultores e interventores externos que necesiten acceso a la información institucional deberán leer y reconocer por escrito que los empleados de su empresa han leído y entendido las normas de seguridad de información y normas para la clasificación de información de las unidades institucionales y que las observarán.
- 11.2 Deberán firmarse acuerdos de confidencialidad con aquellos terceros que podrían tener acceso a la información confidencial de la Universidad.
- 11.3 Toda divulgación a terceros deberá llevarse a cabo según los Procedimientos para la Divulgación de Información a Terceros, promulgado en documento normativo separado.

XII. Envío de información confidencial

- 
- 12.1 La información clasificada como confidencial no deberá enviarse por correo electrónico. Esta información se enviará por correo interno o postal. El sobre deberá estar identificado y cada persona que lo reciba deberá firmar por el sobre como recibido.
- 12.2 Cuando se vaya a hacer una transferencia de archivos a otra localidad, deberá asegurarse de que la transferencia sea segura. El proceso de transferencia de archivos, en su inicio, debe contar con la aprobación del Centro de Informática y Telecomunicaciones.

XIII. Resguardos de información

- 13.1 Los usuarios autorizados deberán proteger sus archivos correctamente cuando creen o copien un archivo. Además, deberán realizar resguardos frecuentes de sus archivos. Estos archivos, al igual que los que podrían contener información confidencial, deberán guardarse en lugares seguros.
- 13.2 La información de las bases de datos deberá resguardarse con una frecuencia previamente establecida. Se deberán conservar, como mínimo, los últimos tres resguardos de todas las bases de datos.
- 13.3 Deberán enviarse resguardos de información a las bóvedas externas.

XIV. Uso inapropiado de la información confidencial

Los usuarios autorizados no utilizarán los sistemas de información para uso no apropiado, según se define en la Política Institucional para el Uso Apropriado de la Tecnología de Información, los Sistemas de Información Computadorizados y las Telecomunicaciones.

- 14.1 Se prohíbe a los usuarios tener acceso a la información, de cualquier naturaleza o medio, para lo cual no hayan sido autorizados.
- 14.2 Se prohíbe compartir información confidencial de cualquier índole con personas que no estén autorizadas a conocer dicha información.
- 14.3 Se prohíbe el acceso no autorizado a cualquier información de naturaleza confidencial.
- 14.4 El manejo inadecuado de información confidencial está prohibido en la Institución. El hacerlo puede violar leyes y reglamentos estatales y federales, así como las normas y reglamentos de la Universidad. El incurrir en tal práctica expone a la Universidad a diferentes sanciones y expone también, en su carácter personal, al usuario que incurra en tal conducta.
- 14.5 Los usuarios autorizados tienen la responsabilidad de saber que a cualquier usuario autorizado al que se descubra haciendo uso inapropiado de la confidencialidad de la información institucional puede negársele el acceso futuro a la información y estará sujeto a las sanciones disciplinarias, suspensión, despido, u otras sanciones disciplinarias establecidas.

XV. Acciones disciplinarias

En el caso de empleados regulares o estudiantes, cuando se determine que ha habido una violación a lo establecido en este documento, se aplicarán las acciones correctivas y disciplinarias establecidas por la Universidad, sin excluir una demanda legal. La acción que se tome en cada caso dependerá de las circunstancias particulares del mismo.

Cuando el usuario no sea empleado regular de la Universidad, el Presidente o la persona que él designe, recibirá el asesoramiento necesario para determinar la acción correspondiente.

XVI. Separabilidad

Si cualquier parte o sección de estas normas es declarada nula por una autoridad competente, tal decisión no afectará las restantes.

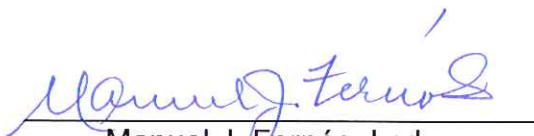
XVII. Derogación o enmiendas

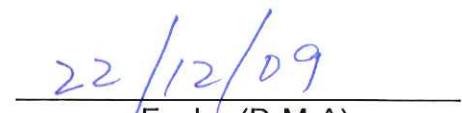
Estas normas dejan sin efecto cualesquiera otras directrices que estén en conflicto con lo aquí dispuesto. Este documento puede ser enmendado o derogado por el Presidente de la Universidad.

XVIII. Vigencia

Estas normas tendrán vigencia inmediata a partir de la aprobación y firma del Presidente.

XIX. Aprobación


Manuel J. Fernós, Lcdo.
Presidente


Fecha (D-M-A)

ymc