Universidad de Puerto Rico
Oficina de Sistemas de Información
Administración Central

Guía para el Manejo de los Datos de la Universidad de Puerto Rico
Versión Marzo 2022[1]

Guía para el Manejo de Datos

Basado en la Política Institucional de Clasificación de Datos de la Universidad de Puerto Rico, se establece esta guía para el manejo de los datos. Los custodios y usuarios de la información tienen que estar seguros de la clasificación de los datos que manejan y tienen la responsabilidad de garantizar el control adecuado de los mismos, garantizando así la confidencialidad, integridad, disponibilidad, y disposición de estos cuando es requerido.

La confidencialidad de los datos se compromete cuando es accedida y/o divulgada sin autorización. El principio primario para salvaguardar la confidencialidad de los datos es que su acceso debe ser concedido en base a la estricta "necesidad de conocer" para ejecutar una tarea institucional genuina.

La pérdida de integridad sucede cuando los datos son alterados o destruidos por error, o sin autorización. La integridad de los datos se garantiza cuando se verifica que los mismos no han cambiado sin autorización o su debido procedimiento, y cuando el origen de cada acción sobre los mismos puede ser verificado y asociado con un proceso o usuario legítimo.

Por otra parte, la no disponibilidad o interrupción al acceso de la información es un aspecto crítico en la operación de la Universidad. La no disponibilidad no solo ocurre cuando los datos se pierden o destruyen, sino además cuando su acceso es denegado o no está disponible en el momento que se necesita.

La disposición de los datos está reglamentada en la Certificación 33 (2021-2022) "Reglamento para la Administración, Conservación y Disposición de Documentos de la Universidad de Puerto Rico".

A continuación, se presenta los requisitos para el manejo de los datos en la Universidad de Puerto Rico basados en la clasificación de estos:

[1] Documento revisado y aprobado por el Comité Institucional de Seguridad en los Sistemas de Información

Clasificación de Datos	Manejo
Datos Restrictos	● Requiere ser empleado con los debidos roles y autorizaciones, para obtener acceso. ● Los datos deben ser accedidos y manejados exclusivamente desde los sistemas de información administrativos institucionales. ● Bajo ninguna circunstancia debe ○ ser enviada por correo electrónico sin haber sido cifrados. ○ ser guardada en repositorios de almacenaje en la nube no institucionales. ○ almacenarse en dispositivos removibles como discos externos y *USB Drives* sin haber sido cifrados. ○ guardarse en computadoras de trabajo de escritorio, ni laptops o móviles por períodos prolongados de tiempo. De ser necesario almacenar la información, tienen que almacenarse de forma segura (cifrada). ○ almacenarse en dispositivos personales de los usuarios. ● Se tiene que utilizar una conexión segura para acceder los servicios que contienen los datos (https, ssh, vpn institucional, otros). ● Los datos no pueden ser accedidos desde facilidades fuera de la institución, a menos que sea a través de una conexión segura y debidamente aprobada. ● Terceros deben ser evaluados y autorizados por la autoridad nominadora mediante un acuerdo de confidencialidad para tener acceso a dichos datos. ● Se requiere uno o más mecanismos de autenticación para acceder a los sistemas que contienen los datos. ● Los datos sólo deben ser impresos cuando se requiere por una necesidad legítima y reconocida. Se debe identificar los mismos con la palabra “Confidencial” y deben manejarse de esta forma. ● Los datos no pueden dejarse desatendidos o expuestos en escritorios (copias impresas) o visible en pantallas. ● La disposición de los datos debe hacerse mediante destrucción física de los documentos impresos, o de mecanismos certificados de disposición de medios electrónicos, y deberá regirse según la Certificación 33 (2021-2022) “Reglamento para la Administración, Conservación y Disposición de Documentos de la Universidad de Puerto Rico”.
Clasificación de Datos	**Manejo**
Datos Internos	● Requiere ser empleado con los debidos roles y autorizaciones para obtener acceso. ● Bajo ninguna circunstancia debe ○ ser enviada por correo electrónico sin haber sido cifrados. ○ ser guardada en repositorios de almacenaje en la

	nube no institucionales. ○ guardarse en dispositivos de almacenajes removibles como discos externos y *USB Drives*. De ser esto necesario de forma temporera, la información tiene que almacenarse de forma segura (cifrada). ○ guardarse en computadoras de trabajo de escritorio, ni laptops o móviles por períodos prolongados de tiempo. De ser necesario almacenar la información, tienen que almacenarse de forma segura. ○ almacenarse en dispositivos personales de los usuarios. ● Se tiene que utilizar una conexión segura para acceder los servicios que contienen los datos (https, ssh, vpn institucional, otros). ● Terceros deben ser evaluados y autorizados por la autoridad nominadora mediante un acuerdo de confidencialidad para tener acceso a dichos datos. ● Se requiere uno o más mecanismos de autenticación para acceder a los sistemas que contienen los datos. ● Los datos sólo deben ser impresos cuando se requiere por una necesidad legítima y reconocida. ● Los datos no pueden dejarse desatendidos o expuestos en escritorios (copias impresas) o visible en pantallas. ● La disposición de los datos debe hacerse mediante destrucción física de los documentos impresos, o de mecanismos certificados de disposición de medios electrónicos, y deberá regirse según la Certificación 33 (2021-2022) “Reglamento para la Administración, Conservación y Disposición de Documentos de la Universidad de Puerto Rico”.
Datos Públicos	● No hay restricción para acceder y ver la información. ● Se requiere autorización del custodio de la información para ser modificada. ● Puede residir en redes públicas y sistemas de almacenaje externos reconocidos o contratados con la institución.

Cifrado de Datos

En los casos excepcionales en que los datos restrictos o privados deban ser almacenados temporeramente fuera de los sistemas administrativos institucionales, o compartidos mediante mecanismos de comunicación electrónica por alguna razón justificable, estos deberán mantenerse cifrados. Esto incluye, además, cualquier movimiento de estos datos a un destino diferente para uso legítimo institucional.

En dicho caso, la Universidad recomienda algunas herramientas para el cifrado de los datos, de tal forma que pueda almacenarse o transmitirse de forma segura. Para obtener los beneficios reales de cifrado, se debe utilizar tecnologías modernas de cifrado certificadas como seguras.

A continuación, las alternativas apoyadas por la Institución:

Nombre de la Herramienta	Descripción y uso sugerido
7-Zip	Los archivos de 7z apoyan cifrado AES-256 de forma nativa. Útil para cifrar archivos que requieren ser almacenados localmente, o en dispositivos temporeramente con el propósito de moverse de un sistema a otro, o ser enviados por correo electrónico.
BitLocker (Windows) FileVault 2 (Apple) TrueCrypt (Linux)	Cifrado de discos de las computadoras. Una vez instalado y configurado, todo el contenido de las unidades de discos es cifradas y su contenido solo puede ser accedido con las credenciales correspondientes.

Las unidades de apoyo técnico en las Unidades pueden orientar a los usuarios que manejan datos críticos y privados en el uso de estas herramientas.

Datos Regulados por Leyes Federales y Estatales

A continuación, una lista de datos regulados por algunas leyes federales o estatales, y las consideraciones institucionales para el manejo de estos:

1. Récord del estudiante que lo identifica (cubierto bajo Ley FERPA - Derechos Educativos de la Familia y la Ley de Privacidad de 1974, o Enmienda Solomon “Buckley”)

   Para los estudiantes activos e inactivos, los siguientes datos identificables son restrictos:
   a. Número de identificación (número de estudiante)
   b. Notas
   c. Promedio
   d. Créditos matriculados
   e. Raza
   f. Género
   g. Lista de características personales o cualquier otro dato que permita que el estudiante pueda ser identificado o rastreado fácilmente.
   h. Record financiero
   i. Códigos de accesos (PIN)
   j. Identificadores biométricos

Para los estudiantes activos, la siguiente información identificable puede ser revelada siempre y cuando lo autorice el estudiante:

a. Nombre, dirección postal o permanente, teléfonos
b. Fecha y lugar de nacimiento
c. Fecha de asistencia a clases, estatus estudiantil, clasificación, grado obtenido, reconocimientos y honores recibidos
d. Instituciones educativas previas
e. Pueblo de nacimiento
f. Dirección y nombre de los padres
g. Participación en actividades deportivas reconocidas, peso, altura y fotos de los miembros de equipo atléticos
h. Estado civil
i. Fotos del estudiante

2. Información personal financiera que identifique la persona (cubierta bajo Ley GLBA - Ley de Modernización de Servicios Financieros del 1999).

   Con el propósito de cumplir y no violentar los requerimientos de notificación, estos campos se consideran restrictos:

   a. Número de seguro social
   b. Tarjetas de créditos
   c. Acuerdos contractuales
   d. Identificadores biométricos
   e. Número de licencia de conducir
   f. Fecha de nacimiento
   g. Número de cuenta financiera en combinación con un código de seguridad, código de acceso o contraseña que permita acceso a la cuenta

3. Información protegida sobre la salud (*Personal Health Information - PHI*) (cubierta bajo Ley HIPAA - Ley de Portabilidad y Responsabilidad de Seguros de Salud del 1996 privacidad, seguridad y violación de reglas de notificación)

   PHI se define como cualquier información “identificable” de una persona, almacenada por una entidad o cubierta, y relacionada a uno o más de los siguientes:

   a. Condición de salud mental o física del pasado, presente o futuro
   b. Provisión de cuidados de salud
   c. Pagos de cuidados de salud provistos en el pasado, presente o futuro

   PHI se considera “identificable” y confidencial, solo si contiene uno o más de los siguientes elementos adicionales:

   a. Nombre
   b. Dirección

c. Todos los elementos de cualquier fecha que lo relacione, excepto el año
d. Teléfono o FAX
e. Direcciones de correos electrónicos
f. Número de seguro social
g. Número de record médico
h. Número del plan beneficiario de salud
i. Número de cuenta
j. Número de certificado/licencia
k. Número que identifica vehículo o número de serie, incluyendo número de la tablilla
l. Identificadores de dispositivos y números de serie de estos
m. Localizador de recursos uniforme (URL's) de la web
n. Direcciones de protocolo de internet (IP)
o. Identificadores biométricos, incluyendo impresión de huellas y voz
p. Imágenes fotográficas completas del rostro y cualquier imagen comparable
q. Cualquier otro número identificador único o características que pueda identificar al individuo

Si la información de salud no contiene alguno de los identificadores en referencia antes mencionados, y no hay base razonable para creer que la información puede ser utilizada para identificar un individuo, no es considerada "identificable" y como resultado no debe ser considerada PHI.