Universidad de Puerto Rico
Recinto de Ciencias Médicas

Política de Seguridad de Tecnologías de Información del RCM

1 Base Legal

1.1 Ley Federal "Family Education Rights and Privacy Act" (FERPA) de 1974
1.2 Ley Federal "Health Insurance of Portability and Accountability Act" (HIPAA)
1.3 Ley Número 1 del 20 de enero de 1966 (Ley Universidad de PR)
1.4 Ley Número 16 de 16 de junio de 1993
1.5 Reglamento General de la UPR
1.6 Certificación Núm. 35 JS (2007-2008): *Política Institucional sobre el Uso Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico*
1.7 Certificación Núm. 049 JS 1994-95: Cotejo de Equipo
1.8 Procedimiento para la adquisición, instalación, conservación y uso oficial de los programas en computadoras de la Universidad de Puerto Rico.
1.9 Certificación Núm. 192 JS 2002-2003: Normas sobre el Uso de las Telecomunicaciones
1.10 Ley Federal de Derechos de Autor, Pub. L. 94-553, Título I, § 101, Oct. 19, 1976, según enmendada, 90 Stat, 2541, 17USCA § 101.
1.11 Ley Federal de Patentes y Marcas de Fábrica, Pub. L. 93-59, 88 Stat, 1949, 35USCA § 1.
1.12 Política Institucional de la U.P.R. sobre Derechos de Autor, Certificación #93-140 del Consejo de Educación Superior.
1.13 Política Institucional de la UPR sobre Patentes e Invenciones, Certificación #132, Serie 2002-03 de la Junta de Síndicos de la U.P.R.
1.14 Mejores Prácticas de Infraestructura Tecnológica (OGP TIG-011)

2 Responsabilidad Compartida

Debido al ambiente compartido y de colaboración de los recursos de tecnologías de información, se considera en esta política el aspecto de Responsabilidad Compartida entre Rectoría, OSI y los Decanatos a través de los Directores (as) de Unidades de Informática con su respectivo personal técnico de Informática y usuarios en relación a la responsabilidad de proteger y salvaguardar la seguridad y privacidad de los recursos.

3 Definiciones

3.1 Rector

Autoridad administrativa y académica del Recinto de Ciencias Médicas, conforme a la Ley de la Universidad de Puerto Rico, Ley Número 1, artículo 7, del 20 de enero de 1996 según enmendada.

3.2 Gerencia

Como Gerencia se incluyen los Decanos (as), Director (a) de OSI, Directores (as) de Departamento, Directores (as) de Unidades de Informática y otro personal gerencial relacionado, que tienen la responsabilidad de aprobar, evaluar los mecanismos, estándares, guías y procedimientos creados en sus respectivos Decanatos o Departamentos.

3.3 Oficina de Sistemas de Información (OSI) RCM

La Oficina de Sistemas de Información (OSI) provee a la comunidad del Recinto de Ciencias Médicas (RCM) igualdad de acceso a los recursos de Tecnologías de Información (TI) y facilita su uso e integración en los procesos estudiantiles, académicos, de investigación, administrativos y de servicios clínicos del Recinto.

El objetivo principal de la OSI es establecer y promulgar políticas, guías, procedimientos y estándares de TI que faciliten y promuevan el uso de las TI en forma integrada para satisfacer las necesidades de los usuarios de TI en el Recinto. La OSI es responsable por la administración, desarrollo y mantenimiento de la infraestructura de comunicación de data, voz y video en el Recinto. Además, es responsable de proveer a la comunidad del Recinto acceso al Internet Doméstico e Internet2.

3.4 Personal Técnico de Informática

El personal técnico de informática comprende al personal de los decanatos, departamentos, proyectos especiales (propuestas federales, otros) que manejan recursos o servicios de tecnologías de información. Estos son responsables de administrar equipo, manejo de usuarios, seguridad, entre otros.

3.5 Usuarios

Bajo usuario se incluye toda aquella persona que utiliza cualquiera de los recursos de tecnología de información del RCM, ya sea de forma permanente o temporera.

3.6 Sistemas Centralizados

Servicios ofrecidos por OSI a todo el RCM, entre ellos E-mail, Sistema Administrativo, etc.

3.7 CAN (Computer Area Network)

Es la red de comunicación de data, voz y video del RCM.

4 Principios y Filosofía

4.1 Apoyo Institucional

OSI contará con el apoyo y recursos fiscales institucionales para poder presentar e implantar los mecanismos necesarios para cumplir con esta política, incluyendo programas educativos.

4.2 Desarrollo de Políticas Existentes

El RCM tiene la responsabilidad de crear políticas, procedimientos y estándares de seguridad de Tecnología de información, a tenor con la *Política Institucional sobre el Uso Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico*, Certificación Núm. 35 (2007-2008).

4.3 Educación

El RCM tiene la responsabalidad de concienzar sobre los deberes, responsabilidades y derechos de los usuarios sobre el acceder, utilizar, manejar, resguardar y disponer de la información, sistemas y equipo que manejan.

4.4 Niveles Razonables y Costo Efectividad en la Seguridad

4.4.1

No todos los recursos necesitan los mismos niveles de seguridad, por lo cual esta política busca establecer los indicadores razonables para que los Directores (as) de las Unidades de Informática con su Personal Técnico de Informática puedan determinar los niveles de costo efectividad adecuados y funcionales de seguridad, control de acceso y privacidad necesarios para sus recursos de información. La oficina de OSI asignará niveles de seguridad, acorde a los riesgos, prioridades y seguridad establecida.

4.4.2

El RCM es una Institución de Educación Superior ("Higher Education Institution"), la cual incluye áreas Académicas, Investigación y Administrativa, por ello se deben de ajustar los niveles y requisitos de seguridad a base de requerimientos de entidades reguladoras (Agencias Acreditadoras, National Institutes of Health (NIH), Food and Drug Administration (FDA), Contralor de PR, etc.), funciones realizadas y necesidades de estas tres (3) áreas del RCM.

4.5 Prácticas de Seguridad Comúnmente Aceptadas

Los requisitos y recomendaciones mencionadas en esta política buscan estar acorde con la Prácticas Comúnmente Aceptadas para Instituciones de Educación Superior.

4.6 Responsabilidad Institucional de OSI

OSI es la oficina responsable por velar que se cumplan con todos los requisitos y aspectos de seguridad y privacidad según requerido por leyes estatales, federales y entidades afines como el Contralor de Puerto Rico, Oficina de Auditoria Interna de la Junta de Síndicos de la Universidad de Puerto Rico y entidades del gobierno federal tales como: *National Institutes of Health (NIH), Food and Drug Administration (FDA), Health Resources and Services Administration (HRSA)* y otras entidades reguladoras.

5 Propósito

5.1

Establecer elementos uniformes para el cumplimiento de los estatutos reglamentarios pertinentes y con el uso adecuado de tecnologías de información en todo el RCM.

5.2

Proveer los procedimientos necesarios para el uso adecuado de las tecnologías garantizando la protección de la información, los derechos de autor y las amenazas en distintos niveles a la seguridad y privacidad de información de los usuarios y pacientes.

5.3

Coordinar con todos los decanatos y unidades la mejor estrategia y los procedimientos para determinar los niveles, prácticas óptimas y funcionales de seguridad, uso de los equipos y programas en el RCM.

5.4

Establecer los mecanismos para divulgar los requisitos y especificaciones mencionados en la *Política Institucional sobre el Uso Aceptable de los Recursos de la Tecnología de Información de la Universidad de Puerto Rico*, relacionados con los distintos niveles de privacidad y seguridad.

6 Alcance

6.1

Esta política cubre a todos los miembros de la comunidad del RCM, entre ellos los estudiantes, facultativos, investigadores, personal administrativo, personal destacado en facilidades externas, compañías e individuos asociados de forma alguna con el RCM y cualesquiera que solicite acceder a alguno de los sistemas o fuentes de información del RCM.

6.2

En adelante esta política establecerá las obligaciones y responsabilidades de las personas que utilizan cualquiera de los recursos de Tecnologías de Información del Recinto (*Usuario*); aquellos responsables de proveer, mantener, administrar y dar apoyo a los recursos de tecnología de información (*Personal Técnico de Informática*); y aquellos que tienen la responsabilidad gerencial o administrativa de departamentos o decanatos (*Gerencia*).

6.3

Este documento no busca restringir, limitar o excluir prácticas existentes en los sistemas de información del RCM. El contexto bajo el cuál se crea esta política es en el marco de establecer una base o principios básicos aceptables de procedimientos de seguridad y operacionales que promuevan la uniformidad en los trabajos y estrategias para proteger los datos y recursos de información del RCM.

7 Políticas

7.1 Elementos Generales

7.1.1

Todo usuario es responsable del uso y contenido de la (s) computadora (s) y otras tecnologías de información asignadas para su uso.

7.1.2

La Oficina de Sistemas de Información (OSI) proveerá las guías para el uso de los *Sistemas Centralizados* existentes, mediante el *Manual sobre Tecnologías de Información en el RCM* (creado en noviembre 2002 y revisado junio 2012), disponibles en el Portal de Empleados del RCM.

7.1.3

OSI es la oficina que administra y mantiene directamente la red de comunicación del RCM y la seguridad global que impera en esta.

7.1.4

Por la naturaleza de los servicios en la red de comunicación del RCM, OSI integra el concepto de Red Privada, Red Extranet y Zona Intermedia "DMZ", las cuales permiten ubicar los servicios estratégicamente, a base de sus necesidades de acceso, seguridad y otras peculiaridades.

7.1.5

Se considera *abuso de recurso de información* cuando un usuario utiliza, accede o modifica información, equipo o ambas para actividades personales y no oficiales acorde con la *Política Institucional sobre el Uso Aceptable de los Recursos de la Tecnología de Información de la Universidad de Puerto Rico*. Esto comprende acceso no autorizado, violación de derecho de autor, uso de la red para acceder o descargar archivos no relacionados con las tareas y/o funciones oficiales, entre otras.

7.1.6

OSI utiliza el Procedimiento de Manejo de Incidente, donde se establece que se interviene con la computadora y otras tecnologías de información o equipo que esté en *abuso de recurso de información acorde con la Política Institucional sobre el Uso Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico* y se toman las medidas para notificar a la Gerencia sobre el incidente y determinar la acción apropiada o correctiva a tomar.

7. 2 Adquisición de equipo y programado

7.2.1

OSI evaluará y autorizará la adquisición de programado o equipo, para evaluar su conectividad con la red de comunicación del RCM, a tenor con las Certificaciones de la Junta de Síndicos de la UPR, 192 de 2002-2003 y 35 de 2007-2008.

7.2.2

OSI en coordinación con los decanatos, colaborará en la integración del nuevo equipo o programado a la red de comunicación del RCM de forma óptima y aceptable, que no resulte en conflicto alguno.

7. 3 Privacidad y Confidencialidad

7.3.1 Acceso no autorizado

7.3.1.1

Todo sistema de datos localizado en una estación de trabajo o servidor deberá tener un mecanismo de control de acceso, privilegio y registro de bitácora (Log). Es responsabilidad de los Directores (as) de Unidades de Informática con su respectivo personal técnico de informática el implantar los mecanismos para cumplir con este requisito. Esto requiere incluir las notificaciones de "Prohibido el Acceso no Autorizado" y una notificación de privacidad.

7.3.1.2

OSI por su parte es responsable de responder por el control de acceso, seguridad y aspectos relacionados de *Sistemas Centralizados* que OSI administra.

7.3.1.3

OSI es también responsable de responder por el control de acceso, seguridad y aspectos relacionados con la red de comunicación del RCM.

7.4 Responsabilidades

7.4.1 Responsabilidades de la Oficina de Sistemas de Información (OSI) RCM

7.4.1.1

OSI en conjunto con las unidades de informática y otro personal gerencial relacionado creará los programas de educación y publicación de manejo de incidentes en forma general (sin incluir detalles) del(los) usuarios, además de proveer cualquier información que sea de carácter público sobre el mecanismo adoptado durante el incidente, su efectividad e historial.

7.4.1.2

OSI en coordinación con los Directores (as) de Unidades de Informática con su respectivo personal técnico de informática, tendrá los criterios y la discreción de otorgar la cualificación a la hora de brindar el acceso y privilegio basado en el concepto de necesidad de saber ("need to know") y necesidad de tener ("need to have").

7.4.1.3

En el ejercicio de su responsabilidad de administrar la red de comunicación del RCM, OSI debe analizar, evaluar, someter y recomendar para probar toda petición, plan de proyecto o propuesta alguna que requiera o proponga el integrar componente o programado alguno a la red de comunicación del RCM.

7.4.1.3.a

Por otro lado es responsabilidad de OSI viabilizar las diferentes opciones que estén disponibles para hacer posible cualquiera de las peticiones de los individuos, Directores (as) de Unidades de Informática con su respectivo personal técnico de informática, Administradores, Departamentos o Decanatos.

7.4.1.4

OSI ha de mantener la evidencia, historial y documentación relacionados a incidentes de seguridad, peticiones, cambios realizados, procedimientos y estándares de seguridad y privacidad.

7.4.2 Responsabilidades de los Usuarios

7.4.2.1 Acceso

7.4.2.1.1

Los usuarios son responsables por el acceso a recursos de información de sus áreas de trabajos, entre estos archivos, computadoras y documentos internos. Esto también incluye el acceso a través de puertas y otro tipo de acceso requerido específicamente para su área. En caso de ser requerido por el usuario, OSI o la Unidad correspondiente proveerá la orientación y guías para que el usuario cumpla con esta responsabilidad.

7.4.2.1.2

Es responsabilidad del usuario implantar las medidas adecuadas para proteger la privacidad y acceso a la información guardada en su computadora y otras tecnologías de información o Archivo Histórico acorde a las normas internas establecidas en su área de trabajo y procedimientos existentes.

7.4.2.1.3

La autenticación de usuarios es requerida para el acceso a computadoras, laptops y servicios centralizados.

7.4.2.1.4

Es requerido el notificar y coordinar con OSI o los Directores (as) de las Unidades de Informática o el personal técnico de informática correspondiente a la unidad que aplique la disposición de toda información contenida en cualquier equipo (incluyendo computadoras y otras tecnologías de información) que vaya a ser dado de baja o intercambiado con otra persona perteneciente a la comunidad universitaria.

7.4.2.2 Contraseña

7.4.2.2.1

Se requiere que todo acceso a *Recursos Centralizados* sea mediante una cuenta de usuario ("username") y contraseña, esta última con un mínimo de ocho (8) caracteres. Los caracteres deben incluir una letra mayúscula y un símbolo.

7.4.2.2.2

Toda contraseña debe de cumplir con el requisito de expirar en un periodo no mayor de 90 días, usando el enfoque de *contraseña histórica* en donde la misma *contraseña* no sea usada 4 veces en un periodo de un año.

7.4.2.2.3

La autenticación es requerida para el acceso a computadoras y laptops, incluyendo la opción de crear secciones o instancia ("profiles") para cada usuario por separado.

7.4.2.3 Virus y Vulnerabilidades

7.4.2.3.1

La UPR participa de la iniciativa gubernamental de hacer uniforme el uso de antivirus.

7.4.2.3.2

Es requerido que el usuario utilice y apoye el uso de programados de actualización automática para su antivirus.

7.4.2.3.3

El usuario debe seguir las recomendaciones mencionadas en el Procedimiento para Manejo de Antivirus.

7.4.2.3.4

Es responsabilidad del usuario utilizar las herramientas incluidas en los sistemas operativos para la actualización de vulnerabilidades, entre estas parchos, “hotfix” y “service packs”. También el usuario deberá observar y seguir las notificaciones de OSI relacionados con los asuntos antes mencionados. OSI enviará estas notificaciones vía email y a través de los boletines publicados en la página de seguridad. OSI en unión a los Directores (as) de Unidades de Informática con su respectivo personal técnico de informática implantarán servicios que faciliten la automatización de estas tareas.

7.4.2.4 Backup

7.4.2.4.1

Los usuarios son responsables de realizar resguardo (backup) de la información de sus computadoras y otras tecnologías de información u otro equipo de información.

7.4.3 *Responsabilidades del Personal Técnico de Informática*

7.4.3.1

Al Personal Técnico de Informática le aplican las observaciones mencionadas en la sección 7.4.2 de Usuarios, dado a que ellos también utilizan recursos provistos por el RCM a través de OSI.

7.4.3.2

El Personal Técnico de Informática es responsable de ejecutar el plan de resguardo (“backup”) para los sistemas que administra y el personal gerencial en las Escuelas y Decanatos es el responsable de crear y mantener actualizado el plan de resguardo.

7.4.3.4

El Personal Técnico de Informática estará encargado del apoyo técnico de seguridad a los usuarios.

7.4.4 *Responsabilidades de la Gerencia*

7.4.4.1

La gerencia puede emitir políticas, procedimientos y estándares que atiendan aspectos mencionados de forma general en esta política o aspectos nuevos no contemplados. Las nuevas políticas no deberán entrar en conflicto con esta política una vez establecida.

7.4.4.2

La gerencia debe participar en la planificación, evaluación, y aprobación de nuevas tecnologías que fortalezcan la estructura de sistemas computadorizados de sus Decanatos o Departamentos.

7.4.4.3

La gerencia deberá delegar en los Directores (as) de Unidades de Informática con su respectivo personal técnico de informática y en OSI el coordinar los adiestramientos o programas educativos para informar a los usuarios sobre la (s) políticas de seguridad vigentes y el mejor uso de los sistemas disponibles.

7.4.4.4

Los Directores (as) de Unidades de Informática con su respectivo personal técnico de informática deben proveer un Plan de Contingencia para la eventualidad de falla no esperada o desastre natural que interrumpa el funcionamiento de los servicios que estos administran. Este plan debe incluir entre otras cosas su estrategia de resguardo y restauración, equipo alterno que se pueda usar en caso de falla del equipo principal. También debe de participar en conjunto con OSI para integrarse en el Plan de Contingencia Central de RCM, en caso de que dicho (s) servicio (s) sea considerado crítico.

7.4.4.5

Es responsabilidad de los Directores (as) de Unidades de Informática con su respectivo personal técnico de informática evaluar e implantar medidas para la seguridad de las computadoras, mediante el uso de cuenta de usuario ("username") y contraseña ("password") u otra estrategia similar que aplique.

7.4.4.6

Los Directores (as) de Unidades de Informática con su respectivo personal técnico de informática pueden emitir guías y/o estándares que no estén contemplados en esta política o respondan a sus necesidades específicas, esto previa aprobación de OSI y con la aprobación del Decano o Director de Departamento o programa según aplique.

8 Administración de la Política de Seguridad

8.1

Acorde con la *Política Institucional sobre el Uso Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico*, se delega en las unidades (recintos) en coordinación con la Oficina de Sistemas de Información (OSI), la implantación de esta política y otras relacionadas.

8.2

OSI en conjunto con las unidades de informática y otro personal gerencial relacionado revisará la política cada dos (2) años, o antes de ser neceario, para atemperarla a las nuevas necesidades de la comunidad del RCM relacionadas con las Tecnologías de Información.

9 Fuentes y Referencia

9.1

Política Institucional sobre el Uso Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico

9.2

Política Computacional y de Comunicaciones Recinto Universitario de Mayagüez, www.uprm.edu/politicas/politicas01.pdf

9.3

Manual sobre Tecnologías de Información en el RCM (creado noviembre 2002 y revisado junio 2012)

9.4

Ley Federal de Derechos de Autor, Pub. L. 94-553, Título I, § 101, Oct. 19, 1976, según enmendada, 90 Stat, 2541, 17USCA § 101.

9.5

Ley Federal de Patentes y Marcas de Fábrica, Pub. L. 93-59, 88 Stat, 1949, 35USCA § 1.

9.6

Política Institucional de la U.P.R. sobre Derechos de Autor, Certificación #93-140 del Consejo de Educación Superior.

9.7

Política Institucional de la UPR sobre Patentes e Invenciones, Certificación #132, Serie 2002-03 de la Junta de Síndicos de la U.P.R.

9.8

"Principles to Guide Efforts to Improve Computer and Network Security for Higher Education", agosto 2002, publicado por EDUCAUSE/Internet2 Computer and Network Security Task Force.

9.9

SANS Security Institute, www.sans.org.

9.10

EDUCAUSE, www.educause.edu.