Universidad de Puerto Rico en Humacao
Sistemas de Información, Computación y Comunicación

Procedimiento de la Oficina de SICC para la Administración y Utilización de las Tecnologías de Información

(versión 4.2)

Edición Junio 2013

Procedimiento de la Oficina de SICC para la
Administración y Utilización de las Tecnologías de Información

Dra. Carmen A. Miranda
Rectora Interina

10 - junio - 2013
Fecha

Sr. Hiram Ortiz Rosa
Director SICC

10 - junio - 2013
Fecha

Sr. Ernesto Soto
Editor

10 - junio - 2013
Fecha

Tabla de Contenido

Introducción

Este procedimiento es aplicable para la administración de tecnologías de informática en la oficina de Sistemas de Información, Computación y Comunicación (SICC) de la Universidad de Puerto Rico en Humacao (UPRH). Este procedimiento queda subordinado y sujeto a la Certificación Núm. 35, 2007-2008, de la Junta de Síndicos titulada *Política Institucional para la Utilización Aceptable de los Recursos de la Tecnología de la Informática en la Universidad de puerto Rico* (la Política) y a los estándares para la utilización aceptable de tecnología informática aprobados por la Vicepresidencia de Investigación y Tecnología de la Universidad de Puerto Rico. Además, este procedimiento se sustenta sobre el procedimiento de la oficina de Administración Central. Todos los usuarios y administradores de tecnología deben cumplir cabalmente con los mismos para asegurar que se haga el mejor uso posible de las tecnologías disponibles a la Universidad de Puerto Rico (UPR).

Este documento establece las guías para llevar a cabo las siguientes actividades relacionadas a administración de la tecnología informática (IT por sus siglas en inglés): Adquisición, asignación, protección, donación, transferencia, préstamo, control de inventario, reparación y movimiento de equipo de tecnología informática; Adquisición e instalación de programados, utilización de la tecnología informática, medio oficial de comunicación electrónica en la UPRH, cumplimiento con la Política y los estándares institucionales, protección lógica de la información, protección física de los equipos, acceso a los sistemas, resguardo periódico de los datos.

1
Ciclo de vida del equipo de *IT*

La figura 1 presenta el ciclo de vida de todo equipo de *IT*. Alguno de los procesos presentados en el diagrama quedan fuera del alcance de este documento. Los mismos son atendidos por otros reglamentos de la UPR.

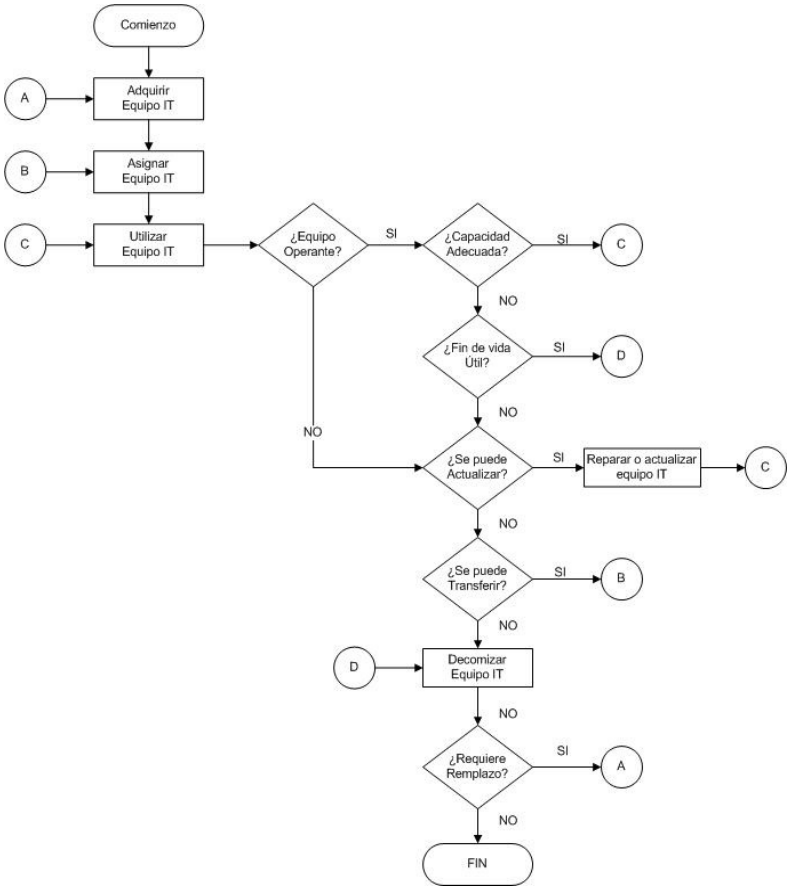


Figura 1. Ciclo de vida de equipo de tecnología de información

2
Adquisición de tecnología informática

Las siguientes certificaciones regulan el proceso requerido para la adquisición de tecnología informática:

2.1. Certificación Núm. 22, 1995-1996, de la Juna de Síndicos titulada *Reglamento General para la Adquisición de Equipo, Materiales y Servicios no Personales de la Universidad de Puerto Rico.*

2.2 Certificación Núm. 35, 2007-2008, de la Junta de Síndicos titulada *Política Institucional para la Utilización Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico*, Sección VII-B-2.

Estas certificaciones están publicadas en el portal de la Junta de Síndicos en la siguiente dirección:

http://www.vcertifica.upr.edu/certificaciones/External/Certificaciones.aspx

Toda oficina o departamento que planifique adquirir un equipo de tecnología informática o que haya comprado un equipo con la intención de conectarlo a la red de telecomunicaciones de la UPRH debe coordinar con el SICC para:

- la debida orientación sobre especificaciones de uso del equipo,
- la evaluación del equipo y autorización de conexión a la red de modo que no experimente problemas de conexión,
- que los programas adquiridos sean instalados en las condiciones establecidas por el manufacturero,
- solicitar la instalación del equipo y la autorización de conexión a la red de la UPRH.

Esta práctica facilita el manejo del equipo conforme a los estándares de modo que no experimente problemas de conexión a la red y que los equipos y programados adquiridos funcionen según lo esperado.

3
Recibo en donación de equipo tecnológico o programa de computadora

El recibo en donación de un equipo tecnológico o un programa de computadoras por la universidad es una alternativa válida mediante la cual se puede procurar tecnología. Sin embargo, la gratuidad no debe ser el único criterio para adoptar lo que se ofrece donar. A veces lo donado puede tener costos ocultos. De nada sirve que el costo inicial a la universidad sea cero, si la propiedad a donarse es obsoleta, cuesta demasiado operar o mantenerla o que no se cuente con el conocimiento o peritaje disponibles para apoyarla. Se debe evaluar el quipo o programa con la misma metodología que si el equipo o programa se fuera a adquirir mediante compra.

Cuando surja la oferta de donación de un equipo tecnológico o programa de computadoras, el SICC debe ser consultado para que evalúe criterio tales como:

- ¿Quién se beneficia primordialmente con el equipo o programa por donar? ¿La institución o el usuario al cual se le asignaría dicha donación?
- ¿Es compatible con los equipos y programas que ya están en uso?
- ¿Qué esfuerzo se requiere para habilitar el equipo o instalar el programa para que se utilice?
- ¿Cuenta el SICC con el personal que tenga el conocimiento y peritaje necesario para brindarle apoyo a dicho programa o equipo?
- Si es un equipo (e.g. una impresora), ¿quién adquirirá los suministros para el equipo?¿es razonable el costo de éstos?

Toda oficina o departamento previo a aceptar una donación debe coordinar con el SICC el apoyo en la instalación y conexión del equipo a la red de la UPRH. De lo contrario, la oficina o departamento que decida aceptar la donación e instalar el equipo o programado sin consultar previamente al SICC, el apoyo para el mismo estará sujeto a que no cuente con los recursos necesarios para evaluar, instalar el equipo o programado. Además, el acceso del equipo a la red de la UPRH no será autorizado hasta que coordina con la administración de la red de telecomunicaciones de a UPRH. El personal de investigación que requiera de tal equipo o programado para sus proyectos y trabajos investigativos, debe también coordinar con el SICC la conexión del equipo a la red de la UPRH si aplica y la instalación del programado. Si necesita privilegios de administración deberá asumir la responsabilidad por operar y por la conectividad del equipo a la red de la UPRH.

4
Adquisición, instalación y utilización de programas para computadoras

El procedimiento que establece las medidas de control para adquirir, instalar y uso oficial y conservación de los programas de computadoras, sus licencias, manuales y derechos en la UPR se describe en detalle en el *Procedimiento Institucional para Utilizar y Administrar Programas de Computadoras en la Universidad de Puerto Rico*, emitido por el Vicepresidencia de Investigación y Tecnología.

5
Asignación del equipo IT

Los equipos informáticos constituyen bienes muebles de la UPR, por lo que están subordinados a la Certificación Núm. 62,1994-1995, de la Junta de Síndicos titulada *Reglamento para el Control de Bienes Muebles en la Universidad de Puerto Rico*. El control de este tipo de inventario impacta la capacidad de una oficina o departamento para identificar equipo que puede requerir reemplazo. En las próximas secciones se presentan trámites informático entre oficinas o departamento.

5.1 Préstamo del equipo de tecnologías de información

Existen momentos específicos donde la necesidad por un equipo de tecnología no es permanente sino que el mismo se requiere por un periodo definido para algún trabajo, actividad o proyecto especial. En este caso, la adquisición de un equipo se puede postergar si la oficina o departamento que necesita el equipo llega a algún acuerdo de préstamo con otra oficina.

Para casos en que dos oficinas o departamentos acuerden prestar equipo entre sí, se debe utilizar el formulario titulado *Solicitud y Autorización para Uso Oficial de Propiedad Universitario Fuera de la Universidad de Puerto Rico* (Apéndice B, p. 58). Éste se puede acceder en el vínculo http://www.uprh.edu/formasuprh/sauopufu.pdf Considere los siguientes criterios cuando llene el formulario:

- Se debe especificar claramente el propósito y la duración del préstamo,
- Se debe obtener la firma tanto de la personal que entrega el equipo como de la persona que lo recibe,
- El director de la oficina que custodia el equipo debe brindar su visto bueno,
- Cumplir con la Política y los estándares institucionales (p. 23),
- La unidad u oficina que presta el equipo retiene la responsabilidad de dar seguimiento para recuperar el mismo al concluir el periodo de préstamo y revisar que el mismo sea devuelto en igual condición a la que se prestó.

5.2 Transferencia del equipo IT

Una oficina o departamento que decida reasignar un equipo de tecnología dentro de la misma oficina o departamento sólo tienen que actualizar su inventario con el nombre y teléfono del nuevo custodio del equipo e informarlo a la persona encargada de la propiedad dentro de su oficina. Cuando la reasignación se lleve a cabo fuera de su oficina o departamento, se considera una trasferencia de equipo, para la cual se debe utilizar el formulario titulado *Informe de Transferencia Interna de Equipo Mueble* (ver Apéndice C, p. 59). Éste se puede acceder en el vínculo http://www.uprh.edu/formasuprh/itiem.pdf Considere los siguientes criterios cuando llene el formulario:

- Se debe obtener la firma tanto de la persona que entrega el equipo como el de la persona que lo recibe,
- El director de la oficina que custodia el equipo debe brindar su visto bueno,
- Una copia del formulario debidamente cumplimentado se debe quedar en la oficina de Propiedad, para que quede registrado el cambio en la custodia del equipo.

5.3 Control del inventario

La oficina que transfiera de manera permanente un equipo a otra oficina es responsable por suministrar copia del formulario *Informe de Transferencia Interna de Equipo Mueble* (ver Apéndice C, p. 59). Éste se puede acceder en el vínculo http://www.uprh.edu/formasuprh/itiem.pdf Esta tarea permitirá que el encargado de la propiedad actualice su inventario de activos para reflejar el cambio de custodio del equipo. Esto garantiza el cumplimiento con la Certificación Núm. 62, 1994-1995 de la Junta de Síndicos titulado *Reglamentación para el Control de Bienes Muebles en la Universidad de Puerto Rico.*

5.4 Movimiento de equipo IT portátil fuera de los predios de la oficina

Existe equipo de tecnología diseñado para ser portátil. Ejemplos de estos incluyen las computadoras portátiles (e.g. *laptops, notebooks)*, proyectores digitales, cámaras digitales, los dispositivos digitales personales (e.g. PDA, tablets, GPS, etc.).

En principio, el usuario al que se le ha asignado la custodia permanente de dicho equipo portátil puede portarlo fuera de los predios de la universidad. Dicho empleado responderá ante la universidad por el cuidado del equipo. Cualquier otra persona que no sea el empleado custodia deberá procurar una autorización escrita del director de la oficina dueña del equipo portátil para poderlo remover de la

oficina. Esta autorización utilizará el formulario titulado *Solicitud y Autorización para Uso Oficial de Propiedad Universitario Fuera de la Universidad* (ver Apéndice B, p. 58). Éste puede ser accedido en el vínculo http://www.uprh.edu/formasuprh/sauopufu.pdf

6
Utilización de la tecnología informática

El uso aceptable de los recursos de tecnología en la UPR se atiende en los siguientes reglamentos:

- Certificación Núm. 35, 2007-2008, de la Junta de Síndicos titulado *Política Institucional para la Utilización Aceptable de los Recursos de la Tecnología de la Información de Puerto Rico*, junto a los *Estándares para la Utilización Aceptable de Tecnología Informática* emitidos por la Vicepresidencia de Investigación y Tecnología,
- Certificación Núm. 192, 2002-2003, de la Junta de Síndicos titulado *Normas sobre el Uso de las Telecomunicaciones*.

Aunque la Política permite la utilización personal aceptable de un equipo tecnológico[1], el mismo:

- No debe interferir con el desempeño de las labores del empleado,
- No debe hacer cambios a la configuración de los equipos,
- Si posee privilegios de administrador en el equipo, será responsable de los cambios que haga y las repercusiones que conlleve dicho cambio en el sistema de telecomunicaciones,
- Frecuencia desmedida de incidentes donde un usuario requiere de apoyo debido a su intervención continua con la configuración de su equipo, el SICC se reserva la prerrogativa de escalar la situación al director de la oficina a la cual responde el usuario, para solicitar su intervención en evitar que persista dicha conducta.

[1] Se refiere aquí a la Certificación Núm. 35 Serie 2007-2008 de la Junta de Síndicos, *Política Institucional para la Utilización Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico*. La sección VI de dicha certificación (Derechos y responsabilidades del usuario), a la página 2, lee de la siguiente manera: *El uso personal ocasional de la tecnología de la información está permitido, mientras dicho uso personal no interfiera con el desempeño en el trabajo ni viola alguna política, reglamento o ley vigente. Una evaluación del desempeño laboral de un empleado puede incluir el uso personal de los recursos de tecnología de la información por parte del empleado; Y un supervisor podría requerirle un cambio en dicho uso personal como una condición para continuar en el empleo, de considerarse necesario.*

7
Recursos de comunicación electrónica de la UPRH

El sistema oficial de comunicación electrónica GAE Mail que provee la UPR se considera el medio de comunicación electrónica oficial. No está permitido:

- El uso de una cuenta personal (Yahoo, Hotmail, Gmail, etc.) para comunicar información oficial de la UPR,
- La transmisión, manipulación o el almacenaje de mensajes y anejos de naturaleza fraudulenta, obsceno, de hostigamiento o que viole cualquier política institucional o ley federal o estatal.

8
Acceso y utilización de propiedad intelectual

Ningún documento, imagen o material que sea considerado propiedad intelectual deberá ser copiado, distribuido o almacenado utilizando recursos de la UPRH, excepto cuando la ley así lo permita o un contrato u otro acuerdo con el dueño de los derechos de autor así lo permita. El desconocimiento de que un archivo, documento o imagen es propiedad intelectual no se considera justificación para eximirlo, si copia el objeto sin autorización, debe enfrentar las consecuencias por tener responsabilidad civil o penal.

Las leyes federales y estatales confieren derechos exclusivos al autor o dueño de una propiedad intelectual, estos derechos radican en la reproducción, distribución, ejecución de trabajos musicales, ejecución o transmisión digital de grabaciones audiovisuales, despliegue público y adaptación de la obra. Además, las leyes vigentes en Puerto Rico conceden derechos morales al autor de una obra, de tal forma que la misma no deberá ser alterada por terceros.

Se permite la reproducción y uso de material intelectual de forma limitada, bajo la doctrina de *Uso Justo* (*fair use doctrine)* que contempla la ley. Esta doctrina permite el acceso y la reproducción limitada de material intelectual por terceros, bajo los siguientes criterios: para crítica, comentario, informe de noticias, educación (incluyendo múltiples copias para uso en el salón de clase), investigación, escolaridad y desplace en el tiempo (esto último radica en que la persona puede haber adquirido, por ejemplo, una grabación digital en un momento determinado, luego ejecutarla tiempo después). La ley considera los siguientes factores al determinar si el uso brindado a una propiedad intelectual constituye o no un uso justo:

- Propósito de la utilización,
- Naturaleza de la obra protegida por derechos de autor,
- Cuán sustancial es la porción a utilizar en relación con la totalidad de la obra,
- Efecto del uso propuesto en el valor de mercado de la obra.

9
Consecuencias de no cumplir con las disposiciones establecidas

El usuario que no cumpla, abuse o esté en violación con las disposiciones en la Certificación Núm. 35 y en este procedimiento, estará sujeto a que se le suspenda su acceso a los servicios aplicables, a penalidades administrativas aplicables o a procesamiento civil y penal.

10
Protección del equipo IT cumplimiento con la política y los estándares institucionales

Según planteado anteriormente en este documento, todo usuario y administrador de tecnología que le pertenezca a la universidad, debe cumplir cabalmente con la Certificación Núm. 35, 2007-2008 de la Junta de Síndicos, *Política Institucional para la Utilización Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico*, junto a los *Estándares para la Utilización Aceptable de Tecnología* emitidos por la Vicepresidencia de Investigación y Tecnología. La universidad suministra el aviso de esta condición de diferentes maneras.

En la UPRH cada vez que los usuarios acceden a su PC, previo a subir el sistema operativo, recibe el mensaje de la *Política Institucional sobre el Uso Aceptable de los Recursos de la Tecnología de la Informática* en la UPR el cual debe seleccionar uno de las siguientes alternativas:

- Seleccione el botón rotulado [Acepto] y proceda a utilizar los servicios autorizados en la red de la UPRH,
- Seleccione el botón rotulado [No Acepto], en cuyo caso se desactiva la computadora (hace *shutdown*),
- Seleccione uno de los enlaces junto a los botones, para acceder la política o a los estándares institucionales.

La selección de la opción de *Acepto* es una aceptación tácita del usuario de que acepta los términos y condiciones estipulados en la *Política Institucional y Procedimiento para el Uso Ético Legal de las Tecnologías de la Informática de la Universidad de Puerto Rico*, junto a los *Estándares para la Utilización Aceptable de Tecnología Informática* emitidos por la Vicepresidencia de Investigación y Tecnología.

Se recomienda que las redes locales de los recintos suministren alguna forma análoga de esta notificación para que los usuarios queden debidamente apercibidos diariamente de su responsabilidad por cumplir con la Política. Puede presentarse al momento de acceder el usuario por primera vez a la red de la UPRH o al momento de acceder a algún portal electrónico que suministre uno de los recintos.

La Junta de Síndicos de la Universidad de Puerto Rico, en su Certificación Núm. 35, 2007-2008, aprobó la *Política Institucional Sobre el Uso Aceptable de los Recursos de la Tecnología de la Información*. La UPR vela por el cumplimiento de esta política. Todo usuario es responsable de usar los recursos informáticos de forma eficiente, efectiva y ética, conforme a la ley y la reglamentación universitaria.

Sin embargo, tal rotulación o aviso no es compulsorio, pues la política claramente estipula que un usuario acuerda cumplir con la Política con la mera utilización de los equipos y recursos de la universidad[2].

[2] La sección VI de la Certificación Núm. 35, Serie 2007-2008 de la Junta de Síndicos (Derechos y responsabilidades del usuario), en su inciso A en la página 3, rotulado como *A. Uso Significa Aceptación de la Política y las Normas*, lee como sigue: *Al usar estos recursos de la TI, los usuarios aceptan seguir esta Política, al igual que todas las políticas, normas y procedimientos pertinentes de la Universidad y las leyes federales y locales vigentes.*

11
Protección lógica

11.1 Reglas generales

Las siguientes reglas generales se han redactado para asistir al usuario o administrador de tecnologías a utilizar el equipo y los sistemas a los que se le ha brindado acceso en un ambiente seguro. Aplican a todos los usuarios y administradores de tecnología de la UPR.

Las cuentas creadas para los empleados, estudiantes y otros miembros de la comunidad universitaria son propiedad de la universidad. Se utilizarán para uso oficial en el desempeño de labores y actividades institucionales asociados a las universidades:

- No se permite que los usuarios compartan sus cuentas,
- Una cuenta puede ser desactivada si se detecta o si se informa que está siendo compartida. En este caso, el dueño de dicha cuenta será notificado de esta acción,
- Cualquier cuenta podrá ser desactivada de no tener actividad por un periodo de 30 días o más,
- Luego de tres fallas consecutivas en el proceso de registrar (*login*) de un usuario, la cuenta se desactiva temporeramente,
- Toda cuenta requiere una contraseña para entrar al sistema,
- Cualquier cuenta que no tenga actividad por un año será eliminada. De esta manera, se elimina la posibilidad de violar la seguridad (*break-in*) a través de dicha cuenta por algún usuario no autorizado.

11.2 Utilización de claves de acceso y contraseñas

La combinación de clave de acceso (clave de acceso, *user id*) y contraseña se asigna de forma única y exclusiva a cada usuario como mecanismo para asegurar que solamente aquel usuario autorizado pueda acceder a los datos y sistemas de la universidad a través de la red de comunicación. Los usuarios tomarán las medidas necesarias para proteger estos mecanismos, sea que accedan de forma local o remota, en cumplimiento a la política, los estándares, guías y

procedimientos subordinados que sean implantados a través de la universidad. Los usuarios tomarán los siguientes controles para salvaguardar la confidencialidad de su clave de acceso y contraseña:

- No comparta la contraseña con persona alguna ni siquiera parientes o amigos cercanos,
- No escriba la contraseña. Si la tiene que escribir, no la mantenga en un sitio visible,
- Confirme que otros no han averiguado ni pueden averiguar la contraseña,
- Elija una contraseña fuerte y cámbiela frecuentemente. Las contraseñas fuertes son difíciles de adivinar o identificar (un proceso comúnmente conocido como *romper* la contraseña).

Algunas técnicas para seleccionar una contraseña fuerte son:

- Escribir la palabra seleccionada en reverso (e.g. *anesartnoc* en lugar de *contrasena*),
- Consulte el procedimiento para utilizar y administrar
- La tecnología informática en la sección 11.3 página 27,
- Utilizar anagramas (una palabra con dos o más letras transpueta, e.g. *trauqne* en lugar de *tranque*),
- Sustituir letras por números o por otras letras, e.g. *c3kur1dat* en lugar de *seguridad*,
- Alternar letras mayúsculas y minúsculas, e.g. *pROTexIOn*.

Contraseñas débiles son fáciles de romper. Algunos ejemplos de contraseñas débiles son fechas (aniversarios, cumpleaños), nombre de parientes y amigos, nombres de mascotas, números de teléfono, etc.

- No utilice la clave de acceso como contraseña.
- No utilice información confidencial, tal como su número de seguro social o pasaporte o algún componente de ellos, como clave de acceso o como contraseña.
- El usuario es responsable de las consecuencias por cualquier acción tomada con la clave de usuario y contraseña, no re utilice contraseñas que utilizó en el pasado.
- Las claves de acceso y contraseñas para acceder a los servidores y equipo de redes y telecomunicación se protegerán de manera aún más estricta que los equipos de los usuarios.

Cambie su contraseña de ocurrir una o más de las siguientes situaciones:

- Cuando un equipo nuevo se instale en ambiente productivo,
- Posterior a brindar la contraseña a terceros para que le brinde servicio de mantenimiento o reparación al equipo informático,
- Cuando personal de administración de redes o sistemas se retira, es despedido o transferido fuera de sus responsabilidades de administración de la red o de los sistemas,
- Cuando la confiabilidad o confidencialidad se la contraseña quede en entredicho. En este caso, el usuario debe notificar del incidente a la administración de redes o sistemas para que se investigue el mismo.

11.3 Política utilizadas de contraseñas

- Las contraseñas expiran cada 90 días para usuarios y se requiere que las nuevas contraseñas sean diferentes a las expiradas,
- Las contraseñas deben ser de, por lo menos, ocho caracteres de largo. Si se intenta utilizar una contraseña menor, el sistema lo rechazará.
- Existe un periodo mínimo de vida para las contraseñas, de esta manera, se evita que un usuario cambie su contraseña, para luego volverla a cambiar a la original.
- Se sugiere que las contraseñas no sean fáciles de adivinar.
- Si el sistema lo permite, deben utilizarse combinaciones de letras, números y caracteres especiales.
- Se debe evitar nombres de familiares, mascotas, etc. o sus respectivas abreviaciones o combinaciones.
- No se debe utilizar palabras relacionadas a computadoras, modelos, etc.
- Evite utilizar el número de seguro social, tablilla de vehículo, teléfono o cualquier tipo de información que sea fácil de obtener.
- Se debe utilizar contraseñas fáciles de recordar, pero no relacionadas directamente con el usuario.
- No anote las contraseñas en lugar alguno.
- No comparta las contraseñas con compañeros u otros usuarios.

11.4 Aplicación de parchos de seguridad

La aplicación de parchos de seguridad es un requisito indispensable para proteger el sistema operativo y las aplicaciones principales en una computadora del impacto destructor de los programas maliciosos que se describen en la próxima sección. Esta programación correctiva (conocida colectivamente como parchos de seguridad), protege los sistemas y los datos que acceden.

Aquellos servidores administrados por el SICC, también se deben actualizar periódicamente. En la medida posible, se debe contar con un servidor dedicado a recibir y centralizar los parchos de seguridad emitido por los suplidores de los sistemas y programas. Esta labor se puede automatizar de modo que se ejecute fuera de horas laborables. Luego, la red se puede configurar para que emita las correcciones a las computadoras conectadas a la red en ventanas de tiempo que permita actualizar las computadoras con un mínimo de impacto a los usuarios.

La práctica anterior aplica también a los equipos de redes de comunicación, los cuales dependen de versiones actualizadas de programas propietarios o *firmware* para operar correctamente.

Se debe dar mantenimiento preventivo periódicamente a las computadoras y otros dispositivos electrónicos tales como componentes de redes de comunicación. Esto incluye la aplicación de parchos críticos de seguridad y actualizaciones del *firmware* dentro de los siguientes 15 días posterior a su liberación comercial por el manufacturero. Equipos que contengan datos sensitivos o privados deben mantenerse con estas actualizaciones con aún mayor frecuencia. Otros parchos no designados como críticos por el manufacturero se deberán aplicar a base de un itinerario regular de mantenimiento.

Muchos suplidores han automatizado el procedimiento de actualizar y aplicar parchos, particularmente para las computadoras de escritorio. Aunque existe una posibilidad de que el suplidor incorpore errores en estos procedimientos, los riesgos son menores que si no se aplican las actualizaciones por omisión.

Los parchos a sistemas en ambientes de producción pueden requerir procedimientos complejos de prueba e instalación, tales como llevar a cabo la instalación y prueba sobre servidores en ambiente de pruebas para garantizar que no surjan problemas mayores cuando se apliquen los mantenimiento en producción. En algunos casos, es preferible mitigar el riesgo por otro mecanismo que no sea la aplicación de un parcho. La mitigación elegida debe ser proporcional al nivel de riesgo. La razón de alejarse de la práctica prevenidamente descrita y las medidas alternas de mitigación tomadas deben estar documentadas por escrito, especialmente para dispositivos que almacenan datos privados.

11.5 Virus y otros programas nocivos

Existen programas de intención maliciosa cuyo efecto representa un riesgo sustantivo a la universidad por su potencial de pérdida de dinero, tiempo y datos que, colectivamente, se conocen en inglés como *malware*. Estos programas se instalan en las computadoras de manera intencional o accidental. La existencia del mismo en una computadora puede ser desconocida por un usuario por tiempo

indefinido. A través del tiempo, el nivel de sofisticación, velocidad de propagación y magnitud del daño de este tipo de programa ha incrementado.

Estos programas se conocen con diferentes nombres: virus, troyanos y gusanos (*worms*), entre otros. Un virus es un programa que se replica de computadora en computadora. Al igual que la trata del Caballo de Troya, el troyano se esconde en un archivo o programa válido para acceder a una computadora. Luego procede a infectar la misma o dañar archivos que residen en ésta. Los gusanos tienen características de virus y de troyanos en cuanto a cómo se propagan y replican, pero difiere de los otros dos en cuanto a que su propósito final es destruir datos o sectores de un disco duro, de modo que la computadora se vuelva inservible. Existen varias fuentes de donde surge este tipo de programación maliciosa:

- Acceder a una computadora infectada,
- Al utilizar disquetes, discos compactos o *pen drives* infectados,
- Al bajar un archivo de una base de datos pública o página web de origen dudoso.
- Ejecutar un programa infectado, particularmente los que llegan como anejos (*attachments*) en correos electrónicos desconocidos,
- Activar el sistema operativo de una computadora con un disquete o disco infectado,
- Por acciones maliciosas intencionales de individuos que buscan acceder remotamente una computadora.

Como norma, el usuario se percata de la invasión de un virus porque el comportamiento de la computadora o de una de sus aplicaciones cambia. Algunos síntomas son:

- Aumento en el tamaño de los archivos,
- Cambio en la fecha de actualización de un programa o archivos,
- Disminución en el espacio disponible de disco o memoria después de correr un programa gratis (*Freeware*) o compartibles (*Shareware*),
- Múltiples accesos inesperados en su disco

La mejor forma de minimizar la probalidad de infección de una computadora es tomar diligencia al momento de acceder páginas o correos que contengan programas o archivos desconocidos. Algunas recomendaciones para evitar una infección son:

- Minimice la práctica de compartir programas,
- Mecanismos de control al regresar a la institución un disquete que fue sacado de la oficina,

- Genere de manera periódica y consistente resguardos de sus datos y documentos (*backups*).

11.6 Programa antivirus

Los programas antivirus son programas preventivos, específicamente diseñados para proteger una computadora de la posibilidad de infección por programas de tipo *malware*. Como parte del esfuerzo de asegurar y proteger todo el equipo que accede a datos de la universidad, toda computador que se conecte a la red de comunicaciones de la universidad tiene que utilizar programas para protegerse contra virus (o programas par filtrar virus, en el caso de computadoras que ejecutan cualquier variante de Unix).

Debido a la frecuencia con que se actualizan los virus existentes o surgen virus nuevos, es crítico que los programas antivirus se mantengan actualizados, como mínimo, a nivel semanal. Esta acción se extiende también a los servidores y los equipos de telecomunicaciones.

El programa de antivirus y los diccionarios de virus que éstos programas utilicen están disponibles para las computadoras de la universidad a través del SICC. Para las computadoras de terceras personas (auditores, consultores, suplidores, contratistas), que soliciten conectarse a la red sistémica o alguna de las redes locales de la universidad, sus dueños deberán procurar un programa antivirus adecuado y actualizado para evitar que se infecte la red.

La próxima sección de este documento suministra instrucciones adicionales para instalar el programa *Symantec Antivirus Corporate Edition* en las computadoras de las unidades.

11.7 Instalación del programa antivirus: Cliente Symantec de Norton

- Invoque el programa de instalación desde el CD de *Symantec Antivirus*,
- Espere a que suba la ventana de *Symantec Antivirus Corporate Edition* y seleccionar *Install Symantec Antivirus*,
- En la próxima ventana, seleccionar *Install Symantec Client*,
- En otros Cds o localidades: Busque el directorio que contenga el archivo *SAVECLT.EXE* y corra este programa.

11.7.1 Instalación nueva

- En la ventana *Welcome to the Symantec Antivirus Client Setup Program*, oprimir el botón [NEXT >],
- En la ventana *License Agreement*, marcar *I accept the terms in the license agreement* y oprimir el botón [NEXT >],
- En la ventana *Mail Snap-IN Selection*, verificar que esté marcada la opción *Microsoft Exchange/Outlook*. Oprimir el botón [NEXT >].
- En la ventana *Destination Folder*, oprimir el botón [NEXT >],
- En la ventana *Network Setup*, seleccionar la opción *Managed*. Oprimir el botón [NEXT >],
- En la ventana *Select Server*, oprimir el botón *Browse*. Si aparece el nombre del servidor donde reside la consola de *Symantec Antivirus*, seleccionar el mismo, oprimir el botón de [OK] y después el de [NEXT >]. Sino aparece el nombre del servidor, oprima el botón [FIND COMPUTER]. Cuando aparezca la ventana *Find Computer*, seleccionar la opción *Name* y escribir el nombre del servidor o seleccionar la opción *IP Address* y escribir la dirección *IP* del servidor. Seleccione el servidor, oprima de [OK] y después el botón [NEXT >],
- En la ventana *Verify Server Name*, observar que el servidor que aparece sea el que se selección en el paso anterior y oprimir el botón [NEXT >],
- En la ventana *Ready to install the program*, oprimir el botón [NEXT >]. Espere mientras se instala el programa,
- En la ventana *Technical Support*, oprimir el botón [NEXT >],
- En la ventana *Install Wizard Completed*, oprimir el botón [FINISH]. Con esto la instalación terminó.

11.7.2 Actualización de versión previa

Cumpla los pasos 1, 2, 8, 9 y 10, según explicados en el proceso para una instalación nueva. Ignorar los demás pasos. El requisito para una actualización es que se tenga instalada una versión anterior del programa.

11.7.3 Cómo resolver una infección

A pesar de la diligencia que se invierta en proteger un equipo, puede que el mismo termine infectado. En este caso, se deberá coordinar con el SICC para que se restauren los programados en la computadora afectada y se recuperen los datos y documentos utilizando el último resguardo creado por un usuario. Los pasos que debe tomar el personal del SICC para atender este problema se describen a continuación:

1. Desconecte la computadora se la red,
2. Analice y determine la gravedad de la infección,
3. Apague la computadora,
4. Reactive la computadora, subiendo el sistema operativo de los medios originales (disco compacto o CD),
5. Coteje que el sistema subió correctamente y de manera estable,
6. Reguarde todos los archivos no ejecutables (documentos, imágenes, hojas de cálculo, presentaciones, bases de datos, etc.), de todos los directorios, en un nuevo medio recién formateado (*pen drive*, CD o DVD nuevo),
7. Enumere los archivos *batch* en el sistema. Si cualquiera de las líneas de codificación resulta cuestionable no se resguardará ese archivo,
8. Una vez se complete le resguardo, proceda a llevar a cabo un *low level format* del disco duro infectado,
9. Una vez el dico duro haya sido reformateado, se procederá a restaurar el sistema operativo en el disco duro previamente infectado. Luego, se reestructurarán los directorios,
10. Se restaurarán los programados utilizando los medios originales del producto tal y como si fuera una nueva instalación de los programados,
11. Se restaurarán los archivos a los que previamente se les hizo resguardo,
12. Ubique todos los medios que hayan sido insertados en la computadora en el transcurso de los últimos seis meses previo a la restauración. Estos medios deberán ser desinfectados. Si no pueden ser desinfectados, deberán destruirse para evitar una nueva infección. Previo a la destrucción, se debe coordinar respaldar los datos no ejecutables contenidos en estos medio desde una computadora aislada de la red.

12
Protección física

12.1 Cuido del equipo en el área de trabajo

Todo equipo electrónico es sensitivo a cambio en el ambiente, por lo cual requiere un cuidado mínimo para que le dure el término de su vida útil. Se recomienda que todo usuario y administrador de tecnología siga los pasos que se presentan a continuación para proteger el equipo que le ha sido asignado:

1. Proteja el equipo de riesgos ambientales tales como polvo, fuego y agua,
2. Suministre ventilación adecuada al equipo en operación,
3. Instale regulador de voltaje y fuente de carga ininterrumpidas (UPS) para extender la vida útil del equipo,
4. Desactive y apague el equipo al concluir el día,
5. Si se debe levantar de su área de trabajo, desactive su sesión (*logoff*) o tranque la pantalla (oprima simultáneamente las teclas CTRL+ALT+DEL, luego haga clic sobre el botón [Lock Computer]),
6. Notifique de inmediato al SICC de cualquier falla con la computadora o en su acceso a la red para mitigar el riesgo de perder información o acceso a servicios básicos,
7. Coordine con el SICC la instalación de cualquier programa (*software*),
8. Siga las recomendaciones aquí suministradas para resguardar sus programas, archivos, datos y documentos electrónicos periódicamente,
9. Remueva información confidencial de su computadora, previo a enviarla para reparación o asigne la reparación a una compañía que tenga un acuerdo de no divulgación con la universidad,
10. No fume o ingiera alimentos o bebidas mientras utilice la computadora,
11. No modifique la configuración de su equipo o la programación o se expone a que se le interrumpa su uso de la computadora o el acceso a la red,
12. No deje su computadora desprotegida, a la vista y acceso de todos propensa al robo,
13. Informe de inmediato la pérdida o robo de su equipo,
14. No utilice equipo módem independiente de la red de comunicaciones sin coordinarlo con el SICC ya que expondría la red de comunicación a riesgos de ataques.

12.2 Cuido del equipo fuera del área de trabajo

Para los usuarios que utilizan computadoras o dispositivos portátiles para conectarse a la red de comunicaciones, además de seguir las recomendaciones de la sección anterior, se recomienda que tome los siguientes pasos adicionales para proteger su equipo:

1. Nunca deje su computadora portátil desatendida, particularmente en sitios públicos,
2. No deje su computadora portátil a plena vista. Si debe alejarse de su área de trabajo por un tiempo extendido, considere guardarla bajo llave (e.g. en un gaveta), o considere asegurarla al escritorio con un cable con candado que viene diseñado para tal propósito,
3. Intente no dejar su computadora portátil en el auto. Si la debe dejar en el auto, guárdela fuera de la vista de terceros, preferiblemente encerrándola en el baúl,
4. Si va de viaje, utilice un bulto no descriptivo (e.g. una mochila), para guardar su computadora. La idea de esta recomendación es que ni la computadora ni el bulto donde la guarda llame la atención de terceros.

13
Solicitud de acceso a los sistemas y redes

Para el empleado que solicita una clave de acceso por primera vez, debe seguir los pasos que se enumeran a continuación para obtener las claves y contraseñas para los sistemas a los cuales la universidad le brindará acceso. Solicite el formulario titulado *Solicitud de Creación de Cuenta a los Sistemas de Información* (ver Apéndice D, p. 61). Puede acceder este formulario en http://www.uprh.edu/formasuprh/sccsi.pdf

1. Identifique si solicita una cuenta nueva o renovación,
2. El solicitante debe suministrar la siguiente información: nombre y apellidos, título o puesto, teléfonos, oficina o división donde está ubicado,
3. Indique la unidad del sistema a la cual responde,
4. Indique los días y horarios para los cuales solicita tener acceso,
5. Indique el propósito principal del acceso a la red local (marque todos los encasillados que apliquen),
6. En el encasillado suministrado a mano derecha, el solicitante debe firmar y colocar la fecha de su petición,
7. Igualmente importante, el solicitante debe leer el dorso de la solicitud y firmar la misma, certificando que ha leído las disposiciones para el uso de tecnologías de información,
8. El director de la oficina o departamento al cual responde el solicitante debe firmar. NO se atenderán solicitudes que no cuenten con la autorización del director de la oficina o departamento.
9. Una vez se haya cumplimentado el formulario con la información solicitada, se deberá remitir la solicitud al SICC. La dirección del SICC autorizará la solicitud y la referirá para que se atienda.

Solicite los siguientes formularios de las oficinas responsables por los sistemas correspondientes:

- SIS - Oficina de Registrador
- HRS - Oficina de Recursos Humanos
- UFIS (Oracle) - Oficina de Finanzas

Para las solicitudes de SIS y HRS se hará lo siguiente:

1. El director de la oficina o departamento solicitará mediante carta los accesos necesarios para que el solicitante tenga los accesos que corresponde,
2. La persona a cargo de la seguridad del módulo pertinente cumplimentará el formulario con los debido accesos y lo enviará al SICC,
3. El personal de seguridad del SICC creará la cuenta con sus respectivas autorizaciones, siempre que la solicitud cumpla con los requisitos establecidos,
4. La persona a cargo de la seguridad del sistema de información administrativa en el SICC devolverá el formulario procesado a la oficina solicitante. El SICC retendrá copia del formulario para su archivo,
5. El coordinador de seguridad de la oficina correspondiente orientará al nuevo usuario sobre dónde obtener el adiestramiento necesario para emplear el sistema según la solicitud. También hará énfasis en la responsabilidad del nuevo usuario en la custodia de las contraseñas y la prohibición de transferir éstas.

NOTA: Los usuarios de SIS y HRS tienen que cumplimentar dos solicitudes: la *Solicitud de Creación de Cuenta a los Sistemas de Información* (indicado en el primer párrafo) y la solicitud a la oficina custodia del sistema (Registrador o Recursos Humanos, según el caso). Tienen que estar ambas solicitudes en el SICC, de lo contrario NO se le crearán los accesos.

14
Acceso y utilización remoto a los servicios de red

14.1 Acceso remoto a los servicios de red

La universidad reconoce que los usuarios pueden tener una necesidad legítima para trabajar fuera de su oficina o lugar normal de trabajo. En estas ocasiones, la posibilidad de trabajar de manera remota redunda en beneficio para la universidad. Sin embargo, el acceso remoto es un privilegio que se asigna con los debidos controles para proteger la red universitaria.

14.2 Utilización remota a los servicios de red

Cuando un usuario se conecte de manera remota, la computadora que utiliza debe estar tan segura como su contraparte local. Esta sección aplica tanta a conexiones remotas para llevar a cabo tareas a favor de la universidad, incluyendo, pero no limitándose a recibir y leer correos electrónicos y acceder a páginas de Web y recursos a Internet.

El acceso remoto será controlado de manera estricta. El SICC controlará este recurso y habilitará esta posibilidad asignando una clave de acceso y contraseña a cada usuario. Todo usuario que se conecte de forma remota a la red de comunicación de la universidad y que acceda datos privados o restringidos deberá utilizar el servicio de red virtual privada (VPN), que provee la universidad. Los usuarios remotos protegerán su clave de acceso y contraseña según se detalla más adelante en este documento.

Mientras una computadora o dispositivo esté conectado a la red de comunicación de la universidad, no deberá estar conectado simultáneamente a otra red de comunicación que no sea una red privada bajo control del usuario. Todo equipo utilizado para conectar a la red universitaria debe tener instalado un programa antivirus en su versión más actualizada. Los archivos que identifican virus se mantendrán actualizados. El programa antivirus se ejecutará periódicamente para proteger el equipo y los datos ubicados en él.

Los usuarios que acceden la red universitaria de forma remota garantizarán que el sistema operativo y los programas en uso por el equipo conectado a la red universitaria tengan aplicados los parchos de seguridad más recientes.

15
Revocación de los privilegio de acceso

La revocación de los privilegio de acceso a un empleado se lleva a cabo cuando un empleado dimite, se retira, es trasladado o despedido. Como parte del trámite de partida, la Oficina de Recursos Humanos le suministra al empleado el formulario *Certificado de Relevo de Responsabilidades* (ver Apéndice E, p. 63). Éste se puede acceder en el vínculo http://www.uprh.edu/formasuprh/cc.pdf Este formulario funciona como lista de cotejo para que el empleado saliente pueda confirmar con las diferentes oficinas de la UPRH que ha devuelto los recursos que la universidad le suministró como herramientas de trabajo. Dicho formulario se divide en apartados, entre los cuales se reserva uno para los cotejos que debe llevar a cabo el SICC.

Al recibir dicha notificación, el SICC refiere el formulario al personal responsable de administrar los siguientes recursos informáticos para suspender los privilegios de acceso del empleado saliente o programar su suspensión a partir de la fecha efectiva de su terminación:

- sistemas de información administrativo (SIA)
- sistema Oracle (OSS, UFIS)
- servidor HP Integrity
- servidores Windows
- bases de datos de la Biblioteca
- acceso remoto
- otros servicios según apliquen

El administrador de cada uno de los servicios anteriores registra la fecha en que se revoca el privilegio y coloca su firma, constando que la tarea se lleva a cabo. Al final, la dirección del SICC suscribe con su firma el documento, previo a devolverlo al empleado o a la Oficina de Recursos Humanos para que continúe su curso.

16
Reparación del equipo IT

La utilización continua del equipo puede dar paso a que surjan averías que requieran reparación en el transcurso de su vida útil. Los equipos se adquieren con una garantía mínima de un año. Se recomienda adquirir una garantía extendida por tres años con la adquisición de equipos tales como computadoras personales (e.g. pc o mac), proyectores digitales o equipo de telecomunicaciones. De ese modo, al ocurrir una avería en algún equipo que cuenta con un contrato vigente de mantenimiento, la oficina o departamento que ubica el equipo debe contactar al SICC para que inspeccione el equipo y pueda darle los detalles técnicos al suplidor de dicho servicio y coordinar su reparación.

En el caso donde un equipo no tenga contrato de mantenimiento, la oficina o departamento debe consultar, de igual manera, al SICC para determinar si tiene disponible el personal para reparar dicho equipo. Aún sino lo tuviera, el SICC podrá suministrar una opinión en cuanto a si vale la pena reparar o no el equipo. Si se entiende que el equipo se puede reparar, la oficina o departamento deberá solicitar cotizaciones para su reparación a través de la Oficina de Compras. Como regla general, el costo de reparar un equipo más allá de su vida útil tiende a incrementar a través del tiempo, hasta llegar a ser oneroso. Esto se debe a que los componentes se hacen cada vez más escasos y caros de procurar y almacenar por el suplidor, debido a la obsolescencia del equipo.

Antes de contratar la reparación del equipo averiado, la cotización se debe comparar contra el valor del equipo averiado y el valor de adquirir un equipo de reemplazo. Si se determina que no amerita reparar el equipo, la oficina o departamento procederá a decomisar el mismo y a justificar la adquisición de su reemplazo.

17
Actualización del equipo IT

En las ocasiones donde un equipo no tenga suficiente capacidad para ejecutar ciertas funciones, la oficina o departamento que custodia el equipo puede optar por reasignarlo a otra persona que pueda utilizar el equipo con su configuración actual según se describe en la sección titulada *Transferencia de Equipo IT* (p. 12). En otros casos, actualizar uno o más de los componentes puede ser suficiente para adecuar el equipo al nuevo uso. A continuación se presentan algunos ejemplos comunes de actualización de tecnología:

- Incrementar la cantidad de memoria de una computadora o impresora,
- Incrementar la cantidad de almacenaje de una computadora o servidor,
- Actualizar la versión del sistema operativo de una computadora,
- Actualizar la versión del micro código de un equipo de comunicación.

La oficina o departamento que desee explorar esta alternativa debe contactar al SICC para solicitar apoyo a llevar a cabo este tipo de evaluación.

18
Reemplazo del equipo IT

Cada oficina o departamento debe contemplar la vida útil de su equipo de tecnología informática al momento de revisar sus respectivos presupuestos anuales, de modo que pueda planificar para la sustitución oportuna de los mismos en el año fiscal en que venza su vida útil. Según requieran de apoyo adicional, pueden solicitar ayuda al SICC para identificar la edad, especificaciones técnicas y costo aproximado de reemplazo de algún equipo en particular.

La mayoría de los equipos informáticos y dispositivos asociados utilizados por usuarios tiene una vida útil promedio de tres años, según se puede ver en la tabla 1. Los servidores de redes locales tienden a estar en operación hasta cinco años. De acuerdo al cuidado y mantenimiento que se le brinde, este equipo pudiera aún estar en condiciones utilizables al final de su vida útil. Si el mismo está en condiciones adecuadas, no existe razón alguna para que no pueda continuar brindando servicios a la oficina o departamento, siempre que cumpla su cometido.

Tabla 1
Vida útil de tecnología de información

Equipo	Vida útil
Computadora de escritorio	3 años
Computadora portátil	3 años
Impresora de usuarios	3 años
Escáner	3 años
Servidores	5 años
Equipo de comunicación: enrutadores, conmutadores, etc	5 años
Proyectores digitales	5 años

En lo referente a equipos críticos, tales como servidores o equipos de comunicación, la oficina o departamento debe considerar también la procura del equipo alterno (de contingencia), que necesitará para recuperar el servicio que brinda el equipo primario ante algún desastre, de acuerdo al plan existente de contingencia.

La capacidad de una oficina de departamento para reemplazar equipo que llegue al final de su vida útil está condicionada a que dicha oficina o departamento cuente con el presupuesto necesario para llevar a cabo el reemplazo. En aquellos casos donde la oficina o departamento cuente con un presupuesto menor, deberá discriminar con respecto a cuáles unidades se habrán de reemplazar durante el año fiscal, de acuerdo al nivel crítico que preste los equipos a reemplazar.

Irrelevante de si cuenta o no con presupuesto para reemplazo de equipos, se recomienda que cada oficina o departamento mantenga actualizado un inventario electrónico que le facilite la identificación y valorización de la tecnología que tiene bajo su custodia. Dicho inventario se debe revisar cada vez que un equipo se adquiere, asigna, actualiza o decomisa. Como mínimo, el inventario de equipo debe incluir los datos que se enumeran a continuación:

- Número de serie o número de propiedad
- Descripción del equipo (incluyendo manufacturero y modelo)
- Fecha aproximada de adquisición
- Ubicación física del equipo
- Nombre y número de teléfono del custodio local
- Categoría bajo la cual se clasifica el equipo: mainframe, mini, servidor, computadora personal, computadora portátil, enrutador, impresora, conmutador, lector óptico, proyector digital, etc.
- ¿Está el equipo bajo garantía? ¿existe contrato de mantenimiento? ¿con qué suplidor? ¿cuál es el término contractual? ¿cuál es su costo? ¿existen niveles de servicio?

Con respecto al SICC o la unidad a cargo del equipo asignado, el personal que brinda apoyo técnico y servicio a los usuarios mantendrá un registro de mantenimiento y reparación de los equipos en los cuales interviene (ver formulario en el Apéndice F, p. 64). De esta forma se facilitará rastrear la cantidad y frecuencia de intervenciones en un mismo equipo. Este dato es útil al momento de recomendarle a la oficina o departamento que reemplace un equipo sino ha determinado su vida útil.

Aún cuando un equipo llegue al final de su vida útil, se recomienda evaluar la posibilidad de reparar el equipo y mantenerlo en uso como alternativa a la adquisición del equipo nuevo. La decisión final es una de costo-beneficio que le permita a la oficina o departamento planificar un reemplazo masivo para aprovecharse de escalas de economía.

19
Decomiso del equipo IT

Cada oficina debe contemplar decomisar equipos individuales de tecnología de información bajo uno de los escenarios que se describen a continuación:

1. El equipo llegó al final de su vida útil,
2. El equipo experimenta una frecuencia continua de intervenciones para su reparación, que lo hace inaccesible al usuario o que evita que el usuario pueda llevar a cabo su tarea, o
3. Reparar la avería de un equipo resulta más caro que adquirir un equipo nuevo.

En cualquiera de los tres casos anteriores, la persona a cargo de la oficina o departamento que custodia el equipo procederá a decomisar el equipo existente y justificar la procura del nuevo equipo según las certificaciones relevantes.

Como parte del proceso para decomisar computadoras, el encargado de la propiedad o el director de una oficina o departamento coordina con el SICC para que inspeccione este equipo previo a decomisarlo. El SICC delega esta tarea en personal del grupo de servicios a usuario (GSU) quienes reformatean el disco duro de la computadora para erradicar las pariciones previamente definidas. Esto elimina de manera permanente cualquier información que hasta el momento haya contenido el disco. El encargado de la propiedad u oficial autorizado autoriza el proceso mediante el formulario titulado *Certificado de Eliminación Segura de Datos* (ver Apéndice G, p. 65). El GSU procede a reformatear los discos en aquellas unidades previamente identificadas en el formulario. Una vez se completa esta tarea, el técnico que atendió la solicitud de servicio firma el formulario y lo devuelve al SICC, donde se archivará la certificación.

El encargado de la propiedad, director de la oficina o departamento u oficial autorizado son las únicas personas que pueden endosar el formulario de certificación. Sin esta autorización, el SICC no puede proceder con la eliminación segura de los datos del disco. Por otra parte, el usuario debe tener presente que una vez ser reformatee el disco, los datos quedan destruidos e inaccesibles. Por lo tanto, antes de proceder con la eliminación, el director de la oficina o departamento u oficial autorizado es responsable por validar que el personal de su oficina haya tomado los pasos necesarios para resguardar previamente cualquier dato, archivo o documento que necesite retener para utilización futura.

El decomiso de equipo se describe en mayor detalle en la Certificación Núm. 62, 1994-1995, de la Junta de Síndicos, *Reglamento para el Control de Bienes Muebles en la Universidad de Puerto Rico.*

20
Evaluación de la ejecutoria del equipo IT

Se recomienda que el SICC utilice algún programado que le permita supervisar de forma proactiva la disponibilidad y ejecutoria de equipos críticos, tales como servidores o equipo de comunicación. De este modo, se puede alertar al personal que administra los mismos en caso de algún incidente que amenace con interrumpir el servicio. Una vez se alerte al administrador de un incidente con un equipo específico, el administrador puede revisar la bitácora de eventos en el servidor o equipo correspondiente para obtener detalles adicionales sobre el incidente. Algunos ejemplos de programas que llevan a cabo esta función lo son el *Operations Manager de Microsoft* o programas de tipo *open source*, tales como *Big Brother* o *Big Sister* en plataforma de Windows.

Aunque los ejemplo brindados anteriormente no tienen impacto en el tiempo de respuesta de la red, el impacto que finalmente tengan los programas que llevan a cabo este tipo de función dependerá de los siguientes criterios:

- La plataforma sobre la cual trabaja el programa (e.g. HP Integrity, Windows o Linux),
- El número de servidores que supervisa el programa,
- La cantidad de parámetros que se le solicita al programa medir (e.g. utilización de la capacidad de procesamiento, disco o memoria). Se le recomienda al lector que al momento de configurar los parámetros que desea medir, contemple la capacidad de los servidores, la red de comunicación y las recomendaciones del manufacturero para evitar sobrecargar la red y los servidores hasta el punto de afectar el servicio que brindan a los usuarios.

Respecto al equipo que utilizan los usuarios, la supervisión de ejecutoria se hace un poco más difícil debido a la cantidad y distribución de los mismos a través de la red de comunicación. La detección de problemas con algún equipo se facilitará en la medida que estos usuarios notifiquen al SICC para solicitar apoyo. La evaluación de los siguientes criterios puede ayudar a un usuario a solicitar reemplazo de un equipo:

- Finalizó la vida útil del equipo que requiere intervención para reparación,
- Un equipo reparado continúa experimentando problemas. En este caso, la determinación de si se reemplaza el equipo depende de la utilización que se le da al equipo, cuán crítico es el propósito para el cual se utiliza y cuál es su costo de reemplazo,
- El equipo que tiene asignado el usuario no tiene la capacidad suficiente para ejecutar alguna de las aplicaciones que requiere utilizar el usuario. En este caso, se puede evaluar la actualización del equipo según se describe en la próxima sección,

- El costo de actualizar (*upgrade*) el equipo no amerita la inversión,
- Sala más económico reemplazar el equipo que repararlo.

21
Resguardo periódico de los datos almacenados en la computadora asignada al empleado

El resguardo es una copia que se hace de los archivos, datos y documentos electrónicos con la intención de poder recuperar cualquiera de ellos, en caso de que la versión con la que se trabaja se dañe o se pierda debido a algún caso fortuito. La copia se hace generalmente a un medio de almacenaje portátil, tal como *pen drive*, un disco compacto (CD), disco de video digital (DVD) o cartucho de cinta magnética. Se recomienda que esta copia se guarde fuera del área de trabajo (en un lugar seguro) por si el problema afecta el área de trabajo del usuario o administrador de tecnología. Como regla general, los archivos, datos y documentos electrónicos con los que trabajan los usuario y administradores de tecnología se deben resguardar semanalmente. De esta manera, un usuario o administrador de tecnología puede recuperar su trabajo de una copia actualizada.

Si la computadora a través de la cual el usuario o administrador de tecnología está conectada a una red local, se recomienda que ausculte con el SICC la posibilidad de que sus documentos, datos y archivos se almacenen en algún servidor de archivos que esté disponible en la red local. Esto tiene el efecto de que los mismos se incluyan en el resguardo periódico que genere el SICC de dicho servidor. Sino hubiera un servidor de archivos disponible en la red local –o si el usuario o administrador de tecnología opta por mantener sus documentos, datos y archivos en su computadora– el usuario o administrador de tecnología asume la responsabilidad de resguardar estos documentos, datos y archivos al menos con una frecuencia semanal.

Como regla general, se recomienda que todo usuario resguarde semanalmente los datos que mantienen almacenados en sus computadoras. De esta forma, cuenta con copias actualizadas de su trabajo, a las cuales puede acudir en caso de que no tuviera acceso a los datos en su computadora. **Es responsabilidad del usuario tomar resguardo de los datos y archivos que mantenga en su computadora o en algún otro dispositivo FUERA de un servidor en la red local que esté bajo la custodia y administración del SICC.** De suceder alguna interrupción o fallo en una aplicación o servicio electrónico (o si ocurriera algún incidente que comprometa la seguridad de una aplicación), la UPRH no será responsable por cualquier daño o pérdida de datos que ocurra ni por las complicaciones que se puedan derivar como resultado del incidente. Una alternativa relativamente sencilla para lograr esto es de resguardar los datos a disco compacto (CD). Para realizar este resguardo, siga los pasos que se describen a continuación.

22.1 Previo a comenzar

- Valide que cuenta con suficiente suministros de Cds en su oficina,
- Este procedimiento supone que sus archivos y documentos están almacenados bajo la ruta *My Documents*

22.3 Resguardar directorio de archivo y documentos

22.3.1 Inserte un CD-R o CR-RW nuevo en el dispositivo correspondiente de su computadora.

22.3.2 De clic derecho sobre el botón **Start** en su computadora. En el menú flotante que aparece, seleccione **Explore**.

22.3.3 En la ventana que aparece, seleccione el directorio *My Documents*. En el lado derecho se presentará su contenido.

22.3.4 Seleccione de la parte superior de la ventana el menú de **Edit** > **Select All** (u oprima CTRL+A). Esto selecciona todos su contenido. Si desea excluir alguna carpeta o documentos, mantenga presionada la tecla CTRL mientras da clic con el ratón sobre el directorio o documento.

22.3.5 Ubique el puntero del ratón sobre alguno de los objetos seleccionados, oprima el botón derecho del ratón y seleccione la opción **Copy** (u oprima CTRL+C).

22.3.6 En el lado izquierdo de la pantalla seleccione la unidad de CD (o DVD) de su PC. El lado derecho de la pantalla aparecerá en blanco mostrando que no hay documentos. Oprima el botón derecho del ratón en el área vacía y seleccione la opción **Paste** (u oprima CTRL+V).

22.3.7 Aparecerán todos los archivos plasmados con una flecha hacia abajo indicando estar listo para ser copiados definitivamente en la unidad óptica reescribible (CD-R, CR-RW, DVD±R o DVD±RW). Para inicial el reguardo, seleccione el menú de **File > Write these files to CD**.

22.3.8 Aparecerá una ventana tipo *wizard*, en el cual podrá designarle un nombre al CD que va a grabar, previo a seguir los pasos subsiguientes hasta completar el proceso de resguardo.

Apéndice A
Glosario

Datos privados

El concepto dato privado se define como información de la universidad que está legal o contractualmente protegida y que la universidad viene obligada a tratar como confidencial y privilegiada, sea información de naturaleza investigativa, clínica, educacional, social o administrativa. Algunos ejemplos de datos privados se presentan a continuación:

- número de seguro social,
- etnicidad,
- propiedad intelectual,
- ciudadanía,
- edad o fecha de nacimiento,
- dirección residencial,
- condición de incapacidad,
- número de teléfono celular o residencial,
- credo o preferencias religiosa o política,
- información sobre su salud,
- género,
- ubicación de activos,
- donantes anónimos,
- identificar el usuario con temas sobre los cuales tiene preferencia o sobre los que ha solicitado en el pasado,
- información personal del estudiante (la cual no tiene preferencia o sobre los que debe ser divulgada, salvo bajo casos específicos).
-

Algunos ejemplos de información que no debe ser divulgada se presentan a continuación:

- calificaciones académicas,
- registros sobre consejerías,
- cursos tomados,
- servicios educativos recibidos,
- itinerarios,
- acciones disciplinarias,

- resultados de exámenes.

A continuación se presentan algunos ejemplos de información contractualmente protegida:

- número de tarjeta de crédito,
- número de identificación personal (PIN), utilizado para identificar usuarios en sistemas financieros.

Eliminación segura de Datos

La eliminación segura de datos se refiere al proceso de erradicar los datos almacenados en medios electrónicos (disco duro, cinta magnética, CD, DVD, *flash drive o pen drive*), de modo que estos datos ya no se puedan recuperar. Esto se logra de varias maneras: Utilizar un programa especializado de eliminación segura para escribir caracteres aleatorios en múltiples pases sobre los datos, sustituyendo el contenido del disco duro con una imagen que no contiene datos privados o destruyendo el disco duro. Medios electrónicos tales como cintas magnéticas, Cds, u otros medios con datos privados, deben también someterse a eliminación segura o destruirse totalmente, previo a disponer de ellos.

Equipo (*hardware*)

Término genérico utilizado para referirse a los artefactos y dispositivos físicos de tecnología, tales como computadoras, impresoras o equipos de comunicación.

Medio de almacenaje

Cualquier dispositivo que se utilice para contener o acceder datos o archivos a través de una computador. Puede ser fijo, como en el caso de los discos duros. También puede ser removible, como lo es un disquete, disco compacto (CD), disco de video digital (DVD), cartucho de cinta magnética o dispositivo *pen drive.*

Portal electrónico

Como regla general, el portal electrónico es una página estilo Web a través de la cual los usuarios de un recinto acceden en un punto común los servicios aplicativos a los que han sido autorizados. Estos servicios pueden incluir correo electrónico, calendario y agencia, enlaces a páginas de Internet y aplicaciones administrativas.

Programa (*software*)

Los programas son componentes lógicos de instrucciones que rigen la operación de los equipos tecnológicos (*hardware*), mediante funciones especializadas tales como el sistema operativo, las aplicaciones comerciales, sistemas de manejo de bases de datos o sistemas de correo electrónico.

Propiedad intelectual

El diccionario Merriam-Webster define la propiedad intelectual como propiedad (tal como un idea, un invento o un proceso), que se deriva del trabajo mental o intelectual. También se conoce como propiedad intelectual la aplicación, derecho o registro asociado con la propiedad (traducción suministrada).

Red de comunicación

Una red de computadoras conectadas mediante algún sistema de telecomunicaciones para transmitir información y compartir recursos. También se le conoce como red de telecomunicación.

Red local de comunicación

Red de comunicación que cubre un área geográfica relativamente pequeña, tal como el área cubierta por una oficina, recinto o grupo de edificios.

Resguardo (*backup)*

El resguardo es una copia que se hace de los archivos, datos y documentos electrónicos con la intención de poder recuperar cualquiera de ellos, en caso de que la versión con la que se trabaja se dañe o se pierda debido a algún caso fortuito. La copia se hace generalmente a un medio de almacenaje portátil. Se recomienda que esta copia se guarde fuera del área de trabajo –en un lugar seguro– por si el problema afecta el área de trabajo del usuario o administrador de tecnología. Como regla general, los archivos, datos y documentos electrónicos con los que trabajan los usuarios y administradores de tecnología se deben resguardar semanalmente. De esta manera, un usuario o administrador de tecnología puede recuperar su trabajo de una copia actualizada.

Tecnología informática o tecnología de la información

La tecnología informática abarca las disciplinas que estudian, diseñan, desarrollan, implantan, apoyan o mantienen aplicaciones de sistemas de información. Incluye los equipos, redes de comunicación, programas y datos que componen estas

aplicaciones. IT atiende la utilización de estos equipos y programas para recopilar, almacenar, convertir, proteger, procesar, transmitir, recuperar y comunicar la información de manera segura y exacta.

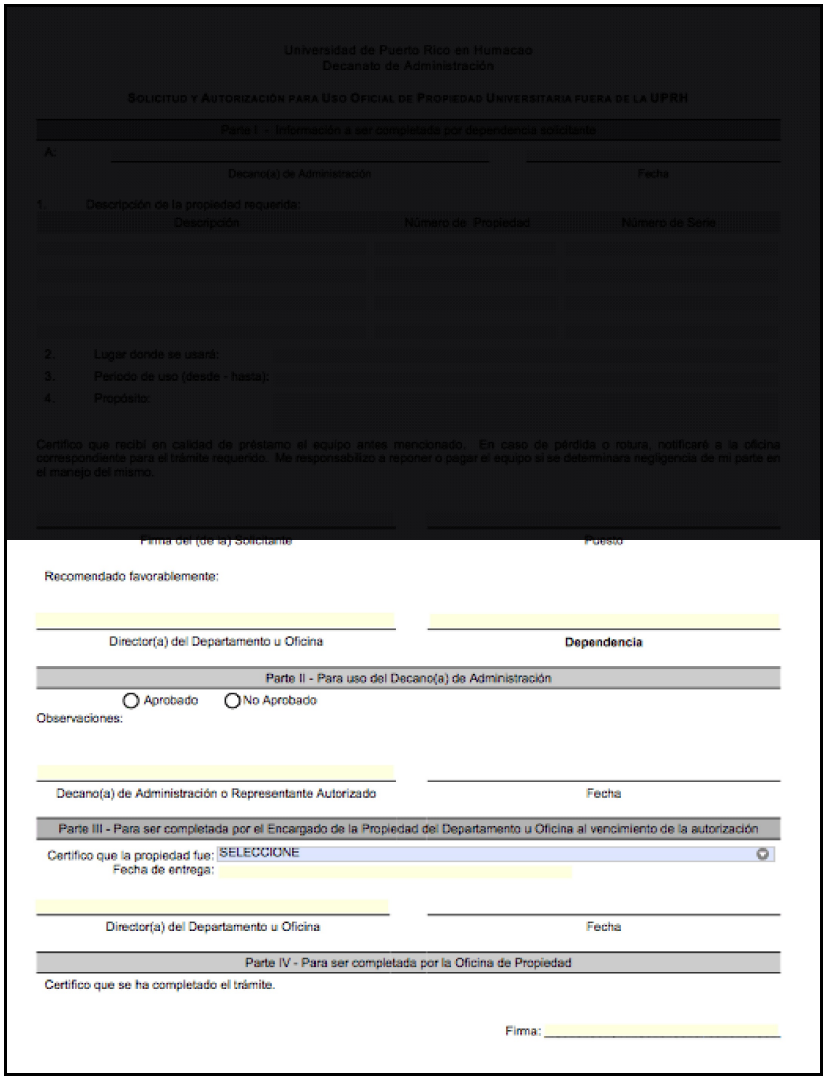
Vida útil

Concepto fiscal que se refiere al número de años que debe durar un activo –en este caso, el equipo tecnológico– siempre que se le dé una utilización normal y el cuidado mínimo que recomiende las especificaciones del suplidor y las prácticas generales para dicho tipo de equipo. Existe una relación directa entre el cuidado que se le brinde al equipo y la vida útil: a mayor cuidado, mayor será su vida útil (Merriam Webster Online, Merriam-Webster, Incoporated. 2007. Accedido el 28 de abril de 2008 de la página http://www.merram-webster.com/dictionary/ Intellectual%20Property

Historial de revisiones

Revisión	Fecha	Descripción
0	30-mar-2007	Procedimiento del SICC para administrar tecnología informática implantación inicial.
1	30-oct-2007	Revisión del procedimiento para expandir la sección de decomiso de equipo: • Se incluye párrafo describiendo la eliminación segura de los datos en el disco duro de la computadora, previo a disponer del equipo. • Se incorpora forma a utilizar prospectivamente para certificar dicha eliminación sujeta a la autorización previa por parte del encargado de la seguridad o el director oficial autorizado de la oficina custodia del equipo. Se incluye tabla de historial de revisión al final del procedimiento.
2	17-mar-2008	Revisión del procedimiento para incorporar una sección que describa el proceso para resguardar los datos almacenados en el computadora asignada al empleado.
3	23-jul-2008	• Subordinación de este procedimiento, mediante referencias, a la política institucional, Certificación Núm. 35, Serie 2007-2008 y a los Estándares Institucionales (p. 1). • En la sección de adquisición de tecnología informática se sustituyó la referencia a la Certificación Núm. 49, Serie por una referencia a la Certificación Núm. 35, Serie 2007-2008, que la derogó (p. 5). • Inclusión de sección sobre el recibo de donación de equipo tecnológico o programa de computación (p. 7). • Se incluyó una sub sección sobre el control de inventario bajo la sección de asignación de tecnología informática para fundamentar que el encargado de la propiedad debe estar al tanto de las transferencias permanentes del equipo para mantener actualizado su inventario (p. 12). • Se incluyó una sub sección sobre el movimiento de equipo de IT fuera de los predios de la oficina (p. 12). • Se incluyó una sub sección sobre cómo aplicar el uso personal aceptable permitido bajo la política IT: Uso personal aceptable del equipo (p. 15). • Se incluyó referencia a la aceptación de la Política y Estándares mediante la ventana que aparece al acceder a la red local de la UPRH y mediante la rotulación de las computadoras que no se conecten a la red (p. 23). • Se incluyó una sección para la aplicación de parchos de seguridad y actualización de antivirus incluyendo los pasos a seguir para recuperar de una infección (pp. 27-32). • Se incluyó una sección para protección física de computadoras, en especial de las computadoras portátiles para atender el cuidado que los usuarios deben brindarle al equipo tanto en el área de trabajo como fuera de los predios de la universidad (pp. 33-34). • Revisión del segundo párrafo de la sección de reparación del equipo IT para incluir el acudir al SICC para solicitar apoyo en la reparación de equipo averiado o en su evaluación para determinar que se sustituya por equipo nuevo (p. 41). • Se incluyó un relevo de responsabilidad a favor de la universidad, de ocurrir alguna pérdida de datos como resultado de la falta de resguardo por parte del usuario (p. 51). • Se incluyó un Glosario como Apéndice A (p. 53).
4	8-jun-2012	• Se eliminó el capitulo 5 (Solicitud para acceso remoto a la red de comunicación) • Se eliminó la sección *Reguardo buzón electrónico (e-Mail) de Outlook* en el capítulo 21. La UPRH no utiliza Outlook.

Apéndice B
Solicitud y Autorización para Uso Oficial de Propiedad Universitario fuera de la Universidad de la UPRH



Universidad de Puerto Rico en Humacao
Decanato de Administración

SOLICITUD Y AUTORIZACIÓN PARA USO OFICIAL DE PROPIEDAD UNIVERSITARIA FUERA DE LA UPRH

Parte I - Información a ser completada por dependencia solicitante

A: _____ _____
Decano(a) de Administración Fecha

1. Descripción de la propiedad requerida:

Descripción	Número de Propiedad	Número de Serie

2. Lugar donde se usará:
3. Periodo de uso (desde - hasta):
4. Propósito:

Certifico que recibí en calidad de préstamo el equipo antes mencionado. En caso de pérdida o rotura, notificaré a la oficina correspondiente para el trámite requerido. Me responsabilizo a reponer o pagar el equipo si se determinara negligencia de mi parte en el manejo del mismo.

_____ _____
Firma del (de la) Solicitante Puesto

Recomendado favorablemente:

_____ _____
Director(a) del Departamento u Oficina **Dependencia**

Parte II - Para uso del Decano(a) de Administración

◯ Aprobado ◯ No Aprobado

Observaciones:

_____ _____
Decano(a) de Administración o Representante Autorizado Fecha

Parte III - Para ser completada por el Encargado de la Propiedad del Departamento u Oficina al vencimiento de la autorización

Certifico que la propiedad fue: SELECCIONE
Fecha de entrega:

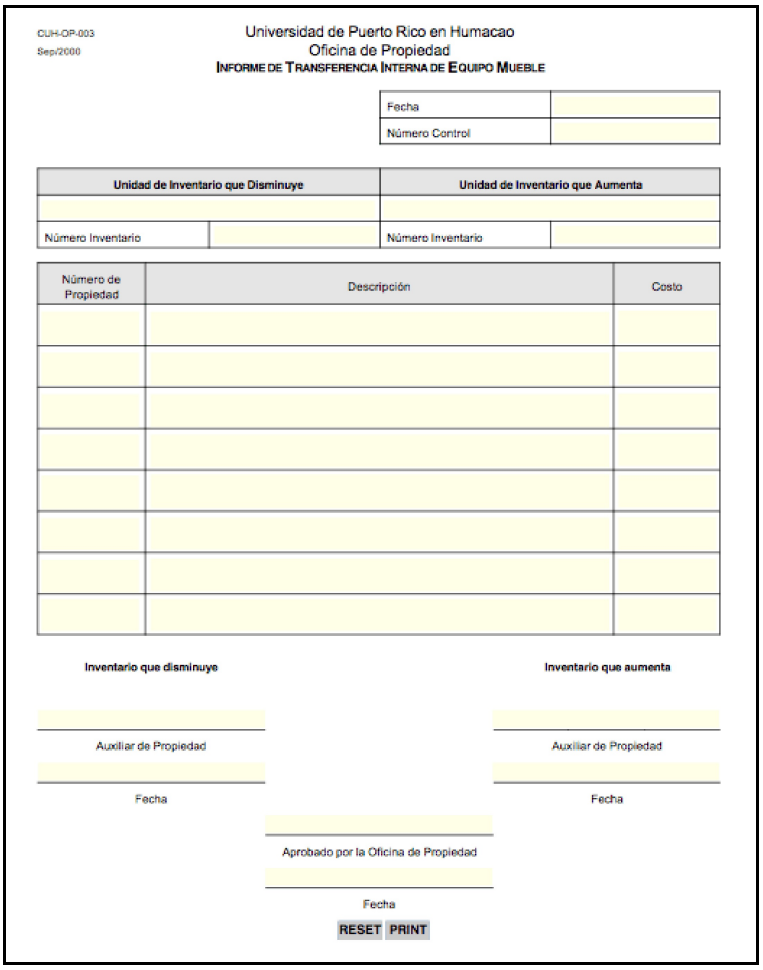
_____ _____
Director(a) del Departamento u Oficina Fecha

Parte IV - Para ser completada por la Oficina de Propiedad

Certifico que se ha completado el trámite.

Firma: _____

Apéndice C
Informe de Transferencia Interna de Equipo Mueble



CUH-OP-003
Sep/2000

Universidad de Puerto Rico en Humacao
Oficina de Propiedad
INFORME DE TRANSFERENCIA INTERNA DE EQUIPO MUEBLE

Fecha	
Número Control	

Unidad de Inventario que Disminuye		Unidad de Inventario que Aumenta	
Número Inventario		Número Inventario	

Número de Propiedad	Descripción	Costo

Inventario que disminuye

Auxiliar de Propiedad

Fecha

Inventario que aumenta

Auxiliar de Propiedad

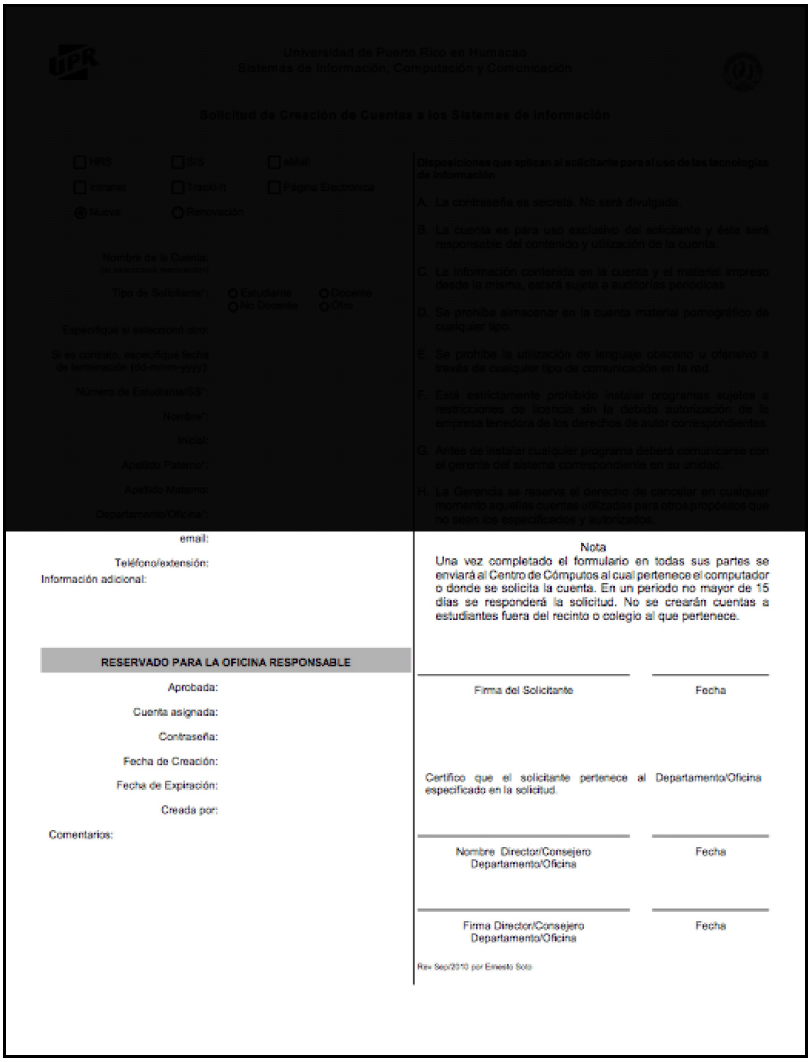
Fecha

Aprobado por la Oficina de Propiedad

Fecha

RESET PRINT

Apéndice D
Solicitud de Creación de Cuentas a los Sistemas de Información



Universidad de Puerto Rico en Humacao
Sistemas de Información, Computación y Comunicación

Solicitud de Creación de Cuentas a los Sistemas de Información

☐ RIO ☐ SIA ☐ eMail
☐ Internet ☐ Tesoro II ☐ Página Electrónica
◉ Nueva ○ Renovación

Nombre de la Cuenta
(si solicitan renovación)

Tipo de Solicitante* ○ Estudiante ○ Docente ○ No Docente ○ Otro

Especifique si seleccionó otro

Si es contrato, especifique fecha de terminación (dd-mmm-yyyy)

Número de Estudiante/SS*

Nombre*

Inicial

Apellido Paterno*

Apellido Materno

Departamento/Oficina*

Disposiciones que aplican al solicitante para el uso de las tecnologías de información

A. La contraseña es secreta. No será divulgada.

B. La cuenta es para uso exclusivo del solicitante y éste será responsable del contenido y utilización de la cuenta.

C. La información contenida en la cuenta y el material impreso, desde la misma, estará sujeta a auditorías periódicas.

D. Se prohíbe almacenar en la cuenta material pornográfico de cualquier tipo.

E. Se prohíbe la utilización de lenguaje obsceno o amenazante a través de cualquier tipo de comunicación en la red.

F. Está estrictamente prohibido instalar programas sujetos a restricciones de licencia sin la debida autorización de la empresa tenedora de los derechos de autor correspondientes.

G. Antes de instalar cualquier programa deberá comunicarse con el gerente del sistema correspondiente en su unidad.

H. La Gerencia se reserva el derecho de cancelar en cualquier momento las cuentas utilizadas para otros propósitos que no sean los especificados y autorizados.

email:

Teléfono/extensión:

Información adicional:

RESERVADO PARA LA OFICINA RESPONSABLE

Aprobada:

Cuenta asignada:

Contraseña:

Fecha de Creación:

Fecha de Expiración:

Creada por:

Comentarios:

Nota

Una vez completado el formulario en todas sus partes se enviará al Centro de Cómputos al cual pertenece el computador o donde se solicita la cuenta. En un periodo no mayor de 15 días se responderá la solicitud. No se crearán cuentas a estudiantes fuera del recinto o colegio al que pertenece.

Firma del Solicitante Fecha

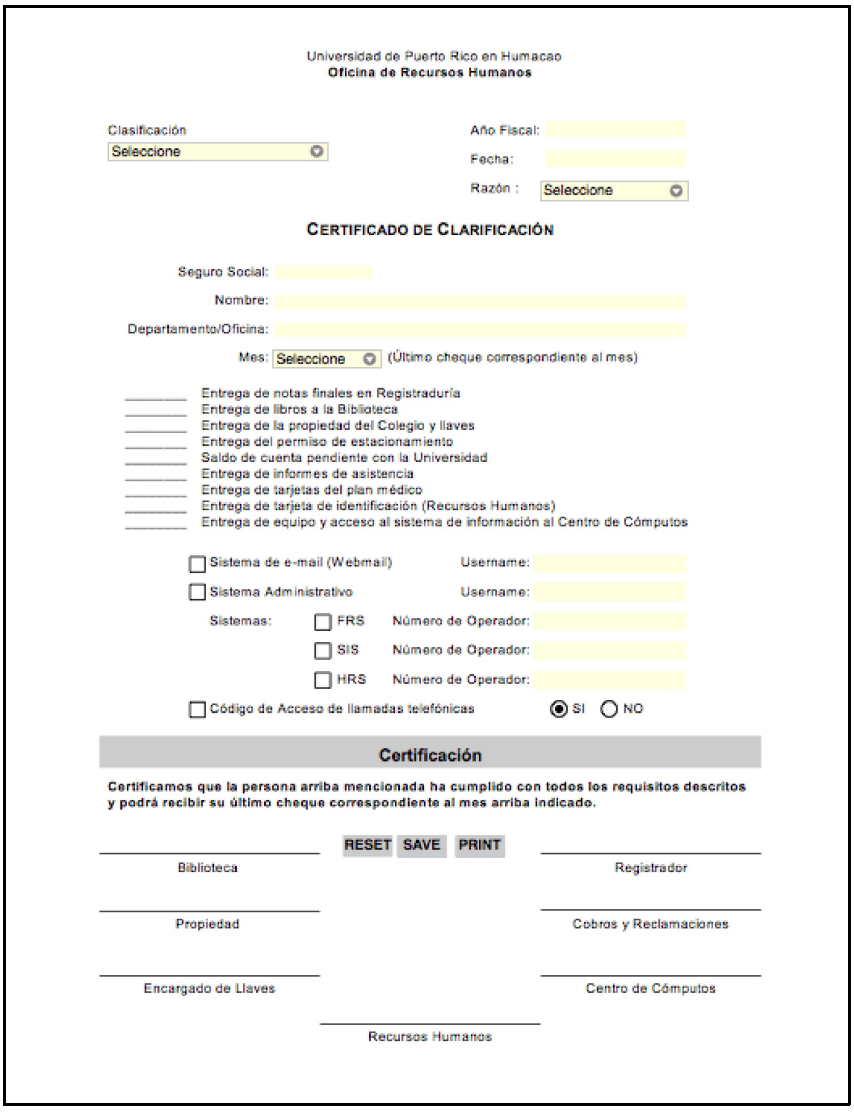
Certifico que el solicitante pertenece al Departamento/Oficina especificado en la solicitud.

Nombre Director/Consejero Departamento/Oficina Fecha

Firma Director/Consejero Departamento/Oficina Fecha

Rev Sept/2010 por Ernesto Sola

Apéndice E
Certificado de Relevo de Responsabilidades



Universidad de Puerto Rico en Humacao
Oficina de Recursos Humanos

Clasificación: Seleccione

Año Fiscal:

Fecha:

Razón : Seleccione

CERTIFICADO DE CLARIFICACIÓN

Seguro Social:

Nombre:

Departamento/Oficina:

Mes: Seleccione (Último cheque correspondiente al mes)

_____ Entrega de notas finales en Registraduría
_____ Entrega de libros a la Biblioteca
_____ Entrega de la propiedad del Colegio y llaves
_____ Entrega del permiso de estacionamiento
_____ Saldo de cuenta pendiente con la Universidad
_____ Entrega de informes de asistencia
_____ Entrega de tarjetas del plan médico
_____ Entrega de tarjeta de identificación (Recursos Humanos)
_____ Entrega de equipo y acceso al sistema de información al Centro de Cómputos

☐ Sistema de e-mail (Webmail) Username:

☐ Sistema Administrativo Username:

Sistemas: ☐ FRS Número de Operador:
☐ SIS Número de Operador:
☐ HRS Número de Operador:

☐ Código de Acceso de llamadas telefónicas ◉ SI ○ NO

Certificación

Certificamos que la persona arriba mencionada ha cumplido con todos los requisitos descritos y podrá recibir su último cheque correspondiente al mes arriba indicado.

RESET SAVE PRINT

_____ Biblioteca

_____ Registrador

_____ Propiedad

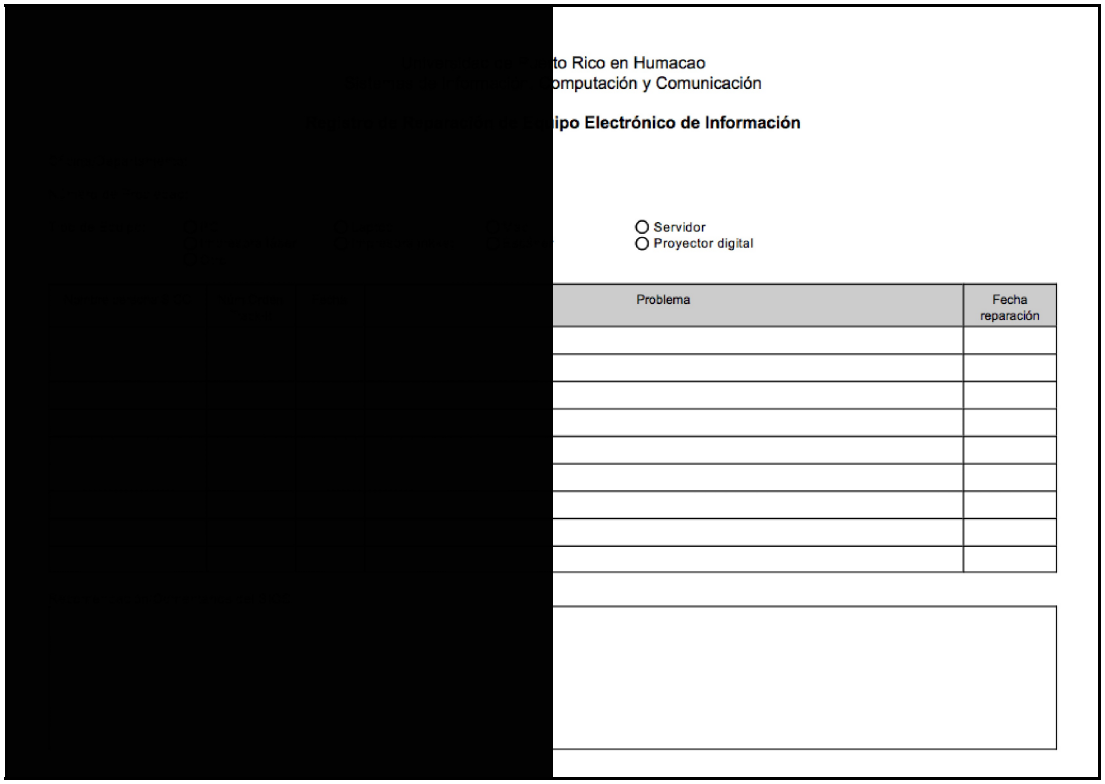
_____ Cobros y Reclamaciones

_____ Encargado de Llaves

_____ Centro de Cómputos

_____ Recursos Humanos

Apéndice F
Registro de Reparación de Equipo Electrónico de Información



to Rico en Humacao
omputación y Comunicación

ipo Electrónico de Información

○ Servidor
○ Proyector digital

Problema	Fecha reparación

Apéndice G
Certificado de Eliminación Segura de Datos

Universidad de Puerto Rico eh Humacao
Sistemas de Información, Computación y Comunicación

Certificación de Eliminación Segura de Datos

Descripción de Equipo			
Número(s) de Propiedad			
		Total de Equipos (unidades)	

Custodio en la Oficina:
Nombre del Solicitante:
Ubicación del Equipo:
Comentarios:

Encargado de la Propiedad, Director de la Oficina o Departamento o Oficial Autorizado

He solicitado al SICC que elimine de forma segura los datos contenidos en los equipos y computadoras identificados arriba. Reconozco que, al completar este procedimiento, los datos ya no estarán disponibles, por lo cual asumo la responsabilidad de resguardar previamente cualquier dato, archivo o documento que necesite retener para utilización futura.

Nombre/Firma Fecha/Extensión

Oficina de Sistemas de Información, Computación y Comunicación

Certifico que los discos duros de los equipos antes descritos han sido reformateados de modo que ha borrado toda y cualquier información que previamente haya contenido.

Nombre/Firma Fecha