Universidad de Puerto Rico
Recinto Universitario de Mayagüez
JUNTA ADMINISTRATIVA

CERTIFICACIÓN NÚMERO 14-15-215

La que suscribe, Secretaria de la Junta Administrativa del Recinto Universitario de Mayagüez, de la Universidad de Puerto Rico, **CERTIFICA** que en reunión ordinaria celebrada el jueves, 6 de noviembre de 2014, este organismo recibió el informe final del Comité Ad Hoc que atiende la encomienda para delinear el siguiente procedimiento y **APRUEBA** el mismo con efectividad inmediata:

POLÍTICA PARA LA ADMINISTRACIÓN DE SISTEMAS

La política forma parte de esta certificación.

Y para que así conste, expido y remito la presente certificación a las autoridades universitarias correspondientes, bajo el Sello del Recinto Universitario de Mayagüez, de la Universidad de Puerto Rico.

En Mayagüez, Puerto Rico, a los diez días del mes de noviembre del año dos mil catorce.

Judith Ramírez Valentín
Secretaria

nep

Anejos

RECINTO UNIVERSITARIO DE MAYAGUEZ
C.A.A.M.
UNIVERSIDAD DE PUERTO RICO

Política para la Administración de la Red y Sistemas

Propósito

Esta política establece las responsabilidades, guías y procedimientos para todo individuo que asume la responsabilidad de administrar u operar sistemas o equipos que componen la infraestructura de comunicaciones y de los sistemas de información del Recinto Universitario de Mayagüez.

Aplicabilidad

Un administrador de sistema o de red se considera un individuo que realiza trabajos de administración o provee apoyo técnico a sistemas, equipos u otros elementos que forman parte de la infraestructura de comunicaciones u otros sistemas que a su vez son utilizados por otros individuos, equipos o servicios.

Un *webmaster* será considerado un administrador de sistema para propósito de la aplicabilidad de esta política.

Un administrador de sistema puede emplear estudiantes para apoyar sus trabajos en cuyo caso el estudiante es considerado un administrador y está cubierto por esta política.

Un estudiante no puede asumir trabajos de administración de sistemas si no está bajo la supervisión de un empleado técnico cualificado.

Bases Legales

El acceso y uso de recursos electrónicos está gobernado por la Política Institucional y Procedimiento Para el Uso Ético Legal de las Tecnologías de Información de la Universidad de Puerto Rico, Certificación Número 072, 1999-2000, de la Junta de Síndicos y la Política Computacional y de Comunicaciones del Recinto Universitario de Mayagüez, Certificación Número 02-03-268 de la Junta Administrativa.

CALEA (*Communications Assistance for Law Enforcement Act*) establece requerimientos para la operación de infraestructura de comunicaciones. En cumplimiento con esta ley la operación de la red de comunicaciones del Recinto debe ser tal, que la misma constituya una red privada según la ley.

La Sección 18 del U.S.C, Capítulo 119, "*WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS*" requiere que la institución asista a agencias del orden público con interceptaciones legales.

La Ley Número 151 (Ley de Gobierno Electrónico) de 22 de junio de 2004, establece que la Oficina de Gerencia y Presupuesto (OGP) tendrá la facultad para instrumentar, establecer y emitir la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales con el objetivo primordial de lograr la interconexión de los organismos para facilitar y agilizar los servicios al Pueblo. La OGP publica procedimientos y requerimientos en las siguientes cartas circulares: TIG-011 Mejores Prácticas de Infraestructura Tecnológica, TIG-003 Seguridad de los Sistemas de Información, entre otras. El cumplimiento de estas políticas y circulares es auditado por la Oficina de Auditores Internos de la Junta de Gobierno de la Universidad de Puerto Rico y la Oficina del Contralor del Estado Libre Asociado de Puerto Rico.

Responsabilidades de un Administrador

El administrador de un equipo o recurso del Recinto es responsable de conocer y cumplir con las políticas institucionales y leyes aplicables en el contexto de su empleo.

El administrador de un equipo o recurso hará un esfuerzo legítimo para mantenerse familiarizado con los cambios asociados a la seguridad de sus equipos y sistemas, en particular cambios de tecnología, vulnerabilidades y sus implicaciones.

El Centro de Tecnologías de Información (CTI) establecerá procedimientos para la administración de sistemas. Una dependencia del Recinto podrá establecer sus procedimientos para la administración de sistemas siempre y cuando los mismos cumplan con los requerimientos establecidos en el procedimiento publicado por CTI y esta política. Todo administrador será responsable de cumplir con estos procedimientos.

Se espera que un administrador coopere de forma diligente con el personal de IT y CTI en la resolución de cualquier incidente u otros asuntos técnicos y administrativos.

El administrador de un equipo o recurso del Recinto deberá participar de reuniones y adiestramientos según requerido por el Centro de Tecnologías de Información del Recinto.

El administrador de un equipo o recurso del Recinto tomará precauciones para prevenir el hurto, vandalismo o daño del equipo/propiedad o data.

El administrador de un equipo o recurso del Recinto es responsable de salvaguardar la seguridad de la información y equipos. Deberá tomar las precauciones requeridas para mantener la confidencialidad de la información transmitida o almacenada en la red, equipos o sistemas.

El uso o administración de un equipo o sistema puede implicar el acceso del administrador a información sensitiva o protegida por ley. En cuyo caso el administrador está obligado a acceder dicha información solamente según requerido por sus tareas. El administrador mantendrá dicha información protegida del acceso por terceros. El administrador mantendrá la confidencialidad de cualquier información o dato al cual tuvo acceso.

El administrador NO utilizará sus privilegios en un sistema o equipo para acceder información o datos de terceros fuera de lo requerido para completar una tarea o trabajo en particular o fuera del alcance de sus responsabilidades.

Un administrador podrá acceder información o datos de carácter confidencial almacenados en equipos o servicios de la Institución (incluyendo emails) de ser requerido por un agente autorizado de la Institución en caso de surgir una situación de riesgo inmediato a la salud o seguridad de individuos o de la propiedad. Todo pedido de esta índole será tramitado por una solicitud formal escrita o por medio electrónico que pueda ser mantenida como evidencia. El administrador documentará dicha solicitud incluyendo información solicitada, qué se accedió y a quién se le entregó dicha información. Si el administrador tiene dudas sobre la naturaleza del pedido, éste deberá consultar a la Oficina del Asesor(a) Legal de Rectoría.

A un administrador se le podrá requerir acceder información o datos de carácter confidencial almacenados en equipos o servicios de la institución (incluyendo emails) para cumplir con: solicitudes legales, procesos legales, órdenes de agencias de ley, auditorías o investigaciones internas tramitadas por un asesor legal de la institución.

A un administrador se le podrá requerir acceder información o datos de carácter confidencial almacenados en equipos o servicios de la institución (incluyendo emails) para poder almacenar o remover datos, archivos, mensajes y otros archivos de computadoras como resultado de la separación de un empleado o estudiante de la Institución.

El administrador NO utilizará sus privilegios en un sistema o equipo para evadir un procedimiento o control de seguridad existente. El administrador de sistema utilizará un acceso o cuenta privilegiada (ej.: "root", "administrator") estrictamente cuando la tarea así lo requiera.

El administrador informará a su supervisor inmediato, al administrador de su unidad, y de ser requerido a CTI de cualquier incidente donde un equipo o sistema ha sido comprometido o donde la integridad de la red se ha comprometido, incluyendo pero no se limita a:

- Notificaciones de entidades y/o personas externas sobre cualquier incidente, incluyendo violaciones de derecho de autor o propiedad intelectual.
- Pérdida o robo de data, incluyendo eventos donde se sospecha de una pérdida o potencial robo de datos.
- El uso inapropiado de equipos o sistemas o el acceso indebido a información.
- Cualquier violación de política institucional o leyes.

El administrador trabajará de forma diligente para completar los requerimientos de información y procedimientos en cumplimiento con los requisitos de los Planes de Contingencia y Continuidad de Negocios de la Institución. El administrador mantendrá actualizada cualquier información pertinente requerida por estos planes.

Manejo de aplicaciones y servicios en sistemas bajo la responsabilidad de un administrador

El administrador debe asegurar que el uso de aplicaciones (software) u otros servicios cumplen con los términos de licencia del manufacturero o proveedor de un servicio.

El administrador mantendrá documentación y registros apropiados para evidenciar el cumplimiento con los términos de licencia.

La documentación debe incluir:

- Información de números de serie (llaves), dispositivos, credenciales u otros mecanismos de control de uso de la aplicación o servicio.
- Información de versión, nombre u otros detalles que permitan identificar la aplicación.
- Información del equipo donde es instalado o utilizado.

- Información relevante a la compra o adquisición de la aplicación o servicio cuando el mismo es adquirido con fondos institucionales o federales.

En circunstancias particulares las llaves, dispositivos, credenciales u otros mecanismos de control de uso de una aplicación o servicio tienen que ser mantenidas por un usuario u otro tercero que no es el administrador. En estos casos el administrador se limitará a documentar el uso y la compra de dicha aplicación o servicio. La dependencia u oficina tiene que poder evidenciar una persona que asume responsabilidad por su uso y el cumplimiento de los términos de licencia independientemente del mecanismo utilizado para adquirir el mismo.

El administrador no será responsable por aplicaciones instaladas por terceros. Sin embargo, será responsable de informar cualquier incumplimiento con licencias o violación de la política institucional, reglamentos o ley. El administrador será responsable de cotejar de forma aleatoria equipos y sistemas donde terceros pueden instalar aplicaciones para asegurar el cumplimiento con las licencias, políticas, reglamentos o ley. Este muestreo debe ocurrir por lo menos una vez al año. Los hallazgos serán informados a su supervisor.

Aplicaciones con licencias de uso de tipo "shareware", "donationware", "freemium" u otras similares son permitidas siempre y cuando:

- Su uso no requiere un compromiso de pago de parte de la Institución.
- El uso no requiere que su usuario acceda, participe o utilice un mecanismo o herramienta promocional que violente las políticas institucionales o implique un uso inapropiado de los recursos institucionales.
- La dependencia u oficina ha acordado previamente incurrir en los costos asociados al uso de la aplicación o servicio y el mismo puede ser pagado o adquirido utilizando los procedimientos de compra establecidos en la Universidad.
- La aplicación no se utiliza como parte de operaciones o procedimientos que se pueden ver afectados o interrumpidos cuando la misma no se pueda utilizar por requerir un pago u otra limitación.

Aplicaciones con licencias de uso de tipo "demoware", "trialware" u otras similares son permitidas estrictamente para propósitos de evaluación o cuando la dependencia u oficina tiene una intención legítima de comprar o adquirir la misma. La aplicación no se utilizará como parte de operaciones o procedimientos que se pueden ver afectados o interrumpidos cuando el periodo de prueba culmine.

Aplicaciones con licencias de uso de tipo "opensource", "communitysource" u otras similares son permitidas. No obstante el administrador tiene que evaluar si la licencia de la aplicación establece requisitos de uso, distribución u otros que sean incompatibles con el uso del mismo en la institución, requerimientos o trabajos que impliquen propiedad intelectual de la Universidad o violenten políticas institucionales o leyes.

Administración de un sistema o equipo

Los equipos y sistemas serán configurados y manejados para reducir o eliminar el riesgo de daño a la propiedad, acceso o uso indebido de datos institucionales o el uso en violación de las Políticas de Uso Ético Legal de las Tecnologías de Información de la Universidad de Puerto Rico, Certificación Número 072, 1999-2000 de la Junta de Síndicos y la Política Computacional y de Comunicaciones del Recinto Universitario de Mayagüez, Certificación Número 02-03-268 de la Junta Administrativa del RUM.

Controles y procedimientos utilizados en la administración de sistemas y equipos serán de un nivel apropiado para garantizar el cumplimiento de ley, reglamento y otros requerimientos sin crear obstáculos no justificados que puedan afectar las operaciones o servicios ofrecidos.

El CTI establecerá requerimientos mínimos y procedimientos para la administración de sistemas y equipos. Las dependencias podrán establecer procedimientos para el manejo de sistemas y equipos siempre y cuando los mismos cumplan con los requisitos mínimos establecidos.

Los procedimientos para administrar un equipo o sistema serán determinados en función del nivel de riesgo, seguridad y confidencialidad asociada al mismo.

Los equipos y sistemas serán evaluados para categorizar el nivel de riesgo y seguridad utilizando como referencia la metodología establecida en "Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199)"Y "Security Self_Assessment Guide for Information Technology Systems (NIST SP26)".

Esta categorización será utilizada en el desarrollo de procedimientos para los equipos y como parte de los Planes de Contingencia y Continuidad de Negocios del Recinto.

Todo procedimiento para la administración de sistemas y equipos tendrá que incorporar procedimientos para:

- La asignación de accesos y contraseñas a un sistema o equipo.
- Cambio de accesos y contraseñas.
- Mecanismos para validar accesos otorgados a un sistema o equipo con frecuencia.
- Revocar accesos de personas una vez no se requiera el mismo o culmine
- Mecanismos de resguardos cónsonos con el riesgo asociado al uso de un sistema o equipo o su data.
- Cambios de configuración del sistema o equipo.
- Instalación de aplicaciones en el sistema o equipo.
- Disposición o transferencia del sistema o equipo.

El administrador mantendrá documentación adecuada y actualizada de los sistemas y equipos que incluya:

- Información para identificar la propiedad y equipos, incluyendo número de propiedad, manufacturero, modelo y número de serie de los equipos.
- Sistemas operativos y aplicaciones, incluyendo información relevante a la adquisición y licencias.
- IP y "MAC Address" de todos los interfaces en los sistemas.
- La localización física del equipo o sistema.
- Información pertinente al uso, incluyendo información de usuarios.
- Descripción de los servicios y uso (web server, etc.).

La documentación de equipos y sistemas debe proveer detalles de configuraciones, dependencias y operación de los sistemas tal que los mismos puedan ser operados en ausencia del administrador o restablecidos en caso de una contingencia.

El administrador mantendrá copias de credenciales, contraseñas u otra información pertinente al acceso de un equipo, sistema o servicio en un lugar seguro para ser utilizados en su ausencia y así garantizar la continuidad de los servicios u operaciones. La unidad debe mantener un protocolo para el uso de estas credenciales. Dicho protocolo debe evidenciar su acceso y uso. En ausencia de un protocolo se utilizará el siguiente procedimiento:

- El administrador del sistema deberá escribir la información de cómo acceder el sistema o servicio, y la contraseña en un sobre sellado y debidamente rotulado, incluyendo la fecha.
- Este sobre sellado será entregado a un custodio de dicha información nombrado por el director del Departamento.
- En el caso de que se necesite tener acceso al equipo, servidor o el servicio electrónico cuando el administrador no esté disponible, se procederá a buscar el sobre sellado en custodia de la persona encargada, con la debida autorización del director del Departamento.
- Se documentará la fecha, hora y razón por la cual fue necesario tener acceso a dicha información y se mantendrá un registro de esta actividad, el cual permanecerá en custodia con el resto de los sobres.
- El sobre abierto con la información permanecerá en posesión del custodio.
- El administrador deberá cambiar la contraseña tan pronto sea posible y deberá escribirla en un sobre sellado para ser entregadas al custodio nuevamente, y destruir el sobre abierto.

El administrador será responsable de los aspectos requeridos para mantener la integridad de los sistemas y equipos. Esto incluye:

- Actualizaciones periódicas de los sistemas y equipos.
- Instalación, configuración y mantenimiento apropiado de antivirus u otra aplicación según aplique.
- Configuración apropiada para mitigar riesgos de seguridad, por ejemplo: cambios de contraseñas iniciales del manufacturero, cerrar puertos y servicios, entre otros.

Todo equipo, servidor o sistema de información que requiera control de acceso administrativo debe tener activada una contraseña segura para su administración. Estas contraseñas deben ser diferentes a las que se utilizan para acceder a los sistemas como usuarios regulares y diferentes entre sistemas o servicios. La contraseña sólo debe ser conocida por el administrador o usuario autorizado para la administración del equipo, el servidor o el servicio electrónico.

El administrador llevará a cabo resguardos regulares de los sistemas y equipos que así lo ameriten según el nivel de riesgo asociado al equipo. Los resguardos serán almacenados en un lugar seguro.

Cuando un equipo es removido, decomisado o movido a una nueva localidad, el administrador hará las gestiones pertinentes para: asegurar que el registro de la propiedad es debidamente actualizado, que los datos institucionales son removidos de equipos de acuerdo a los procedimientos establecidos para la disposición de información sensitiva y equipos de la institución.

Manejo de incidentes y procesos de ley

Para propósito de esta política se considera un incidente los siguientes:

- El uso inapropiado de un recurso, equipo o servicio, o evento inusual.
- La violación de política institucional, reglamento o ley.
- Intentos (ejecutado o con potencial de ocurrir) o eventos que impliquen una posible violación de la política institucional, reglamento o ley, en particular aquellos que implican daños a la propiedad o recursos institucionales.

El CTI será responsable de establecer y publicar requerimientos y procedimientos mínimos para el manejo de incidentes.

Todo administrador será responsable de documentar cualquier incidente según definidos en este documento. El administrador informará a su supervisor o director de su unidad de dichos incidentes.

En incidentes que impliquen violaciones de ley, reglamento u otros se debe consultar con CTI los pasos a seguir para atender el incidente.

En incidentes de acceso indebido a información sensitiva o protegida por ley (incluyendo "Personally Identifiable Information") (data breach) ya sea que ocurrió o con potencial de ocurrir o con algún grado de incertidumbre, el administrador debe notificar a CTI de inmediato una vez el acceso al equipo o sistema fue removido. Si la información comprometida incluye "Personally Identifiable Information", el incidente será reportado a la Oficina del Rector para asesoría legal.

Solicitudes de información, datos, accesos u otras por medio de "subpoenas", agencia de ley u otra serán enviadas a la Oficina del Asesor Legal de la Oficina del Rector para su evaluación y trámite. Instrucciones adicionales de cómo proceder serán provistas por un asesor legal de la institución.

Según requerido, el administrador atenderá solicitudes de información o datos por parte de la Oficina del Asesor Legal de la Oficina del Rector como parte de

investigaciones o procesos legales. De ser requerido, el administrador podrá seguir procedimientos distintos a los establecidos en esta política para atender estos pedidos. El administrador mantendrá documentación de las acciones tomadas y datos o información suministrada a la Oficina del Asesor Legal. Los pedidos se trabajarán con el grado de confidencialidad requerida.

Registro de Equipos y Servidores

El Centro de Tecnologías de Información (CTI) mantendrá un registro de equipos y servidores que comprenden la infraestructura de comunicaciones del Recinto, proveen servicios a la institución, o equipos que son identificados con un carácter operacional importante.

Equipos y servidores que cumplan con cualquiera de los siguientes requisitos tendrán que ser registrados para operar en la red del Recinto:

- Un servidor o equipo que controle o provea información, configuración u otro servicio requerido para acceder la red (ej.: *DNS, proxy, DHCP, firewall, NAT, authentication services,* etc). Un servidor o equipo que controle o provea información, configuración u otro servicio requerido para operar una serie de computadoras. (ej.: *MS Domain Controller, MS Active Directory, authentication services (kerberos),* etc).
- Un servidor que manipule o filtre tráfico de la red (ej.: *proxy, load balancer, NAT, firewall, packet shapers,* etc.).
- Un servidor o equipo que recibe tráfico "inbound" a través del *firewall* institucional u otro *firewall* administrado por CTI.
- Un servidor o equipo que provee servicios a un segmento de la comunidad universitaria cuya interrupción o fallo puede afectar adversamente los servicios ofrecidos.

CTI establecerá el procedimiento para el registro de equipos y sistemas. Los administradores de sistemas o redes serán responsables del registro de equipos y servidores y de mantener la información actualizada.

Esta política podrá ser revisada y actualizada periódicamente para responder a cambios en leyes, políticas o cambios tecnológicos.