JUNTA DE SÍNDICOS
UNIVERSIDAD DE PUERTO RICO

14 de diciembre de 2011

Carta Circular 12-02

A la Gerencia de las Unidades del Sistema Universitario

Mejores Prácticas en el Establecimiento de Controles Físicos en el Diseño y Construcción de un Centro de Cómputos

Con el propósito de promover los controles internos adecuados en las facilidades de tecnologías de información, como por ejemplo los Centros de Cómputos, a continuación presentamos las prácticas a considerar en el diseño y construcción de éstas para minimizar los riesgos en el área de Seguridad Física.

Durante el diseño estructural de las facilidades de tecnología de información, se deben proveer los controles físicos necesarios considerando:

- La distribución de cada área de trabajo de modo que se garantice el debido control de acceso. Esto, basado en la segregación de funciones entre el personal, la ubicación de los equipos y en la protección de la información.
- La utilización de materiales adecuados en la construcción de la estructura para mitigar el riesgo de daños a la propiedad.
- La instalación de equipos de seguridad para la prevención y detección de amenazas en y alrededor del Centro.

Esto, a su vez, conlleva la implantación de medidas de seguridad para proteger los equipos, materiales y empleados en caso de peligros naturales o fallas humanas. Entre los puntos a evaluar para determinar si existe la seguridad física adecuada están:

- Techo acústico que retarde la propagación de fuego.
- Paredes que circundan el cuarto de máquinas, biblioteca y cuarto de telecomunicaciones deben cerrar contra el techo estructural del edificio y estar construidas de material que retarden la propagación de incendios.
- Instalación y condición de detectores de humo y de agua.
- Falso piso del salón, en buen estado y libre de polvo.
- Ventanas y puertas de exterior (resistentes a escalamiento, huracanes, etc.) (evitar los recursos de informática no se vean desde el exterior) (no cristal).
- Paredes movibles (*fake wall*, cortinas, divisiones internas) no permitan acceso indebido.
- Puertas de entrada (puertas de acceso a la oficina y cuarto de máquinas con cerraduras electrónicas).
- Puertas de salida, emergencia (rotuladas y de fácil apertura hacia fuera (*panic bar*).

- Caja de interruptores automáticos (*main breaker*) del sistema está protegido (tapa y localización) y si los interruptores (*switches*) estén debidamente identificados.
- Unidades de aire (brinden la temperatura recomendada, y filtros limpios).
- Sistema de Supresión de Incendios y extintores (funcionamiento óptimo, inspeccionado y rotulados).
- Sistema de ventilación (funcionamiento óptimo y limpio).
- Conductos u otro medio de acceso al Centro sin protección.
- Amenazas en los alrededores, inclusive la planta superior e inferior (Ej. almacenes con productos propenso al fuego, laboratorios, tuberías de agua y gas, etc.)
- Generador alterno de energía (funcionamiento óptimo y protegido).
- Bóveda cuya clasificación sea adecuada para el almacenamiento de los medios magnéticos.
- Indicadores del control de temperatura y humedad.
- Ruta de desalojo rotulada.

Dichas prácticas se sostienen en las guías emitidas por entidades reconocidas en el campo de auditoría, en las cuales se detallan los controles requeridos. Entre éstas podemos mencionar:

- **ISACA**
  Los objetivos de control para las tecnologías de información **COBIT** mencionan este aspecto de la seguridad en el proceso DS12 Administración del ambiente físico[1].
  El **CISA Review Manual 2009**, Capítulos 5.7 *Auditing Environmental Controls* y 5.8 *Auditing Physical Access* indica que en la inspección de un Centro de Informática se debe verificar la existencia de las medidas de seguridad. Además, en el Inciso 3.6 de la Guía **G40** de ISACA *REVIEW OF SECURITY MANAGEMENT PRACTICES* se detallan los controles correspondientes a la seguridad física http://www.isaca.org/Knowledge-Center/Standards/Documents/G40-Rev-Sec-Mgmt-Prac-15Oct08.pdf .

- **Oficina de Gerencia y Presupuesto (OGP)**
  La Política Núm. TIG-003 de la Carta Circular Núm. 77-05 de la OGP indica en el Inciso J (Controles Físicos) que el acceso a las facilidades de sistemas de información deberá estar controlado para que solamente el personal autorizado pueda utilizarlas.
  http://www2.pr.gov/GobiernoAGobierno/ComunidadIT/Documentacion/Documents/Politicas%20y%20Guias/TIG-003.pdf

[1] DS12.1 Selección y diseño del centro de datos, DS12.2 Medidas de seguridad física, DS12.3 Acceso Físico, DS12.4 Protección contra factores ambientales y DS12.5 Administración de instalaciones físicas.

- **OFICINA DEL CONTRALOR DE PUERTO RICO (OCPR)**
  El folleto Informativo titulado "Las Mejores Prácticas para la Adquisición, Desarrollo, Utilización y Control de la Tecnología de Información" disponible en el siguiente enlace: http://www.ocpr.gov.pr/folletos_publicados/2006/LasMejoresPracticasAdquiTec/FolletoTecnologia20061.pdf

Para información adicional se puede comunicar con el Sr. Germán Cabrera, Gerente de Auditoría del área de Tecnología de Información al 787-758-3350 ext. 2404. Reafirmamos nuestro compromiso con la excelencia y para ello contamos con cada uno de ustedes.

Cordialmente,

Karla Aguirre Astacio
Directora Interina
Oficina de Auditoría Interna

jeg