BUENAS PRÁCTICAS EN ENTORNOS DE TECNOLOGÍAS DE INFORMACIÓN

Conocidas las amenazas que pueden afectar los activos de información, se deben aplicar una serie de buenas prácticas, medidas organizativas y de cumplimiento legal, como lo son:

GESTIÓN DE LOS ACTIVOS

Identifique los activos de la organización y defina las responsabilidades de protección sobre los mismos, así como la gestión correcta, acorde a una clasificación de seguridad.

SEGURIDAD DE LAS OPERACIONES

Cree actividades que aseguren el correcto funcionamiento de la infraestructura donde se realiza el tratamiento de la información, desde su instalación, puesta en marcha, actualización y protección ante software malicioso, respaldo para evitar la pérdida de datos, monitoreo y manejo de los incidentes.

Cree procedimientos y responsabilidades garantizando la continuidad de los servicios ante variaciones de personal.

Tenga Sistemas informáticos actualizados y realice una correcta gestión de parches de seguridad, tomando en cuenta:

- Realizar revisiones periódicas de los sitios oficiales de los proveedores de las aplicaciones, en especial la correcta programación automática de las notificaciones de seguridad.
- Verificar que los sistemas informáticos actualizados funcionen correctamente una vez aplicada la actualización.

Gestión y control de sistemas antivirus y cortafuego (firewall), además de realizar un análisis periódico de los equipos, para evitar infecciones, habilite funciones de protección que brinda el cortafuego de los sistemas operativos, por ejemplo: Windows Defender, IpTables o Firewall de MacOS.

Copias de seguridad, garantizando la recuperación de los datos (respaldos) y la continuidad de las operaciones. Incluya pruebas de restauración periódica para garantizar que se realizan adecuadamente, protegiendolas además de pérdidas, daños o accesos no autorizados.

Gestión del monitoreo en sistemas tecnológicos tales como equipos de UPS, plantas eléctricas, aires de precisión, prevención y detección de incendios, redes, infraestructura tecnológica como servidores, virtualización, entre otros; así como parámetros necesarios como lo son temperatura y humedad, para velar por el correcto funcionamiento de cada sistema. Brinde alertas ante cortes eléctricos, pérdidas de conexión o fallas, y que además permitan obtener informes periódicos de cada elemento para tener un registro y poder prever de manera proactiva cambios o sustituciones que pueden evitar fallos posteriores.

Gestión de incidentes. Los incidentes de seguridad son eventos de diferente naturaleza y a menudo con consecuencias negativas: fallos en los sistemas, acceso no autorizado a datos sensibles, ataques de denegación de servicio, entre otros. El área de informática tiene la responsabilidad de gestionar dichos incidentes de seguridad de una manera eficaz y eficiente. Se deben abordar una serie de actividades conjuntas, como lo son:

- Establecer sistemas de recolección de eventos que nos permita monitorear las alertas de seguridad.
- Analizar los incidentes de seguridad detectados, documentarlos y catalogarlos según su prioridad.
- Gestionar una adecuada solución de los incidentes.
- Estudiar los incidentes que se hayan producido, analizar sus causas y establecer medidas adicionales que protejan a los activos de nuevos incidentes de similar naturaleza.
- Poner en marcha un punto central de comunicación, tanto para recibir como para difundir información de incidentes de seguridad a las partes correspondientes de la solución y contingencia.
- Establecer procedimientos de respuesta ante incidentes para determinar los pasos que debemos de dar para una correcta gestión.

Recuperación y continuidad de servicios ante desastre. Consiste en una serie de pautas a ejecutar cuando ocurra una eventualidad. Permiten la recuperación de datos y equipos físicos, para que un negocio o institución pueda reanudar lo antes posible sus operaciones en caso de un desastre natural o causado por falla humana. Cada plan debe ser personalizado según las necesidades de las organización o negocio. Los elementos esenciales para un plan de recuperación ante desastres son:

- Conocimiento del negocio para poder definir el plan de recuperación
- Establecimiento de procesos vitales para la continuidad
- Selección de estrategias de recuperación
- Componentes esenciales de de la gestión y recuperación
- Copias de seguridad
- Criterios y procedimientos de prueba del plan de recuperación

central 2511-5000
ci5000@ucr.ac.cr
www.facebook.com/ciucr/
twitter.com/ciucr
UNIVERSIDAD DE COSTA RICA
CI
Centro de **Informática**