NORMAS TÉCNICAS DE SEGURIDAD

SEGURIDAD FÍSICA[1]

La seguridad física es uno de los aspectos más olvidados al diseñar un sistema informático. Consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención, ante situaciones de amenazas a la información confidencial. Los controles y mecanismos de seguridad de los sistemas informáticos así como los medios de acceso remoto, son implementados para proteger el hardware y medios de almacenamiento de datos.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el sistema. Las principales amenazas que se prevén son:

- Desastres naturales, incendios accidentales y cualquier variación producida por las condiciones ambientales.
- Amenazas ocasionadas por el hombre como robos o sabotajes.

AMBIENTE INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN

- La Universidad procura un ambiente integral de seguridad de información, resguardando la infraestructura física como el esquema básico de aseguramiento, tomando en cuenta aspectos de seguridad informática en la creación, constitución e implementación de seguridad física y viceversa.
- Al implementar el esquema integral de administración de seguridad de la información, proporciona protección a todos sus elementos como parte de un sistema.

ÁREAS SEGURAS Y CONTROLES DE ACCESO FÍSICO

- La Universidad establece determinar áreas resguardadas por un perímetro de seguridad

UCR

definido, provisto para regular el acceso a fin de que sólo el personal autorizado pueda ingresar en las instalaciones de procesamiento de la información crítica o sensible, propiedad de la Institución y/o en su custodia.

SEGURIDAD DE LOS BIENES FÍSICOS

- Cada persona que tenga un equipo de cómputo asignado, está en la obligación de conocer y cumplir el "REGLAMENTO PARA LA ADMINISTRACIÓN Y CONTROL DE LOS BIENES INSTITUCIONALES DE LA UNIVERSIDAD DE COSTA RICA", donde se establecen pautas para evitar daños y/o exposiciones al riesgo de los bienes institucionales, así como la interrupción de las actividades críticas de la Universidad.

SEGURIDAD DE BIENES FÍSICOS FUERA DE LA ORGANIZACIÓN

- Los recursos informáticos de la Universidad de Costa Rica, pueden ser utilizados fuera de la institución con autorización previa válidamente emitida por la autoridad correspondiente.
- El usuario debe observar las disposiciones establecidas para la protección de estos bienes, dentro y fuera de las instalaciones de la Universidad.

CONTROLES GENERALES CONTRA LA EXPOSICIÓN AL RIESGO DE ROBO Y/O HURTO DE LA INFORMACIÓN

- Todo el personal usuario de la Universidad de Costa Rica, es responsable de que la información confidencial, así como los bienes institucionales valiosos que le han sido asignados, estén adecuadamente protegidos en todo momento.

---

1 Directrices de Seguridad de la Información de la Universidad de Costa Rica, capítulo 10.

2 http://cu.ucr.ac.cr/normativ/bienes_institucionales.pdf

central 2511-5000
ci5000@ucr.ac.cr
www.facebook.com/ciucr/
twitter.com/ciucr
www.instagram.com/ci_ucr
CI
Centro de **Informática**