NORMAS TÉCNICAS DE SEGURIDAD

RESGUARDO Y PROTECCIÓN DE LA INFORMACIÓN[1]

La información constituye uno de los activos más importantes de cualquier organización, independientemente de su tamaño o actividad, es por esta razón que se deben implantar medidas preventivas y reactivas en la Universidad, destinadas a resguardar y proteger la confidencialidad, disponibilidad e integridad de la información.

El concepto de resguardo de información está vinculado a la protección de ciertos datos que transmiten información, ya sea física o digital. El resguardo se puede realizar de varias formas:

- Haciendo copias de seguridad ("backup") en otro medio físico como un disco duro, CD-ROM o un DVD-ROM.
- Subiendo archivos a un servicio de almacenamiento en Internet (almacenamiento en la nube) o repositorios determinados para este fin.
- Usando controles referentes a la propiedad de la información, tales como la elaboración de respaldos y la protección de registros.
- Protegiendo la información a través de la implementación de las medidas de seguridad basadas en hardware, software y recursos humanos, que estén complementadas con adecuadas normas de seguridad y que sean conocidas por el personal de la organización en todos sus niveles.

LA INFORMACIÓN SE RESGUARDA Y PROTEGE PORQUE ES PROPIEDAD DE LA UNIVERSIDAD:

La información que se almacene, transite, recopile, distribuya, reproduzca, procese y/o sea creada en los sistemas de información de la Universidad de Costa Rica es propiedad de esta Institución, salvo que el ordenamiento jurídico establezca lo contrario. Por lo tanto:

UCR

NORMAS TÉCNICAS DE SEGURIDAD

- La información institucional debe ser protegida por todos los actores de la Universidad, no debe transmitirse sin autorización a terceros bajo ninguna circunstancia.

- Para modificarla o eliminarla, se debe obtener la autorización formal de los jerarcas y titulares subordinados (direcciones)[2], responsables de la gestión del resguardo la información.

- Su custodia debe ser tratada con extrema cautela y ser conocida únicamente por quienes estén expresamente autorizados para tales efectos.

- Su clasificación debe ser sometida a requerimientos de confidencialidad, siempre y cuando no se determine lo contrario.

- La información que se determine como esencial, debe ser respaldada y resguardada en instalaciones seguras y controladas.

- Los jerarcas y titulares subordinados (direcciones), deben velar porque existan procedimientos que permitan recuperar la información y controles en sus áreas y unidades.

-Los controles deben ser evaluados periódicamente, para asegurar la continuidad de las operaciones en productos y servicios.

---

1 Directrices de Seguridad de la Información de la Universidad de Costa Rica, capítulo 8.

2 Ley de Control Interno.

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