

# GESTIÓN DE LA SEGURIDAD DE LAS OPERACIONES<sup>1</sup>

---

Se trata de garantizar la operación correcta y segura de las instalaciones de procesamiento de información, mediante la definición de procedimientos documentados de operación, la gestión de cambios, la gestión de la capacidad y la separación de los ambientes para desarrollo, prueba y operación.

## RESPONSABILIDADES Y PROCEDIMIENTOS

- Los procedimientos operacionales de la Universidad tienen que ser planeados, creados, aprobados y documentados, con base en los requerimientos específicos de cada proceso.
- Incluir aspectos tales como: control satisfactorio de cambios en las operaciones, segregación de funciones, separación de ambientes de desarrollo y producción, requisitos para la contratación de personas ajenas a la Institución para la administración de ambientes de procesamiento de información y cualquier otro que sea requerido.

## PLANIFICACIÓN DE LA CAPACIDAD Y APROBACIÓN DE LOS SISTEMAS DE INFORMACIÓN

- Los criterios de capacidad de los sistemas a implementar en la Universidad, así como los de aprobación de nuevos sistemas, actualizaciones, modificaciones, nuevas versiones y procedimientos de prueba, deben ser definidos y documentados.
- La aprobación de los sistemas, sus modificaciones o actualizaciones y de su paso al ambiente de producción, están sujetos a la comprobación de que los mismos cumplan con los requerimientos de seguridad de la información, aprobados por la Universidad.

## CONTROLES CONTRA INSTRUCCIONES MALICIOSAS

- La Universidad provee para todos sus equipos que así requieran, un software antivirus contra instrucciones maliciosas.
- El personal usuario al cual se le asigne un equipo, es responsable por velar por que la aplicación antivirus esté instalada y funcionando en su última versión.
- El uso de cualquier tipo de software en los equipos de la Institución debe contar con la aprobación de las autoridades competentes.

## ADMINISTRACIÓN DE LA RED

- La administración de las redes de la Universidad corresponde únicamente al personal que se encuentra debidamente calificado y capacitado con regularidad.
- Los accesos a los servicios asignados a cada persona, dependen de la relación que mantenga con la Universidad.

## ELIMINACIÓN DE MEDIOS DE ALMACENAMIENTO

- La eliminación de la información confidencial, crítica, sensible o de uso interno de la Universidad contenida en medios de almacenamiento, se lleva a cabo por la unidad responsable de dicha información. De igual manera, la eliminación de medios informáticos de almacenamiento, sólo se lleva a cabo por el personal autorizado de la Unidad de Bienes Institucionales.
- La Universidad nunca confiará a personas ajenas a la Institución la destrucción de medios informáticos de almacenamiento, sin autorización escrita emitida por la autoridad correspondiente.

## MANTENIMIENTO DE RECURSOS INFORMÁTICOS

- Únicamente quienes hayan sido designados al mantenimiento de recursos informáticos pueden implementar controles y procedimientos para mantener la integridad, disponibilidad y confiabilidad de los servicios de procesamiento de información.

---

1 Directrices de Seguridad de la Información de la Universidad de Costa Rica, capítulo 13.