| | | |
|---|---|---|
| | **UNIVERSIDAD PSICOLOGÍA INDUSTRIAL DOMINICANA UPID**<br><br>**POLITICAS DE SEGURIDAD OPERACIONAL PARA INSTALACION DE HARDWARE Y SOFTWARE** | |

| CÓDIGO | VERSIÓN | FECHA |
|---|---|---|
| | 1 | 2022 |

# POLÍTICA DE SEGURIDAD OPERACIONAL PARA LAINSTALACIÓN DE HARDWARE Y SOFTWARE

## Objetivo

Regular las actividades referidas a la instalación, operación y respaldo de Hardware y Software en las instalaciones propias o de terceros prestadores de servicio, para mitigar los riesgos asociados a la seguridad de los sistemas y la información de la universidad.

## Alcance

Esta Política se aplica en toda la Universidad UPID, sus edificios e instalaciones, a sus autoridades, directivos, docentes, funcionarios y terceros que de acuerdo a la normativa interna se consideran relacionados con la Universidad, siendo todos responsables del cumplimiento de esta Política.

## POLÍTICA

Se establecerán responsabilidades y procedimientos para la gestión y operación segura relacionada con las actividades referidas a la instalación, operación y respaldo de Hardware y Software

### Restricciones sobre la instalación de software o hardware

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo de la Universidad es responsabilidad de Soporte TI perteneciente a la Vicerrectoría de Tecnología, y por tanto esta Unidad es la única autorizada para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por la Universidad a través de esta Unidad.
- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios pueden ser realizados únicamente por personal de Soporte de TI.
- El Vicerrector de TI o en quien éste delegue la responsabilidad, definirá y actualizará, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizará el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

**<u>Los controles a definir deben considerar las siguientes acciones:</u>**

- Prohibir el uso de software no autorizado por la Universidad.
- Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las

medidas de protección a tomar.

- Instalar y actualizar periódicamente software de detección y reparación de virus, examinando computadores y medios informáticos, como medida precautoria y rutinaria.
- Mantener los sistemas operativos y aplicaciones actualizadas a la última versión disponible, siempre y cuando no afecten la compatibilidad de plataformas y/o operación de la universidad. Para evitar incidentes que afecten la seguridad de la información, asociados a esta actividad.
- Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- Concientizar al personal acerca del problema de los falsos virus o alertas infundadas y de cómo proceder frente a los mismos.

**Respaldo**

**Respaldo de la información**

La Vicerrectoría de TI y/o las empresas proveedoras de servicios externos relativos a esta materia deberá proporcionar los medios de respaldo adecuados para asegurar que toda la información esencial y software se puedan recuperar después de un desastre o falla. Esto deberá considerar los siguientes aspectos:

- Se deberá definir, el nivel necesario de respaldo de la información, de acuerdo con su criticidad y vigencia.
- Las copias de respaldo se deberán almacenar en un lugar apartado, a distancia suficiente como para escapar de cualquier daño por un desastre en el local principal.
- A la información de respaldo se le deberá dar el nivel de protección física y ambiental apropiado, consistente con los estándares aplicados en el local principal.
- Los medios de respaldo se deberán probar regularmente para asegurar que se pueda confiar en ellos para usarlos cuando sea requerido.
- Los procedimientos de restauración se deberán chequear y probar regularmente para asegurar que sean efectivos y que pueden ser completados dentro de tiempos determinados.
- En situaciones cuando la confidencialidad es de importancia, las copias de respaldo deberán ser protegidas por medio de una codificación.
- Para sistemas críticos, los procedimientos de respaldo deberán abarcar toda la información, aplicaciones y data de todos los sistemas, necesarios para recuperar el sistema completo en caso de un desastre.
- Se deberá contar con un procedimiento para eliminar permanentemente la información de los medios de almacenamiento antes de desecharlos.

**ROLES Y RESPONSABILIDADES**

**Vicerrectoría de TI**

- Definir controles de detección y prevención para la protección contra software malicioso y desarrollar procedimientos adecuados de concientización de usuarios en la materia.
- Definirá y actualizar la lista de software y aplicaciones autorizadas a ser instaladas en las

estaciones de trabajo de los usuarios.

- Realizar el control y verificación de cumplimiento del licenciamiento del software y aplicaciones instaladas en las estaciones de trabajo del personal de la Universidad.

**Coordinador TI**

- Autorizar la instalación de cualquier tipo de software o hardware en los equipos.

| ELABORADO POR: | REVISADO POR: | APROBADO POR: | FECHA |
|---|---|---|---|
| Lic. Rinaldo Suberví Martínez<br>Vicerrector de Tecnología | Nicole Winter<br>Vicerrectora de Postgrados y Proyectos | Lic. Ricardo Winter<br>Rector UPID | |