CICLO FORMATIVO DE GRADO MEDIO

SISTEMAS MICROINFORMÁTICOS Y REDES

# SEGURIDAD INFORMÁTICA

UT2 – Gestión de dispositivos de almacenamiento

# PRÁCTICA 1: POLÍTICAS DE ALMACENAMIENTO

|  |  |
| --- | --- |
| Resultado de aprendizaje evaluado  2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información. | |
| Criterio de Evaluación | Calificación |
| a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento. |  |

## Introducción

Para poder mantener de un modo seguro y eficaz todos estos sistemas de información es importante que la empresa especifique cuáles son las reglas, criterios y procedimientos que deben seguir todos los usuarios de los sistemas para:

* Que se garantice el acceso de los recursos de información por los usuarios o programas autorizados.
* Evitar la fuga de información.
* Evitar el deterioro de la información almacenada o que deba ser conservada.
* Evitar el uso de dispositivos no autorizados.
* Proveer métodos de recuperación de la información y la actividad en caso de fallos técnicos, accidentes o desastres.
* Garantizar que al terminar su vida útil los soportes son desechados correctamente (que se tratará en otra guía).
* Conocer cómo tratar las incidencias, las fugas de información y los desastres u otras contingencias.

Así, se identifican relacionadas con el almacenamiento las siguientes políticas necesarias en la empresa, para que sean conocidas por los propios usuarios y controladas por los responsables:

* Política de almacenamiento local en los equipos de trabajo.
* Política de almacenamiento en la red corporativa.
* Política sobre el uso de dispositivos externos.
* Política de almacenamiento en cloud.
* Política de copias de seguridad.

Otras políticas necesarias para la buena gestión de la información en la organización son:

* Política de conservación o archivo de documentos
* Política para el uso de dispositivos móviles personales o BYOD.

CICLO FORMATIVO DE GRADO MEDIO

SISTEMAS MICROINFORMÁTICOS Y REDES

## SEGURIDAD INFORMÁTICA

## Caso práctico

Como miembros del departamento de Informática del ICETEX, debemos conocer el Manual de políticas de seguridad de la información de dicho organismo.

Vamos a comprobar si realmente conoces su contenido. Para ello debes leer detenidamente todo el manual y responder a las siguientes preguntas:

1. Indica cuáles son las normas dirigidas a la dirección de tecnología, relativas al uso de los teléfonos móviles, relacionadas con la protección de la información almacenada en dichos dispositivos.

### 8.2.1. Normas para uso de dispositivos móviles

Normas dirigidas a: DIRECCION DE TECNOLOGIA

* La Dirección de Tecnología debe investigar y probar las opciones de protección de los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por el instituto.

* La Dirección de Tecnología debe establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por el ICETEX.

* La Dirección de Tecnología debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.

* La Dirección de Tecnología debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.

* La Dirección de Tecnología debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

* La Dirección de Tecnología debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales de ICETEX; dichas copias deben acogerse a la Política de Copias de Respaldo de la Información.

* La Dirección de Tecnología debe instalar un software de antivirus tanto en los dispositivos móviles institucionales. como en los personales que hagan uso de los servicios provistos por el instituto

* La Dirección de Tecnología debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

Normas dirigidas a: TODOS LOS USUARIOS

* Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

* Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

* Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

* Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.

* Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

* Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

* Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

1. ¿Qué departamento es el encargado de definir los niveles de clasificación de la información dentro de la organización?

El Comité de Seguridad de la Información debe recomendar los niveles de clasificación de la información propuestos por la Oficina de Riesgos y la guía de clasificación de la Información del ICETEX para que sean aprobados por la Junta Directiva.

1. ¿Se permite el uso de medios de almacenamiento personales dentro de la organización?

Los funcionarios y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica del ICETEX.

1. ¿Contempla la normativa de intercambio de información entre el instituto y terceras partes algún tipo de documento o acuerdo que deba ser firmado por ambas partes, donde se incluyan los compromisos adquiridos y las penalizaciones en caso de incumplimiento? Indica cuál.

## Plazo de entrega

Para completar las tareas incluidas en el caso práctico se ha estimado un tiempo de trabajo de 1 hora. La entrega deberá realizarse antes de la fecha del examen de la unidad. No se calificarán las prácticas que se entreguen fuera de plazo.

## Criterios de calificación

|  |  |  |
| --- | --- | --- |
| Criterios de calificación | Hecho | Calificación |
| Pregunta 1 |  |  |
| Pregunta 2 |  |  |
| Pregunta 3 |  |  |
| Pregunta 4 |  |  |
| Cada pregunta respondida correctamente se puntuará con 2,5 puntos. Las preguntas sin responder 0 puntos, y aquellas que no estén perfectamente respondidas obtendrán una puntuación intermedia (entre 0 y 2,5 puntos) | | |