ISO/IEC 27001:2013

SEGURIDAD DE LA INFORMACIÓN

Tribunal Electoral de la Provincia de Misiones

Mayo 2022 N° - 002/22

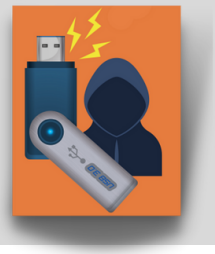
Medios Extraibles "USB"

Los medios de almacenamientos extraíbles (memorias USB, discos duros portátiles, tarjetas de memoria, etc), hoy en día lo podemos considerar como un elemento más de nuestro día a día, casi tan imprescindibles como disponer de una PC, notebook o teléfono móvil.

Debido a que nos permiten generar un entorno de transferencia de información mucho mas rápida y directa; pero a la vez son tan pequeños y discretos que requieren un nivel de atención y seguridad mayor.

Riesgos asociados.

- Robo de dispositivo.
- Perdida del dispositivo



- Perdida de información reservada /confidencial.

Riesgos de poseer dispositivo de almacenamiento infectado.

- Infección de la red corporativa.

- Infección y perdida de archivos confidenciales.
- Encriptación de información.

Prevención - Recomendaciones

- ***CONCIENTIZACIÓN DE LOS USUARIOS:*** *Generar material para exponer los riesgos asociados al uso de los dispositivos de almacenamiento, y recomendaciones sobre posibles controles a tener en cuenta.*

- ***EVITAR UTILIZAR UNIDADES DE ALMACENAMIENTO PERSONALES:*** *Dentro de la institución se debe utilizar únicamente medios de almacenamientos suministrados y configurados por la Secretaria de TIC.*
- ***MANTENER UN REGISTRO ACTUALIZADO DE LOS PRIVILEGIOS DE USUARIOS Y DISPOSITIVOS EXISTENTES EN LA ORGANIZACIÓN:*** *Dentro del TEPM la Secretaria de TIC posee un registro actualizado de los permisos otorgados a cada usuario.*

- ***RESGUARDAR LOS MEDIOS DE ALMACENAMIENTO EN LUGARES SEGUROS Y PROTEGIDOS:*** *Es indispensable que los medios de almacenamiento se encuentren resguardado del acceso fisico por parte de cualquier usuario no autorizado.*
- ***CIFRAR LA INFORMACIÓN ALMACENADA:*** *Utilizar herramientas que permitan encriptar la información contenida en los medios de almacenamiento extraíbles.*

- ***UTILIZAR ALTERNATIVAS DE ALMACENAMIENTO.***
  - Directorios compartidos.
  - Almacenamiento en la nube (cloud).
- ***CONFIGURAR MEDIDAS DE SEGURIDAD EN LOS PUERTOS USB.***
  - Autenticación (usuario y contraseña)
  - Bloqueo de dispositivos no autorizados
  - Deshabilitar puertos USB

- ***BORRADO DE LA INFORMACIÓN CONTENIDA DESPUÉS DE SU USO.***
  - Destrucción físico del dispositivo.
  - Formateo de la unidad.

- ***EVITAR CONECTAR CUALQUIER DISPOSITIVO DE ORIGEN DESCONOCIDO.***
  - Ante la mínima duda sea prudente y solicite soporte técnico a la Secretaria de TIC.