Programa de especialización en Ciberdefensa y Ciberseguridad Estratégica (PECCE)

PROTECCIÓN DE LA INFORMACIÓN

Protección de la información

Objetivo general

- Ser capaz de planificar, implementar y/o supervisar las medidas de protección de los sistema de información de una organización.

Objetivos específicos

- Conocer las buenas prácticas de seguridad en diversas áreas (credenciales y autenticación, gestión de datos e información, equipos).

Protección de la información

Contenido curricular

- Buenas prácticas de seguridad
  - ✓ Gestión de credenciales
  - ✓ Autenticación multi-factor
  - ✓ Copias de seguridad
  - ✓ Seguridad del Endpoint

Protección de la información

Contenido curricular

- Buenas prácticas de seguridad
  - ✓ Gestión de credenciales
  - ✓ Autenticación multi-fact
  - ✓ Copias de seguridad
  - ✓ Seguridad del Endpoint

Protección de la información

Copias de seguridad

Protección de la información

Protección de la información

Principios de la Seguridad de la Información

Confidencialidad: Sólo acceden quienes están autorizados.

Disponibilidad: Acceso cuando sea requerido.

Integridad: La información y su procesamiento son exactos y completos. Solo modificados por quienes están autorizados.

Protección de la información

Copias de seguridad

Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Son útiles ante:

- Desastres naturales.
- Daños físicos de los equipos o robos.
- Ataques informáticos.
- Eliminación accidental o intencional.

Protección de la información

Copias de seguridad

Consideraciones:

- Se debe definir junto a los principales steakholders de la información los datos que se deben respaldar.
- Estimar el volumen de datos a respaldar y realizar proyecciones de crecimiento.
- Definir dónde los usuarios deben guardar los datos a ser respaldados y los tipos de archivos que serán copiados..

Protección de la información

Copias de seguridad

Consideraciones:

- Establecer la manera de las efectuar las copias y establecer revisiones para confirmar exactitud de las copias.
- De acuerdo al volumen y criticidad establecer la frecuencia de las copias.
- Periódicamente probar restaurar los datos copiados a fin de detectar o descartar inconvenientes en la utilización de las copias de respaldo.

Protección de la información

Copias de seguridad

Consideraciones:

- Deben mantener las mismas medidas de seguridad que tenían los sistemas de información de origen.
- El acceso a las copias de respaldo está restringido mediante control físico, lógico, o cifrado de la Información.
- Establecer el lugar en el que se almacenarán las copias de respaldo.
- Las copias se deben guardar en sitios diferentes al lugar de origen.

Protección de la información

Copias de seguridad

Consideraciones:

- Se debe contar con procedimientos formales tanto para las copias como para las restauraciones de datos.
- Se debe establecer el plazo mínimo por el cual se guardará la información.
- Se deben monitorear periódicamente el volumen ocupado.

Protección de la información

Copias de seguridad

Inventariar Activos

Decidir qué, cómo y cuando copiar

Verificar exactitud de las copias

Probar las copias de respaldo

Proteger el acceso a las copias

Destruir las copias

Protección de la información

Copias de seguridad

Tipos de Backups

- **Full o Normal**: se hace un respaldo completo de todos archivos. Abarca el 100 % de la información, por lo que requiere de más tiempo en realizarse y ocupa más espacio.
- **Diferencial**: contiene los archivos que han cambiado desde la última vez que se hizo una copia Full. Incluye los archivos nuevos y los modificados. Su punto de referencia siempre es el último backup full.

Protección de la información

Copias de seguridad

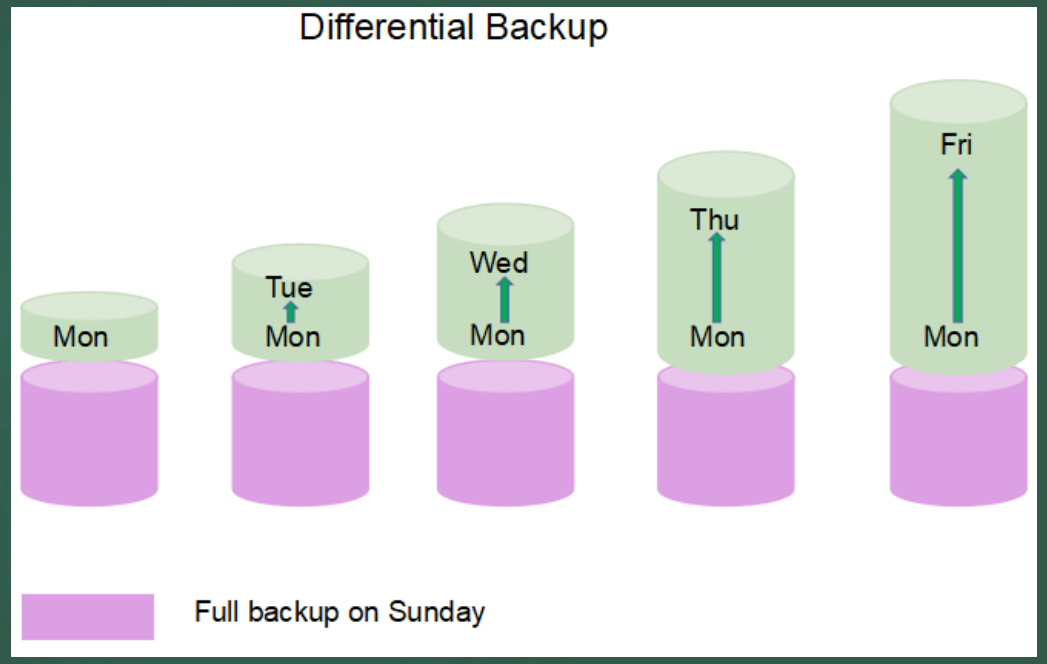
Tipos de Backups

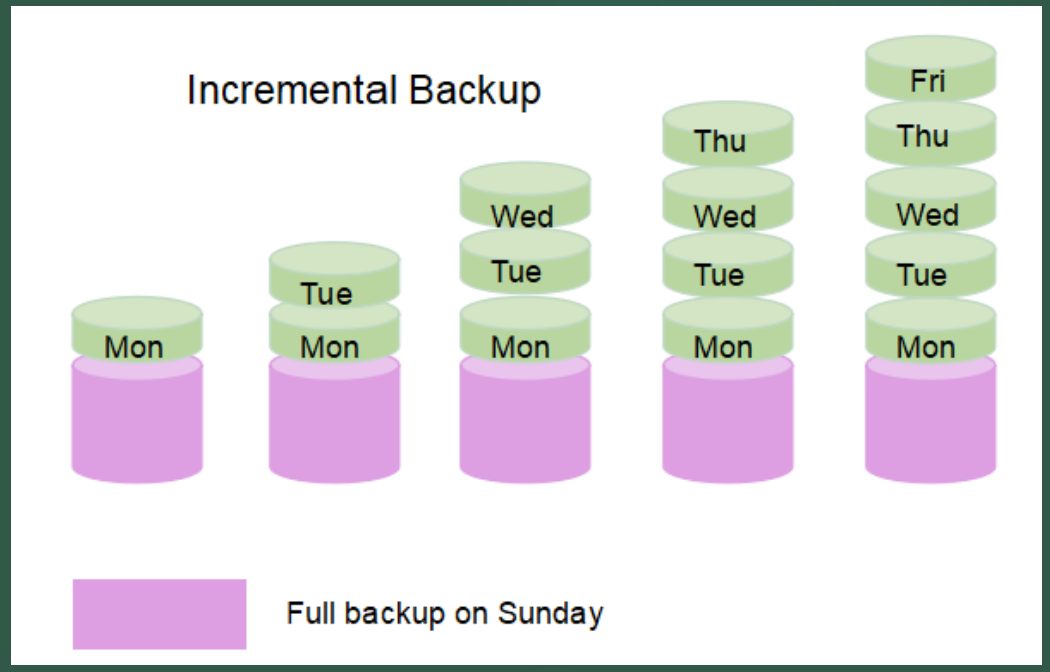
- **Incremental**: contiene los archivos que han cambiado desde la última vez que se hizo una copia full o desde la última vez que se hizo una backup incremental.

Protección de la información

Copias de seguridad

Tipos de Backups





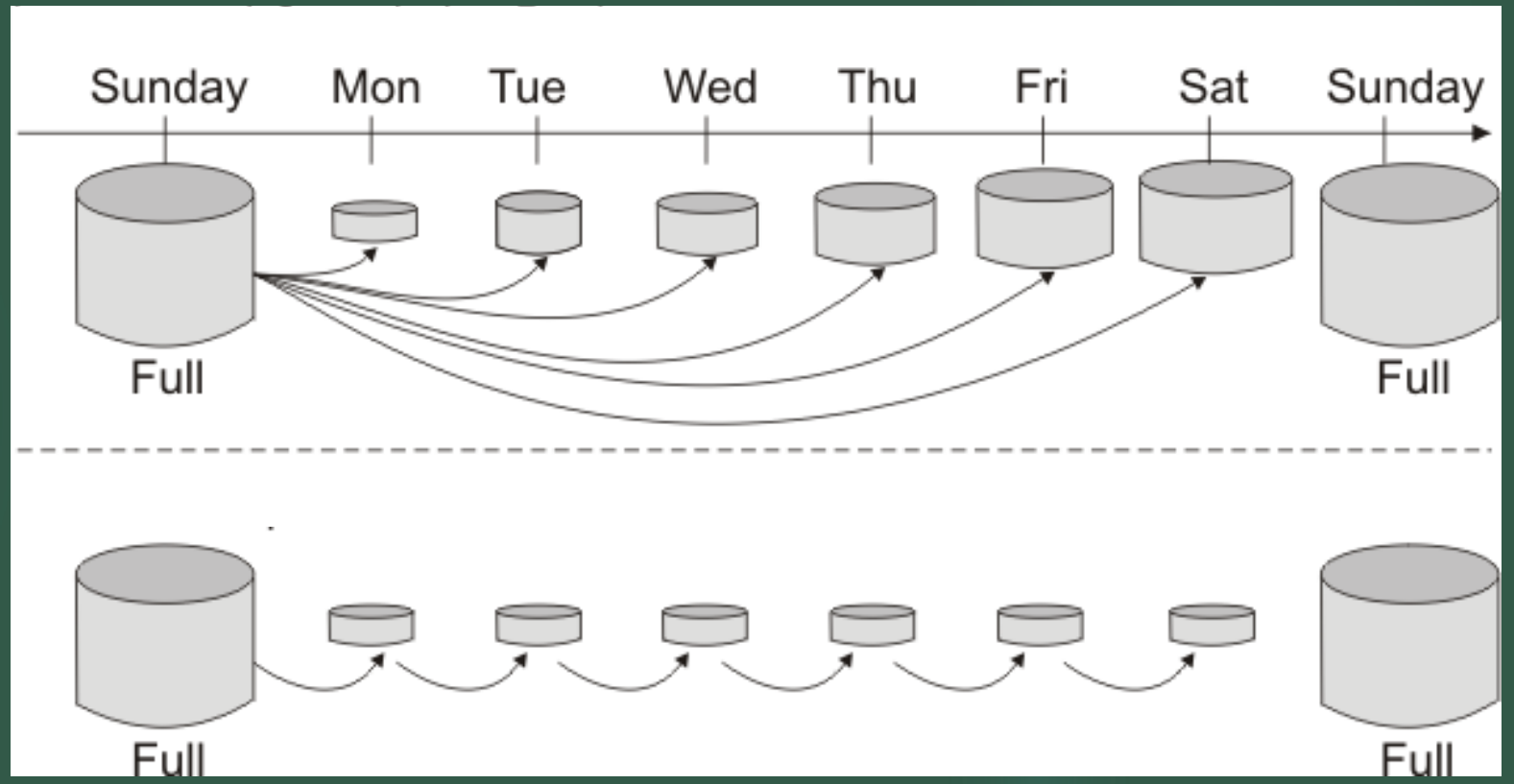
Protección de la información

Copias de seguridad

Tipos de Backups

Diferencial

Incremental



Protección de la información

Copias de seguridad

Herramientas corporativas de Backups

- Tivoli Storage Manager - IBM
- Backup Exec - Symantec
- NetBackup – Veritas

Protección de la información

Seguridad del Endpoint

Protección de la información

Seguridad del Endpoint

¿Por qué proteger?

- Con mucha frecuencia se exponen públicamente vulnerabilidades que pueden ser explotadas por ciberdelincuentes.
- Ante la explotación de las vulnerabilidades se podría afectar los activos y la operativa de la entidad.
- Se podrían filtrar datos que después se pueden utilizar para fraudes o para ataques mayores.

Protección de la información

Seguridad del Endpoint

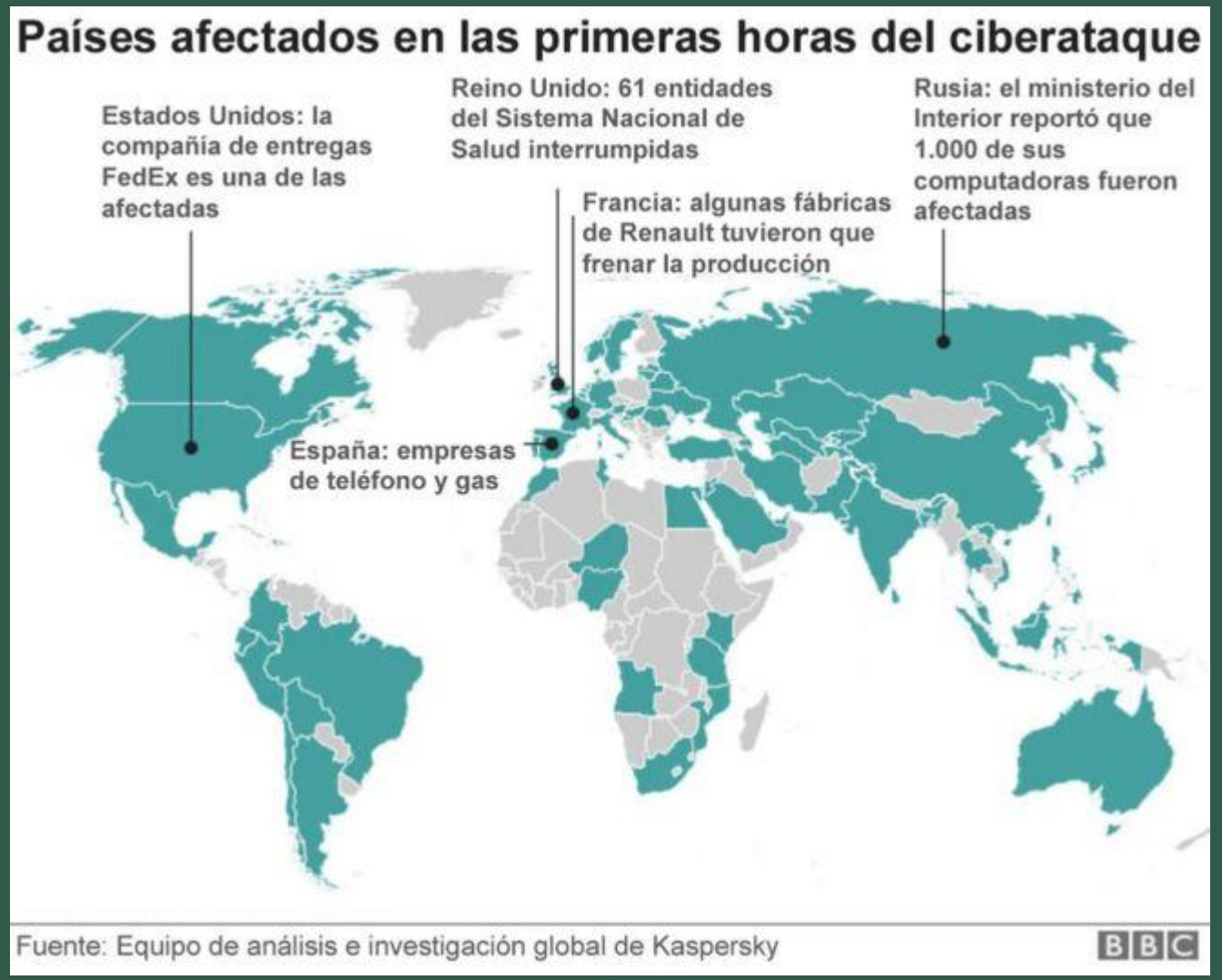
¿Por qué proteger?

- Incidentes importantes de seguridad podría restar competitividad a la entidad.
- Ante incidentes importantes de seguridad la entidad puede ver afectada su imagen y generar desconfianza en sus clientes.
- La entidad podría recibir fuertes sanciones por parte del Ente Regulador.

Protección de la información

Seguridad del Endpoint

¿Por qué proteger?



Protección de la información

Seguridad del Endpoint

¿Por qué proteger?

La automotriz Renault debió paralizar su producción para detener el ataque.

Los pacientes en el hospital de Yakarta tuvieron que esperar varias horas para ser atendidos.

Protección de la información

Seguridad del Endpoint

¿Por qué proteger?

La demanda por el pago en Bitcoin apareció en las pantallas en una estación de Frankfurt

Protección de la información

Seguridad del Endpoint

Gestión de usuario

AV de navegación

Firewall

Parches

Proxy

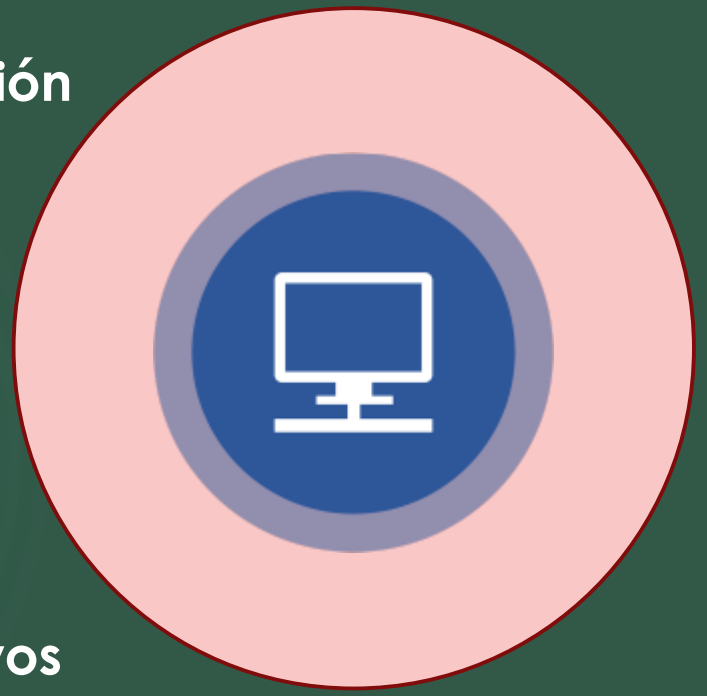
AntiAPT

Antivirus

NAC

Ctrl. dispositivos

DLP



Redes segmentadas

Protección de la información

Seguridad del Endpoint

Gestión de Usuario

- No utilizar usuario con privilegio Admin
- Inhabilitar cuenta invitado
- Cambiar contraseña por defecto usuario Admin

Firewall

- Tener habilitado Firewall de Endpoint
- Bloquear conexiones laterales
- Bloquear puertos sensibles

Parches

- Suscribirse a boletines de vulnerabilidades
- Inventario de activos
- Mantener actualizado el S.O. y aplicaciones

Protección de la información

Seguridad del Endpoint

AntiAPT

- Tener instalado y configurado
- Monitorear o generar esquema de alertas

NAC

- Controlas equipos que se unen a la red
- Controla la salud de la equipos
- Enviar a cuarentena equipos “no sanos”

DLP

- Establecer reglas de bloqueos para correo
- Bloqueos de copia de datos USB
- Depuración de falsos positivos

Protección de la información

Seguridad del Endpoint

Red. Segm.

- Separar ambientes de producción y de desarrollo
- Separar ambientes de servidores y usuarios

Ctrl. Disp.

- Bloquear uso disp. almacenamiento masivo
- Bloquear copia en CDs

Antivirus

- Antivirus
- Cargar IOC con Hash o MD5
- Verificar permanentemente % de equipos actual.

Protección de la información

Seguridad del Endpoint

Proxy

- Bloquear sitios peligrosos
- Limitar accesos por áreas

AV Naveg.

- Controlar sitios de navegación
- Controlar descargas