

SESIÓN

07

PROTECCIÓN CONTRA CÓDIGO MALICIOSO CÓDIGO DE SEGURIDAD

- Protección contra código malicioso
- Copia de seguridad

Protege las instalaciones de procesamiento de información contra código malicioso y contra la pérdida de datos

Protección contra
código malicioso



Copia de Seguridad



/ PROTECCIÓN CONTRA CÓDIGO MALICIOSO

AGENDA

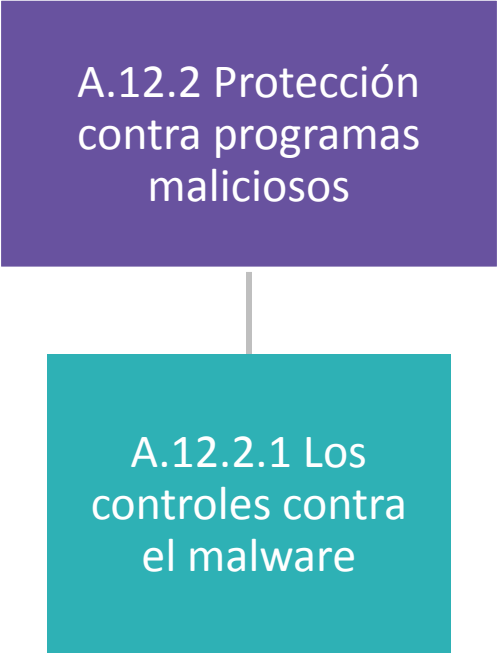
Objetivo

Controles

Phishing

SPAM

Malware



A.12.2 Protección contra programas maliciosos

A.12.2.1 Los controles contra el malware



“PROTEJA SUS

DATOS”

<https://www.youtube.com/watch?v=EQmkBHTcsbw>

OBJETIVO

A.12.2 Protección contra el malware

Objetivo: Garantizar que la información y servicios de procesamiento están protegidos contra el malware.

A.12.2.1 Los controles contra el malware

Deberán llevarse a cabo controles de detección, prevención y recuperación para la protección contra el malware, junto con la debida conciencia del usuario.

PHISHING

- El phishing es una forma de fraude en internet.
- Fraude: realización de una transacción no autorizada.



SPAM

- Nombre colectivo para los mensajes no deseados.
- El término se utiliza normalmente para correo no deseado, los mensajes no deseados de publicidad en los sitios web también son considerados como spam.



MALWARE: SOFTWARE MALICIOSO

- Malware = malicioso + software.
- Se refiere a software no deseado, tales como virus, gusanos, troyanos y spyware
- La medida estándar contra el malware es utilizar escáneres antivirus y un cortafuegos.



MALWARE: VIRUS

- Un virus es un pequeño programa informáticos que se replica a propósito, a veces en una forma alterada.
- A fin de que el virus se propague su funcionamiento depende de los portadores que contienen código ejecutable.



MALWARE: GUSANO

- Un gusano es un pequeño programa informático que se replica a propósito. Los resultados de la replicación son copias de la difusión original a otros sistemas, haciendo uso de las instalaciones de la red de su anfitrión.



/ COPIA DE SEGURIDAD

AGENDA

Objetivo

Concepto

Tipos

Estrategia de Respaldo

Estrategia de Restauración

A.12.3 Copia de
seguridad

A.12.3.1 Copia de
seguridad de la
información

OBJETIVO

A.12.3 Copia de seguridad

Objetivo: Proteger contra la pérdida de datos.

A.12.3.1 Copia de seguridad de la información

Se deberán realizar copias de seguridad de la información y del software, y se deberán probar periódicamente en conformidad con la política de copias de seguridad acordada.

CONCEPTO

Las copias de respaldo (backups) son copias parciales o totales de información en otro sistema de almacenamiento masivo como por ejemplo: discos duros externos, CD-ROM, DVD, cintas magnéticas, espacio en la nube u otros.

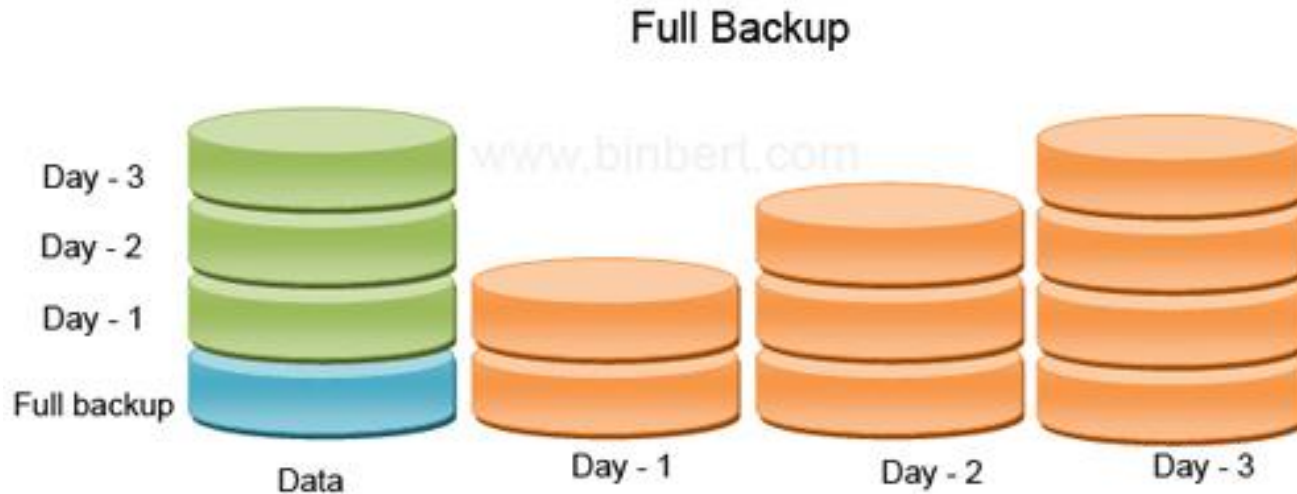


PROCEDIMIENTO BÁSICO DE COPIA DE SEGURIDAD

- Para efectuar los backups correctamente, el primer paso consiste en identificar qué datos se deben proteger (ficheros, bases de datos, imágenes, archivos de configuración, etc.).
- En el caso de un centro de información, al menos deberían ser los siguientes: Bases de datos, sitio web del centro, colección de recursos de información, correo electrónico, archivos de trabajo de acuerdo a su importancia.

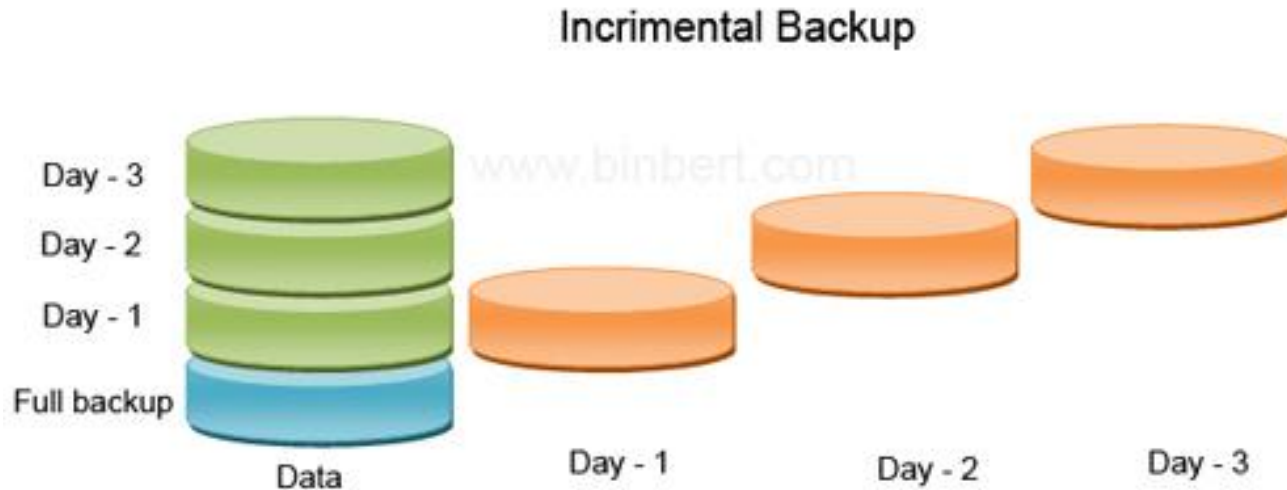
TIPOS: TIPO 1. BACKUP COMPLETO

- Se crea una copia de respaldo de todos los archivos y carpetas del servidor.
- El proceso consume mucho tiempo y soporte de almacenamiento pero garantiza la disponibilidad de todos los archivos.



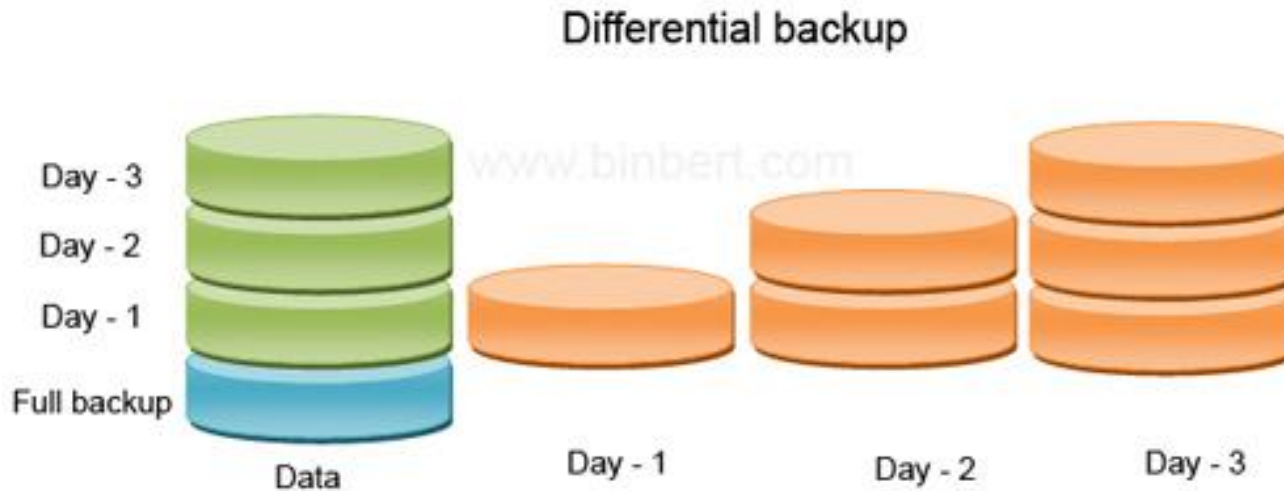
TIPOS: TIPO 2. BACKUP INCREMENTAL

- Crea copias de aquellos archivos que hayan sido modificados o creados después del último backup.
- Este proceso se basa en la fecha de creación de los archivos y la primera vez que se ejecute realiza un respaldo completo.



TIPOS: TIPO 2. BACKUP DIFERENCIAL

- Este tipo de backup funciona de forma similar al backup incremental, pero comparando efectivamente el contenido de los archivos.
- Solo copia aquellos archivos nuevos o modificados.



ESTRATEGIAS Y LINEAMIENTOS PARA REALIZAR LOS RESPALDOS

Definir una estrategia de los respaldos que le garantice su correcto funcionamiento en el momento en que se requiera. ¿Qué debe hacer?:

- Establecer un horario en el que se realizará el proceso (se recomienda que se realice cuando menos usuarios/as estén trabajando en la red) y el lugar donde se almacenarán las copias de respaldo.

ESTRATEGIAS Y LINEAMIENTOS PARA REALIZAR LOS RESPALDOS

- Realizar revisiones periódicas del soporte de almacenamiento y de la información que se respalda.
- Es conveniente efectuar “simulacros” de restauración de los archivos almacenados en las copias de respaldo.

GUÍA PARA LA RESTAURACIÓN DE INFORMACIÓN

- En todos los niveles de la organización, debe entenderse que “backup” no es el problema. El problema es que sea posible restaurar toda la información pertinente en el plazo establecido.
- Cuando se entiende que “restaurar” es el problema, es evidente que “copia de seguridad” es solo una parte de la solución.



GUÍA PARA LA RESTAURACIÓN DE INFORMACIÓN

Para restaurar existen otros requisitos, tales como:

- Conocer el plazo para la restauración.
- Comprender el orden en que los sistemas se deben restaurar.
- Disponibilidad de los sistemas para restaurar.
- Personal con conocimiento en actividades de restauración.
- Software necesario para hacer la restauración.
- Procedimientos de prueba después de una restauración.

TAREA GRUPAL

Objetivo

- Elaborar un Cronograma de Copias de Respaldo.

TAREA GRUPAL

En grupos de 5 participantes trabajar lo siguiente:

- Elaborar un Cronograma de Copias de Respaldo, de las bases de datos de una entidad financiera.
- Las bases de datos son: clientes, proveedores, personal de la entidad, servicios (Plazo fijo, ahorro), transacciones.
- El cronograma debe contar con los siguientes campos: tipo de base de datos, frecuencia, tipo de respaldo, fecha, entre otros.

TAREA GRUPAL

Instrucciones para la entrega de la tarea.

- La tarea deberá ser realizada en clase, por todos los miembros del grupo.

/ RESUMEN

Protección contra
código malicioso.



Copia de Seguridad.

