SEGURIDAD. Curso 2020-2021

Tema 9: Seguridad en la Gestión de los Datos
Parte 3: GDPR y Plan de Continuidad de Negocio

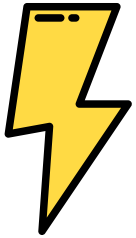
Agenda

- Introducción
- Protección de datos
- Plan de continuidad del negocio

Introducción

Introducción

- Casos de usos
  - Banco con 1 millón de cuentas, números de seguridad social, tarjetas de crédito, prestamos.
  - Aerolínea que atiende a 50.000 personas en 250 vuelos diarios.
  - El sistema de farmacia que llena 5 millones recetas por año.
- Riesgos y vulnerabilidades identificadas
  - Fallo de servidores, discos, alimentación
  - Robo de criminales informáticos, ataque DoS, malware
  - Tormenta de nieve, terremoto
  - Error humano (accidental o malicioso)
- ¿Cuál es el plan de continuidad? ¿Hay un plan de recuperación?



Introducción - Análisis de Impacto

- Identificar los procesos empresariales de importancia estratégica
- Identificar los riesgos (incluso para desastres naturales)
- Identificar las repercusiones…
  - … desde el punto de vista financiero
  - … desde el punto de vista legal
  - … en tema de relaciones internas y externas
  - … en tema de reputación
- ¿Hay un plan de recuperación que establezca limites temporales?
  - Las respuestas pueden ser obtenidas mediante cuestionarios, entrevistas o reuniones con usuarios clave de la parte IT.
  - Fundamentales el estudio del impacto (gestión de riesgos).

Análisis de Impacto y Gestión de Datos

- La mayoría de las veces, el activo más importante de una empresa de servicios es representado de sus datos:
  - Datos de clientes (e-commerce, newsletters, consumidores previos, etc.)
  - Datos de propiedad intelectual (patentes, análisis, etc.)
  - Datos sensibles (datos sanitarios, religiosos, perfilamiento, etc.)
- Proteger los datos no solo es aconsejable, es también un requisito de ley:
  - Normativa Nacional
  - Normativa Europea

Agenda

- Introducción
- Protección de datos
  - Nivel Nacional
  - Nivel Europeo
- Plan de continuidad del negocio

Protección de datos

Protección de Datos – Nivel Nacional

- Regulado por la Agencia Española de Protección de Datos
  - Ley orgánica de protección de datos (LOPD)
  - Derechos ARCO
    - Acceso: Obtener información sobre si los datos personales están siendo tratado
    - Rectificación: Modificar los datos inexactos o incompletos
    - Cancelación: Suprimir los datos inadecuados o excesivos
    - Oposición: Denegar en tratamiento de datos personales
- Integrado y ampliado desde el 25 de mayo 2018
  - Reglamento Europeo de Protección de Datos (RGPD)
  - Se ha unificado a nivel europeo la norma de protección de datos.

Protección de Datos – Nivel Europeo

- El **Reglamento General de Protección de Datos** es la normativa que establece las pautas a seguir en lo relativo al tratamiento de los datos personales de **personas físicas**.
- También se encarga de indicar las normas en cuanto a la *libre circulación* de dichos datos.
- Objetivos principales:
  - Proteger el derecho de las personas físicas a preservar sus datos personales.
  - Asegurar el respeto a los derechos y libertades individuales.

Protección de Datos – GDPR en síntesis

Se considera lícito el tratamiento siempre y cuando se haya obtenido en base a las siguientes condiciones:

- Consentimiento del interesado.
- Necesarios para la ejecución de un contrato.
- Para cumplir con obligaciones legales.
- Su objetivo es proteger derechos fundamentales del interesado.
- Se trata de datos de interés público.
- Son fundamentales para que el responsable o un tercero puedan ejercer sus derechos legítimos.

Protección de Datos – Datos sensibles

1. **Identificativos**: Nombre, apellidos, DNI o NIE, número de seguridad social, domicilio, teléfono, correo electrónico, fotografías o audios de voz.
2. **Circunstancias sociales**: Propiedades, aficiones y formas de vida, inscripciones en foros, clubes o asociaciones.
3. **Personales**: Fecha y lugar de nacimiento, edad, estado civil, datos familiares.
4. **Académicos y de formación**: Expediente académico, formación y titulaciones.
5. **Profesionales y de empleo**: Experiencia en el mundo profesional, categoría o puesto a desarrollar o desarrollado por el trabajador, expediente profesional.
6. **Sindical**: Datos de afiliación sindical, pertenencia a un comité de empresa.
7. **Económico-financieros**: Datos bancarios, ingresos, rentas, créditos, préstamos, avales, plan de pensiones, jubilación.
8. **Médicos o de salud**: Historial clínico de la persona física y controles sanitarios.

Protección de Datos – Datos sensibles

9. **Administrativos**: Procedimientos administrativos, reclamaciones y recursos, sanciones, registros, solicitudes, concesiones.
10. **Judicial**: Expediente o historial judicial, sanciones, procedimientos judiciales.
11. **Sociales**: Ayudas o subvenciones, percepción de prestaciones de asistencia social, subsidios, pensiones.
12. **Dirección IP.** La dirección IP es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en red de un dispositivo, por lo que puede resultar un dato identificativo a nivel de geolocalización.
13. **Comerciales.** Actividades o negocios, licencias comerciales, subscripciones a publicaciones o medios de comunicación, creaciones artísticas, literarias, científicas o técnicas.

Protección de Datos – Obligaciones 1/2

Protección de Datos – Obligaciones 2/2

- **Consentimiento**: Procurar el consentimiento inequívoco de los afectados para el uso de sus datos
- **Notificación de Brechas de Seguridad**: si las mismas afectan a datos personales
- **Informar Propietarios de los Datos**: más información, más transparencia
- **DPO**: obligatorio en muchas situaciones
- **Evaluación de Impacto**: sobre el riesgo de la exposición de los datos
- **Derecho de los Afectados**: derechos ARCO
- **Registro de las Actividades de Tratamiento**: registro interno de las actividades relacionadas con los datos personales
- **Elaboración del Documento de Seguridad**: resumen de los procesos relativos al tratamiento de datos personales
- **Formación y Certificación**: la persona encargada en el tratamiento deberá tener una mínima formación en la materia
- **Auditoría Periódicas**: internas o externas, analizando el cumplimiento de la ley

Protección de Datos – El rol del DPO

Data Protection Officer
Es el encargado del tratamiento de las obligaciones legales en la materia de protección de datos.

Es obligatorio si:

- Se trata de una **autoridad u organismo público**;
- cuando las actividades principales consisten en elaborar perfiles de comportamiento de los clientes o usuarios;
- en caso de tratar **categorías especiales de datos** (de salud, por ejemplo) o datos personales relacionados con condenas y delitos penales.

GDPR y Gestión de Riesgos

Cuanto hemos visto en clase por el tema de análisis y gestión de los riesgos se aplica también a los flujos de datos.

- Identificar el contexto y las características de los datos
- Identificar los procesos de la información y sus características
- Identificar y valorar las amenazas (brechas de seguridad)
- Identificar, seleccionar y valorar las salvaguardas
- Medir el impacto y valorar los riesgos

https://www.aepd.es/es/guias-y-herramientas/herramientas

Movilidad y teletrabajo

Algunos procesos de la empresa se pueden ejecutar en situaciones de:

- Movilidad
  - Hay que realizar una planificación previa
- Teletrabajo
  - Según las circunstancias de urgencia se puede obligar a poner en marcha soluciones con carácter provisional

De esto dependen tanto la resiliencia del Estado, la continuidad de los procesos de negocio, y los derechos y libertades de los interesados cuyos datos se están tratando.

- Documento AEPD en tema de movilidad
- Documento CCN-CERT CNI en tema de teletrabajo

AEPD – Buenas practicas – Empresa

- Definir una política de protección de la información para situaciones de movilidad.
- Elegir soluciones y prestadores de servicio confiables y con garantías.
- Restringir el acceso a la información.
- Configurar periódicamente los equipos y dispositivos utilizados en las situaciones de movilidad.
- Monitorizar los accesos realizados a la red corporativa desde el exterior.
- Gestionar racionalmente la protección de datos y la seguridad.

AEPD – Buenas practicas – Empleados

- Respetar la política de protección de la información en situaciones de movilidad definida por el responsable.
- Proteger el dispositivo utilizado en movilidad y el acceso al mismo.
- Garantizar la protección de la información que se está manejando.
- Guardar la información en los espacios de red habilitados.
- Si hay sospecha de que la información ha podido verse comprometida comunicar con carácter inmediato la brecha de seguridad.

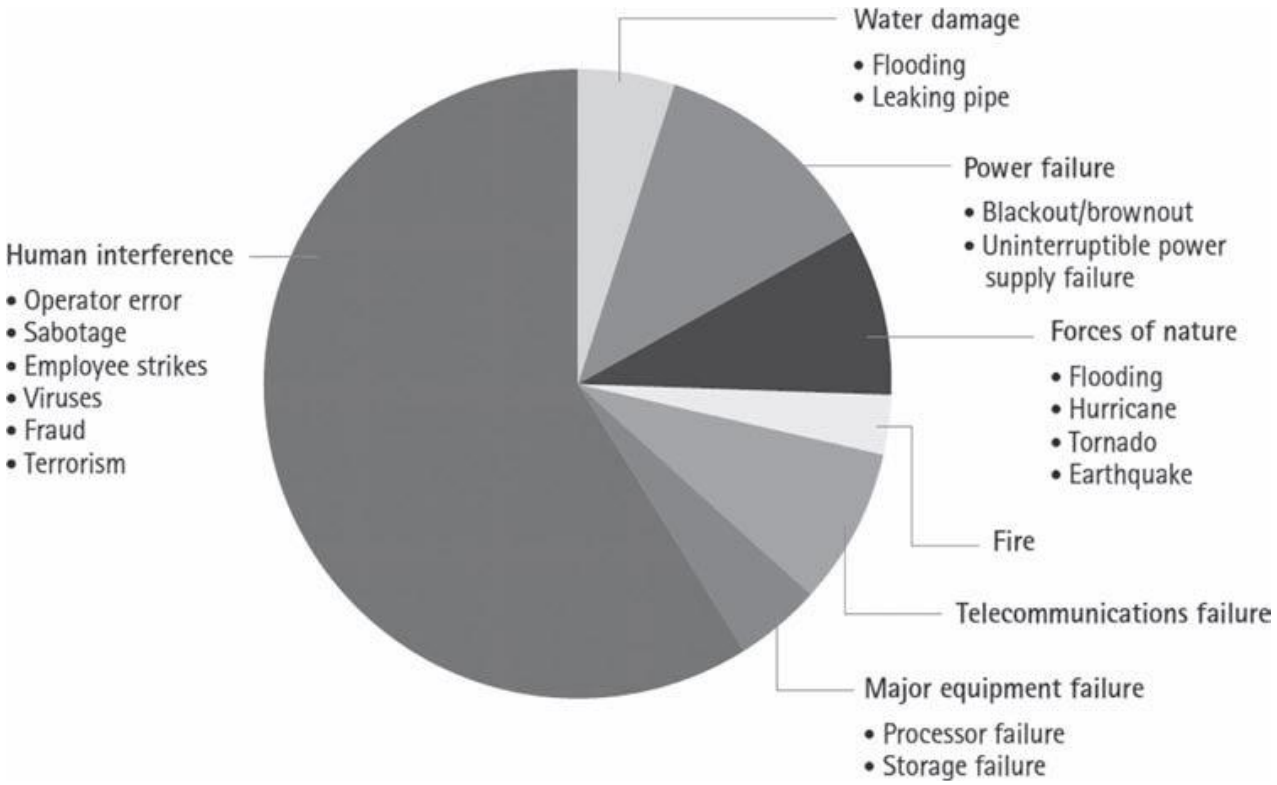
Agenda

- Introducción
- Protección de datos
- Plan de continuidad del negocio
  - Gestión de la continuidad
  - Administración de desastres y plan de urgencias
  - Estrategias de recuperación

Plan de continuidad del negocio

Introducción - Desastre

- Un incidente natural o causado por humanos que afecta negativamente a las organizaciones o al medio ambiente



Continuidad de Negocio

- Desde el ingles, Business Continuity (BC)
- Indica la capacidad de una empresa de continuar las operaciones con una mínima interrupción o tiempo de inactividad después de un desastre.
  - Fuerte conexión con el concepto de disponibilidad
  - Se refiere a las actividades realizadas constantemente para mantener el servicio (backup, redundancia, etc.).
- Objetivos principales:
  - Asegurar servicios críticos ininterrumpidos.
  - Minimizar las pérdidas comerciales.
  - Asegurarse de que la empresa pueda cumplir con sus objetivos a corto y a largo plazo.

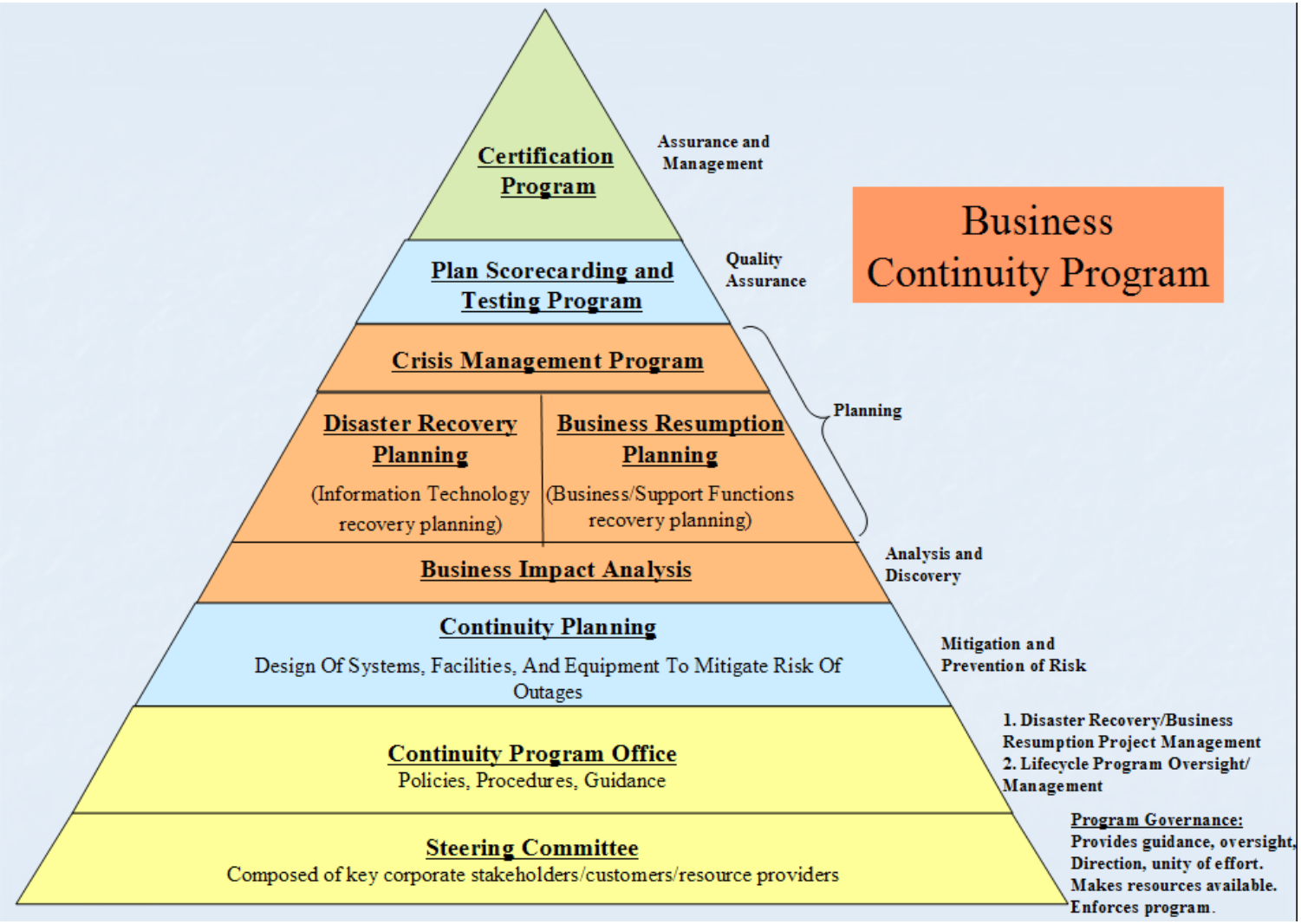
Posibles implicaciones

- Legal
  - Requisitos reglamentarios
  - Requisitos contractuales
  - SLAs
- Productividad
  - Pérdida de productividad
  - Empleados afectados
  - Tasa de carga horaria
- Reputación
  - Clientes
  - Proveedores
  - Mercados financieros
  - Bancos
  - Socios de business

- Ingresos
  - Pérdida directa
  - Pérdidas diferidas
  - Pagos compensatorios
  - Pérdida de ingresos futuros
  - Pérdidas de facturación
  - Pérdidas de inversión

- Rendimiento financiero
  - Pérdida de cuota de mercado
  - Reconocimiento de ingresos
  - Flujo de efectivo
  - Descuentos por pérdida
  - Garantías de pago
  - Clasificación de crédito

Plan de continuidad del negocio



Plan de recuperación ante desastres 1/2

- Desde el ingles, Disaster Recovery (DR)
- Se compone de medidas en tema de:
  - procesos – todas las acciones necesarias para el correcto funcionamiento del plan de DR.
  - políticas – asegurar el funcionamiento de procesos claves.
  - procedimientos – estrategias de recuperación de los datos.
- Es necesarios para la recuperación de las operaciones y la continuación de las funciones críticas de una organización en consecuencia de un desastre.
- Objetivos principales:
  - Limitar los efectos del desastre en las funciones comerciales.
  - Volver a las condiciones normales de funcionamiento.
  - Minimizar la ocurrencia de ciertos tipos de desastres en el futuro.

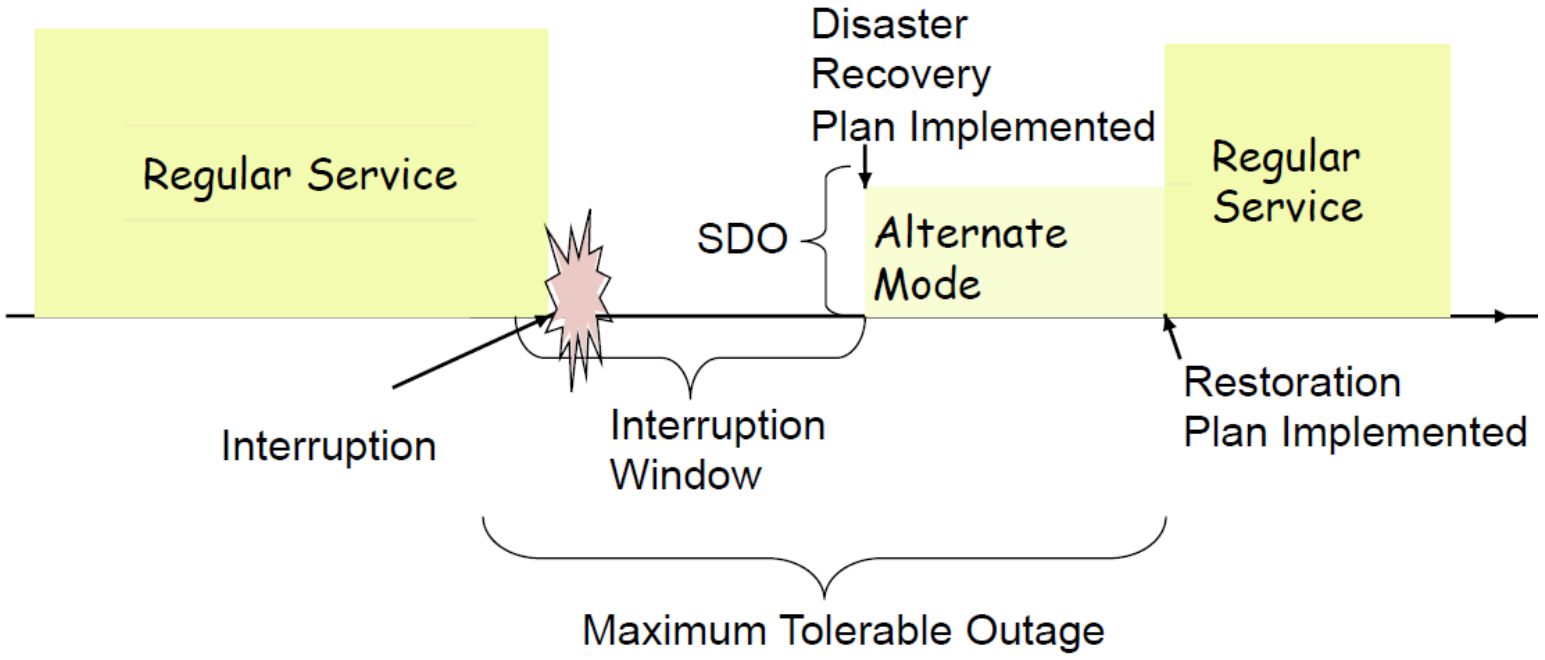
Plan de recuperación ante desastres 2/2

Aborda las siguientes áreas:

- Prevención (antes del desastre)
  - Asegurar los sistemas vulnerables, proteger los sistemas que contienen datos importantes.
- Continuidad (durante un desastre)
  - Mantener y continuar las operaciones críticas que permiten a la organización funcionar adecuadamente.
- Recuperación (después del desastre)
  - Restablecer todos los sistemas y recursos a su estado regular y plenamente operativo.

Desastre - Tiempo de recuperación

- Ventana de interrupción: La organización de la duración del tiempo puede esperar entre el punto de fallo y la reiniciación del servicio
- Objetivo de prestación de servicios (SDO): Nivel de servicio en modo alterno
- Interrupción máxima tolerable: Tiempo máximo en modo alterno



Desastre - Análisis del impacto

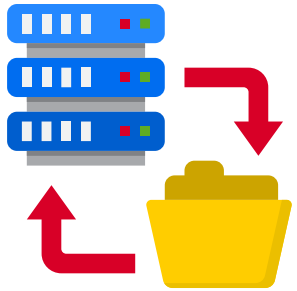
- Identificación del impacto comercial y operacional de un desastre.
- Identificación de los procesos críticos:
  - Determinar todos los posibles efectos financieros, jurídicos y reglamentarios.
  - Determinar el máximo tiempo de interrupción y recuperación permitido.
  - Identificar los recursos necesarios para la reactivación y la recuperación.
  - Fuertemente conexo con el proceso estudiado en la parte de gestión de riesgos

Diferencias DR y BC

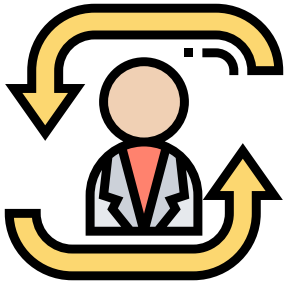
- DR se ocupa de recuperar los sistemas a su estado normal en caso de desastre.
  - Es reactiva, ya que su objetivo es restaurar el negocio después de un desastre.
- BC implica priorizar varios procesos comerciales y recuperar primero los más importantes.
  - Es proactiva, ya que se centra en evitar o mitigar los riesgos.

Estrategias de recuperación

- Métodos de copias de seguridad
  - Copias de seguridad regulares, uso de dispositivos extraíbles y/o almacenamiento de datos fuera del sitio.



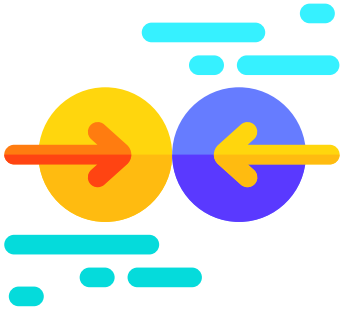
- Sitios alternativos
  - Cold, warm, hot backup.
- Reemplazo de equipo
- Funciones y responsabilidades
  - Los equipos de DR deben ser entrenados para implementar las estrategias de recuperación y los planes de contingencia.



- Consideraciones sobre el costo
  - Todos los gastos están dentro de las limitaciones del presupuesto.

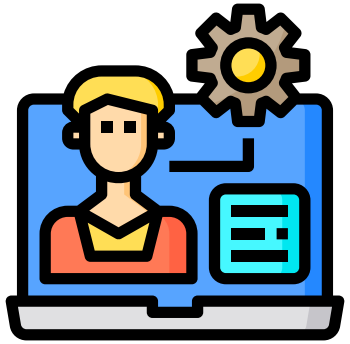
Plan de pruebas

- El plan de recuperación tiene que seguir siendo relevante y fiable en caso de desastre.
- Las pruebas consisten en una combinación de:
  - Pruebas de escenario:
    - Los procedimientos de recuperación se prueban en un escenario para asegurar que siguen siendo pertinentes.
  - Transferencia de sistemas a un sitio alternativo:
    - Para asegurar que los sistemas puedan ser reproducidos dentro de un marco de tiempo determinado.
  - Walk-through estructurado:
    - Para exponer errores u omisiones sin la planificación y los gastos asociados a la realización de una prueba de operaciones completa.



Plan de mantenimiento

- Los cambios en los sistemas informáticos implican actualizaciones de tecnología, cambios en las necesidades comerciales y las políticas de la organización
- El plan de recuperación debe actualizar de forma constante:
  - Requisitos operacionales y de seguridad
  - Procedimientos técnicos
  - Hardware, software y otros equipos
  - Información de contacto de:
    - Los miembros del equipo
    - Los proveedores
    - El personal en sitios alternativos
  - Requisitos de las instalaciones alternativas y externas.

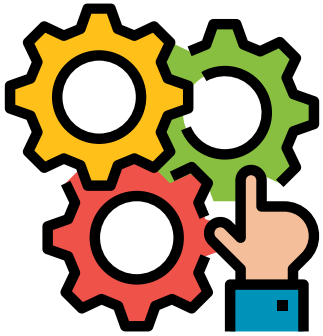


Backup – Definiciones 1/2

- La copia de seguridad (backup) es una copia adicional de los datos que puede utilizarse para fines de restauración y recuperación.
- La copia de backup se usa cuando la copia primaria se pierde o se corrompe.
- Esta copia de seguridad puede ser creada por:
  - Simplemente copiando los datos (puede haber una o más copias).
  - Haciendo mirroring de datos (la copia siempre se actualiza con lo que se escribe en la copia primaria).

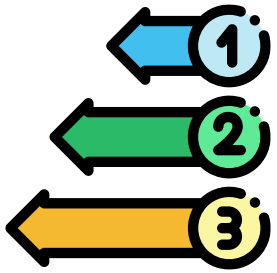
Backup – Definiciones 2/2

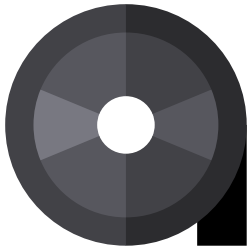
- El backup asegura que un sistema puede volver a su estado original si los datos se han perdido o corrompido.
  - Guarda copias secundarias de los datos en caso de que se pierdan los datos originales.
- Una buena política de copias de seguridad puede reducir o eliminar los daños causados por la pérdida de datos.
- Confiar en las copias de seguridad manuales puede ser poco fiable
  - Necesidad alta de automatización



Backup – Best practices

- Copiar frecuentemente y sabiamente.
- Dar prioridad a los datos para la recuperación de desastres
  - Redundante (necesidad inmediata)
  - Altamente disponible (de minutos a horas)
  - Respaldado (de cuatro horas a días)
- Archivar datos importantes a largo plazo.
- Almacenar los datos de forma rentable.
  - La mayoría de las PYMEs pueden desear adquirir una solución integrada.





Backup - Procedimientos de recuperación

- Una estrategia de backup necesita de:
  - un procedimiento de recuperación bien documentado y comprobado para asegurar que los datos de respaldo se restauren adecuadamente
  - disponibilidad de equipos y alojamientos alternativos si los originales han sido destruidos.
  - disponibilidad de software original como el sistema operativo personalizado y los programas de aplicación
  - Los datos de backup actualizados deben ser fácilmente accesibles
- ¡No es una simple copia de los datos!
  - Recuperación de sistemas operativos enteros, softwares, configuraciones..

Estrategia de backup

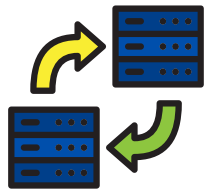
- ¿Cuántos datos deben ser protegidos?
  - Entonces se elige un dispositivo adecuado para esa cantidad
- ¿Cómo hacer una copia de seguridad de los datos?
- ¿Cuándo hacer una copia de seguridad de los datos?
- ¿Dónde almacenar las copias de seguridad?
- ¿Qué procedimientos de recuperación? ¿Qué tan rápido se necesitan los datos correctos?
- ¿Qué plataforma de copia de seguridad de datos es la mejor para proteger los datos?

Metodología de backup

- Discos mirrored
  - Copia exacta bit a bit de todos los datos de una unidad de disco físico.
  - Almacenados fuera de la sede y mantenidos sincronizados.

- Instantáneas (snapshots)
  - Contiene un conjunto de marcadores de referencia que apuntan a los datos almacenados en un dispositivo.

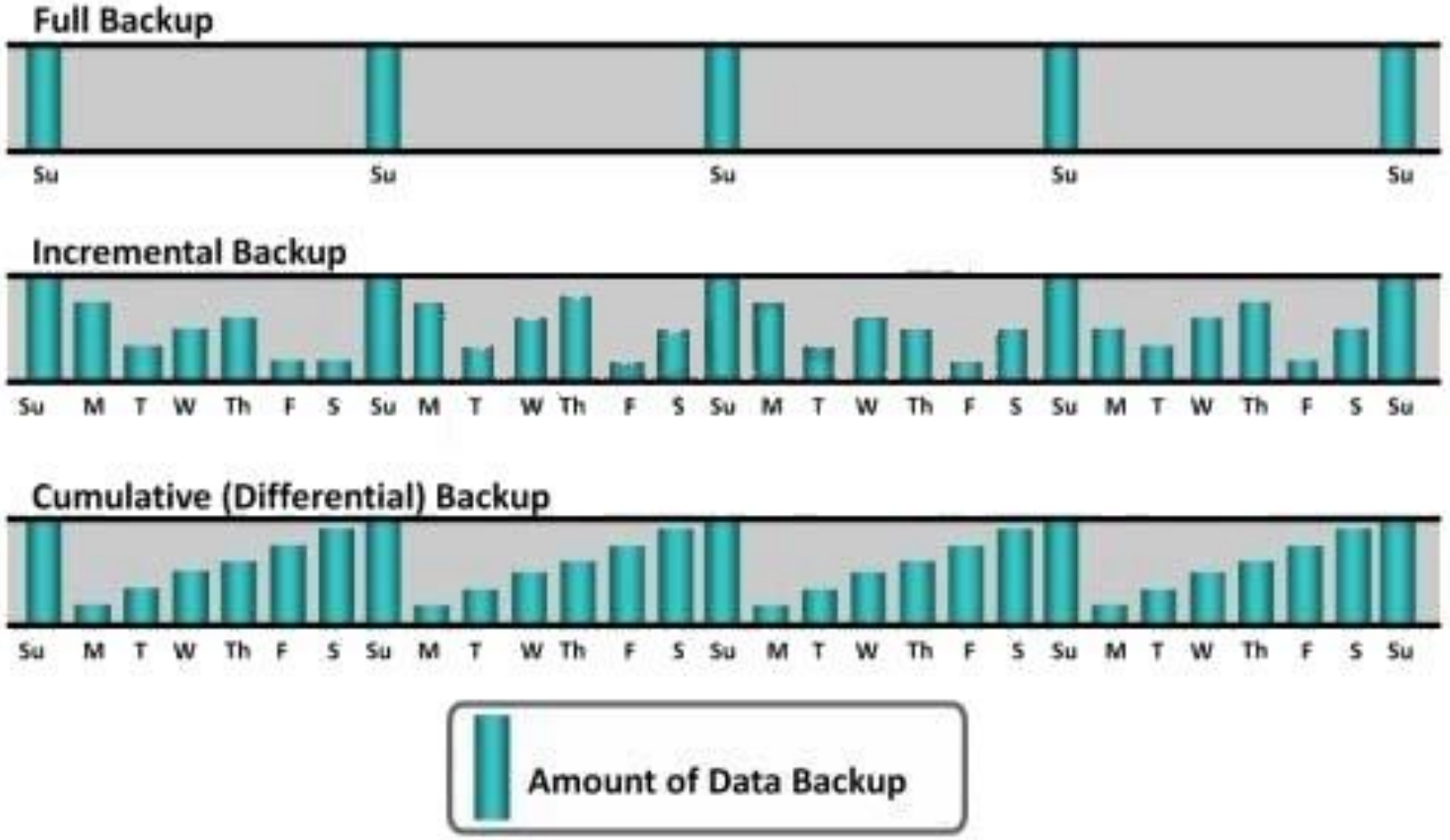
- Protección continua de datos (CDP)
  - Guardando automáticamente una copia de cada cambio.
  - Un registro electrónico de instantáneas de almacenamiento, con una instantánea de almacenamiento por cada instante que se modifiquen los datos.



Granularidad de backup 1/2

- Backup completo
  - Copia la totalidad de los datos en otro juego de soportes (cintas o discos).
  - Se dispone de la totalidad de los datos en un único conjunto. Permite restaurar los datos en un tiempo mínimo.
- Backup incremental
  - Copia los datos que han variado desde la última operación de backup de cualquier tipo.
  - Más rápido y exige menos espacio para almacenar.
- Backup diferencial (o cumulativo)
  - Copia los datos que han cambiado desde el ultimo backup completo.

Granularidad de backup 2/2



Sitios de backup

- Cold backup
  - Sitio de respaldo que no tiene hardware ya configurado para restaurar rápidamente los backup (p.ej., dispositivos externos cuales cintas magnéticas o copias de datos que requieren reinstalar las herramientas).
- Worm backup
  - Sitio configurado de forma compatible a la versión actual, pero sin todos los recursos adecuado para restablecer el servicio al 100% (p.ej., maquinas virtuales sub-dimensionadas)
- Hot backup
  - Sitio configurado de forma idéntica a la versión actual, el uso de dicho sitio es solo subjeto a cuestiones de direccionamiento (p.ej., mirroring).
  - Es un clon perfecto del sitio primario.

Tecnologías para el backup

- Cintas magnéticas
  - Baratas, altas capacidades de almacenamiento, bajo mantenimiento, capacidad de almacenamiento de archivo externo.
  - Bajo rendimiento en comparación con otra tecnologías.

- Discos
  - Fácil de implementar, gastos reducidos, QoS mejorado.
  - Depende de otras tecnologías como la replicación local y remota. Se necesitan módulos y configuraciones adicionales (RAID).

- Cloud
  - Se delega a servicios externos la gestión del almacenamiento y/o la estrategia de backup.
  - Coste más alto, necesita un concepto de confianza.

Bibliografía

- ISO 22301:2012
  - Societal security
  - Business continuity management systems
  - Requirements
- ISO/IEC 27031:2011
  - Security techniques
  - Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 24762:2008
  - Guidelines for ICT disaster recovery services