Da Vinci
PRIMERA ESCUELA DE ARTE MULTIMEDIAL

Clase 08

Análisis de Sistemas

Materia:
Sistemas Empresariales

Docente contenidista: CASTIÑEIRAS, José

Revisión: Coordinación

Contenido

Clase 8

¡Te damos la bienvenida a la materia **Sistemas Empresariales**!

En esta clase vamos a ver los siguientes temas:

- Seguridad de la Información.
- Pilares.
- Estándares de Seguridad de la Información.
- Amenazas.
- Controles.
- Plan de Recuperación de Desastres (DRP).
- Plan de Continuidad de negocio (BCP).

Muchos de ustedes se preguntarán:
¿Cómo se protege la seguridad de datos y la información en las organizaciones?

¿Cuál es la importancia de la seguridad de la información en las organizaciones?

¿Cuáles son los estándares de seguridad más conocidos?

¿Qué controles existen como elementos de mitigación de riesgos?

Seguridad de la Información

En el mundo digital en el que nos encontramos, las empresas y sus sistemas son igual o más vulnerables a ataques cibernéticos.

Hoy en día los activos más importantes que tienen las empresas son sus datos; éstos son claves para el crecimiento de los negocios y, adquirirlos implica grandes inversiones de dinero y tiempo por lo que la seguridad informática y la protección de dichos datos e infraestructura empresarial es una preocupación importante.

Es en este contexto la comprensión de conceptos como seguridad de la información, seguridad en aplicaciones y ciberseguridad, se vuelve esencial para salvaguardar activos digitales y proteger la privacidad. Con ello conocer las mejores prácticas usadas para proteger sistemas, redes y datos contra las amenazas cibernéticas es fundamental.

Seguridad de la Información es la disciplina responsable de sostener la confidencialidad, integridad y disponibilidad de la información, resguardando el procesamiento, almacenamiento y transmisión de la misma.

Pilares de seguridad

Conocido como el triángulo CIA por sus siglas en inglés, son la Confidencialidad, Integridad, y Disponibilidad.

Confidencialidad

Por confidencialidad entendemos a la cualidad de la información para no ser divulgada a personas o sistemas no autorizados. Se trata básicamente de la propiedad por la que esa información sólo resultará accesible con la debida y comprobada autorización de los dueños de esa información.

¿Cómo se pierde la confidencialidad? Generalmente, haciendo caso omiso a las recomendaciones de seguridad o no implantando un sistema adecuado; como por ejemplo cuando se comparten contraseñas entre usuarios, se decomisionan equipos sin eliminar los datos, se dejan sesiones abiertas, se transmite información mediante protocolos inseguros, no ciframos los datos de manera adecuada, la información deja de ser confidencial (o está en alto riesgo).

Integridad

El diccionario define el término como "estado de lo que está completo o tiene todas sus partes". La integridad hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.

Esta integridad se pierde cuando la información se modifica, cuando parte de ella se elimina, o se crean datos espurios.

Disponibilidad

Por disponible entendemos aquella información a la que puedan acceder las personas autorizadas, cuando la requieran, a través de los canales adecuados y siguiendo los procesos correctos.

La seguridad de información y de las comunicaciones abarca también la autenticación de los mensajes que incluye la identificación de las partes (Emisor y receptor), verificar, registrar la aprobación, autorización de la información, la no alteración de los datos y el no repudio de la comunicación o la información almacenada.

En el sentido jurídico la seguridad de información se refiere a las obligaciones legales relativas a mantener o mejorar la seguridad de la información y las medidas requeridas por la ley para proteger, promover la eficiencia de la información, su procesamiento de acuerdo con los derechos y libertades de los individuos.

La seguridad de la información puede ser vista como uno de los elementos necesarios que constituyen la calidad de la información en sistemas de información.

El aumento de las regulaciones en materia de seguridad de la información habla de la importancia global de las infraestructuras y de los derechos en el contexto de la sociedad.

Para poder gestionar la seguridad de la información, se debe realizar una adecuada gestión de riesgos, que incluyen la identificación y valoración de los riesgos y las medidas de control, preventivas y correctivas, sobre todos los medios a través de los cuales fluya la información (servidores, equipos de comunicación, aplicaciones, computadoras personales, personas, archivos físicos, etc.), los cuales se denominan ***Activos de Información*.**

Estos activos se pueden encontrar en diferentes formatos, por ejemplo, en formato digital, de forma física o en forma de ideas o conocimientos de personas que pertenecen a una organización.

La seguridad de la información debe proteger el negocio de la Organización.

La Seguridad de la Información es un concepto estratégico transversal a la organización, y tiene un alcance mayor que la ciberseguridad, ya que la seguridad de la información quiere proteger la información en todos los estados o formas, de los diferentes tipos de riesgos a los que se enfrentan.

Su objetivo es proteger la información de riesgos que puedan afectar a los activos de información en formato digital y los sistemas informáticos que los procesan y almacenan, indistintamente si están interconectados o no.

Se sustenta en metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, que soportan la idea de protección en las distintas facetas de la información; involucra la aplicación y gestión de medidas de seguridad apropiadas para la protección de la información.

La ciberseguridad se aplica a los sistemas que se encuentran interconectados, en los que "circula" y en los que "vive" la información a proteger.

Se centra únicamente en los datos en formato digital. Mantiene su atención principalmente en los riesgos provenientes únicamente del ciberespacio.

Amenazas

En el contexto de la seguridad de la información, **una amenaza se refiere a cualquier evento o acción que pueda comprometer la confidencialidad, integridad o disponibilidad de los datos o sistemas**.
Estas amenazas pueden provenir de diversas fuentes y pueden manifestarse de diversas maneras.

A continuación, se describen algunas de las amenazas más comunes:

Ataques cibernéticos

Incluyen una amplia gama de actividades maliciosas en línea, como virus informáticos, malware, ransomware, troyanos y ataques de phishing. Estos ataques pueden ser utilizados para robar información, dañar sistemas o extorsionar a las víctimas.

Acceso no autorizado

Las personas no autorizadas que intentan acceder a sistemas, aplicaciones o datos sensibles representan una amenaza significativa. Esto puede incluir intentos de fuerza bruta para adivinar contraseñas, el uso de credenciales robadas o la explotación de vulnerabilidades de seguridad.

Robo de identidad

Los ciberdelincuentes pueden robar identidades o información personal para llevar a cabo actividades ilegales en nombre de otra persona, lo que puede tener graves repercusiones para las víctimas y las organizaciones afectadas.

Ataques de denegación de servicio (DDoS)

Estos ataques buscan inundar un sistema o red con tráfico malicioso, sobrecargándolo y haciendo que sea inaccesible para usuarios legítimos.

Vulnerabilidades de software y hardware

Las debilidades en el software o el hardware pueden ser explotadas por atacantes para ganar acceso no autorizado o realizar acciones maliciosas en sistemas o aplicaciones.

Amenazas internas

Los empleados, contratistas o personas con acceso legítimo a los sistemas de una organización pueden representar una amenaza si abusan de ese acceso o cometen acciones maliciosas.

Desastres naturales y fallas técnicas

Eventos como incendios, inundaciones, terremotos o fallas en la infraestructura técnica pueden interrumpir los servicios y la disponibilidad de datos.

Fugas de datos

Las filtraciones de datos pueden ocurrir debido a errores humanos, fallos de seguridad, ataques o malas prácticas de gestión de datos, lo que puede resultar en la exposición no autorizada de información confidencial.

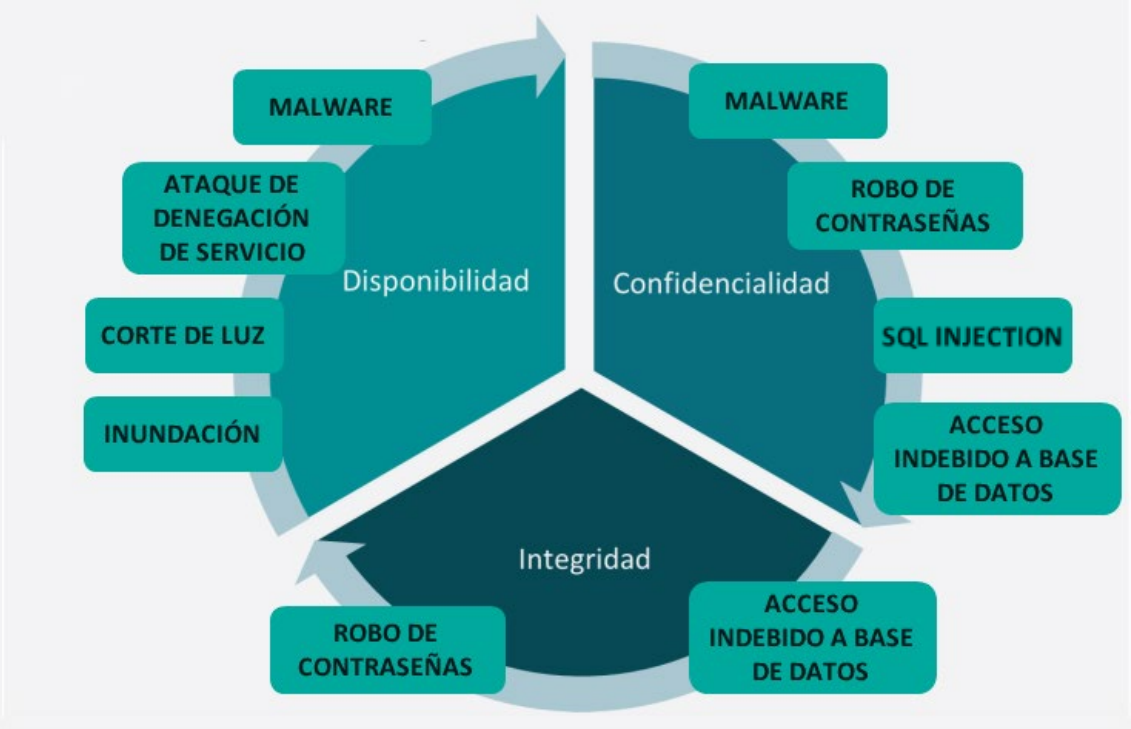
Espionaje cibernético

Gobiernos y actores maliciosos pueden llevar a cabo actividades de espionaje cibernético para recopilar información sensible, secretos comerciales o propiedad intelectual de otras organizaciones.

Sociales y humanas

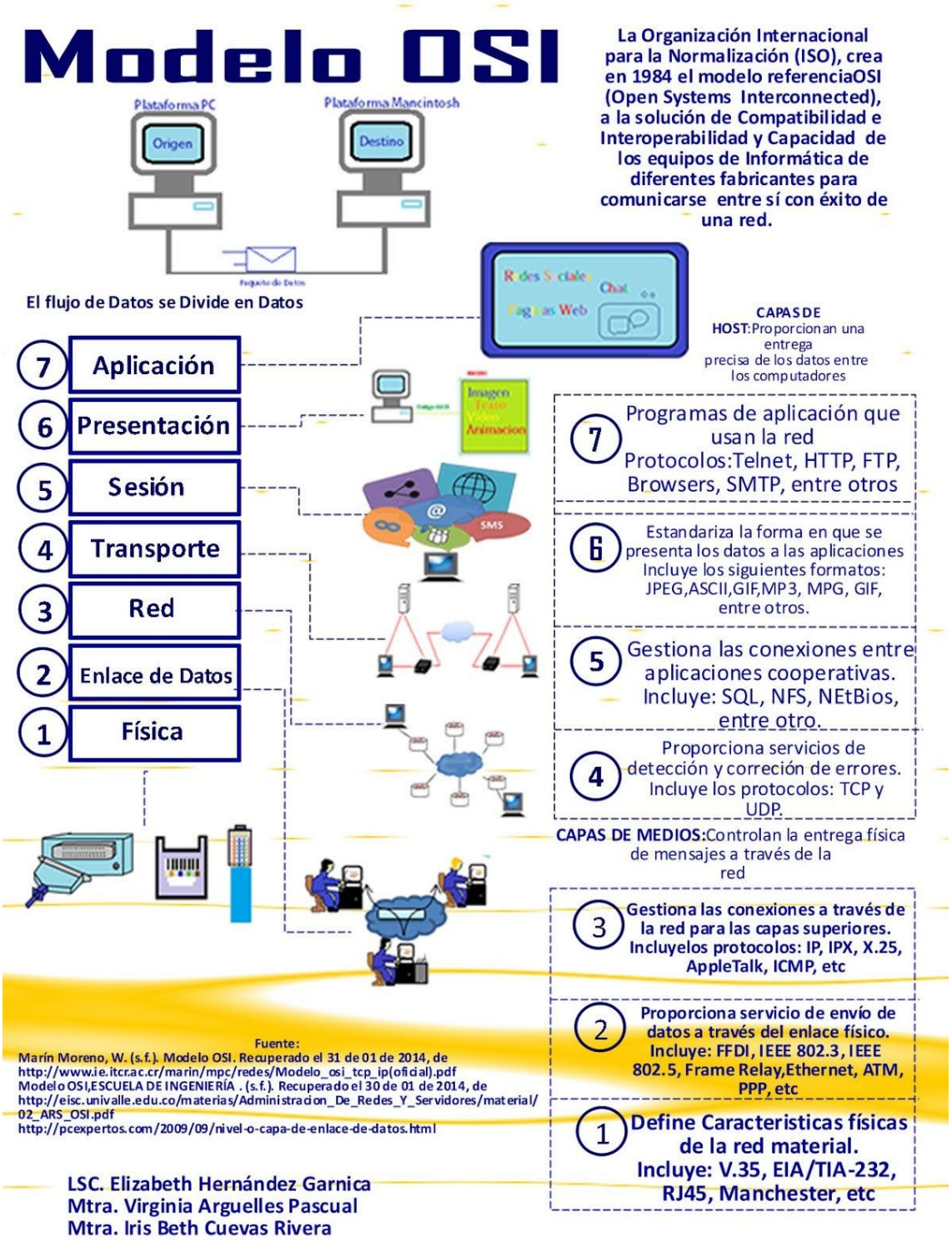
Las amenazas sociales involucran la manipulación de personas para obtener información confidencial o acceso no autorizado, a menudo a través de la ingeniería social, como el engaño o el phishing.

Las organizaciones deben tomar medidas proactivas para evaluar y gestionar los riesgos asociados con estas amenazas y mantener sus sistemas y datos con un adecuado nivel de seguridad, acorde al valor de la información protegida.



Algunas amenazas comunes y su impacto en los pilares- Imagen adaptada de ESET Curso de ciberseguridad.

El modelo OSI simplificado



(Se verá en detalle el modelo OSI en materia de Redes)

Tipos de Ataques y su relación con el Modelo OSI

User ----> Social Engineering

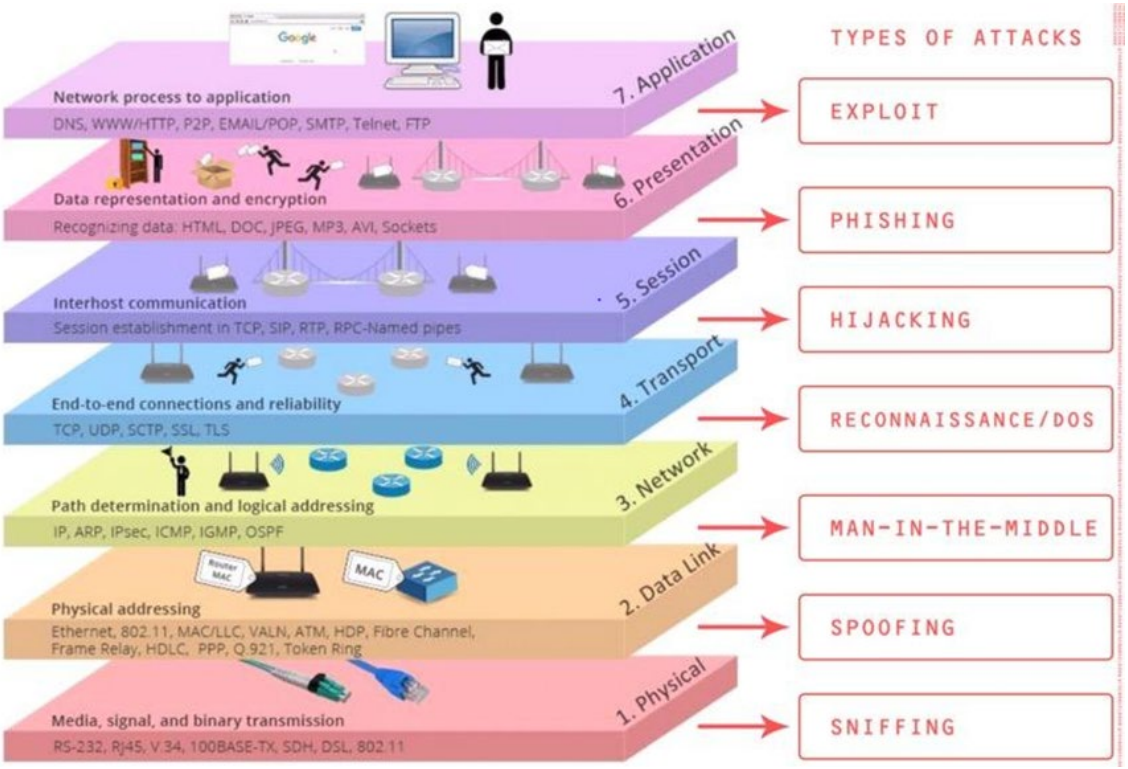
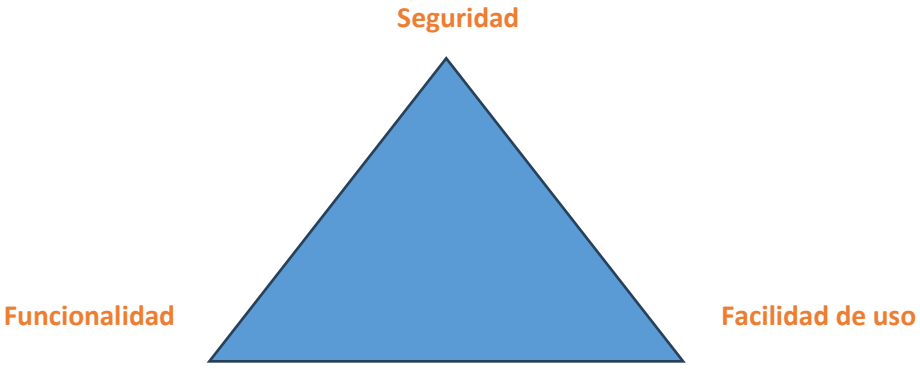


Imagen adaptada de https://platzi.com/clases/2225-redes/35587-modelo-osi/

El Triángulo de la Seguridad, Funcionalidad y Facilidad de Uso

La tecnología está evolucionando a un ritmo sin precedentes, y como resultado, muchos de los productos informáticos que llegan al mercado están diseñados más orientados a la facilidad de uso que a la seguridad.



Esto que es conocido como "deuda técnica" debería ser mitigado incorporando la seguridad en el modelo seguro de desarrollo de software (SSDLC), como ejemplo mencionaremos SDL de Microsoft.

Recomendamos leer el modelo SDL en detalle: https://www.microsoft.com/es-co/download/details.aspx?id=12379

Por otra parte, es cada vez es más difícil para los administradores de sistemas y otros profesionales asignar los recursos exclusivamente para los sistemas de seguridad.

Esto incluye el tiempo necesario para revisar los archivos de registro (logs), detectar vulnerabilidades e incluso para aplicar los parches de actualizaciones de seguridad que se publican periódicamente.

Hay muy poco tiempo disponible para implementar medidas y asegurar los recursos de computación en forma regular e innovadora. Esto ha aumentado la demanda de profesionales dedicados a la seguridad que harán un seguimiento continuo (monitoreo) y protegerán los activos de información.

En un principio, para hackear o vulnerar se necesitaba poseer habilidades extraordinarias, se requería una gran habilidad por parte del atacante.
Sin embargo, hoy en día existen herramientas automatizadas y códigos disponibles en Internet que hacen posible que cualquier persona con tiempo disponible y la voluntad y el deseo de hackear, pueda tener altas chances de éxito en su esfuerzo.

Estándares de Seguridad de la Información

Al momento de tener que implementar seguridad en una organización es importante evitar improvisar y para ello es recomendable alinearse a algún estándar conocido, en caso que no aplique alguno mandatorio por cuestiones de regulación como:

- **PCI DSS:** El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) es un conjunto de requisitos diseñados para garantizar la seguridad de las transacciones con tarjetas de crédito y débito.

- **HIPAA:** La Ley de Portabilidad y Responsabilidad del Seguro Médico, establece estándares de seguridad y privacidad para proteger la información de salud identificable (Aplica en USA).

- **GDPR:** El Reglamento General de Protección de Datos (GDPR) de la Unión Europea se centra en la protección de datos personales y la privacidad de los ciudadanos de la UE.

- **FISMA:** La Ley Federal de Administración de Seguridad de la Información de Estados Unidos establece requisitos para asegurar y proteger la información del gobierno federal.

Es importante mencionar que la elección de los estándares de seguridad de la información para una organización dependerá de su alcance, industria, ubicación y necesidades específicas.

Normativas de alcance local

En Argentina hay varias leyes y regulaciones, podemos mencionar:

- **Ley de Protección de Datos Personales (Ley 25.326):**
  Esta ley argentina regula la protección de datos personales y establece las obligaciones para el tratamiento de información personal. Las organizaciones que manejan datos personales deben cumplir con esta normativa.

- **Ley 26.529:**
  Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud.

A su vez hay actividades reguladas, entre otras la de entidades financieras como los bancos, las cuales deben cumplir con normativa del Banco Central de la República Argentina (BCRA) que es la entidad encargada de regular y supervisar el sistema financiero en Argentina.

- **Comunicación "A" 4609:**
  Esta norma establece los requisitos mínimos de seguridad informática que deben cumplir las entidades financieras y otras entidades supervisadas por el BCRA. Define aspectos como la clasificación de la información, la seguridad física y lógica, las políticas de acceso y control, entre otros aspectos.

- **Comunicación "A" 5460:**
  Esta comunicación establece las pautas de seguridad de la información que deben seguir las entidades financieras para protegerse de los riesgos emergentes en el ciberespacio. También aborda temas como la gestión de incidentes de seguridad y la protección de los sistemas de información.

El estándar ISO 27000

El estándar más general y completo para la gestión de la seguridad de la información es la familia ISO 27000, que incluye en sus dominios, entre otros, la gestión de activos, la seguridad asociada al recurso humano, la gestión de comunicaciones y operaciones, el control de acceso y la gestión de la continuidad del negocio, todo enmarcado en un ciclo PHVA (planear-hacer-verificar-actuar (ajustar); en inglés se denomina PDCA, plan-do-check-act) que busca la mejora continua de los procesos, concepto introducido por Walter A. Shewhart y desarrollado por Edward Deming como parte de la teoría del Total Quality Management (TQM).

Imagen de https://safetyculture.com/es/listas-de-verificacion/ciclo-pdca/

Otros estándares de seguridad de la información son Magerit, Marion, Mehari y Octave, COBIT son más específicos, desarrollados para una región particular y para la gestión de riesgos de empresas con diferente naturaleza operativa.

Suelen ser menos robustos y según el alcance que se le quiera dar al proyecto de aseguramiento pueden ser una alternativa.

Familia ISO 27000

- **ISO/IEC 27000** - es un vocabulario estándar para el SGSI. Introducción y base para el resto. Tercera versión: enero de 2014. Quinta versión: febrero 2018. ISO/IEC 27000:2018.

- **ISO/IEC 27001** - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005. Revisada en octubre de 2022.

- **ISO/IEC 27002** - Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es un código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007. Última versión: 27002:2022, de febrero de 2022.

- **ISO/IEC 27003** - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero de 2010. No es certificable.

- **ISO/IEC 27004** - son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre de 2009, no se encuentra traducida al español actualmente.

- **ISO/IEC 27005** - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada con la actual British Standard BS 7799 parte 3. Publicada en junio de 2008. Revisada en junio de 2011.

- **ISO/IEC 27006** - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma especifica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación. Publicada en 2007 y revisada en diciembre de 2011 y septiembre de 2015.

- **ISO/IEC 27007** - es una guía para auditar al SGSI. Publicada en noviembre de 2011.

- **ISO/IEC 27008** - es una guía para auditar los controles seleccionados para implantar un SGSI. No es certificable. Publicada en octubre de 2011.

- **ISO/IEC 27009** - detalla los requisitos para usar la norma ISO/IEC 27001 en cualquier otro ámbito. No es certificable. Publicada en junio de 2016.

- **ISO/IEC 27010** - es una guía para gestionar la seguridad de la información cuando se comparte entre distintas organizaciones. Es aplicable a todas las formas de intercambio y difusión de información. Publicada en octubre de 2012 y revisada en noviembre de 2015.

- **ISO/IEC 27011** - es una guía de interpretación de la información y gestión de la seguridad de esta información en organizaciones del sector de telecomunicaciones. Publicada en diciembre de 2008, fue revisada en diciembre de 2016.

- **ISO/IEC 27014** - es una guía de gobierno corporativo de la seguridad de la información. Publicada en abril de 2013.

- **ISO/IEC 27015** - es una guía de SGSI orientada a organizaciones del sector financiero y de seguros. Publicada en noviembre de 2012.

- **ISO/IEC 27016** - es una norma que se concentra en un análisis financiero y económico de equipos y procedimientos de la seguridad de la información. Publicada en febrero de 2014.

- **ISO/IEC 27017 -** es una guía de seguridad para Cloud Computing. Publicada en diciembre de 2015.

- **ISO/IEC 27018** - es una guía para controlar la protección de datos para servicios de computación en cloud computing. Publicado en julio de 2014.

- **ISO/IEC 27019** - es una guía para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía.

- **ISO/IEC 27031** - es una guía de apoyo para la adecuación de las tecnologías de la información y comunicación. No es certificable. Publicada en marzo de 2011.

- **ISO/IEC 27032** - es una guía de apoyo para identificar las líneas generales para fortalecer el estado de la Ciberseguridad en una empresa. Publicada en julio de 2012.

- **ISO/IEC 27033** - es una guía detallada de seguridad de la administración, operación y uso de las redes. Publicada en 2010.

- **ISO/IEC 27034** - es una referencia en el área de tecnología de la información, técnicas de seguridad y seguridad de la aplicación. Publicado en 2011.

- **ISO/IEC 27035:2011** - Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este estándar hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades. Publicada en agosto de 2011.1

- **ISO/IEC 27036** - 2013 Tecnología de la información - Técnicas de seguridad - Seguridad de la información para las relaciones con los proveedores.

- **ISO/IEC 27038** - es una guía de especificación para seguridad en la redacción digital.

- **ISO/IEC 27039** - es una guía para la selección, despliegue y operación de sistemas de detección y prevención de intrusión.

- **ISO/IEC 27040** - es una guía para la seguridad en medios de almacenamiento.

- **ISO/IEC 27041** - es una guía para garantizar la idoneidad y adecuación de los métodos de investigación.

- **ISO/IEC 27042** - es una guía con directrices para el análisis e interpretación de las evidencias digitales.

- **ISO/IEC 27043 -** desarrolla principios de investigación para la recopilación de evidencias digitales.

- **ISO/IEC 27050** - desarrolla en tres partes sobre la información almacenada en dispositivos electrónicos.

- **ISO/IEC 27103:2018** - es una norma desarrollada para proporcionar orientación sobre cómo aprovechar las normas **existentes en un marco de ciberseguridad.**

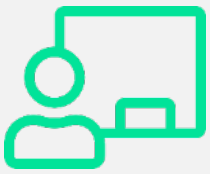
- **ISO/IEC 27799:2008** - es una guía para implementar ISO/IEC 27002 en la industria de la salud.

¿Dónde interviene la gestión de seguridad de la información en una empresa?

Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información:

Imagen: Correlación entre la Continuidad del Negocio, Ciberseguridad y las Tecnologías de la información.
Fuente: Dirección General de Modernización Administrativa, P. e. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas. Madrid: Ministerio de Hacienda y Administraciones Públicas.

Lista de Controles de ISO 27002



En este archivo encontrarás una lista de controles ISO27002:

https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

Como se observa en los controles de la ISO 27002, hay distintos tipos de dominios, controles y niveles de aplicación.

Uno de ellos, dentro del grupo de controles del dominio 12 *Seguridad en las operaciones* y que tiene importancia vital es:

Copias de resguardo (Backup Plan)

Cada empresa genera diariamente datos corporativos en una multitud de formas, como ser registros de transacciones de bases de datos, correos electrónicos, archivos de texto, presentaciones, voicemails, faxes, facturas, registros de empleados, contenido del sitio web, fotografías e incluso muestras físicas, tales como muestras de productos o documentos impresos históricos.

Al mismo tiempo, muchos negocios deben cumplir con un período de conservación de sus registros históricos definidos por diversos marcos regulatorios como leyes (normativas impositivas, PCI, SOX, HIPAA, regulaciones para entidades financieras tales como BCRA para bancos en la República Argentina, etc.).

Los datos corporativos son un activo estratégico, y si están mal gestionados, pueden convertirse en una responsabilidad legal de importancia significativa. En el caso de una solicitud de litigio, por ejemplo, las empresas son responsables de producir la información necesaria para su defensa- y esto incluye el correo electrónico.

Como resultado de esta evolución, las empresas y los ejecutivos corporativos han adquirido una clara conciencia de la necesidad de resguardar sus datos como parte de su plan general de continuidad de negocios y recuperación de desastres.

Básicamente un backup es una copia de la información clave que se almacena en una locación diferente de donde la información original reside.

Esto incluye la copia de seguridad y el archivado periódico de los datos para que, en caso de un desastre natural, como un incendio, daños causados por el agua, etc., o bien un ataque malintencionado (o incluso un error no intencionado), se pueda acceder rápidamente a otra copia de sus datos corporativos y regresar a los negocios de nuevo tan pronto como sea posible.

"*Con el costo del tiempo de inactividad del sistema de TI tan elevado -entre USD 84.000 y USD 108.000 por cada hora- el costo de un día de negocios perdidos puede ser devastador, particularmente en la economía de hoy*". (Fuente: Gartner, IDC, Forrester, Yankee Group - Valores de USA)

"*De hecho, se informa que el 90% de las empresas que pierden todos sus datos quedan fuera del negocio dentro de los siguientes 12 meses. Sin embargo, el 40% de todas las pequeñas y medianas empresas (PYMES) no respaldan sus datos en absoluto, y el 60% de todos los datos se almacenan en computadoras de escritorio y portátiles*". (Fuente: Small Business Computing).

Tipos de Backup

- **Backups completo o full**:

  El tipo de operación de backup más básico y abarcativo es el backup completo o full backup. Como su propio nombre indica, copia la totalidad de los datos en otro juego de soportes, que puede consistir en cintas, discos, DVD, u otro medio magnético, incluyendo un sitio remoto. La ventaja principal de la realización de un backup completo en cada operación es que se dispone de la totalidad de los datos en un único juego de soportes. Esto permite restaurar los datos en un tiempo mínimo, lo cual se mide en términos de objetivo de tiempo de recuperación (RTO). No obstante, el inconveniente es que lleva más tiempo realizar un backup completo que de otros tipos (a veces se multiplica por un factor 10 o más), y requiere importante espacio de almacenamiento.

  Por lo tanto, sólo se suelen realizar backups completos periódicamente. Los centros de datos que manejan un volumen de datos (o de aplicaciones críticas) reducido pueden optar por realizar un backup completo cada día, o más a menudo en ciertos casos.

  Lo normal es que en las operaciones de backup se combine el backup completo con backups incrementales o diferenciales.

- **Backups incrementales**:

  Sólo copia los datos que han variado -o los nuevos-, desde la última operación de backup de cualquier tipo. Se suele utilizar la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha del último backup. Las aplicaciones de backup identifican y registran la fecha y hora de realización de las operaciones de backup para identificar los archivos modificados desde esas operaciones. Para recuperar todos los datos se necesitan todos los incrementales a partir del último completo o full.

- **Backups diferenciales**:

  Una operación de backup diferencial es similar a un backup incremental la primera vez que se lleva a cabo, pues copiará todos los datos que hayan cambiado desde el backup anterior. Sin embargo, cada vez que se vuelva a ejecutar, seguirá copiando todos los datos que hayan cambiado desde el anterior completo. Por lo tanto, en las operaciones subsiguientes almacenará más datos que un backup incremental, aunque normalmente muchos menos que un backup completo. Además, la ejecución de los backups diferenciales requiere más espacio y tiempo que la de los backups incrementales, pero menos que la de los backup completos.

- **Backups selectivos:**

  Se elige qué tipo de archivos o carpetas resguardar.

- **Backups continuos**:

  Se replican los datos a otro medio, local o remoto.

  Normalmente, cada alternativa y opción estratégica tiene sus ventajas e inconvenientes en términos de rendimiento, niveles de protección de los datos, cantidad total de datos conservados, y costo.

Herramientas de backup

Entre otras aplicaciones podemos mencionar

- Symantec
- Arcserve
- Veritas
- Acronis
- Veeam

Algunas de estas soluciones permiten realizar backup a infraestructura de Nube (Cloud Computing), que facilitan el plan de recuperación de desastres (DRP) que veremos a continuación.

Plan de Recuperación de Desastres (DRP) y Plan de Continuidad de Negocio (BCP):

En ocasiones, suelen utilizarse de manera indistinta los términos BCP y DRP cuando se hace referencia a planes encaminados a restablecer las operaciones primordiales de una organización en caso de alguna contingencia.
Sin embargo, existen diferencias sustanciales entre un plan y otro, y la principal característica que permite identificarlos es su alcance.

Ambos son componentes utilizados para contribuir a que los sistemas esenciales para el funcionamiento de la organización estén disponibles cuando sean necesarios, con la característica de que el DRP se limita a los procesos e infraestructura de TI de la organización y está considerado un subconjunto del BCP.

Por su parte, la continuidad del negocio está encaminada a describir los pasos a seguir por una organización cuando no puede funcionar de manera normal debido a un desastre natural o uno causado por el hombre. El BCP puede ser escrito para un proceso de negocio específico o para todos aquellos de misión crítica, y se compone de un conjunto de planes, incluido el DRP.

Entonces, la recuperación ante desastres (DRP) se enfoca en el restablecimiento de los sistemas e infraestructura de TI que soportan los procesos de negocio críticos después de eventos de interrupción, mientras que la continuidad del negocio (BCP) está orientada a la recuperación de los procesos de negocio críticos que son necesarios para la operación, por lo que no solo incluye lo anterior, sino también todos los demás aspectos operativos necesarios dentro de la organización.

Desarrollo y activación del DRP

En el blog de Eset (www.eset.com), el especialista Miguel Angel Mendoza (2014) señala que existen diferentes maneras de abordar el desarrollo de un plan de recuperación, y que éste debe estar alineado con el plan de continuidad, por lo que debe considerar los elementos que definen la razón de ser de una organización.

Además, el DRP debe incluir los criterios para determinar cuándo un incidente de seguridad no se puede resolver mediante los procedimientos comunes de atención y se considera como un desastre, es decir, cuando se presenta un evento catastrófico y repentino que nulifica la capacidad de las organizaciones para llevar a cabo los procesos esenciales.

Un desastre podría ser el resultado de un daño importante a una parte de las operaciones, la pérdida total de una instalación o la incapacidad de los empleados para acceder a las instalaciones, generado por algún tipo de desastre natural, una contingencia sanitaria o una huelga, por ejemplo.

A continuación, se presenta una propuesta para el desarrollo y aplicación del DRP en 6 puntos claves:

1. **Desarrollar una política de continuidad del negocio (BCP)**
   Todas las actividades deben estar alineadas con los objetivos de continuidad del negocio, por lo que un punto de partida puede ser el desarrollo de una política encargada de establecer el marco de operación de los planes, así como la clasificación de los sistemas o aplicaciones para identificar aquellos que sean considerados como críticos.

2. **Realizar una evaluación de riesgos**
   Llevar a cabo una evaluación de riesgos permite identificar, analizar y evaluar las amenazas que podrían afectar a la organización, especialmente aquellos que puedan provocar un evento que se incluya en la categoría de desastre.

   La gestión de riesgos implica una serie de estrategias para abordarlos de manera efectiva. A continuación, se presentan las definiciones de cuatro enfoques comunes en la gestión de riesgos: mitigar, aceptar, transferir y evitar.

   - **Mitigar riesgos:**

     Definición: La mitigación de riesgos implica tomar medidas proactivas para reducir la probabilidad de que ocurra un riesgo o minimizar su impacto si ocurre.

     Ejemplo: Implementar medidas de seguridad cibernética, como firewalls y sistemas de detección de intrusiones, para reducir el riesgo de un ataque cibernético.

   - **Aceptar riesgos:**

     Definición: Aceptar riesgos significa conscientemente asumir la posibilidad de que un riesgo se materialice, sin tomar medidas adicionales para reducirlo o transferirlo. Por lo general, se hace cuando el costo de mitigación es demasiado alto o cuando el riesgo es considerado aceptable por la organización.

     Ejemplo: Una organización podría aceptar el riesgo de que sus servidores estén indisponibles durante una breve interrupción de energía, ya que considera que los costos de implementar una infraestructura de respaldo son prohibitivos.

- **Transferir riesgos:**

  Definición: Transferir riesgos implica la transferencia de la responsabilidad de gestionar un riesgo a otra entidad. Esta entidad puede ser un tercero, como una compañía de seguros, que asume la responsabilidad financiera en caso de que ocurra el riesgo.
  Ejemplo: Comprar un seguro contra incendios para cubrir los daños materiales en caso de un incendio en una propiedad.

- **Evitar riesgos:**

  Definición: Evitar riesgos significa tomar medidas para eliminar por completo la posibilidad de que un riesgo se materialice. Esta estrategia implica evitar la actividad, el proceso o la situación que presenta el riesgo.
  Ejemplo: Una empresa que fabrica productos peligrosos puede optar por evitar los riesgos de responsabilidad legal al cesar la producción de esos productos.

  Es importante que las organizaciones evalúen cuidadosamente sus riesgos y utilicen una combinación de estas estrategias según corresponda a sus objetivos y recursos. La gestión adecuada de riesgos ayuda a las organizaciones a tomar decisiones informadas sobre cómo abordar los riesgos en función de sus tolerancias y prioridades específicas.

3. **Realizar un análisis de impacto al negocio (BIA)**
   En este paso se definen principalmente los objetivos de recuperación para los sistemas que soportan los procesos de negocio. Se define el Tiempo Objetivo de Recuperación (RTO por sus siglas en inglés), que es el período permitido para la recuperación de una función o recurso de negocio a un nivel aceptable luego de un desastre, y el Punto Objetivo de Recuperación (RPO) que describe la antigüedad máxima de los datos para su restauración, con base en los requisitos del negocio.

Otros elementos pueden definirse, por ejemplo, el tiempo de inactividad máximo tolerable (Maximum Tolerable Downtime, MTD) o la interrupción máxima tolerable (Maximum Tolerable Outage, MTO), es decir, el período máximo de no disponibilidad para las actividades, activos o procesos, antes de que la organización deje de operar.

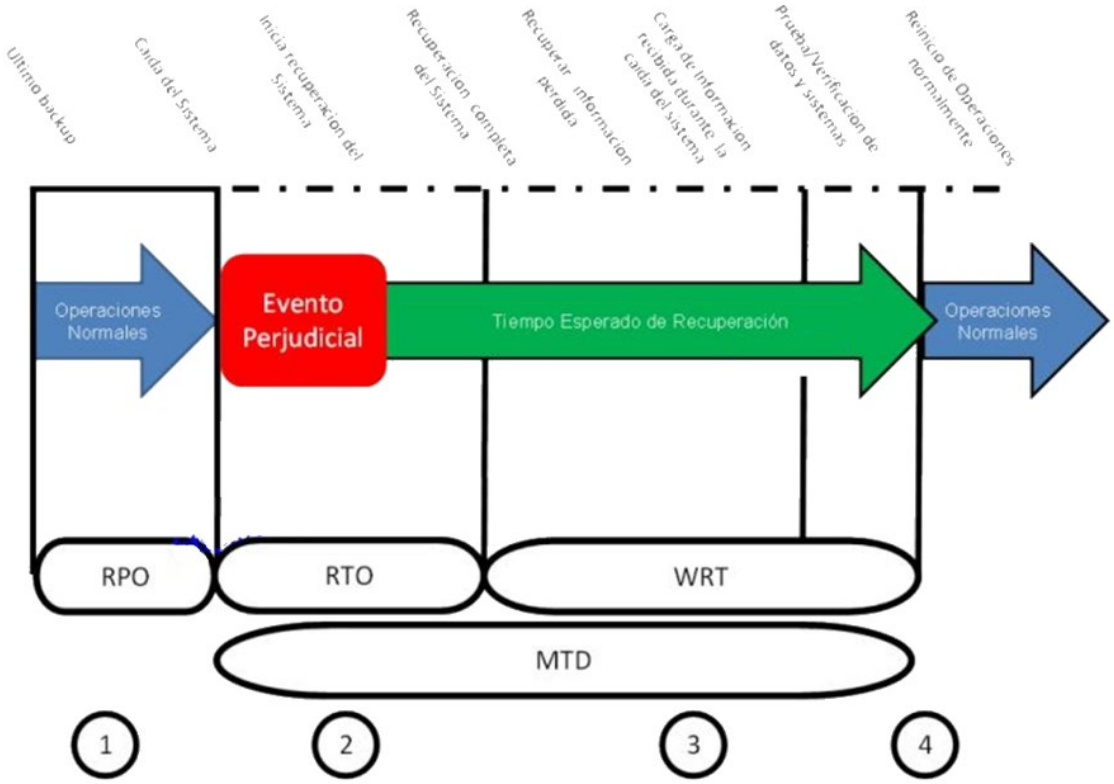


Imagen: https://seguridadinformacioncolombia.blogspot.com

Punto 1: RPO En tiempo, la máxima cantidad de información que se puede perder de acuerdo al cronograma de realización de copias de respaldo y/o necesidades de información que se presenten.

Punto 2: RTO Tiempo requerido para que los sistemas críticos de la Organización estén nuevamente operando luego de un evento disruptivo.

Punto 3: WRT Work recovery time - Tiempo requerido para recuperar la información perdida (Basado en el RPO), así como de ingresar al sistema todos los datos que se generaron durante la caída del sistema.

Punto 2 y 3: MTD tiempo de inactividad máximo tolerable - La duración del RTO + WRT

Punto 4: Pruebas, verificación e inicio normal de operaciones

Ejemplos: Podríamos tener RTO de 24 horas y RPO de 1 hora, o RTO de 2 horas y RPO de 12 horas.

Ambos valores son determinantes para el análisis del impacto empresarial y para la gestión de la continuidad del negocio, sin embargo, hay que tener en cuenta el impacto económico de las medidas de protección.

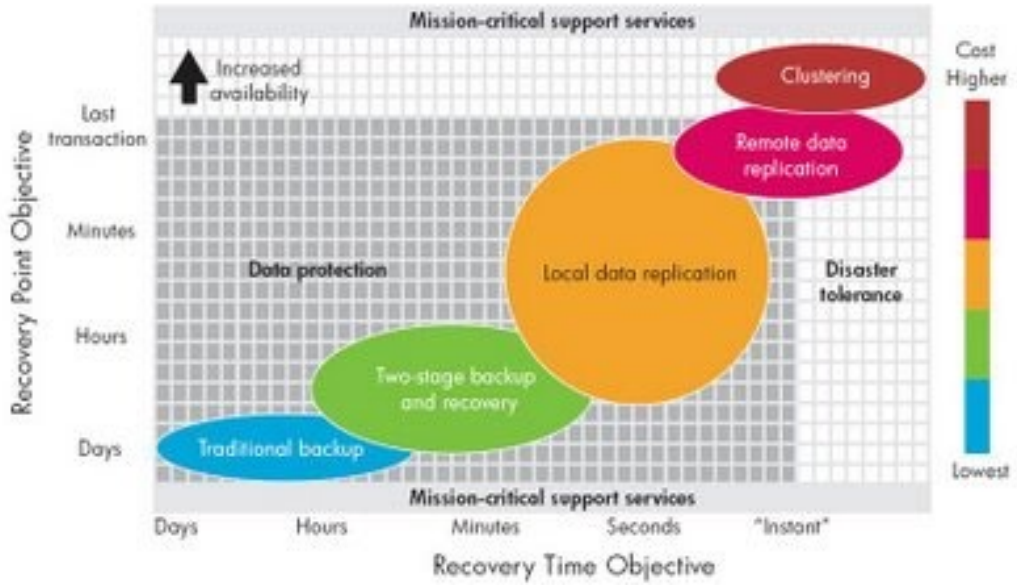


Imagen:https://www.swgreenhouse.com/conceptos-de-continuidad-de-negocio/rto-rpo

4. Desarrollar estrategias de recuperación y continuidad del negocio

En este paso se busca dejar en claro todas las medidas a poner en práctica para regresar a la operación tan pronto como sea posible, con base en una priorización derivada de la clasificación del primer punto.

5. Concientizar, capacitar y probar los planes

Un elemento necesario con relación a los planes consiste en realizar su difusión entre los miembros de la organización, especialmente entre aquellos que serán los encargados de ponerlo en ejecución en caso de ser requerido.

Además, es necesario que se lleven a cabo pruebas de este, para ello se puede hacer uso de diferentes opciones, desde una revisión de la lista de verificación (checklist) de la recuperación hasta una prueba de interrupción completa (full interruption test) donde las operaciones se interrumpen en el sitio primario y se transfieren a un sitio de recuperación.

6. Mantener y mejorar el plan de recuperación ante desastres

A partir de los resultados de la prueba de los planes se deben llevar a cabo los ajustes correspondientes para contar con documentación actualizada y apropiada a los intereses de la organización, una vez que han sido consideradas las situaciones de desastre que podrían afectarla, las actividades y recursos necesarios para restablecer las operaciones críticas.

De manera general, las organizaciones que desarrollan los planes de recuperación deberán considerar los recursos a su alcance, los servicios previamente identificados y que se desean recuperar tan pronto como sea posible, así como los tipos y severidad de las amenazas que enfrenta la organización y pueden llegar a convertirse en un problema de mayor magnitud para la misma.

Conclusión

La seguridad de la información es crucial en las organizaciones debido a varias razones.
En primer lugar, protege los activos valiosos de la organización, como datos confidenciales, propiedad intelectual y secretos comerciales, evitando su robo o exposición no autorizada.
Además, garantiza la confidencialidad, integridad y disponibilidad de los datos, lo que contribuye a mantener la confianza de los clientes y socios comerciales.

La seguridad de la información también ayuda a cumplir con las regulaciones y estándares de seguridad, evita interrupciones en la operación del negocio y minimiza los riesgos financieros y legales asociados con la pérdida o filtración de información.

En resumen, la seguridad de la información protege la reputación, la continuidad del negocio y el cumplimiento normativo, al tiempo que garantiza la toma de decisiones basada en datos confiables y promueve una cultura de responsabilidad y conciencia de seguridad en la organización.

Hemos llegado así al final de esta clase en la que vimos:

- Seguridad de la Información.
- Pilares.
- Estándares de Seguridad de la Información.
- Amenazas.
- Controles.
- DRP y BCP.

Te esperamos en la **clase en vivo** de esta semana.
No olvides realizar el **desafío semanal**.

¡Hasta la próxima clase!

Bibliografía

Laudon, J. P., & Laudon, K. C. (2012). Sistemas de información gerencial. Pearson Educación.

Guías. Recuperado el 9 de julio de 2023, de Aepd.es website: https://www.aepd.es/es/guias-y-herramientas/guias

Gascó, G. E. (2013). Seguridad informática. MACMILLAN IBERIA, S.A. ISBN EDICIÓN ELECTRÓNICA: 978-84-15991-41-0

Guías de Seguridad. Recuperado el 1 de agosto de 2023, de Europa.eu website: https://www.cert.europa.eu/static/security-guidance/TLP-WHITE-CERT-EU_Security_Guidance-22-001_v1_0.pdf

Para ampliar la información

Recuperación ante desastres RTO/RPO:
https://www.youtube.com/watch?v=EIO072-Jkg0

Cloud disaster recovery:
https://www.ionos.es/digitalguide/servidores/seguridad/cloud-disaster-recovery/

Veeam backup:
https://youtu.be/F37PkkNXnAY