IV JORNADA DE TRANSFORMACIÓN DIGITAL - 2025

GLOSARIO

SEGURIDAD DE LA INFORMACIÓN/CIBERSEGURIDAD

1) Análisis de Brechas (GAP Analysis) según ISO 27001

Un **Análisis de Brechas (GAP Analysis)** es una evaluación sistemática que compara el estado actual del Sistema de Gestión de Seguridad de la Información (SGSI) de la universidad con los requisitos de la norma internacional **ISO 27001:2022**. Su objetivo es identificar discrepancias ("brechas") para crear un plan de acción que permita alcanzar el cumplimiento normativo. Es el diagnóstico esencial que fundamenta el desarrollo de un **Plan Integral**.

2),Norma ISO 27001:2022

La norma se estructura en dos pilares principales:

1. **Cláusulas 4-10 (Los requisitos obligatorios del SGSI):** Establecen el "esqueleto" del sistema de gestión, desde el contexto de la organización hasta la mejora continua.
2. **Anexo A (Los 93 controles de seguridad):** Ofrece un catálogo de mejores prácticas para tratar los riesgos identificados, organizados en cuatro categorías: *Organizacionales, Personas, Físicas y Tecnológicas*.

Un principio fundamental es el **ciclo de mejora continua** (Planificar-Hacer-Verificar-Actuar), integrado en las cláusulas, que asegura que el SGSI se adapte y mejore constantemente.

3) Seguridad de la información

Según la norma ISO/IEC 27001:2022, la Seguridad de la Información se define como la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Este concepto fundamental, conocido como la "Tríada CID", se logra mediante la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

La Tríada CID: Las Tres Propiedades Fundamentales

Propiedad	Definición	Pregunta que Responde	Ejemplo
Confidencialidad	Garantizar que la información no sea puesta a disposición o revelada a individuos, entidades o procesos no autorizados.	¿Quién puede ver la información?	El cifrado de un documento para que solo lo abran personas con la contraseña correcta.
Integridad	Salvaguardar la exactitud y completitud de la información y los métodos de procesamiento.	¿Es la información correcta y auténtica?	Utilizar firmas digitales para asegurar que un contrato no ha sido alterado después de su firma.
Disponibilidad	Asegurar que los usuarios autorizados puedan acceder a la información y a los sistemas asociados cuando lo necesiten.	¿Puedo acceder a la información cuando la necesito?	Tener servidores en cluster y copias de seguridad para evitar tiempos de inactividad.

4) Sistema de Gestión de Seguridad de la Información (SGSI)

La norma ISO 27001 no se limita a definir estos conceptos; establece los requisitos para crear, implementar, mantener y mejorar de forma continua un Sistema de Gestión de la Seguridad de la Información (SGSI). Un SGSI es un marco de trabajo sistemático que gestiona los riesgos de seguridad de la información de toda la organización.

Los principios clave de un SGSI según ISO 27001 son:

1. **Enfoque basado en riesgos:** El núcleo del estándar. La organización debe:

   Identificar los riesgos para la confidencialidad, integridad y disponibilidad de su información.

   Evaluar estos riesgos según su probabilidad e impacto.

   Tratar los riesgos (por ejemplo, aplicando controles, aceptándolos o transfiriéndolos).

2. **Mejora continua:** El SGSI sigue el ciclo PDCA (Planificar-Hacer-Verificar-Actuar) para adaptarse constantemente a los cambios y nuevas amenazas.
3. **Compromiso de la dirección:** La alta dirección debe demostrar su liderazgo estableciendo la política de seguridad, asignando recursos y asegurando que el SGSI se integra en los procesos de la organización.

Los Controles de Seguridad (Anexo A)

La norma incluye un anexo (Anexo A) con 93 controles de seguridad organizados en 4 temas principales. Estas son medidas que una organización puede implementar para tratar sus riesgos:

- **Controles Organizativos:** Políticas de seguridad, asignación de roles y responsabilidades, gestión de proveedores.
- **Controles de Personas:** Concienciación y formación, procedimientos de disciplina.
- **Controles Físicos:** Seguridad de oficinas, controles de acceso a salas de servidores.
- **Controles Tecnológicos:** Cifrado, gestión de vulnerabilidades, controles de acceso lógico.

En resumen, para la ISO 27001:2022, la seguridad de la información es un proceso de gestión integral y continuo, respaldado por la dirección y centrado en la protección proactiva de la información a través de la Confidencialidad, Integridad y Disponibilidad.

5) Riesgos, amenazas y vulnerabilidades

En el contexto de la seguridad de la información y la ciberseguridad, riesgo, amenaza

y vulnerabilidad están estrechamente relacionados pero representan conceptos distintos.

La relación entre ellos se puede resumir en esta **fórmula** básica:

Riesgo = Amenaza x Vulnerabilidad

Amenaza (Threat)

¿Qué es? Una causa potencial de un incidente no deseado. Es algo o alguien que puede explotar una vulnerabilidad para dañar un sistema o robar información.

Característica clave: Es externa al activo que se quiere proteger. Representa el "quién" o el "qué" que podría atacar.

Ejemplos:

Un hacker intentando entrar en un sistema.
Un software malicioso (malware) como un ransomware.
Un empleado descontento que busca dañar la empresa.
Un desastre natural como un incendio o una inundación.
Un error involuntario de un usuario interno.

Vulnerabilidad (Vulnerability)

¿Qué es? Una debilidad o una falla en un sistema, procedimiento, control o diseño que puede ser explotada por una amenaza.

Característica clave: Es interna al activo que se quiere proteger. Representa el "punto débil" o la "grieta" en nuestras defensas.

Ejemplos:

Software sin actualizar (con vulnerabilidades de día cero o parches sin aplicar).
Contraseñas débiles o predeterminadas.
Falta de concienciación en los empleados (que hacen clic en enlaces de phishing).
Un firewall mal configurado.
Procedimientos de respaldo inexistentes.

Riesgo (Risk)

¿Qué es? El potencial de que ocurra un incidente que, aprovechando una vulnerabilidad, cause daño a una organización. Es la consecuencia o el impacto que preocupa a la organización.

Característica clave: Es la intersección de una Amenaza y una Vulnerabilidad. Mide la probabilidad de que un ataque ocurra y el daño que causaría.

Ejemplos (combinando los conceptos anteriores):

Amenaza: Un hacker.
Vulnerabilidad: Un servidor con un parche de seguridad sin aplicar.
Riesgo: Alto riesgo de que el hacker explote el servidor para robar datos de clientes, lo que generaría multas y daño reputacional.

Amenaza: Un incendio.
Vulnerabilidad: No tener un plan de recuperación ante desastres ni copias de seguridad en una ubicación remota.
Riesgo: Alto riesgo de perder toda la información y que la empresa no pueda seguir operando.

Analogía para entenderlo fácilmente: Imagina que quieres proteger tu casa (tu sistema de información):

Amenaza: Un ladrón (alguien que quiere causar daño).
Vulnerabilidad: Una ventana abierta (el punto débil en tus defensas).
Riesgo: La probabilidad de que el ladrón entre por la ventana y te robe tus objetos de valor, y el impacto (pérdida económica, sensación de inseguridad) que eso tendría.

Para gestionar el riesgo, puedes:

Tratar la amenaza: Aumentar la vigilancia del barrio (dificultar la acción del ladrón).
Corregir la vulnerabilidad: Cerrar y poner un buen cerrojo a la ventana (eliminar el punto débil).

Aceptar el riesgo: Decidir que el riesgo es bajo y no hacer nada.

Transferir el riesgo: Contratar un seguro para que, si te roban, te compensen.

En resumen, la gestión de riesgos en ciberseguridad consiste en identificar las amenazas, encontrar y corregir las vulnerabilidades, y así reducir el riesgo global para la organización.

6) Política de seguridad

Es un documento formal aprobado por la alta dirección de una organización que establece el marco de referencia para gestionar y proteger los activos de información.

Propósito y Objetivos

Demostrar el compromiso de la dirección con la seguridad de la información.

Establecer los lineamientos generales para proteger los activos de información.

Definir las responsabilidades de todos los miembros de la organización.

Servir como base para desarrollar procedimientos y controles específicos.

Contenido Típico de una Política de Seguridad

Según las mejores prácticas y estándares como ISO 27001, una política de seguridad generalmente incluye:

1. **Alcance**

   Especifica a quiénes aplica la política (empleados, contratistas, proveedores, etc.)

   Define los activos de información cubiertos

2. **Declaración de principios**

   Establece el compromiso de la organización con la seguridad de la información
   Reconoce la importancia de proteger la confidencialidad, integridad y disponibilidad

3. **Objetivos de seguridad**

   Protección de información crítica
   Cumplimiento de requisitos legales y contractuales
   Continuidad del negocio

4. **Roles y responsabilidades**

    Define quién es responsable de implementar y mantener la política
    Establece el rol del responsable de seguridad de la información

5. **Principios generales de seguridad**

    Clasificación de la información
    Control de acceso
    Manejo de incidentes
    Concienciación y formación

Características Esenciales

Una política de seguridad efectiva debe ser:

- Aprobada por la alta dirección ✅
- Comunicada a todo el personal ✅
- Actualizada periódicamente ✅
- Aplicable y realista ✅
- Alineada con los objetivos del negocio ✅

Ejemplo simple de Declaración de Política

"La Dirección de [Nombre de la Organización] se compromete a proteger sus activos de información mediante la implementación de controles adecuados que garanticen la confidencialidad, integridad y disponibilidad de la información, en cumplimiento con los requisitos legales y contractuales aplicables."

Importancia en el SGSI

La política de seguridad es el documento más importante de un Sistema de Gestión de Seguridad de la Información (SGSI) porque:

- Establece la postura de seguridad de la organización
- Sirve como base para la auditoría y evaluación de cumplimiento
- Orienta la asignación de recursos para seguridad
- Demuestra el compromiso formal ante clientes y partes interesadas

7) Ciberseguridad

Es la práctica de proteger sistemas, redes, programas y datos de ataques digitales, accesos no autorizados o daños.

Mientras que la "Seguridad de la Información" es un concepto más amplio que protege la información en cualquier formato (físico o digital), la ciberseguridad se enfoca específicamente en el entorno digital y cibernético.

Objetivos Principales de la Ciberseguridad

1. Proteger la infraestructura digital (servidores, redes, dispositivos).
2. Prevenir el acceso no autorizado a sistemas y datos.
3. Garantizar la confidencialidad, integridad y disponibilidad de la información digital.
4. Minimizar el impacto de los incidentes de seguridad cuando ocurren.

Ámbitos o Dominios de la Ciberseguridad

Ámbito	¿Qué protege?	Ejemplos
Seguridad de Redes	La infraestructura de red y el tráfico.	Firewalls, sistemas de detección de intrusos (IDS), VPN.
Seguridad de Aplicaciones	El software y las aplicaciones.	Pruebas de código seguro, protección contra inyecciones SQL.
Seguridad de los Endpoints	Los dispositivos de los usuarios finales.	Antivirus, protección avanzada (EDR) en computadoras y móviles.
Seguridad de los Datos	La información misma, en reposo y en tránsito.	Cifrado, máscaras de datos, controles de acceso.

Ámbito	¿Qué protege?	Ejemplos
Respuesta a Incidentes	Los procedimientos para manejar una brecha de seguridad.	Plan de contención, erradicación y recuperación.
Concienciación del Usuario	El eslabón humano, a menudo el más débil.	Formación para identificar phishing y buenas prácticas.

Ciclo de la Ciberseguridad

La ciberseguridad no es un producto, sino un proceso continuo que generalmente sigue estas fases:

1. **Identificar:** Descubrir qué activos digitales existen y qué riesgos enfrentan.
2. **Proteger:** Implementar defensas (controles) para prevenir ataques.
3. **Detectar:** Monitorizar continuamente para identificar actividades sospechosas rápidamente.
4. **Responder:** Activar el plan de respuesta ante incidentes para contener el daño.
5. **Recuperar:** Restaurar sistemas y servicios a la normalidad y aprender de lo sucedido.

8) Protocolo de respuesta ante incidentes

También conocido como Plan de Respuesta a Incidentes, es un conjunto documentado de procedimientos y acciones diseñados para detectar, contener, erradicar y recuperarse de un incidente de seguridad de manera organizada, rápida y efectiva.

Su objetivo principal es minimizar el impacto en la organización y restaurar la normalidad de las operaciones lo antes posible.

Objetivos Clave de un Protocolo de Respuesta

1. Minimizar el daño y el impacto financiero/operacional.
2. Contener la propagación del incidente.
3. Reducir el tiempo de recuperación.
4. Preservar la evidencia digital para análisis forense.
5. Mantener o restaurar la confianza de clientes y partes interesadas.
6. Cumplir con requisitos legales y regulatorios.

Fases de un Protocolo de Respuesta a Incidentes (Ciclo de Vida)

Un protocolo efectivo generalmente sigue estas 6 fases:

1. Preparación *(la fase más importante, antes de que ocurra un incidente)*

Desarrollar y mantener el protocolo documentado.
Establecer el Equipo de Respuesta a Incidentes (CSIRT) con roles definidos.
Capacitar al personal y realizar simulacros.
Implementar herramientas de detección y monitorización.

2. Detección y Análisis

Identificar potenciales incidentes mediante alertas o reportes.
Analizar el evento para confirmar si es un incidente real.
Determinar el alcance, impacto y categoría del incidente.
Recopilar evidencias iniciales.

3. Contención

Implementar medidas para detener la propagación del incidente.

Estrategias:

. Contención a corto plazo: Acciones inmediatas (desconectar un sistema).
. Contención a largo plazo: Soluciones más permanentes.

4. Erradicación

Identificar y eliminar la causa raíz del incidente.
Ejemplos: Eliminar malware, parchear vulnerabilidades, remover cuentas comprometidas.

5. Recuperación

Restaurar sistemas y servicios a la normalidad.
Verificar que los sistemas estén limpios y seguros.
Restaurar datos desde backups limpios.
Monitorear intensivamente los sistemas recuperados.

6. Lecciones Aprendidas *(fase crucial para la mejora continua)*

Realizar una revisión post-incidente.
Documentar qué salió bien y qué puede mejorarse.
Actualizar el protocolo y los controles de seguridad.
Compartir conocimientos con toda la organización.

Componentes Esenciales del Protocolo

Componente	Descripción
Equipo de Respuesta (CSIRT)	Grupo multidisciplinario con roles definidos (Líder, Investigadores, Comunicaciones, Legal).
Matriz de Clasificación	Criterios para categorizar incidentes por severidad (Bajo, Medio, Alto, Crítico).
Procedimientos Específicos	Instrucciones detalladas para diferentes tipos de incidentes (phishing, ransomware, denegación de servicio).
Plantillas de Comunicación	Comunicados pre-aprobados para diferentes audiencias (clientes, prensa, autoridades).

Componente	Descripción
Lista de Contactos	Números y contactos clave (directivos, legal, autoridades policiales, aseguradora).

Ejemplo de Flujo de Actuación Rápida

1. DETECTAR → Alerta de sistema antivirus o usuario reporta anomalía.
2. CLASIFICAR → Equipo determina severidad (Ej: Alto - Ransomware).
3. ACTIVAR CSIRT → Se convoca al equipo completo.
4. CONTENER → Desconectar equipos afectados de la red.
5. INVESTIGAR → Analizar origen, vectores de ataque, sistemas comprometidos.
6. COMUNICAR → Informar a dirección legal y alta dirección.
7. ERRADICAR → Eliminar malware, cambiar contraseñas, parchear sistemas.
8. RECUPERAR → Restaurar sistemas desde backups limpios.
9. DOCUMENTAR → Registrar todas las acciones y lecciones aprendidas.

Importancia en el Marco de Ciberseguridad

Un protocolo de respuesta es fundamental porque:

Reduce el tiempo de respuesta de días/horas a minutos.
Evita el pánico y la toma de decisiones erróneas bajo presión.
Cumple con requisitos de estándares como ISO 27001, NIST, CIS Controls.
Demuestra diligencia debida a clientes, reguladores y aseguradoras.
