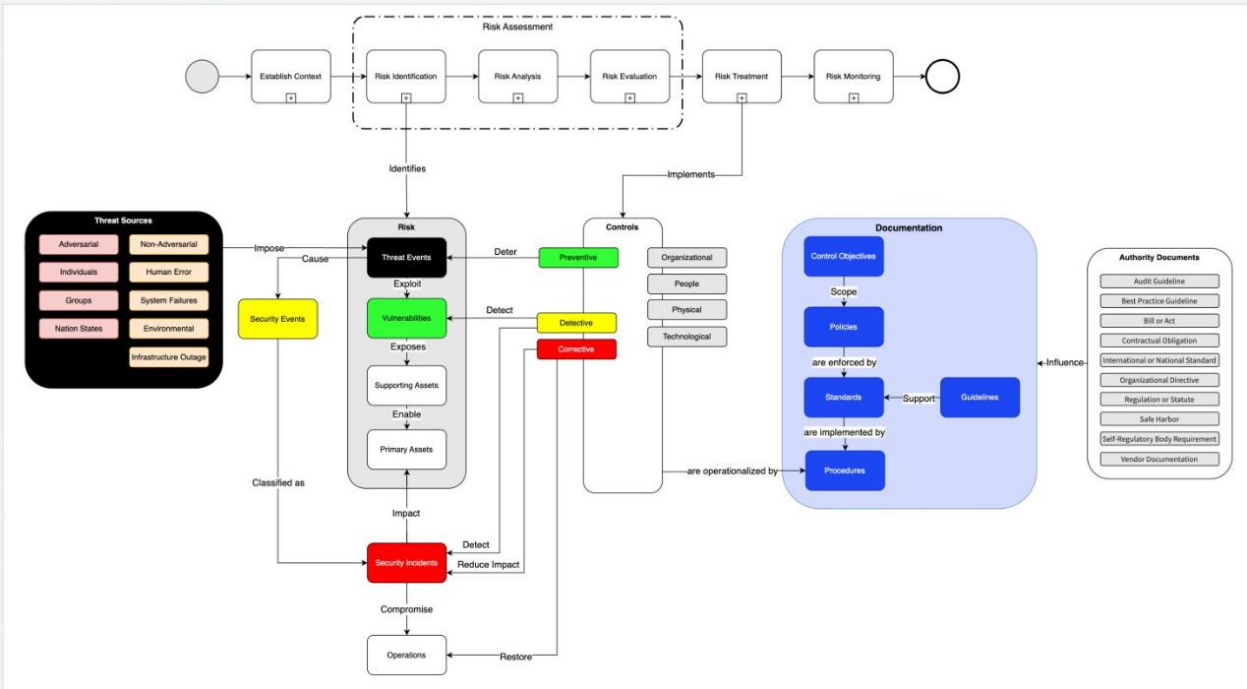
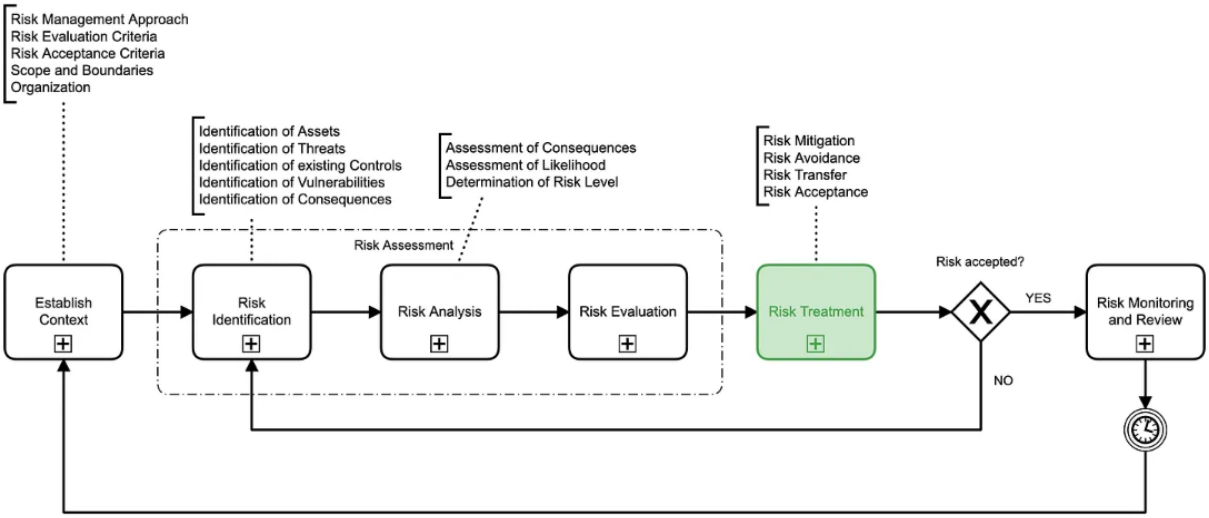
Las Interacciones de un SGSI basado en ISO 27001:2022

Los sistemas de gestión de seguridad de la información (SGSI) constan de varios elementos interconectados. Este artículo pretende servir como hoja de ruta, aprovechando un diagrama detallado para desentrañar las complejas relaciones entre estos componentes. Desarrollar una comprensión sólida de cómo se interrelacionan estos elementos le ayudará a proteger los activos de su organización de forma más eficaz.



La gestión de la seguridad de la información sigue un enfoque basado en riesgos.



Establecer el Contexto

Antes de sumergirse en la identificación o análisis de riesgos, es fundamental establecer el contexto en el que opera la organización. Esto implica comprender los factores internos y externos que pueden afectar los activos de la organización. Establecer el contexto proporciona una lente a través de la cual se pueden identificar y evaluar los riesgos.

Identificación de riesgo

Esta etapa implica identificar qué podría salir mal, cómo y por qué. De manera similar a detectar los jugadores clave y las estrategias de un equipo contrario, la identificación de riesgos consiste en reconocer las fuentes de amenazas, los eventos de amenazas, las vulnerabilidades y los activos en riesgo. Esto proporciona una lista completa de riesgos que deben analizarse más a fondo.

Análisis de riesgo

Una vez identificados los riesgos, es necesario analizarlos para comprender su naturaleza, probabilidad e impacto. El análisis de riesgos proporciona una visión detallada de cada riesgo, ayudando a la organización a priorizarlos. Esto ayudará a las organizaciones a comprender qué escenarios tienen más probabilidades de ocurrir y cuán dañinos pueden ser si no se tratan adecuadamente.

Evaluación de riesgo

La evaluación de riesgos implica comparar los riesgos analizados con criterios predefinidos para decidir qué riesgos deben tratarse. Se puede considerar que esto decide qué jugadas del

oponente necesitan el mayor enfoque defensivo. La evaluación ayuda a asignar recursos de manera más efectiva al centrarse en los riesgos más críticos.

Tratamiento de riesgos

Esta etapa implica seleccionar una o más opciones para modificar los riesgos e implementar esas opciones. El tratamiento del riesgo puede implicar evitarlo, modificarlo, compartirlo o retenerlo. Tenga en cuenta que el impacto de los riesgos no se puede mitigar a cero. Siempre habrá un riesgo residual, a menos que pueda evitarse por completo.

Monitoreo de riesgos

Por último, pero no menos importante, los riesgos deben ser monitoreados y revisados continuamente para evaluar la efectividad del proceso de gestión de riesgos e identificar cualquier cambio en el panorama de riesgos. Esto equivale a hacer ajustes en el tiempo de juego en función de qué tan bien está funcionando la estrategia inicial.

Fuentes de amenazas: el punto de partida

Según el Instituto Nacional de Estándares y Tecnología (NIST), las Fuentes de Amenazas se definen como el origen de eventos adversos que potencialmente podrían dañar los activos y operaciones de una organización. Estas fuentes pueden ser intencionales o no y pueden provenir de una variedad de lugares, como la naturaleza, individuos u organizaciones.

NIST clasifica las fuentes de amenazas en dos tipos principales:

1. Adversariales: Son acciones intencionales tomadas por individuos, grupos u organizaciones con la motivación de causar daño o explotar vulnerabilidades. Las amenazas adversas incluyen piratas informáticos, terroristas, amenazas internas e incluso competidores.
2. No adversariales: son acciones no intencionales o eventos naturales que podrían dañar potencialmente a una organización pero que carecen de una intención específica. Los ejemplos incluyen desastres naturales como inundaciones o terremotos, eliminación accidental de datos por parte de un empleado o fallas del sistema debido a un error.

Al comprender la naturaleza y los tipos de fuentes de amenazas según las define el NIST, las organizaciones pueden prepararse mejor y mitigar los diversos riesgos que pueden afectarlas.

De las fuentes de amenazas a los eventos de amenazas

Las fuentes de amenazas imponen **Eventos de amenazas**, que son acciones o incidentes específicos que potencialmente pueden dañar a su organización. Por ejemplo, un pirata informático (fuente de amenaza) podría intentar ingresar a su red (evento de amenaza).

Vulnerabilidades: los puntos débiles

Las vulnerabilidades son los puntos débiles de su sistema donde los eventos de amenazas pueden colarse. Estos podrían ser software desactualizado, contraseñas débiles o incluso un miembro del personal que no está capacitado en protocolos de seguridad.

Activos de respaldo

Las vulnerabilidades a menudo exponen los **activos de soporte**, que son los diversos componentes de su sistema que no son fundamentales para su negocio pero que siguen siendo importantes. Estos pueden incluir:

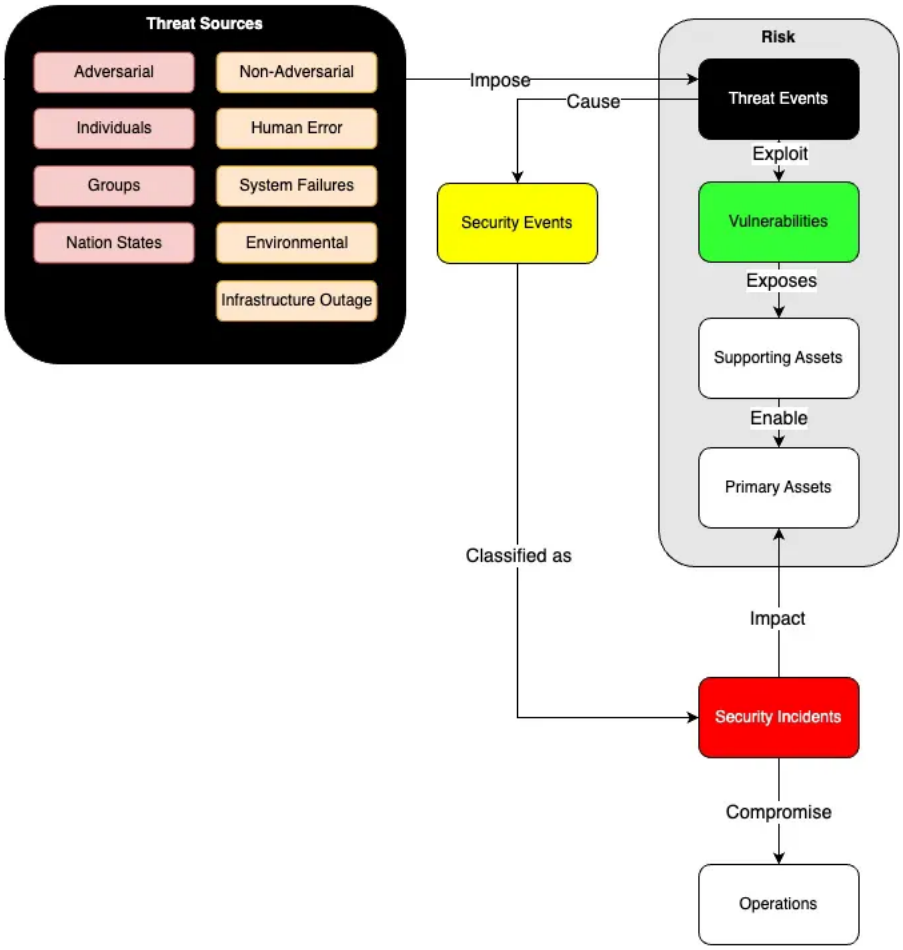
- **Hardware**: Servidores, computadoras
- **Software**: Aplicaciones, bases de datos
- **Red**: conexión a Internet, firewalls
- **Personal**: Empleados, contratistas
- **Sitios**: ubicaciones físicas como oficinas o centros de datos.

Activos primarios

Los **activos primarios** son lo que su empresa necesita absolutamente para funcionar. Estos pueden ser sus principales procesos comerciales o piezas de información cruciales. Los Activos de Apoyo permiten que estos Activos Primarios funcionen. Por ejemplo, su red (Activo de soporte) habilita su plataforma de ventas en línea (Activo principal).

La reacción en cadena: eventos e incidentes de seguridad

Cuando un evento de amenaza explota una vulnerabilidad, provoca un **evento de seguridad**. No todos los eventos de seguridad son desastrosos; algunos podrían contenerse fácilmente o ser inofensivos. Sin embargo, cuando un Evento de Seguridad tiene un impacto negativo significativo, se clasifica como un **Incidente de Seguridad**. Estos incidentes pueden comprometer sus operaciones y, en última instancia, sus activos principales.



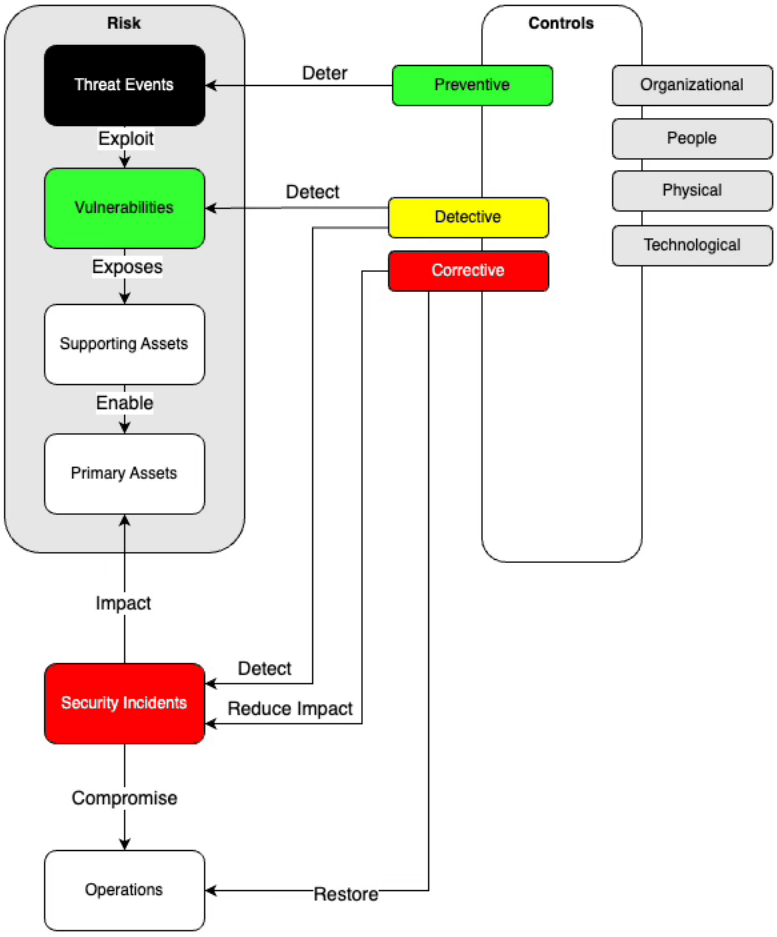
Implementación de controles mediante el tratamiento de riesgos

Una vez que haya identificado sus fuentes de amenazas, analizado sus vulnerabilidades y evaluado sus riesgos, el siguiente paso es implementar controles para gestionar estos riesgos de manera efectiva. En el ámbito de la seguridad de la información, los controles son salvaguardias o contramedidas para evitar, detectar, contrarrestar o minimizar los riesgos de seguridad de la propiedad física, la información, los sistemas informáticos u otros activos.

Tipos de controles basados en el tratamiento de riesgos

Los controles generalmente se determinan durante la fase de Tratamiento de Riesgos y se pueden clasificar en tres tipos principales:

1. **Controles Preventivos**: Son medidas diseñadas para evitar que ocurra una actividad no deseada o no autorizada. Actúan como la primera línea de defensa en la mitigación de riesgos. Por ejemplo, una autenticación sólida del usuario puede evitar el acceso no autorizado.
2. **Controles de detección**: Estos controles tienen como objetivo detectar y alertar cuando ocurre una actividad no autorizada o no deseada. No impiden una acción, pero pueden desencadenar una alerta o iniciar medidas correctivas. Un ejemplo serían los sistemas de detección de intrusos que notifican a los administradores sobre actividades sospechosas.
3. **Controles correctivos**: entran en juego después de que ha ocurrido un evento de amenaza, con el objetivo de minimizar el impacto y devolver el sistema a su estado seguro. Las copias de seguridad de datos y los planes de recuperación del sistema son ejemplos de controles correctivos.


Risk
Threat Events
Exploit
Vulnerabilities
Exposes
Supporting Assets
Enable
Primary Assets
Impact
Security Incidents
Compromise
Operations
Deter
Detect
Reduce Impact
Restore
Controls
Preventive
Detective
Corrective
Organizational
People
Physical
Technological