SEGURIDAD DE LA INFORMACIÓN (INFOSEC) O CIBERSEGURIDAD

Es la protección de los datos sobre robos, ataques o daños.

La seguridad de la información tiene 3 propiedades conocidas como la "triada CIA o AIC":

Confidencialidad
Integridad
Disponibilidad
No Repúdio

El **NO REPUDIO** es la capacidad de demostrar o probar la participación de las partes tanto del emisor como el receptor de un mensaje, mediante su identificación, en una comunicación o en la realización de una determinada acción.

MARCOS DE CIBERSEGURIDAD

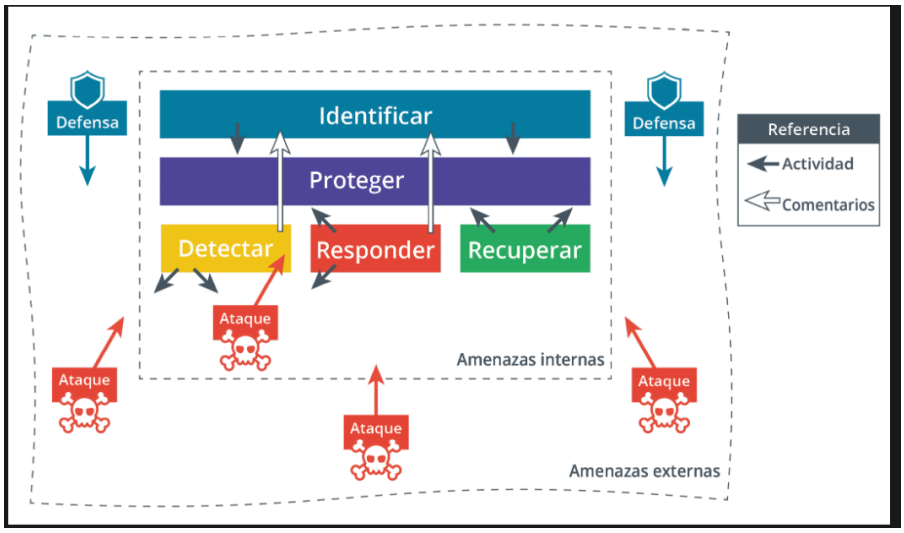
Se refieren a normas las cuales se pueden aplicar en las organizaciones con el objetivo de llevar una correcta implementación de la seguridad en una organización

Marcos conocidos:

ISO/IEC 27001 – Organización Internacional de Normalización
NIST Cibersecurity Famework (CSF)
ISACA Information Systems Audit and Control Association
CIS Centro de Seguridad de Internet
ENISA Agencia de Ciberseguridad de la Unión Europea

Las tareas de l seguridad de la información pueden clasificarse en 5 Funciones (Probablemente Varíen despendiendo del marco utilizado*):

Identificar (Amenazas y Vulnerabilidades) Actua en Pro de Proteger
Proteger (De Amenazas y Vulnerabilidades)
Detectar (Ataques y Amenazas y Vulnerabilidades)
Responder (A Ataques y responder es proteger)
Recuperar (Es un método de protección)



ANALISIS DE DEFICIENCIAS/BRECHAS

Es un Metodo para identificar las áreas donde una organización no cumple con los estándares, políticas, mejores prácticas o requisitos regulatorios establecidos para la seguridad de la información.

El **análisis de deficiencias** muestra la **cantidad de controles** recomendados que no se implementaron por función y **categoría**; más los riesgos para **la confidencialidad, integridad y disponibilidad** de los controles faltantes; y la fecha de remediación objetivo

Cada una de las **funciones** de **Seguridad de la información** tienen **controles de seguridad** los cuales deben ser cumplidos

CONTROL DE ACCESO

Un sistema de **control de acceso** garantiza que un sistema de información cumpla con los objetivos de la **tríada de CIA**.

El **control de acceso** moderno generalmente se **implementa** como un sistema de **gestión de identidad y acceso** (IAM). La IAM comprende cuatro procesos principales:

- **Identificación**
- **Autenticación**
- **Autorización**
- **Registro**

CLASIFICACIÓN, TIPOS O CATEGORIAS DE LOS CONTROLES DE SEGURIDAD

Un **control de seguridad** es una medida o mecanismo implementado para **proteger la integridad, confidencialidad y disponibilidad** (**La Triada CIA**) de los sistemas, datos y recursos dentro de una organización.

Una serie de acciones o medidas que buscan proteger a una empresa o organización de los ciberataques y la pérdida o robo de datos.

Los controles se pueden dividir en 4 grandes categorías en función de la forma en que se implementa el control:

Gerencial

Supervisa el sistema de información.

- **Identificación de riesgos**
- **Una herramienta que permita evaluar y seleccionar otros controles de seguridad**.
- Políticas de seguridad de la información

Operacional

Es ejecutado, principalmente, por personas.

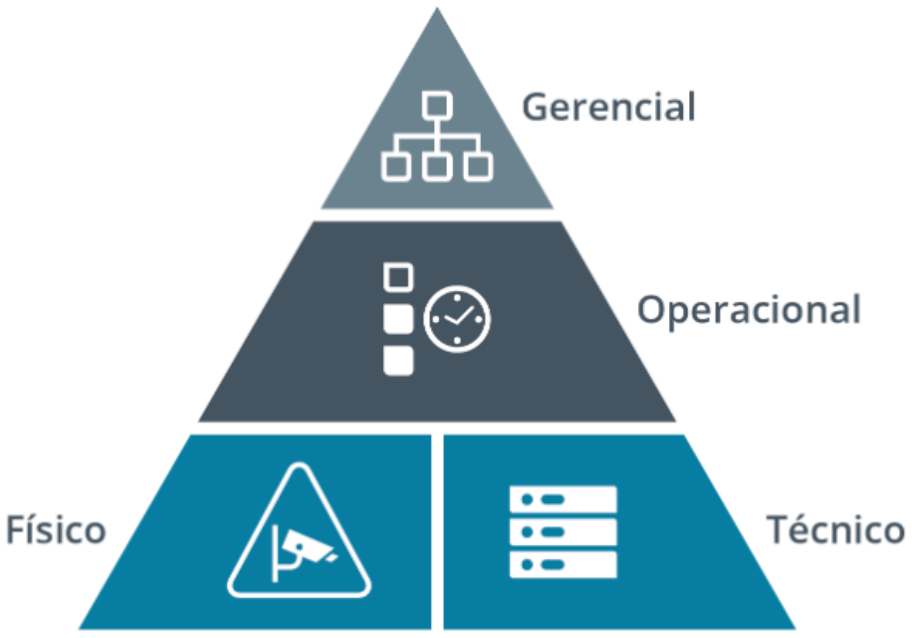
- **Guardias de seguridad**
- **los programas de capacitación**.

Técnico

- los cortafuegos
- El software antivirus
- los modelos de control de acceso al sistema operativo
- Sistemas de detección y prevención de intrusos (IDS/IPS)

Físico

Los controles como **alarmas**, **puertas de enlace**, **cerraduras**, **iluminación** **y** **cámaras de seguridad** que disuaden y detectan el acceso a las instalaciones y al hardware se suelen colocar en una categoría diferente a la de los controles técnicos.



TIPOS FUNCIONALES, CLASIFICACION O CATEGORIAS DE CONTROLES DE SEGURIDAD SEGÚN SU FUNCION

Además de como una **categoría**, un control de seguridad puede definirse **según el objetivo o la función** que realiza:

Preventivo

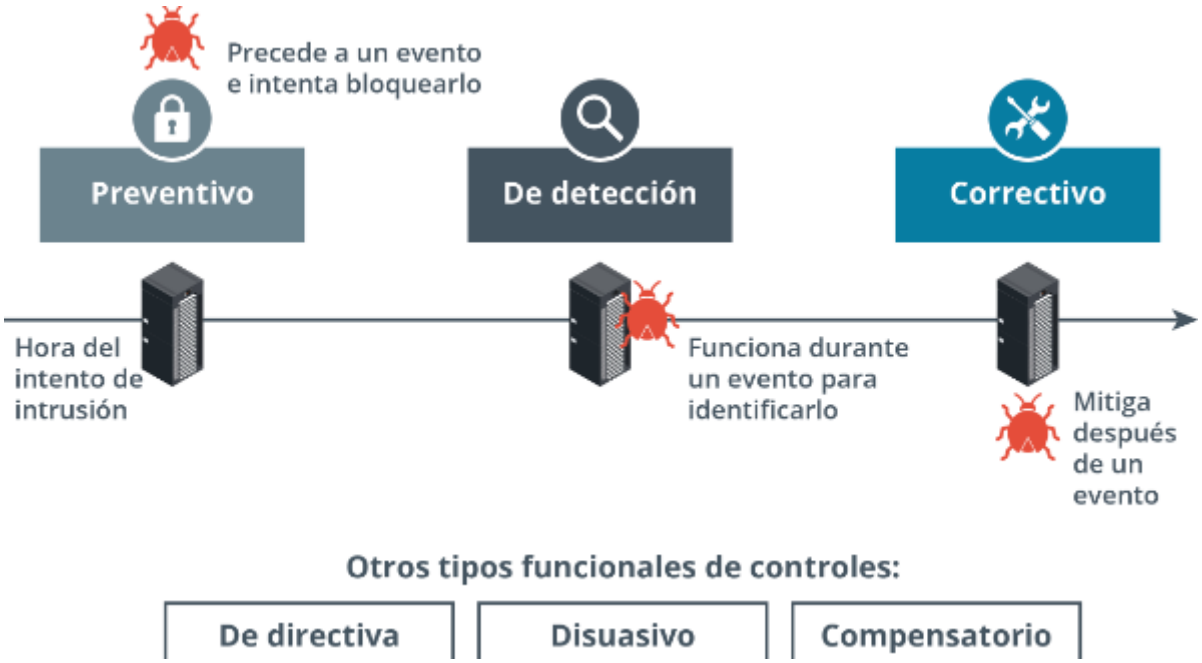
- El uso de personal cualificado
- Segregación de tareas (División de Tarea)
- Procedimientos de autorización
- Procedimientos de controles de acceso
- Cortafuegos o barreras físicas.

De detección/Detectivo

- Auditorías internas
- Revisiones
- Monitorización de logs (registros)
- Puntos de control en cadena de trabajo o los mensajes de error.

Correctivo/ De Correccion

- Plan de recuperación ante desastres
- Plan de respuesta ante incidentes
- Procedimientos de copias de seguridad.



Si bien la mayoría de los controles pueden clasificarse funcionalmente (o Segun su Funcion) como preventivos, de detección o correctivos, existen algunos otros tipos que pueden utilizarse para definir otros casos:

De directiva/Direccional

Se enfocan en proteger el acceso y movimiento dentro de una organización o instalación y hace cumplir una regla de comportamiento.

- El **contrato de un empleado** establecerá procedimientos disciplinarios o causas de despido si no cumple con las políticas y procedimientos.
- Los programas de capacitación y concientización también pueden considerarse controles directivos.

- Controles de acceso físico

Disuasivo

- Cámaras de videovigilancia
- Señales de advertencia

Compensatorio

Consisten en medidas alternativas que se utilizan para mitigar una debilidad o vulnerabilidad en un sistema cuando no se puede cumplir con un requisito o control establecido.

- Un ejemplo: Aislar Completamente el sistema vulnerable para evitar acceso a la explotación de la vulnerabilidad

FUNCIONES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

Director de Tecnologías de información (CIO) Tiene La responsabilidad general de la función de TI.

Director de Recursos tecnológicos (CTO) Tiene un rol más específico, garantizar el uso eficaz de los productos y soluciones de TI nuevos y emergentes para lograr los objetivos comerciales.

Director de Seguridad (CSO) o **Director de Seguridad de la información (CISO)**. Se le asigna la responsabilidad interna de la seguridad puede asignarse a un departamento dedicado

Los administradores de sistemas y redes Tienen la responsabilidad de implementar, mantener y monitorear la política.

COMPETENCIAS DE LA SEGURIDAD DE LA INFORMACIÓN

Los **profesionales de TI** que desempeñan una función con responsabilidades en materia de seguridad deben ser competentes en una amplia gama de disciplinas, desde el diseño de redes y aplicaciones hasta **las adquisiciones y los recursos humanos (RR. HH.).**

UNIDADES DE NEGOCIO DE SEGURIDAD DE LA INFORMACIÓN

Un **centro de operaciones de seguridad (SOC)** es un lugar donde los profesionales de la seguridad monitorean y protegen los activos de información críticos en otras funciones comerciales, como finanzas, operaciones, ventas/marketing, etc. Debido a que los SOC pueden ser difíciles de establecer, mantener y financiar, por lo general, son empleados por corporaciones más grandes, como una agencia gubernamental o una empresa de atención médica.

Desarrollo y operaciones (DevOps) DevOps se enfoca en la integración y colaboración entre los equipos de desarrollo y operaciones para acelerar la entrega de software. **DevSecOps** añade la seguridad como una responsabilidad compartida en todo el ciclo de vida del desarrollo, integrando prácticas de seguridad en cada etapa del proceso DevOps.

Equipo de respuesta a incidentes de seguridad informática (CSIRT)
Equipo de respuesta a emergencias informáticas (CERT) Dedicado es un punto de contacto único para la notificación de incidentes de seguridad. Esta función puede estar a cargo del SOC o puede establecerse como una unidad de negocio independiente.

RESUMEN DEL RESUMEN DE COMTIAP ACADEMY +

Usted debería poder comparar y contrastar los **controles de seguridad** por medio de categorías y tipos funcionales. También debería ser capaz de explicar cómo se utilizan los **conceptos y marcos generales de seguridad** para desarrollar y validar las **políticas de seguridad** y la **selección de controles**.

DIRECTRICES PARA RESUMIR LOS CONCEPTOS DE SEGURIDAD Y LOS CONTROLES DE SEGURIDAD

Siga estas directrices cuando evalúe el uso de controles y marcos de seguridad en su organización:

Cree una declaración de misión de seguridad y políticas de apoyo que enfaticen la importancia de la **tríada de CIA**: confidencialidad, integridad y disponibilidad.

Asigne funciones para que las tareas y responsabilidades de seguridad se entiendan claramente y que los impactos en la seguridad se evalúen y mitiguen en toda la organización.

Considere la posibilidad de crear unidades de negocio, departamentos o proyectos para respaldar la función de seguridad, como un SOC, CIRT y DevSecOps.

Identifique y evalúe las leyes y regulaciones de la industria que imponen requisitos de cumplimiento a su negocio.

Seleccione un marco que cumpla con los requisitos de cumplimiento y las necesidades comerciales de su organización.

Cree una matriz de controles de seguridad que estén vigentes actualmente para identificar categorías y funciones; considere la posibilidad de implementar controles adicionales para cualquier capacidad inigualable.

Realice un análisis de deficiencias para evaluar las capacidades de seguridad frente a los requisitos del marco e identifique objetivos para desarrollar competencias adicionales de ciberseguridad y mejorar la garantía general de la seguridad de la información.