MEDIDAS DE PROTECCIÓN Y SU CLASIFICACIÓN

Medidas Preventivas

Evitar que ocurran incidentes de seguridad

Medidas Detectivas

Identificar la ocurrencia de un incidente de seguridad de manera temprana.

Medidas Correctivas

Responder a un incidente de seguridad y minimizar sus consecuencias.

Medidas Físicas

Control de acceso a instalaciones, protección de dispositivos, seguridad de centros de datos.

MEDIDAS PREVENTIVAS

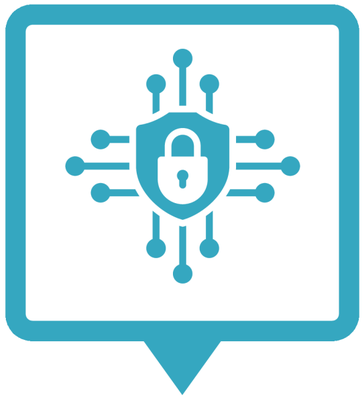
Su objetivo es evitar que ocurran incidentes de seguridad.

Controles de Acceso

Restricción del acceso a sistemas y datos a usuarios autorizados.

Capacitación

Educación de los usuarios en temas de seguridad informática.



Cifrado

Protección de datos en tránsito y en reposo mediante algoritmos criptográficos.

Políticas de Seguridad

Establecimiento de normas claras sobre el uso de los sistemas informáticos.

Segmentación de redes

División de la red en segmentos más pequeños para limitar la propagación de ataques.

MEDIDAS DETECTIVAS

Su objetivo es identificar la ocurrencia de un incidente de seguridad de manera temprana.

Sistemas de detección de intrusiones (IDS)

Monitoreo del tráfico de red en busca de actividad sospechosa.

Logs de seguridad

Registro de eventos y actividades en los sistemas para su posterior análisis.

Análisis de vulnerabilidades

Identificación de debilidades en los sistemas y aplicaciones.

Monitoreo de seguridad

Vigilancia continua de los sistemas y redes para detectar anomalías.

Análisis de comportamiento de usuarios y entidades

Monitorea continuamente las acciones de los usuarios y entidades dentro de un sistema para identificar patrones de comportamiento inusuales o anómalos.

MEDIDAS CORRECTIVAS

Su objetivo es responder a un incidente de seguridad y minimizar sus consecuencias.

Planes de respuesta a incidentes

Procedimientos detallados para responder a diferentes tipos de incidentes.

Restauración de datos

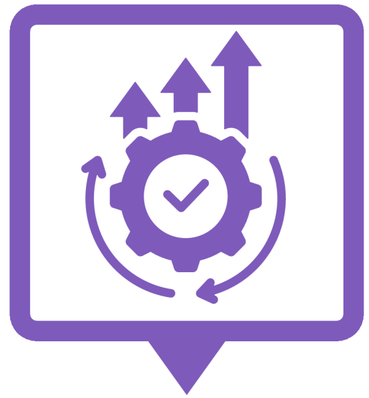
Recuperación de datos a partir de copias de seguridad.

Análisis forense

Investigación de incidentes para determinar su causa y alcance.

Parcheo de sistemas

Aplicación de parches de seguridad para corregir vulnerabilidades explotadas.



Aprendizaje y Mejora

Analizar los procesos existentes y identificar las áreas que necesitan ser mejoradas.

MEDIDAS FÍSICAS

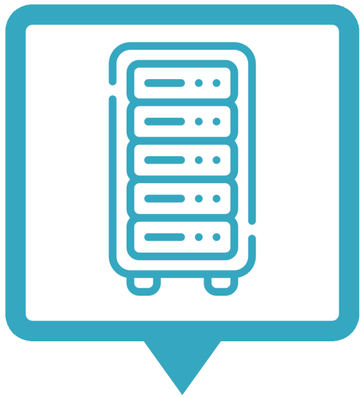
Su objetivo es proteger los activos físicos que soportan los sistemas informáticos, como equipos, instalaciones y datos físicos

Control de Acceso Físico

Ya sea a través de sistemas de acceso como reconocimiento facial, huella dactilar o tarjetas de acceso

Protección de Equipos

Fijación de equipos a superficies para evitar su desplazamiento o robo, protector contra sobretensiones.



Protección de Datos Físicos

Uso de armarios o salas seguras para almacenar dispositivos de almacenamiento y documentación confidencial.

Protección de las Instalaciones

Cercas, muros, rejas y otros obstáculos para delimitar el perímetro, detección de intrusos en áreas restringidas.

Controles Ambientales

Mantenimiento de una temperatura y humedad adecuadas para proteger los equipos, protección contra cortes de energía y fluctuaciones de voltaje.