La Ciberseguridad como parte del nuevo paradigma de la seguridad física

Área de Trabajo Ciberseguridad – Hitos alcanzados en 2020

Enero - Diciembre 2020

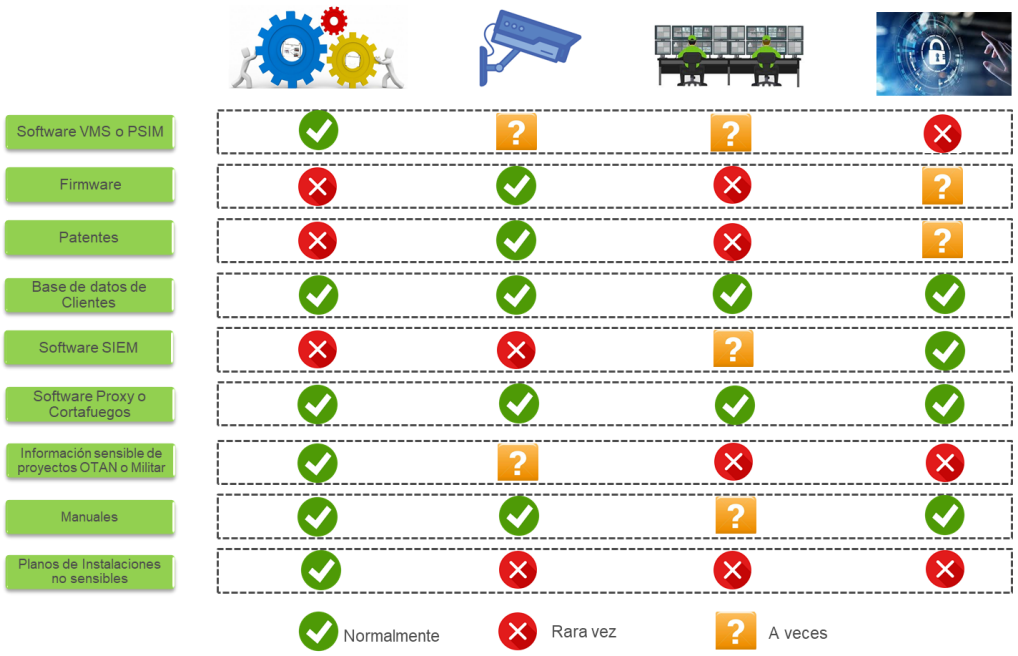
Dinamizando la Industria de la Seguridad

Asociación Española de empresas de Seguridad

Desarrollo de Hitos 2020

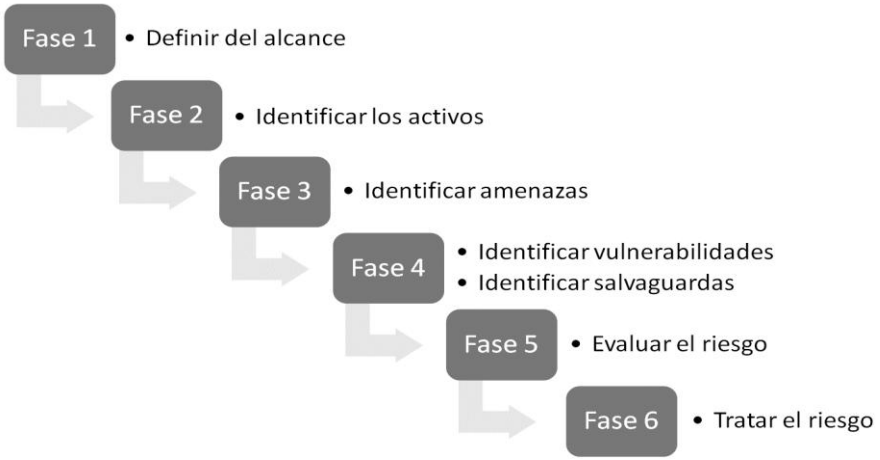
Clasificar los activos IT de las empresas

Establecer niveles de categorización de la información comunes



Desarrollo de Hitos 2020

Establecer una metodología de riesgos común



Determinar los elementos mínimos para la correcta gestión de incidentes

Cualitativo	Cuantitativo	Descripción
Bajo	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio	2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto	3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año.
Media	2	La amenaza se materializa a lo sumo una vez cada mes.
Alta	3	La amenaza se materializa a lo sumo una vez cada semana.

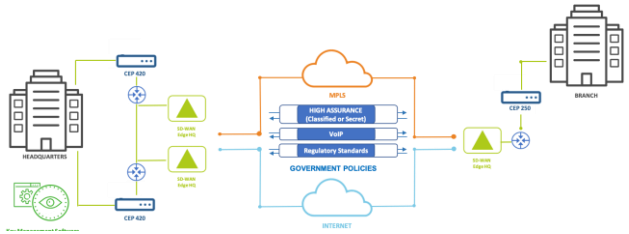
Ciberseguridad en redes de seguridad física

Protección por defecto: (no recomendable)

Políticas de ciberseguridad en sistemas de CCTV

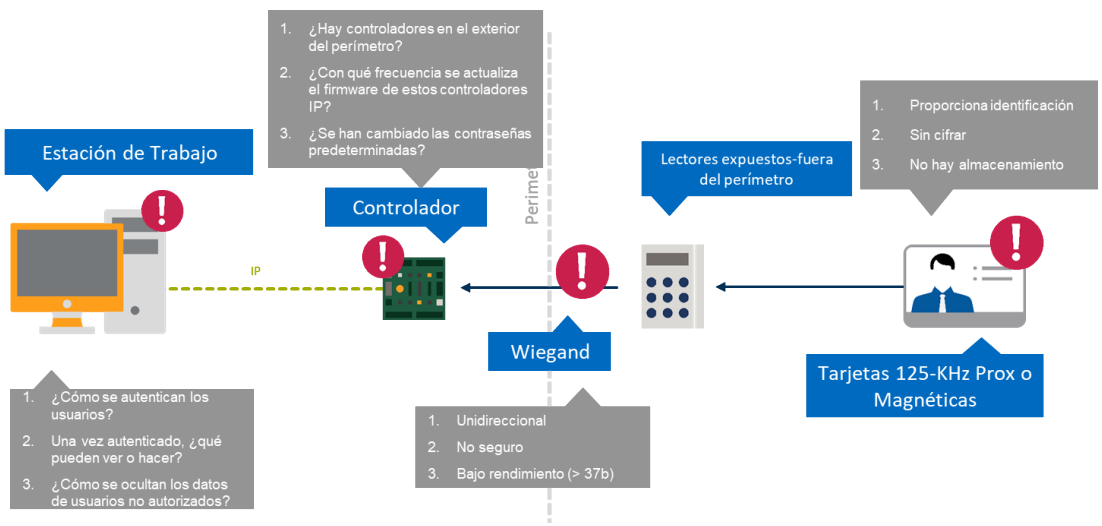
La mayor parte de los sistemas de CCTV comerciales ejecutan una pequeña versión linux/unix susceptible a un barrido de IPs buscando Telnet/SSH con contraseñas fáciles, para entrar en el sistema y colocar un binario ELF malicioso (como por ejemplo .btce) con el que seguir atacando a otros sistemas, efectuar DDoS o cualquier otra acción maliciosa.

El cifrado proporciona la última línea de defensa óptima para la protección de los datos generados por CCTV. Las redes de CCTV suelen tener un ancho de banda considerable (100Mbps - 1Gbps) y, debido a que el video se transmite en alta definición y en tiempo real, son sensibles a la latencia y la sobrecarga del cifrado.



La encriptación de alta seguridad supone emplear elementos software y hardware. Según lo recomendado por los líderes en seguridad de datos y analistas de cifrado esta es la solución más segura que sin aportar latencia permite ser un sistema verdaderamente robusto y proporcionar protección de datos a largo plazo.

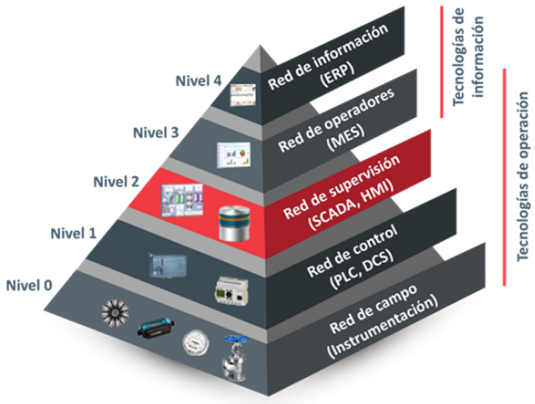
Políticas de ciberseguridad en los sistemas de control de acceso



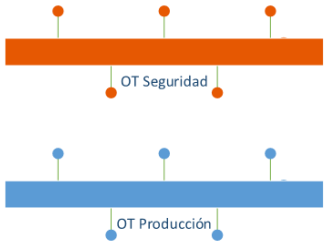
El Protocolo de Dispositivo Supervisado Abierto (OSDP) es un estándar que ha sido desarrollado por la Asociación de la Industria de Seguridad (SIA) para ofrecer comunicaciones de control de acceso más seguras. Este protocolo funciona en varios tipos de lectores, controladores y software, y se ha desarrollado como una forma de mejorar los problemas de seguridad que a menudo se enfrentan con otros sistemas heredados.

Además de la seguridad mejorada, mejora la interoperabilidad entre el control de acceso y los dispositivos de seguridad, a través de la comunicación bidireccional. Para mantener su enfoque en la seguridad, se refina constantemente, con OSDP v2.1.7 actualmente ganando reconocimiento como estándar por el American National Standards Institute (ANSI).

Ciberseguridad en entornos SCADA



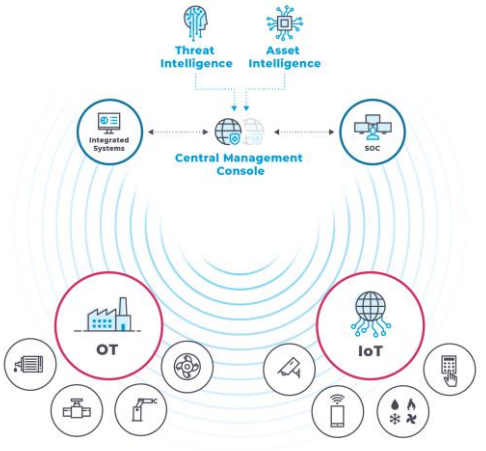
Jerarquía de niveles de automatización industrial, según la norma ISA 99/IEC62443



Alternativas

¿En que nivel?

El escenario ideal en un entorno SCADA es aquel en el que no existe ninguna conexión con ningún otro sistema, es decir, el sistema esta aislado. Este escenario no es siempre posible por, entre otros motivos, el uso de tecnologías TI, la monitorización centralizada de dependencias separadas geográficamente, el uso generalizado de Internet y la necesidad de soporte remoto de terceros.



Ciberseguridad en las soluciones de integración

Autenticación

Aproveche varios métodos de autenticación, autorización y aplicación de contraseñas

RGPD

Proteja la identidad de cualquier persona capturada en vídeo en directo y grabado

Cifrado

Cifrar completamente los datos transmitidos y almacenados dentro de nuestros sistemas

Auditoría

ISMS auditados que cumple con varios estándares gubernamentales y de la industria