PERSONAL TÉCNICO

Dispositivos IoT en el entorno empresarial

básico

Acceso seguro al dispositivo:

Como administrador de dispositivos IoT utilizas una contraseña fuerte y habilitas siempre que sea posible el doble factor de autenticación en todos los perfiles de la organización.

Política de actualización:

Elaboras una política de actualización de los dispositivos IoT que contempla los procedimientos necesarios para corregir las últimas vulnerabilidades descubiertas y tenga en cuenta las últimas funcionalidades implementadas por el fabricante. Además, incluyes los dispositivos IoT como parte de la política de actualizaciones de software.

Servicios y permisos mínimos:

Activas únicamente los servicios y permisos precisos para cumplir con sus funciones, deshabilitando el resto.

Restricciones de acceso:

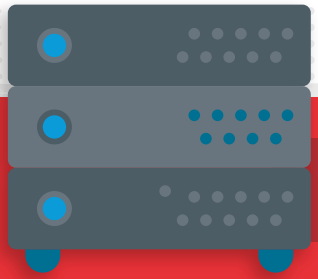
Limitas el acceso físico a los dispositivos para evitar manipulaciones indebidas.

Estar al día de las amenazas:

Estás informado de las distintas campañas utilizadas por los ciberdelincuentes para conseguir acceso a los dispositivos IoT.

Evitar errores humanos:

Formas a los empleados en ciberseguridad para minimizar los riesgos relativos al uso de esta y otras tecnologías.



PERSONAL TÉCNICO

Dispositivos IoT en el entorno empresarial

avanzado

Comunicaciones seguras:

Empleas técnicas criptográficas para cifrar la información que se comparte en las comunicaciones con los dispositivos IoT. Usas protocolos seguros HTTPS en aplicaciones web y conexiones VPN como medidas de seguridad para preservar las comunicaciones.

Seguridad perimetral:

Palias las debilidades de los dispositivos IoT aplicando medidas de seguridad en otros dispositivos y capas de la red de la empresa.

Despliegue de los dispositivos:

Utilizas una red propia segmentada y, en caso de tener que acceder desde Internet, implementas una DMZ empleando las configuraciones de seguridad necesarias.