ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS

INDUSTRIA 4.0

Grupo #2
Integrantes:
Esteban Hidalgo
Johan Baño
Luis Rocha
Nicolas Reinoso

Profesor: Ing. Juan Herrera
Fecha: 08/10/2024

Industria 4.0

Conectividad y automatización

Optimización en tiempo Real

Tecnologías clave

Internet de las cosas IoT

IA

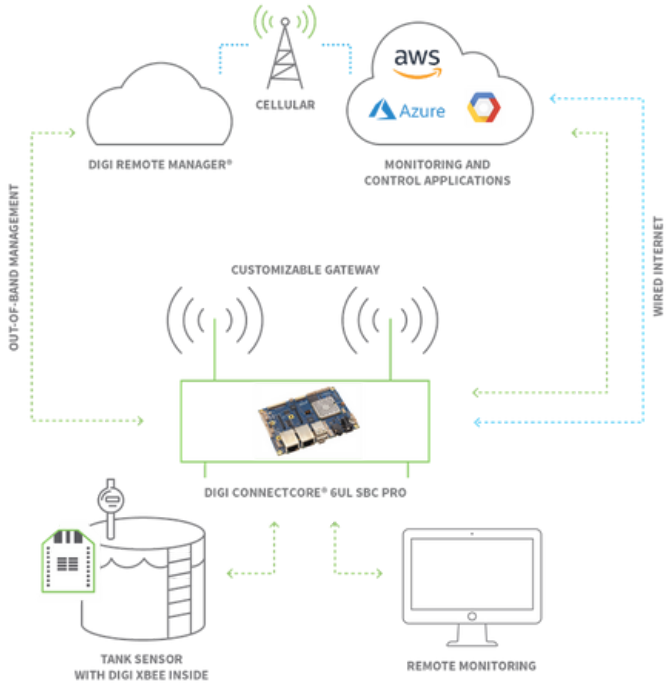
BigData

Cloud computing

Robótica avanzada

Importancia de la Seguridad Informática en la Industria 4.0

La Conectividad Masiva en la Industria 4.0



Principales Amenazas de Seguridad en la Industria 4.0

- Ciberataques Dirigidos: Ransomware y Malware
- Phishing e Ingeniería Social
- Ataques a IoT
- Sabotaje Industrial

Buenas Prácticas en Ciberseguridad para la Industria 4.0

- Seguridad por diseño
- Cifrado de datos
- Seguridad en la cadena de suministros
- Formación y concienciación

Prevención ante los desastres

- Enviar respaldos fuera de sitio semanalmente para que en el peor de los casos no se pierda más que los datos de una semana.
- Incluir el software así como toda la información de datos, para facilitar la recuperación.
- Si es posible, usar una instalación remota de reserva para reducir al mínimo la pérdida de datos.
- El suministro de energía ininterrumpido

Prevención ante los desastre

Redes de Área de Almacenamiento (SANs) en múltiples sitios son un reciente desarrollo (desde 2003) que hace que los datos estén disponibles inmediatamente sin la necesidad de recuperarlos o sincronizarlos.

Protectores de línea para reducir al mínimo el efecto de oleadas sobre un delicado equipo electrónico.

La prevención de incendios - más alarmas, extintores accesibles.

La Norma ISO 27001

La norma ISO 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI).

Implementación de Norma ISO 27001

Fase de planificación

Fase de implementación

Fase de evaluación

Fase de mejora continua

Estructura de la norma ISO 27031

1. Introducción

2. Alcance

3. Referencias normativas

4. Términos y definiciones

5. Contexto de la organización

Estructura de la norma ISO 27001

6. Liderazgo

7. Planificación

8. Soporte

9.Operación

10. Evaluación del desempeño

Controles de la norma ISO 27001

1. Acceso controlado:
Restricción del acceso a los recursos de información solamente a las personas autorizadas.

2. Clasificación de la información:
Identificación y clasificación de la información crítica para determinar el nivel de protección necesario.

Controles de la norma ISO 27001

3. Seguridad física:
Medidas de seguridad para proteger los recursos de información físicos, como dispositivos de almacenamiento, edificios y áreas.

4. Control de dispositivos:
Medidas para proteger y controlar los dispositivos que acceden a la información.

Controles de la norma ISO 27001

5. Criptografía:
Uso de técnicas de cifrado para proteger la información en reposo y en tránsito.

6. Copias de seguridad y recuperación:
Planificación y realización de copias de seguridad regulares para asegurar la disponibilidad de la información en caso de un desastre.

7. Monitoreo y auditoría:
Monitoreo y revisión periódica de los sistemas y registros de seguridad para detectar posibles vulnerabilidades y actividades sospechosas.

Ventajas

- Automatización
- Integración
- Rapidez en la identificación de problemas

REALIZADO POR LUIS

PRINCIPIOS DE ATAQUES EN LA INDUSTRIA

Prevención de ataques

- Separar las redes operativas (OT) de las redes de TI para minimizar el riesgo de acceso no autorizado.
- Cifrado de datos IoT, la transmisión de información entre sensores, máquinas, y sistemas de control.
- Implementación de Zero Trust, ningún dispositivo o usuario tiene acceso sin verificación continua.
- Segmentación de redes es una técnica de prevención muy efectiva para mitigar los riesgos de propagación de ataques.

Detección de Incidentes

Utilización de inteligencia artificial para identificar patrones de comportamiento anómalos en redes industriales.

Implementación de soluciones que monitoreen redes en tiempo real para detectar actividades sospechosas

Centralizar la vigilancia de la seguridad con herramientas SIEM (Security Information and Event Management).

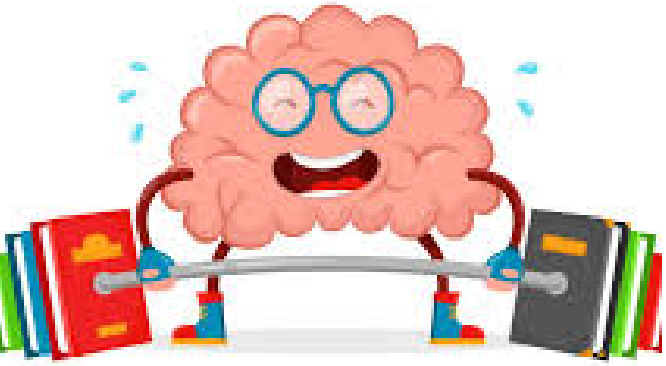
Respuesta

- Uso de SOAR (Seguridad, organización, automatización y respuesta) para ejecutar acciones automáticas como aislamiento de redes infectadas.
- Definir pasos claros que deben seguir los equipos de seguridad ante incidentes
- Coordinación entre equipos de IT, OT y directivos para garantizar decisiones rápidas.
- Aislar las redes y sistemas comprometidos para evitar la propagación del daño
- Activación del Protocolo de Respuesta a Incidentes (IRP)

Recuperación

- Creación de estrategias para restaurar sistemas y datos críticos de manera efectiva.
- Almacenar copias de seguridad en ubicaciones externas o en la nube, y garantizar que no estén conectadas a las redes principales.
- Realización de pruebas periódicas para garantizar que los sistemas puedan restaurarse rápidamente.
- Restaurar primero los sistemas críticos (por ejemplo, los de producción), luego los sistemas de soporte (como administración o finanzas).

Mejora



- Implementar políticas de actualización regulares en sistemas industriales.
- Identificar nuevas vulnerabilidades y evaluar la efectividad de las medidas de seguridad actuales.
- Educar a los empleados sobre las amenazas emergentes y cómo responder ante posibles incidentes.
- Realizar auditorías de seguridad periódicas para evaluar la efectividad de las medidas implementadas, identificar nuevas vulnerabilidades, y ajustar políticas de ciberseguridad.

Beneficios para la organización

- Alinear la disponibilidad de la tecnología con las necesidades del negocio.
- Conocer los riesgos a los que está sujeta la tecnología, así como los impactos de sus interrupciones.
- Dar a conocer las mejores soluciones para una implementación éxitosa.
- Claridad en la determinación de la tecnología crítica y la información a proteger.

CONCLUSIONES

La Industria 4.0 necesita alta seguridad debido a la interconexión de sistemas, aumentando los riesgos cibernéticos.

La norma ISO 27031 asegura la continuidad operativa al facilitar la rápida recuperación ante incidentes, protegiendo sistemas críticos.