INFORME TÉCNICO: INVENTARIO DE ACTIVOS DE TECNOLOGÍA OPERATIVA (OT)

Cliente: Tradebe
Fecha: 08 de abril de 2025
Presentado por: [Su Nombre/Nombre de la Empresa], Responsable de Automática Integral

RESUMEN EJECUTIVO

Este informe presenta el inventario completo de los 102 activos de Tecnología Operativa (OT) identificados en las instalaciones de Tradebe. El objetivo es proporcionar una visibilidad total sobre los sistemas de control industrial (PLCs, HMIs, etc.), sentando las bases para fortalecer la ciberseguridad y cumplir con normativas como la Ley NIS2 y el estándar IEC 62443.

Los hallazgos clave muestran un ecosistema tecnológico diverso, dominado por equipos Siemens, que es fundamental para las operaciones de la planta. Sin embargo, la creciente interconexión de estos sistemas con redes IT introduce riesgos significativos, como la exposición a ciberataques que podrían paralizar la producción.

Las recomendaciones principales se centran en utilizar este inventario para llevar a cabo un análisis de vulnerabilidades exhaustivo, clasificar los activos por su criticidad para el negocio y desarrollar un plan de mitigación. Proponemos avanzar hacia una arquitectura de seguridad robusta, como el modelo Zero Trust, para asegurar el acceso a los sistemas y segmentar la red eficazmente. La implementación de estas medidas es un paso estratégico esencial para garantizar la resiliencia operativa, la competitividad y la autonomía de Tradebe.

---

1. OBJETIVO DEL INFORME

El presente informe tiene como finalidad presentar el resultado del inventario de activos en sus entornos de Tecnología Operativa (OT), un paso fundamental para fortalecer la ciberseguridad industrial en Tradebe. Este inventario proporciona una base sólida de visibilidad sobre sus sistemas de control industrial, esencial para el cumplimiento de normativas como la Ley NIS2 y los estándares IEC 62443, y para facilitar la gestión de riesgos y vulnerabilidades.

2. CONTEXTO Y RELEVANCIA DE LA CIBERSEGURIDAD OT

La ciberseguridad en el ámbito industrial ha cobrado una relevancia significativa en los últimos años debido a la gravedad de los ciberataques que pueden paralizar la producción o exponer información sensible. De hecho, reportes recientes

indican que el 80% de las empresas encuestadas sufrieron un ataque, y el 47% de ellas experimentó un impacto en su entorno de sistemas de control industrial/OT. Más del 60% de estas empresas incluso pagaron rescates, con un 52% pagando $500,000 o más. Ante este panorama, más del 70% de las empresas industriales han incrementado su presupuesto en ciberseguridad.

La norma IEC 62443 es el estándar internacional para la seguridad de los sistemas de control y componentes de automatización industrial (IACS). Su aplicación es crucial para demostrar de forma objetiva que la ciberseguridad es una prioridad. En particular, la IEC 62443-4-1 se enfoca en los requisitos del ciclo de vida del desarrollo seguro de productos, mientras que la IEC 62443-4-2 se centra en los requisitos técnicos de seguridad para los componentes IACS. Es un requisito obtener la certificación IEC 62443 4-1 antes de proceder con la evaluación para la IEC 62443 4-2.

Las redes OT, que incluyen sistemas y dispositivos para monitorear y controlar procesos industriales (como PLCs y SCADA), son vitales en sectores como la energía, manufactura y transporte. La convergencia de OT con las Tecnologías de la Información (IT) ofrece ventajas como el análisis de datos en tiempo real, pero también introduce riesgos de ciberseguridad debido a la conexión de sistemas que antes estaban aislados. Un informe reciente de S2GRUPO advierte que más del 70% de las redes OT industriales presentan debilidades estructurales y un 40% de los dispositivos conectados operan con vulnerabilidades críticas no parcheadas.

3. METODOLOGÍA DEL INVENTARIO

La metodología empleada para la elaboración de este inventario de activos OT en Tradebe se basó en un enfoque estructurado en fases, combinando técnicas pasivas y activas para una recopilación de datos exhaustiva y segura:

- **Fase 1: Revisión y Definición del Alcance:** Se identificaron las zonas OT a inventariar, se evaluó la profundidad de la información requerida por tipo de activo y se coordinó con el personal de planta y los responsables de IT/OT de Tradebe.
- **Fase 2: Recopilación e Identificación de Activos:** Se realizó un inventario mixto, incluyendo:
    - **Inventario pasivo:** Mediante análisis de red con herramientas como Siemens SINEC INSPECT.
    - **Inventario activo controlado:** A través de escaneos dirigidos con NMAP, evitando afectar la operación. Aunque la literatura advierte sobre escaneos activos en redes OT, nuestra experiencia ha

demostrado resultados precisos sin problemas operativos significativos.

    - **Revisión in situ:** De configuraciones físicas cuando fue seguro y autorizado.

- **Fase 3: Clasificación y Documentación:** La información se estructuró en una base de datos con identificadores únicos, tipo y modelo de dispositivo, ubicación física y lógica, **versión de software/firmware (a completar)**, propietario, responsable y una **valoración de criticidad preliminar**. Esto permite agilizar la definición de Zonas y Conductos para el cumplimiento de IEC 62443.
- **Fase 4: Entrega, Revisión y Formación:** El inventario validado se entrega en formato digital editable (Excel), junto con recomendaciones. Se ofrece formación básica para que el equipo de Tradebe pueda mantener el inventario actualizado.

4. RESUMEN GLOBAL DEL INVENTARIO POR CATEGORÍA

Se han identificado un total de **102 dispositivos operativos** en las instalaciones de Tradebe. La distribución de estos activos por categoría principal se muestra a continuación, destacando la predominancia de la Periferia, Switches y PLCs, que constituyen el núcleo del sistema de control.

Distribución de Activos OT por Categoría

Generated code

Periferia: 26.5%

Switch: 18.6%

PLC: 17.6%

HMI: 14.7%

Variador: 8.8%

PC: 7.8%

Adaptador: 2.9%

Otros: 0.0%

Gráfico 1: Porcentaje de dispositivos por categoría sobre un total de 102 activos.

5. DESGLOSE DETALLADO DEL INVENTARIO POR CATEGORÍA Y SUBCATEGORÍA

A continuación, se presenta el inventario detallado. La **Criticidad Preliminar** es una sugerencia basada en la función típica del dispositivo y **debe ser validada y ajustada por el personal de operaciones de Tradebe**. La columna **Versión Firmware/Software** debe completarse para permitir un análisis de vulnerabilidades preciso.

Tabla 1: PC (8 dispositivos)

ID de Dispositivo	Modelo	Versión Firmware/Software (por completar)	Criticidad Preliminar (Sugerida)
PC_EVAPORADOR	PC Station SIMATIC		Alta
PC_BIO	PC Station SIMATIC		Alta
PC_EVAP_VC1	PC Station SIMATIC		Media
PC_A070	PC Station SIMATIC		Alta
PC_A070_VC1	PC Station SIMATIC		Media
PC-A070-VC2	PC Station SIMATIC		Media
PC_A070_VC3	PC Station SIMATIC		Media
PC_A020	PC Station SIMATIC		Alta

Tabla 2: PLC (18 dispositivos)

Modelo	Cantidad	Versión Firmware/Software (por completar)	Criticidad Preliminar (Sugerida)
Siemens 1200 CPU 1214C DC/DC/DC	11		Alta
Siemens 1500 CPU 1511F-1 PN	1		Alta (Seguridad)
Siemens 1500 CPU 1512SP-1 PN	1		Alta
Siemens 1500 CPU 1510SP-1 PN	1		Alta
Siemens 1500 CPU 1512C-1 PN	1		Alta
Siemens 300 CPU 313C	1		Media (Legado)
Siemens 300 CP 343-1 Lean	1		Media (Legado)
Siemens 1200 CPU 1212C DC/DC/Rly	1		Media

Tabla 3: HMI (15 dispositivos)

Modelo	Cantidad	Versión Firmware/Software (por completar)	Criticidad Preliminar (Sugerida)
Siemens HMI KTP900 Basic	6		Media
Siemens HMI KTP400 Basic	4		Media
Siemens HMI KTP700 Basic	3		Media

| Siemens HMI KTP1200 Basic | 1 | | Alta |
| Siemens HMI TP1200 Comfort | 1 | | Alta |

Tabla 4: Periferia (27 dispositivos)
Modelo	Cantidad	Versión Firmware/Software (por completar)	Criticidad Preliminar (Sugerida)
Siemens Periferia In/Out IM 151-3 PN	10		Media
ifm IO-Link Master (AL1303)	6		Media
Siemens Periferia In/Out IM 155-6 PN ST	5		Media
Siemens Periferia In/Out IM 155-6 PN BA	3		Media
SMC EX260 Eth module (EX260-SPN)	2		Media
Siemens Periferia In/Out IM 155-6 PN HF	1		Alta

Tabla 5: Otros Activos (Variador, Adaptador, Switch)
Categoría	Modelo	Cantidad	Criticidad Preliminar (Sugerida)
Variador	Siemens SINAMICS G120C	8	Media
Variador	Schneider ATV630	1	Media
Adaptador	Ibhsoftec IBHLink S7++ (MPI/Profibus)	3	Alta (Acceso a red legada)
Switch	Siemens Scalance X005	13	Baja (No gestionable)
Switch	Siemens Scalance XB008	5	Baja (No gestionable)
Switch	Siemens CSM 1277	1	Baja (No gestionable)

6. CONTEO DE DISPOSITIVOS POR ÁREA

El análisis revela una concentración significativa de dispositivos en las áreas A140, A030, A020 y A070, sugiriendo que estas son las zonas de mayor complejidad y criticidad operativa.

Número de Activos por Área de Planta

Generated code

A140: 23

A120: 8

A110: 15

A100: 5

A070: 11

A050: 2

A040: 4

A030: 12

A020: 11

A000: 8

IGNORE_WHEN_COPYING_START

content_copy download

Use code with caution.

IGNORE_WHEN_COPYING_END

Gráfico 2: Número total de dispositivos identificados en cada área operativa.

7. IMPLICACIONES Y RECOMENDACIONES EN CIBERSEGURIDAD

Este inventario de activos OT es un pilar fundamental para la gestión de la ciberseguridad industrial de Tradebe. Proporciona una visibilidad completa del entorno OT, que es la base para el análisis de vulnerabilidades y la implementación de acciones correctivas.

(Las subsecciones 7.1 y 7.2 permanecen como en el original, ya que son conceptualmente sólidas)

8. PRÓXIMOS PASOS

Este informe concluye la fase inicial de identificación. Para capitalizar esta información y avanzar hacia una postura de seguridad robusta, recomendamos un enfoque estructurado en las siguientes fases, que se valorarán de forma independiente:

Fase II: Análisis de Vulnerabilidades y Plan de Mitigación (Recomendación Inmediata)

- **Objetivo:** Identificar y priorizar las debilidades específicas del entorno de Tradebe.
- **Acciones Clave:**
    1. **Completar Datos del Inventario:** Enriquecer el inventario con las versiones de firmware y software de cada dispositivo.
    2. **Validación de Criticidad:** Realizar talleres con el personal de operaciones para validar y ajustar la criticidad de cada activo según su impacto en el proceso.

3. **Análisis de Vulnerabilidades:** Cruzar la información de software/firmware con bases de datos públicas (como CVE) e realizar escaneos controlados para detectar vulnerabilidades conocidas.
4. **Análisis de Riesgo:** Evaluar la probabilidad y el impacto de la explotación de cada vulnerabilidad, considerando la criticidad del activo.

- **Entregable:** Un **Informe de Riesgos y Vulnerabilidades** detallado, con un plan de mitigación que priorice las acciones correctivas (parcheo, configuración, reemplazo) según el nivel de riesgo.

Fase III: Diseño e Implementación de Controles de Seguridad

- **Objetivo:** Construir defensas activas y pasivas basadas en los hallazgos de la Fase II.
- **Acciones Clave:**
    1. **Segmentación de Red (Zonas y Conductos):** Diseñar e implementar una segmentación de red basada en el estándar IEC 62443 para aislar sistemas críticos y controlar el flujo de comunicación.
    2. **Hardening de Dispositivos:** Aplicar configuraciones seguras a los dispositivos, deshabilitando servicios innecesarios y cambiando credenciales por defecto.
    3. **Implementación de Monitoreo Continuo:** Desplegar herramientas para la detección de anomalías y amenazas en tiempo real dentro de la red OT.
    4. **Estrategia de Acceso Seguro (Zero Trust):** Diseñar una política de "confianza cero" que verifique explícitamente cada solicitud de acceso, independientemente de su origen.

9. CONCLUSIÓN

El presente inventario de activos de Tecnología Operativa de Tradebe representa un hito crucial en la estrategia de ciberseguridad de la compañía. Al proporcionar una visibilidad granular de los dispositivos y sistemas, se establece la base para fortalecer la resiliencia operativa y el cumplimiento normativo. En un entorno industrial cada vez más interconectado y amenazado por ciberataques, la ciberseguridad OT no es solo una necesidad técnica, sino un factor estratégico para la continuidad, competitividad y autonomía de Tradebe. Estamos a su

disposición para discutir los próximos pasos y colaborar en la implementación de una estrategia de ciberseguridad OT robusta y adaptada a sus necesidades.