Incidentes de Ciberseguridad

Tarea 1

ESTHER CARRILLO GÁLVEZ

Índice

1. Descripción de la tarea

Auditorías Internas de Cumplimiento en Materia de Prevención.

Una auditoría interna en materia de prevención resulta fundamental para una organización, pues permite conocer el estado de los activos antes de la aparición de los incidentes, dejando margen de tiempo suficiente para solucionar las posibles debilidades y vulnerabilidades.

Además, una vez se efectúa este tipo de auditoría, también es el momento de implantar un mecanismo de mantenimiento continuo de la protección y la calidad de la información, mediante un esquema de mejora continua o un modelo de madurez.

En esta tarea habrá que diseñar un procedimiento de auditoría para una empresa ficticia, cuyo diseño parcial formará parte también de la práctica.

2. Apartado 1: Diseño del esquema de una Empresa Ficticia.

Información básica para diseñar el esquema de la empresa:

- La empresa ficticia es una **joven PYME industrial** dedicada a la fabricación de repuestos para el sector automotriz. Como empresa orientada a la producción y gestión de inventarios, utiliza tanto Tecnologías de la Información (TI) para sus operaciones administrativas y comerciales, como Tecnologías de Operación (OT) para la gestión y control de los procesos fabriles. Dado que esta empresa depende de sistemas de información para la continuidad de sus operaciones y protección de datos, se ha establecido una arquitectura de red basada en tres zonas principales, conocidas como estructura en trípode.
- La empresa se organiza en tres bloques principales que permiten separar los activos de TI y OT y gestionar los accesos de manera controlada:

  LAN (Red Interna de Gestión Empresarial): Esta red interna incluye todos los sistemas y servicios necesarios para la gestión empresarial y el soporte administrativo. Entre sus activos se encuentran los puestos de trabajo de los empleados, tanto locales como remotos, y los sistemas de bases de datos y almacenamiento para el ERP (Enterprise Resource Planning), utilizados para el manejo de la información económica y financiera. Además, aquí se encuentran los sistemas de análisis avanzados, como Big Data, IA y Machine Learning, empleados para mejorar la toma de decisiones estratégicas.

DMZ (Zona Desmilitarizada): Esta zona se encuentra segmentada de la red interna y la red externa (Internet), y su función principal es albergar los servicios que deben estar expuestos parcialmente a Internet. La DMZ de la empresa contiene el Centro de Operaciones de Seguridad (SOC), desde donde se monitorizan los eventos de seguridad; un IDS (Sistema de Detección de Intrusiones) y SIEM (Gestión de Información y Eventos de Seguridad) para la detección y gestión de incidentes; y el NAS (Network Attached Storage) y Vault, que almacenan documentos de diseño y planos protegidos. Adicionalmente, en esta zona se encuentran un portal web para la presencia pública de la empresa y un servidor de laboratorio destinado a pruebas de software y aplicaciones internas.

Smart Factory (Red de Operación Fabril, aislada de Internet): En esta zona se agrupan todos los sistemas relacionados con la producción y el control de los procesos fabriles. La red de la Smart Factory incluye el sistema ERP y el MES (Manufacturing Execution System), que se usan para la gestión de la producción y el control del inventario. Además, en esta zona se encuentra el sistema SCADA para la supervisión y control en tiempo real de los procesos industriales, los PLC (Controladores Lógicos Programables) que gestionan la maquinaria automatizada y los dispositivos fabriles como sensores y actuadores. Estos activos no están expuestos a Internet para reducir riesgos de ciberseguridad y asegurar la continuidad operativa.

FRONTERA	SMART FACTORY	LAN	DMZ
Switch	Controladores Lógicos Programables (PLCs)	Puestos locales	SOC
Router	Sistema SCADA	Puestos remotos	Servidor IDS
Firewall	Sistema ERP	Switch	Almacenamiento NAS
	Servidor MES	Servidor de Procesamiento Big Data / IA / ML	Servidor laboratorio
	Switch	ERP	Servidor Web
			Servidor SIEM
			Servidor Vault
			Switch

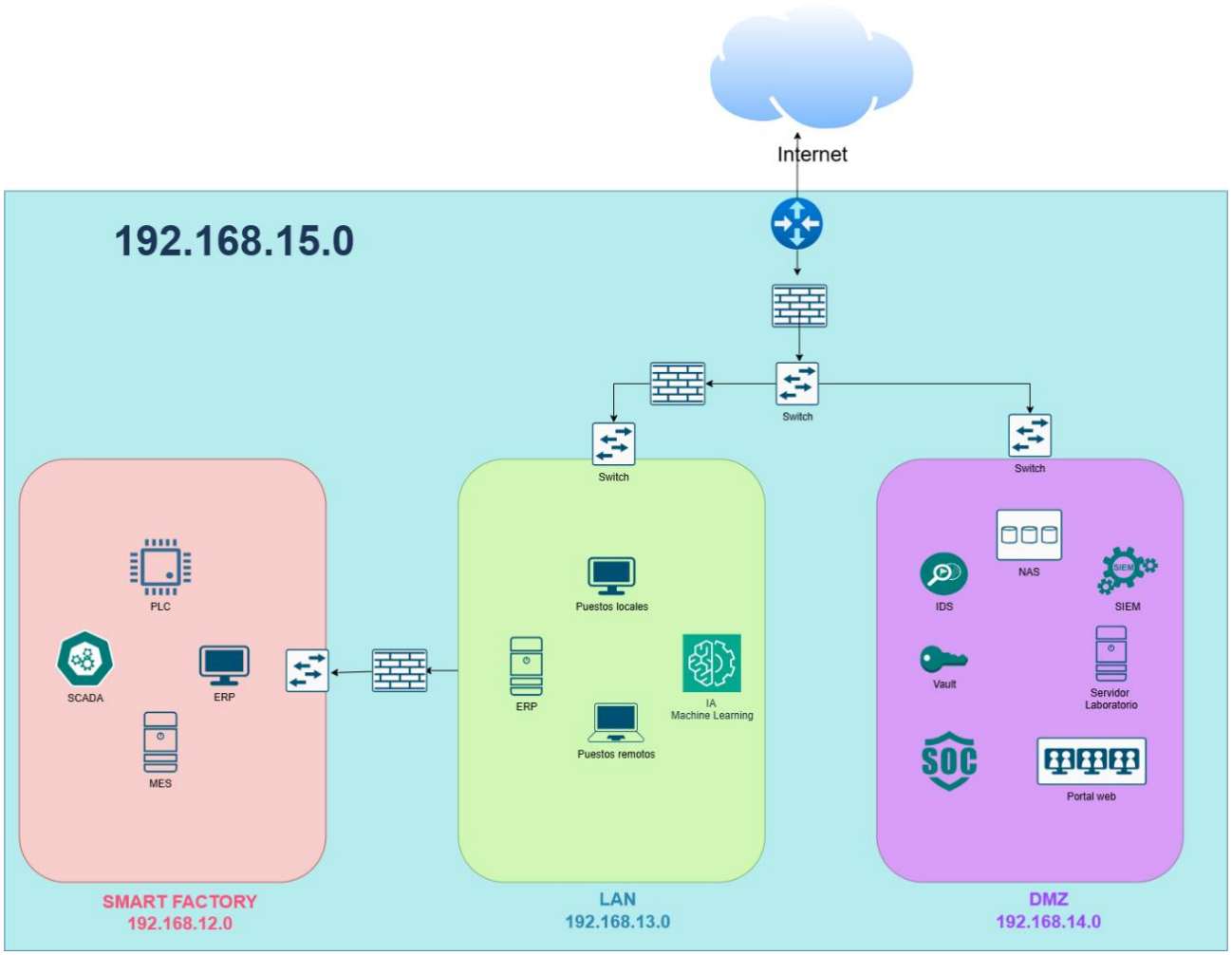

Figura 1. Elaboración propia

3. Apartado 2: Detalle de los Activos Clave que se deberán auditar.

- Para llevar a cabo una auditoría efectiva, es fundamental identificar y documentar los activos clave de la empresa ficticia. Estos activos comprenden tanto elementos de hardware como de software que juegan un papel esencial en el funcionamiento seguro y eficiente de la infraestructura de TI y OT de la organización.
- Para este apartado, deberás realizar un inventario de los activos clave, recopilando la información necesaria en una tabla para los activos que consideres necesarios, tomando un activo por cada zona (LAN,DMZ, Smart Factory) más un activo transversal que pudiera estar en más de una zona o sea perimetral.

Zona	Nombre Activo	Dirección IP/Rango de IP	Sistema Operativo	Modelo de Máquina	Función en la Empresa	Observaciones
Perimetral	Router frontera	192.168.15.1	Cisco IOS XE 17.3	Cisco ISR 4000 Series Router	Gestión y enrutamiento del tráfico entre red LAN e Internet	Dispositivo crítico al estar expuesto directamente a internet.
Smart Factory	Servidor SCADA	192.168.12.2	Linux (PACEdge)	Emerson PACSystems IPC 2010	Funciona como una herramienta integral que recopila datos, los analiza y emite alertas a tiempo real.	Aislado por firewall industrial de la LAN.
LAN	Sistemas ERP	192.168.13.5	Windows Server 2022	Siemens SIMATIC IPC847E	Gestión y supervisión de las órdenes de producción e inventario	Nivel de protección tanto en el almacenamiento de los datos como en el acceso a ellos y su uso. Grado de privacidad, asignación de contraseñas y niveles de cifrado son esenciales.
DMZ	Servidor Web	192.168.14.6	Linux Ubuntu Server	Dell Power Edge R250	Alojar el portal del cliente y garantizar una correcta comunicación.	Punto de entrada más directo para el atacante. Control constante del tráfico entrante para detectar actividad anómala.

4. Apartado 3: Comprobación prioritaria a efectuar para cada uno de los activos anteriores.

Una vez que se ha realizado el inventario de los activos clave, es necesario definir las comprobaciones de seguridad que se deben efectuar sobre cada uno de ellos.

ROUTER (Perimetral)	
Activo	Cisco ISR 4000 Series Router *192.168.15.1*
Comprobación a realizar	Sistema de actualizaciones
Objetivo de la comprobación	Mantener el firmware actualizado para evitar vulnerabilidades públicas
Herramientas	Consola Cisco (CLI)
Procedimiento	· Verificar que existe copia de seguridad. · Confirmar versión del IOS. · Comprobar las versiones del hardware y el firmware de la plataforma y descargar el archivo de imagen correspondiente al hardware.
Criterio de aceptación (PASS/FAIL)	PASS si la versión de IOS está actualizada con el último parche de seguridad y no existen vulnerabilidades críticas.
Servidor SCADA (Smart Factory)	
Activo	Emerson PACSystems IPC 2010 *192.168.12.2*
Comprobación a realizar	Análisis de logs
Objetivo de la comprobación	Registro de eventos realizados por los usuarios. Permite un monitoreo y análisis del estado del sistema
Herramientas	Servidor SIEM, plataforma de almacenamiento de logs, SIEM, sistema de sincronización horaria (NTP) y consola de registro nativa de SCADA.
Procedimiento	· Determinar la retención de los logs. · Comprobar sincronización horaria de dispositivos y el servidor SCADA. · Revisar configuración del SCADA para activar la auditoría de eventos. · Confirmar la integración en el SIEM · Evaluación del análisis del SIEM.
Criterio de aceptación (PASS/FAIL)	PASS si el timestamp está sincronizado con el servidor NTP, si la auditoría de eventos está activada y si el servidor SIEM analiza los logs del SCADA

Sistemas ERP (LAN)	
Activo	Siemens SIMATIC IPC847E *192.168.13.5*
Comprobación a realizar	Administración de permisos
Objetivo de la comprobación	Es crucial revisar el nivel de privilegios de los usuarios con acceso al ERP
Herramientas	Active Directory, permisos NTFS
Procedimiento	· Identificar las cuentas que tienen permiso para restablecer las contraseñas de otros administradores. · Identificar las cuentas que tienen permisos sobre los controladores de cuentas, es decir, las cuentas que pueden modificar las ACL de los administradores. · Identificar los controladores de grupos de administradores, es decir, las cuentas que tienen permiso para agregar o eliminar miembros de grupos privilegiados.
Criterio de aceptación (PASS/FAIL)	PASS si los usuarios básicos con nivel de privilegios mínimos. Usuarios administradores con permisos acotados a sus roles.
Servidor Web (DMZ)	
Activo	Dell PowerEdge R250 *192.168.14.6*
Comprobación a realizar	Protección de Datos / Propiedad Intelectual (PD/PI)
Objetivo de la comprobación	Garantizar la integridad de los datos mediante copias de seguridad almacenadas de forma separada
Herramientas	Herramientas destinadas a las copias de seguridad como Veeam o Acronis
Procedimiento	· Determinar qué información se copiará. · Periodicidad y tipo de copias. · Ubicación de las backups. · Cifrado las backups. · Control de las copias de seguridad.
Criterio de aceptación (PASS/FAIL)	PASS si la copia de seguridad es íntegra, accesible y cifradas para el almacenamiento final.

5. Apartado 4: Auditoría prioritaria por activo

Selecciona para cada uno de los cuatro activos (LAN, DMZ, OT y Transversal) **un único tipo de auditoría**, priorizando la que mejor cubra el riesgo principal del activo.

Zona	Perimetral
Activo	**Router frontera** Cisco ISR 4000 Series Router *192.168.15.1*
Tipo de auditoría seleccionada	Auditoría de red
Justificación de elección	Análisis de la estructura y segmentación de la red. Verificar que la separación entre LAN, DMZ y OT sea correcta.
Alcance y limitaciones	Revisión de tablas de enrutamiento, pero se excluye las reglas de ACL del firewall.
Procedimiento (3–7 pasos)	1.Comprobar tabla de enrutamiento. 2. Comprobar interfaces 3.Ejecutar pruebas ping y traceroute para comprobar que la ruta está bloqueada.
Herramientas	Consola cisco
Criterios de aceptación (PASS/FAIL)	PASS si una ruta en la Smart Factory falla por la segmentación de la red.

Zona	Smart Factory
Activo	**Servidor SCADA** Emerson PACSystems IPC 2010 *192.168.12.2*
Tipo de auditoría seleccionada	Revisión de logs
Justificación de elección	Esta auditoría prioriza la identificación y respuesta oportuna a posibles amenazas de ciberseguridad y operacionales. Se enfoca en aumentar la visibilidad y el conocimiento de la infraestructura SCADA, mediante la recopilación y análisis de los logs, garantizado la trazabilidad de los eventos.
Alcance y limitaciones	Análisis de los eventos generados por el SCADA. Se excluye el análisis post-explotación.

Procedimiento (3–7 pasos)	1. Verificar la sincronización en el servidor NTP. 2. Confirmar que los logs están bien interpretados en el SIEM. 3. Verificar que el SIEM genera la alerta a un evento de prueba. 4. Comprobar que la retención de logs es el tiempo mínimo obligatorio
Herramientas	Servidor SIEM, plataforma de almacenamiento de logs, SIEM, sistema de sincronización horaria (NTP).
Criterios de aceptación (PASS/FAIL)	La sincronización es correcta, si el SIEM interpreta bien los eventos y si la retención cumple el tiempo mínimo obligatorio.

Zona	LAN
Activo	**Sistemas ERP** Siemens SIMATIC IPC847E *192.168.13.5*
Tipo de auditoría seleccionada	Auditoría Legal
Justificación de elección	El ERP centraliza y automatiza procesos de finanzas o producción, por lo que es esta auditoría es esencial para verificar si se cumple con normativas como la LOPD.
Alcance y limitaciones	Revisión del tratamiento de los datos personales y cifrado de bases de datos. Se excluyen las pruebas de denegación de servicios.
Procedimiento (3–7 pasos)	1. Cumplimiento de licencias 2. Evaluar controles de acceso 3. Auditar roles 4. Validar contraseñas robustas y MFA
Herramientas	Normativa oficial (LOPD), herramientas de análisis de datos (Excel)
Criterios de aceptación (PASS/FAIL)	El 95% de los usuarios trabajan con los privilegios mínimos y si los datos más sensibles están cifrados.

Zona	DMZ
Activo	Dell PowerEdge R250 *192.168.14.6*
Tipo de auditoría seleccionada	Test de penetración (Hacking ético)
Justificación de elección	Al ser el activo más expuesto, es el vector de entrada más probable.
Alcance y limitaciones	El alcance es limitado al servidor web. Se excluyen las pruebas DoS.
Procedimiento (3–7 pasos)	1.Uso de nmap para escaneo de puertos y detectar vulnerabilidades. 2.Aprovechar una vulnerabilidad para acceder al sistema explotándola. 3. Si se obtiene acceso, eliminar o modificar archivos críticos.
Herramientas	Nmap, burpsuite, Nessus.
Criterios de aceptación (PASS/FAIL)	No se consigue acceder o modificar los archivos.

6. Bibliografía

Abas ERP. (n.d.). *FAQ: ¿Qué hardware necesita ABAS ERP?* Abas ERP. Recuperado de https://abas-erp.com/es/faq/hardware-necesita-abas

Axarnet. (n.d.). *¿Cómo funciona un servidor?* Blog de Axarnet. Recuperado de https://axarnet.es/blog/como-funciona-servidor

AYDAI. (n.d.). *¿En qué consiste una auditoría de sistemas ERP?* AYDAI. Recuperado de https://aydai.com/en-que-consiste-una-auditoria-de-sistemas-erp/

Cisco Systems. (n.d.). *Routers de servicios integrados (ISR) de la serie 4000.* Cisco Support. Recuperado de https://www.cisco.com/c/es_mx/support/routers/4000-series-integrated-services-routers-isr/series.html#~tab-community

Cursos Aula 21. (n.d.). *¿Qué es un Sistema SCADA?* Cursos Aula 21. Recuperado de https://www.cursosaula21.com/que-es-un-sistema-scada/

HYCU. (n.d.). *Top 14 soluciones de backup SaaS y herramientas de protección de datos.* Blog de HYCU. Recuperado de https://www.hycu.com/es/blog/top-14-saas-backup-solutions-tools-saas-data-protection

INCIBE. (n.d.). *Guía de Copias de Seguridad* (Documento en formato PDF). Instituto Nacional de Ciberseguridad. Recuperado de https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

INCIBE-CERT. (n.d.). *Blog de INCIBE-CERT (Publicaciones sobre Ciberseguridad).* Instituto Nacional de Ciberseguridad. Recuperado de https://www.incibe.es/incibe-cert/blog

INCIBE-CERT. (n.d.). *Registrando eventos en sistemas de control para mejorar la seguridad.* Blog de INCIBE-CERT. Recuperado de https://www.incibe.es/incibe-cert/blog/registrando-eventos-en-sistemas-de-control-para-mejorar-la-seguridad

LookingPoint. (n.d.). *Upgrade Cisco ISR 4000 Series Routers (Actualización de Routers Cisco ISR 4000).* Blog de LookingPoint. Recuperado de https://www.lookingpoint.com/blog/upgrade-cisco-isr-4000-series-routers

Mytra. (n.d.). *Sistemas SCADA para la captura de datos y monitorización de los procesos.* Mytra. Recuperado de https://www.mytra.es/blog-post/sistemas-scada-para-la-captura-de-datos-y-monitorizacion-de-los-procesos

Nunsys. (n.d.). *¿Qué es SCADA? Soluciones de Control Industrial.* Nunsys. Recuperado de https://www.nunsys.com/scada/

Reddit. (n.d.). *Audit ACLs & Permissions in Active Directory [Hilo de discusión].* Reddit. Recuperado de

https://www.reddit.com/r/activedirectory/comments/1nk3lx5/audit_acls_permissions_in_active_directory/?tl=es-419

Spindatos. (n.d.). *Servicio de Auditoría de Sistemas y Seguridad.* Spindatos. Recuperado de https://spindatos.com/auditoria/

Universidad Católica de Manizales (UCM). (n.d.). *Documento Técnico: Seguridad en Sistemas de Control Industrial (SCADA)* (Contenido de repositorio). Repositorio Digital UCM. Recuperado de https://repositorio.ucm.edu.co/server/api/core/bitstreams/5de34283-d0bc-45b2-9af5-019204f05b85/content