TAREA 01

DESARROLLO DE PLANES DE PREVENCIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD

INCIDENTES DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

CETI - Ciberseguridad en Entornos de las Tecnologías de la Información

AUDITORÍA INTERNA DE PREVENCIÓN

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.**

Con la información proporcionada deberás efectuar las siguientes tareas:

- **Crear una lista con todos los activos de la empresa detectados en cada una de las zonas.**
- **Crear un Diagrama de Bloques gráfico de la Empresa Ficticia según la estructura pedida en el que se distribuyan los activos de la lista anterior, es decir, un esquema general de los equipos distribuidos en la red según esta estructura en trípode.**

Lista de Activos:

LAN (Red Interna de Gestión Empresarial)

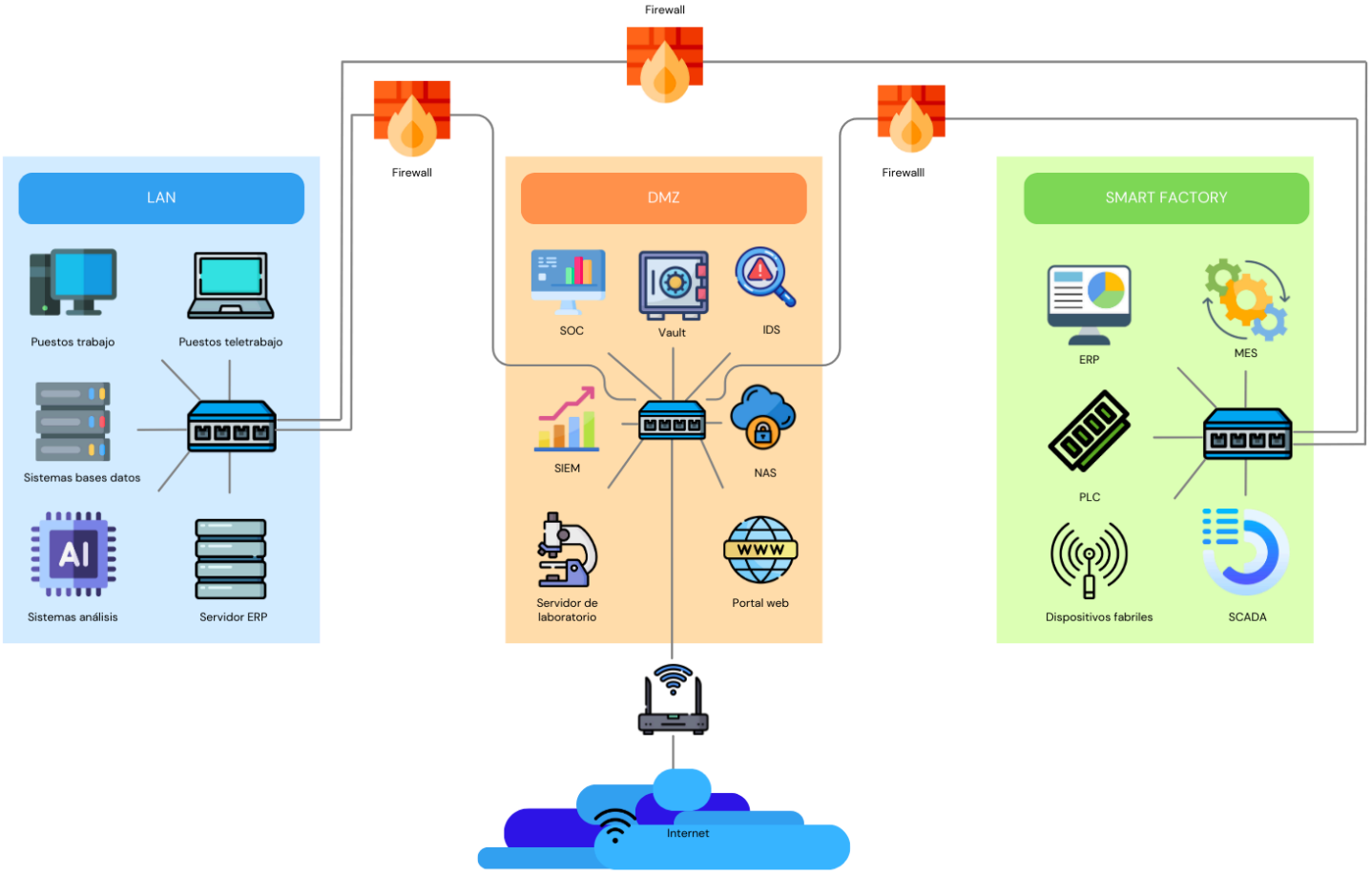
- Puestos de trabajo de los empleados, tanto locales como remotos
- Sistemas de bases de datos y almacenamiento
- ERP (Gestión recursos empresariales)
- Sistemas de análisis (Big Data, IA y Machine Learning)

DMZ (Zona Desmilitarizada)

- Centro de Operaciones de Seguridad (SOC)
- IDS (Sistema de Detección de Intrusiones)
- SIEM (Gestión de Información y Eventos de Seguridad)
- NAS (Almacenamiento conectado a la red)
- Vault
- Portal web
- Servidor de laboratorio

Smart Factory (Red de Operación Fabril, aislada de Internet

- Sistema ERP
- MES (Manufacturing Execution System)
- Sistema SCADA
- PLC (Controladores Lógicos Programables)
- Dispositivos fabriles



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 cada activo.

Nombre Activo	Dirección / Rango de IP	Sistema Operativo	Modelo de Máquina	Función en la Empresa	Observaciones
Router Frontera	192.168.1.1	Askey	RTF3505VW	Router de conexión a Internet	LAN, WiFi habilitado
Switches	192.168.1.2 192.168.1.3 192.168.1.4	Cisco IOS	Cisco Catalyst 2960	Cada zona consta de uno para interconectar los activos	
Puestos trabajo	192.168.1.10 - 192.168.1.90	Windows 11	HP 15-fc0034ns	Equipos de trabajo en local y remoto	Softwares corporativos y conexión red
Servidor ERP	192.168.1.100	Windows Server Essentials 2022	Servidor DELL PowerEdge R740	Gestionar recursos empresariales	Gestión inventario
NAS	192.168.1.150 - 192.168.1.160	Synology DiskStation Manager	DiskStation DS423	Almacenamiento de datos	Conexión red con cifrado de datos
Firewall x3	192.168.1.200 192.168.1.210 192.168.1.220	RouterOS	Fortinet FortiGate-60F	Controlar trafico de la red	Protección contra accesos malintencionados
PLC	192.168.1.240 - 192.168.1.255	Windows 10	CompactLogix 5480	Control maquinaria y procesos	
Servidor de laboratorio	192.168.2.100	Windows Server Essentials 2022	Servidor DELL PowerEdge R340	Sirve para pruebas y desarrollo	Entorno aislado
Servidor Big Data	192.168.2.150	Ubuntu 22	HP ProLiant DL360	Procesar y analizar datos	A tiempo real
Vault	192.168.2.200	Linux Dedian	Customizar servidor	Almacenamiento y gestión contraseñas	
IDS	192.168.3.100	Cisco IOS	Cisco C1000	Monitoriza amenazas	Detección de intrusiones
Portal Web	192.168.3.200	Linux	Servidor Apache HTTP	Acceso web a servicios	
SCADA	192.168.3.250	Windows	Siemens SIMATIC IPC347E	Controlar procesos	
Dispositivos fabriles	192.168.4.100 - 192.168.4.150	Linux	Siemens st72-1200	Optimiza la producción	Sensores o actuadores

Tipos de activos mencionados:

- Estructurales: Router, Switch y Firewall
- Equipos: Puestos de trabajo y Dispositivos fabriles
- Softwares: Portal Web y Servidor ERP
- Bbdd: NAS y Vault

Hemos utilizado direcciones ip dentro del rango de redes privadas (192.168.0.0 - 192.168.255.255) que no están accesibles directamente desde internet. Para la mayoría de activos hemos elegido números redondos porque suelen tener la ip fija por tener funciones de alta importancia, para otros se ha dejado un rango de ip porque las empresas suelen constar de varios dispositivos de ese mismo tipo.

Apartado 3: Detalle de las Comprobaciones a efectuar para cada uno de los Activos.
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. Estas comprobaciones buscan identificar vulnerabilidades y asegurar que los activos cumplen con las medidas de protección adecuadas para minimizar riesgos de ciberseguridad.

A continuación, se detallan algunas de las principales comprobaciones de seguridad aplicables a los activos de la empresa ficticia:

- **Sistemas Antimalware: Verificación de software antivirus y antimalware.**
- **Gestión de Permisos: Revisión de permisos de acceso y privilegios de usuario.**
- **Cumplimiento Legal (Compliance): Asegurar que el activo cumple con normativas de ciberseguridad.**
- **Prevención de Fraude y Fuga de Datos: Comprobación de medidas de protección contra fraudes y exfiltración de datos.**
- **Sistema de Actualizaciones: Verificación de políticas de actualización y parches de seguridad.**
- **Monitorización de Recursos: Revisión de herramientas de monitoreo en tiempo real de rendimiento y actividad.**
- **Protección de Datos / Propiedad Intelectual (PD/PI): Asegurarse de la protección de datos sensibles y propiedad intelectual.**

Completa la siguiente tabla indicando, para cada activo, las comprobaciones de seguridad aplicables. Utiliza una marca de verificación (✓) para señalar las comprobaciones relevantes para cada activo. Además, para cada activo, incluye un razonamiento breve sobre por qué es necesario aplicar una de las comprobaciones de seguridad marcadas o una explicación general y breve de ellas.

Activo	Antimalware	Gestión Permisos	Cumplimiento Legal	Prevención Fraude	Actualizaciones	Monitorización	PD/PI	Justificación
Router	✓	✓	✓	✓	✓	✓		Conexión a Internet, requiere monitoreo y permisos
Switches			✓		✓	✓		Administra la red interna
Puestos trabajo	✓	✓	✓	✓	✓	✓	✓	Puntos críticos por sus interacciones
Servidor ERP	✓	✓	✓	✓	✓	✓	✓	Gestiona información delicada
NAS	✓	✓	✓		✓	✓	✓	Almacena datos sensibles
Firewall		✓	✓		✓	✓		Filtra tráfico en red
PLC						✓		Controla únicamente procesos
Servidor de laboratorio	✓	✓	✓		✓	✓	✓	Realiza simulaciones
Servidor Big Data	✓	✓	✓		✓	✓	✓	Interactúa con datos
Vault	✓	✓	✓	✓	✓	✓	✓	Gestiona credenciales sensibles
IDS			✓		✓	✓		Detecta intrusiones
Portal Web	✓	✓	✓	✓	✓	✓	✓	Expuesto en internet
SCADA		✓	✓		✓	✓	✓	Supervisa procesos
Dispositivos fabriles						✓		Fallos en funcionamiento

Justificación de las comprobaciones seleccionadas para cada activo:

Los switches son cruciales para las conexiones internas, por lo que es fundamental realizar comprobaciones relacionadas con el cumplimiento legal y actualizaciones para garantizar que cumplen la normativa y evitar vulnerabilidades. Es esencial la monitorización para detectar comportamientos anómalos

en la red. Otros elementos no serían necesarios por no afectar directamente por no ser dispositivos usados por usuarios.

Los puestos de trabajo requieren todas las comprobaciones debido a tener interacción directa con Internet y con otros activos, pueden ser objetivo de malware, accesos no autorizados, debido a algún error no tener las actualizaciones de sistema operativo o aplicaciones operativas por tanto es uno de los activos que debe pasar todas las comprobaciones.

Para el servidor ERP todas las medidas son relevantes por su gestión de recursos empresariales importantes, ya sean actividades comerciales, la contabilidad, la gestión de proyectos… Por ello debe estar bien protegido.

El Nas, su función es el almacenamiento de datos sensibles para la empresa, por tanto todas las comprobaciones serán recomendables para que tenga una protección segura debido a la importancia de la información que maneja, excepto la prevención de fraude porque su función es el almacenaje.

El antimalware, no será necesario las comprobaciones antimalware porque sirve para el filtrado en la red, no para ejecutar softwares o almacenaje de archivos posiblemente infectados, por esto mismo tampoco aplican la protección de datos o la prevención de fraude.

El PLC requiere solo de monitorización porque se encarga de controlar procesos y no interviene con softwares o datos que puedan ser vulnerables.

El servidor de laboratorio, no sería necesario la prevención antimalware debido a que no interviene en operaciones comerciales, el resto si es importante porque se ejecutan softwares, necesitamos tener un control de accesos, se deben proteger los datos que almacena…

Para el servidor Big data igual que con el servidor ERP porque trata con datos sensibles necesitamos controlar el acceso, mantener la seguridad con actualizaciones y la protección de esos datos, no sería necesario la prevención de fraude porque no se realizan operaciones.

La función de un vault es almacenar y gestionar credenciales, claves y datos sensibles por esto necesitamos realizar todas las pruebas y garantizar que no haya vulnerabilidades.

El IDS requiere el cumplimiento legal y tener al día actualizaciones, el resto no es necesario porque se encarga de la detección de intrusiones.

El portal web está en internet por eso requiere todas las medidas para prevenir un ataque, la vulnerabilidad de los datos expuestos y asegurar el cumplimiento legal.

Un scada es un sistema que supervisa y controla los procesos industriales, las comprobaciones como la gestión de permisos, la monitorización y el cumplimiento legal, son importantes entre otras para proteger los los procesos, no es vulnerable contra malwares ni contra fraudes.

Por último, los dispositivos fabriles únicamente necesitan ser monitorizados para evitar posibles fallos en su funcionamiento pero no son vulnerables contra las demás amenazas.

Apartado 4: Detallar los tipos de auditorías que aplican y sus procedimientos asociados.
Una vez identificadas las comprobaciones de seguridad de cada activo, es necesario definir las auditorías específicas que se deben realizar para garantizar su correcto funcionamiento y nivel de seguridad. Las auditorías de seguridad son evaluaciones técnicas que se llevan a cabo para identificar vulnerabilidades, medir la efectividad de las medidas de protección, y asegurar que los activos cumplen con los requisitos de seguridad.
A continuación, se detallan algunos tipos de auditorías aplicables en un entorno empresarial con componentes de TI y OT, junto con una descripción general de su objetivo:

- **Test de penetración o de Hacking Ético: Simula un ataque a la infraestructura para detectar vulnerabilidades explotables antes de que los atacantes reales puedan aprovecharlas.**
- **Auditoría de red: Analiza el diseño, configuración y tráfico de la red para detectar posibles fallos de seguridad y mejorar la segmentación y el control de acceso.**
- **Auditoría de seguridad perimetral: Evalúa las medidas de seguridad en los puntos de entrada y salida de la red, asegurando que los sistemas de protección frontera cumplen su función de barrera.**

- **Auditoría web: Se centra en la seguridad de las aplicaciones que ofrecen servicios web.**
- **Auditoría forense: se realiza tras un incidente de seguridad para analizar lo ocurrido, identificar la causa raíz y proponer soluciones de mejora.**
- **Auditoría legal: Asegura que el uso de los sistemas y el manejo de la información cumplan con las normativas legales y regulatorias aplicables, como protección de datos y privacidad.**
- **Registro Logs: Consiste en analizar los registros de actividad de los sistemas y dispositivos para detectar patrones sospechosos y evaluar incidentes.**

En este apartado debes recoger la información solicitada según este formato:
Completa la siguiente tabla indicando, para cada activo, las auditorías aplicables. Utiliza una marca de verificación (✓) para señalar las auditorías relevantes para cada activo.
Acción específica de auditoría: En la última columna, añade una acción específica que debería ejecutarse durante una de las auditorías aplicables al activo. Esta acción debe estar alineada con el tipo de auditoría y el rol del activo en la empresa.

Activo	Hacking Ético	Auditoría de Red	Seguridad Perimetral	Auditoría Web	Forense	Legal	Revisión Logs	Acción Específica
Router	✓	✓	✓			✓	✓	Revisar logs tráfico detectar anomalías
Switches		✓	✓			✓	✓	Revisar configuraciones y autenticaciones acceso
Puestos trabajo	✓				✓	✓	✓	Análisis malware
Servidor ERP	✓	✓	✓		✓	✓	✓	Prevenir manipulaciones
NAS	✓	✓	✓		✓	✓	✓	Cifrar correctamente los datos
Firewall		✓	✓			✓	✓	Revisar reglas de tráfico
PLC			✓			✓	✓	Comprobación firmware
Servidor de laboratorio	✓	✓	✓		✓	✓	✓	Simular ataques controlados
Servidor Big Data	✓	✓	✓		✓	✓	✓	Identificar patrones sospechosos
Vault	✓	✓	✓		✓	✓	✓	Revisar control acceso y cifrado
IDS	✓	✓	✓			✓	✓	Revisar alertas ante amenazas
Portal Web	✓	✓	✓	✓	✓	✓	✓	Comprobar

								cifrado contraseñas y https
SCADA	✓	✓	✓		✓	✓	✓	Actualizar versión
Dispositivos fabriles		✓	✓			✓	✓	Monitoreo irregularidades

Justificación de las auditorías seleccionadas y la acción específica a llevar a cabo:

Los Switches requieren auditoría en red para garantizar la correcta segmentación del tráfico y seguridad perimetral para evitar accesos no deseados en la red. Son relevantes las auditorías de revisión de logs y legal para garantizar que se cumplan las normas y supervisar eventos de seguridad. Se podría revisar la configuración VLAN y las autenticaciones para asegurar que estén correctamente protegidas y segmentadas.

Puestos de trabajo, se han seleccionado esas auditorías para poder identificar las vulnerabilidades en los sistemas operativos/softwares, identificar los posibles incidentes de seguridad, revisar logs y el cumplimiento de la normativa, con la finalidad de hacer un análisis de posibles malwares por si existe alguna amenaza.

Servidor ERP, haremos una simulación de ataque para asegurar la integridad de los datos para prevenir modificaciones no deseadas, protegeremos el acceso, revisaremos logs, investigaremos brechas de datos entre otros.

NAS, identificamos las vulnerabilidades, la conectividad, reforzaremos la protección con algunas de las auditorías, para comprobar el cifrado de los datos y el acceso a ellos

Firewall, vamos a revisar las reglas o políticas de tráfico con el fin de prevenir brechas con el uso de auditorías que evalúen el filtrado de tráfico, revisar que las políticas cumplan la normativa, detectar accesos no autorizados…

PLC, únicamente será necesario comprobar que la comunicación de este con los demás activos sea segura, evaluar cumplimiento normativa, detectar posibles fallos. Auditamos el firmware para prevenir manipulaciones.

Servidor de laboratorio, se requiere auditorías para identificar vulnerabilidades aunque sea para pruebas, asi como protegerlo de accesos no permitidos, nos apoyaremos de las auditorías forense y legal para gestionar adecuadamente los incidentes. Una acción específica sería simular ataques para detectar las vulnerabilidades antes de ser descubiertas.

Servidor Big Data, para este servidor necesitamos verificar la resistencia antes ataques, el correcto intercambio de datos, protegerlo de accesos externos. Para ello detallaremos los registros de acceso para identificar inicio/uso indebido del activo.

Vault, deberemos detectar vulnerabilidades, comprobar conexiones y accesos, e investigar posibles incidentes siguiendo los estándares. Verificaremos los requisitos del control de acceso y cifrado para garantizar protección

IDS, haremos pruebas para ver si puede detectar correctamente las intrusiones, reforzando su eficacia, aseguraremos el cumplimiento de la normativa… Revisaremos configuraciones de aviso ante amenazas

Portal Web, realizando las auditorías seleccionadas observamos las vulnerabilidades, revisar riesgos aplicación web, así como proteger el acceso, haciendo que cumpla la normativa. Verificar que tanto las contraseñas de acceso tengan la complejidad requerida así como que su cifrado sea https.

SCADA, excepto la auditoría web, requiere las demás pruebas para detectar brechas, proteger accesos o monitorizar eventos, entre otras. Una acción sencilla puede ser comprobar que este dispositivo se encuentre en la última versión disponible.

Dispositivos fabriles, comprobar su integración con el respo de la infraestructura, protegerlos contra acceso no autorizados, detectar anomalías ocurridas. Monitorizar dispositivos para identificar comportamientos irregulares.

Apartado 5: Detallar un Esquema de Mejora Continua o un Modelo de Madurez.
Para este apartado, deberás investigar y describir brevemente un modelo de madurez y un esquema de mejora continua, seleccionando uno de cada tipo que consideres relevante para la empresa ficticia.

- **Modelo de Madurez: Selecciona un modelo de madurez aplicable a la ciberseguridad empresarial. Realiza una breve descripción de sus niveles y su enfoque general para la mejora de procesos.**
- **Esquema de Mejora Continua: Describe un esquema de mejora continua que se pueda implementar en la empresa. Expón los pasos o fases clave del esquema y cómo se aplican estos.**
- **Selección Justificada: Una vez que hayas descrito ambos enfoques, decide cuál de los dos (modelo de madurez o esquema de mejora continua) es más conveniente para la empresa ficticia y justifica tu elección.**

Los modelos de madurez son herramientas que ayudan a las empresas a medir que tan avanzadas están en un área en específico, los procesos internos o la gestión de proyectos, también se utiliza como guía para mejorar mostrando los pasos necesarios para pasar de un nivel básico a uno avanzado. Nos indica dónde está situada la empresa, dónde se quiere llegar y los pasos a seguir de un punto a otro. Existen varios modelos dependiendo del área que se quiera trabajar:

- CMMI, Capability Maturity Model Integration, usado para TI y ciberseguridad, evalúa los procesos para ver cómo de eficientes y organizados están.
- COBIT, Control Objetives for Information and related Technologies,enfocado en la gobernanza TI y alineación de los objetivos con las tecnologías utilizadas.
- NIST Cybersecurity Framework (CSF), aplicado a ciberseguridad para evaluar la gestión de riesgos y mejora de la seguridad de una empresa.
- ISO 9001, evalúa a las empresas a garantizar la calidad de sus procesos y productos
- ITIL, Information Technology Infrastructure Library, utilizado para la mejora de los servicios IT.

Todos ellos se dividen en escalones que muestran el progreso de la empresa, en los que se detallan como están organizados los procesos, que objetivos se tienen, ejemplos, que prácticas se emplean y qué mejoras se logran una vez superemos el nivel.

El CMMI (Capability Maturity Model Integration) está adaptado especialmente para ciberseguridad, proporciona un marco para evaluar y mejorar los procesos relacionados con la gestión de seguridad informática en una empresa. Este modelo mide la capacidad de una empresa para protegerse de amenazas y gestionar riesgos. Niveles de madurez:

1. Inicial, los procesos reactivos no están documentados, la seguridad se maneja caso por caso, sin preveerlos. Se responde a los ataques solo cuando pasan.
2. Repetible, existen políticas básicas de ciberseguridad pero no se aplican de la misma forma en todos los casos. Los procesos dependen de personas en lugar de tener sistemas definidos.
3. Definido, los procesos están documentados, estandarizados y aplicados. Se crean políticas claras, como auditorías.
4. Gestionado, procesos monitoreados y medidos, se utilizan métricas para evaluar la efectividad de la empresa en ciberseguridad. Se miden los ataques detectados o bloqueados y se ajustan las medidas según los datos.
5. Optimizado, la seguridad es proactiva, se utilizan tecnologías avanzadas y análisis preventivos para identificar amenazas y detenerlas antes de que afecten.

Para la mejora de los procesos de ciberseguridad de una empresa el modelo CMMI es más adecuado porque permite evaluar el nivel actual de madurez de la organización y proporciona una ruta clara para establecer metas y mejorar de forma progresiva y estructurada. Es útil para estandarizar procesos, establecer métricas y avanzar hacia prácticas más eficientes y proactivas. Esto lo convierte en la mejor opción para empresas que buscan desarrollar y optimizar sus capacidades en ciberseguridad a largo plazo
Mientras que el modelo NIST CSF es excelente para establecer controles específicos y responder a problemas inmediatos, el CMMI se enfoca en la optimización continua de procesos asegurando la mejora progresiva en la gestión de riesgos y en la respuesta ante incidentes. Esto lo convierte en una mejor opción para desarrollar procesos desde cero o elevar sus prácticas.

Un esquema de mejora continua es un proceso que busca identificar y evaluar cambios para hacer que una empresa funcione mejor. Este enfoque fomenta la revisión constante de los procesos, ayudando a identificar los fallos, optimizar recursos y mejorar los resultados. Existen varios tipos de esquemas:

- Ciclo PDCA (Plan-Do-Check-Act), consiste en cuatro pasos para identificar y resolver problemas.
- Six Sigma, se enfoca en reducir errores.
- Kaizen, promueve las mejoras constantes
- Lean, busca hacer más eficientes los procesos.

En la empresa descrita sería más práctico y efectivo implementar un esquema de mejora continua basado en el Ciclo PDCA. Este modelo permitirá mantener la seguridad, optimizar procesos… A continuación se detallan los pasos clave y su aplicación en la empresa:

1. Planificar (identificar y analizar las áreas a mejorar), identificaremos los procesos que necesitan una mejora tanto en la red interna como en la red de operaciones, se establecerán los objetivos priorizando las áreas según su impacto y se realizará un análisis de riesgos de cada una de las zonas de la red.
2. Hacer (implementación soluciones planificadas), desarrollar e implementar las mejoras planificadas, se formará a los empleados para que se adapten a las nuevas directrices, se introducirán tecnologías o configuraciones nuevas y se realizarán pruebas para garantizar el funcionamiento de las mejoras aplicadas.
3. Verificar (medición y análisis de resultados) se monitorean y miden si las acciones implementadas logran el resultado esperado, se comparan indicadores clave antes y después de las mejoras y se analizan los incidentes para comprobar que las soluciones fueron efectivas.
4. Actuar (estandarización y ajustes) en caso de que las mejoras sean exitosas, documentarlas y estandarizarse, en caso de que haya fallos, ajustar las soluciones y repetir el ciclo. Por último se comunicarán los resultados al equipo para fomentar la cultura de mejora.

Algunos aspectos clave de mejora son, en la LAN mejorar la protección de los datos financieros, asegurando que los sistemas ERP y Big Data esten bien configurados y monitoreados, en la DMZ, comprobar la robustez del soc con herramientas avanzadas para la detección de incidentes y en la Smart Factory, minimizar la exposición de los sistemas de operación garantizando la integridad de los PLC y SCADA mediante monitoreo.
Este ciclo ayudará a mantener la seguridad, optimización de los procesos y adaptarse a las nuevas tecnologías. Siendo el ciclo más adecuado por ofrecer un enfoque estructurado para las mejoras continuas, tratando de forma efectiva tanto los procesos administrativos (IT) como los industriales (OT). Su forma repetitiva facilita la identificación y resolución de problemas de seguridad, eficiencia y operatividad de cada una de las zonas de la red, además al retroalimentarse permite ajustar las soluciones, adaptarse y asegurar la continuidad operativa, lo cual es clave para un entorno que depende de la tecnología.

Entre el modelo de madurez CMMI y el esquema de mejora continua PDCA, el PDCA es la opción más conveniente debido a su flexibilidad y facilidad de implementación en un entorno dinámico como lo es en esta PYME ficticia.

El modelo CMMI es ideal para empresas que buscan establecer procesos estandarizados a largo plazo y medir su madurez. Sin embargo, su implementación requiere tener al alcance muchos recursos y experiencia que puede no tener una empresa pequeña. Además se centra en la evaluación de los procesos que pueden no ser urgentes para empresas que se enfrentan a desafíos de amenazas de ciberseguridad y eficiencia operativa. Por otro lado, el PDCA es un enfoque más práctico que permite abordar problemas específicos y mejorar continuamente. Es fácil de aplicar y ajustar, lo que hace ideal para resolver rápidamente los problemas que puedan surgir mientras se establecen bases sólidas para el futuro. Además su repetitividad permite adaptarse a los cambios tecnológicos y operativos.

En conclusión, ambos enfoques son buenas opciones pero el PDCA se ajusta mejor a las necesidades de la empresa por ser más sencillo y práctico y permitir mejorar los procesos y resolver problemas de forma rápida. Aunque el modelo CMMI es útil para medir y organizar procesos, requiere más recursos por ello el PDCA sería mejor opción por su mejora continua sin complicaciones ni tener que detener sus operaciones.