APUNTES 01

DESARROLLO DE PLANES DE PREVENCIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD

INCIDENTES DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

La Cibernética es la ciencia que estudia los flujos de información de un sistema y cómo éste los usa para autocontrolarse. Esta ciencia aplica en muchas disciplinas, desde la Física hasta la Medicina, pero en la actualidad se utiliza principalmente en Teoría de Sistemas y, en especial, en los Sistemas Informáticos.
Por otra parte y como su propio nombre indica, la Ciberseguridad consiste en aplicar las Estrategias, Tácticas y Operativas de la seguridad clásica a la Cibernética. En línea con esto, es importante considerar que la seguridad clásica tiene como pilares básicos la Prevención y la Concienciación de las personas, principios que aplican directamente en el ámbito empresarial.
En esta unidad reflexionaremos acerca de cómo implementar Planes de Prevención y Concienciación que nos ayuden a reforzar la resistencia de una empresa frente a los ataques informáticos de cualquier índole.

La ciberseguridad no es una ciencia exacta. Sus límites coinciden con los del ingenio humano, que siempre trabaja para buscar una solución a cualquier problema, o una salida a cualquier bloqueo. El perímetro de este ámbito es tan variable e imprevisible, que los expertos en Ciberseguridad realmente son auténticos Gestores de la Incertidumbre.
El problema es que esto aplica para el bien y el mal. Cualquier estrategia de prevención en cualquier ámbito profesional será buena para eludir la mayoría de los incidentes de seguridad conocidos, no obstante, estas estrategias serán también retos para los malintencionados, que las verán como objetivos a batir.

Teniendo esto en cuenta, podremos enunciar las Tres Reglas Pragmáticas de la Ciberseguridad de la forma siguiente, según Agile Corporation:

- Prevención. Protegerse de lo conocido. Habilitar siempre todas las medidas de seguridad necesarias frente a los problemas conocidos, desde la instalación de todas las versiones y parches que se precisen, hasta el despliegue de herramientas protectoras ante el malware o los incidentes consecuencia del mismo.
- Concienciación. Alertar de lo desconocido. Implementar protocolos de alarma ante incidentes de naturaleza desconocida o que al menos resulten sospechosos, para frenar su avance lo antes posible. En estos protocolos se deberán incluir tanto procesos mecanizados como actuación de personas previamente formadas.
- Respuesta. Prepararse para el Caso Peor. Lamentablemente casi nunca es posible prever todos los incidentes ni todas las variantes de ataque, por lo que resultará clave implementar mecanismos de respuesta rápida para contener las incursiones y minimizar el daño infligido por ellas en un momento dado.

En este Módulo Profesional se reflexionará acerca de cómo preparar el terreno para la correcta aplicación de dichas reglas pragmáticas, revisando para ello los procedimientos de prevención de incidentes, los mecanismos de alerta temprana y las tácticas de reacción en caso de que finalmente se materialicen dichos incidentes.
Además de revisar las cuestiones de organización en términos de prevención y concienciación, se trabajará en la implementación de una Maqueta Real de un SOC, dotado de un IDS y de un SIEM. Esta maqueta será totalmente operativa y permitirá al alumno comprobar la enorme importancia que tiene implementar mecanismos de alerta temprana, y analizar los incidentes en detalle en un entorno experto y con amplia información de incidentes anteriores acaecidos en un contexto en particular.
Un SOC siempre es la base práctica de cualquier estrategia integral de ciberseguridad, con énfasis en el capítulo de los Incidentes, pues permite crear el entorno de alerta y estudio necesario para detectar y analizar en caliente cualquier incidente de seguridad, acumulando cada vez más experiencia y posibilitando la adopción rápida de planes de reacción contundentes que contengan los ataques y que permitan la continuidad del servicio en todo momento.

1.- PRINCIPIOS GENERALES EN MATERIA DE CIBERSEGURIDAD

El CCN publica y actualiza periódicamente un informe en el que se detallan tanto los Principios Generales en Materia de Ciberseguridad, como recomendaciones, medidas fundamentales y buenas prácticas para concienciar y facilitar el uso seguro de las Tecnologías de la Información y la Comunicación. Dicho informe incluye un Decálogo Básico de Ciberseguridad:

Decálogo Básico de Ciberseguridad:

1.- La cultura de la ciberseguridad, la concienciación del empleado, debe ser uno de los pilares en los que se asiente la ciberseguridad de cualquier organización.

2.- No se deberá abrir ningún enlace ni descargar ningún fichero adjunto procedente de un correo electrónico que presente cualquier indicio o patrón fuera de lo habitual.

3.- Utilizar software de seguridad, herramientas antivirus, herramientas antimalware, cortafuegos personales y herramientas de borrado seguro debe ser algo irrenunciable cuando se utiliza un sistema de las TIC.

4.- Limitar la superficie de exposición a las amenazas, pues no sólo hay que implementar medidas de seguridad que protejan el acceso a la información, sino que hay que determinar los servicios que son estrictamente necesarios.

5.- Cifrar la información sensible y revisar con frecuencia el mecanismo de cifrado para usar el que sea más fuerte en cada momento.

6.- Utilizar contraseñas adaptadas a la funcionalidad, siendo conscientes de que la autenticación de doble o múltiple factor ya es una necesidad. Renovar además con frecuencia dichas contraseñas, puesto que esto complica muchísimo la labor al atacante.

7.- Efectuar un borrado seguro de la información una vez que ésta ya no sea necesaria o se vaya a retirar de uso el soporte en cuestión.

8.- Realizar copias de seguridad periódicas, pues no existe otra alternativa mejor de recuperación en caso de infección de código malicioso tipo ransomware, pérdida de datos, averías del hardware de almacenamiento, borrado de información involuntaria por parte del usuario y otras amenazas. Estas copias de seguridad deberán ser frecuentes y cuidadosas, para asegurar que se disponga de muchas réplicas y que no se esté respaldando también el malware durante el proceso de backup.

9.- Mantener actualizadas las aplicaciones y el sistema operativo es la mejor manera de evitar dar facilidades a la potencial amenaza, en línea con el primer principio pragmático de la Ciberseguridad: protegerse frente a lo conocido.

10.- Revisar regularmente la configuración de seguridad aplicada, los permisos de las aplicaciones y las opciones de seguridad.

Ejercicio Principio 2 - Cualquier acción de un usuario en un sistema informático puede desencadenar la ejecución de un Vector, inyectando código malicioso en el sistema. Instalación de un Troyano de Acceso Remoto en un dispositivo, tomando el control de ambos dispositivos.
Ejercicio Principio 3 - Utilizar software de seguridad, herramientas antivirus y antimalware, cortafuegos personales, herramientas de borrado seguro, etc. debe ser algo irrenunciable cuando se utiliza un sistema de las TIC. La más efectiva es el Cortafuegos, que se puede implementar mediante hardware o software. Se muestra el uso del Cortafuegos, UFW Ubuntu.
Ejercicio Principio 4 - Además de la estrategia lógica a aplicar para reducir la superficie expuesta a los ataques, existen estructuras físicas y topologías de red que también suman. Se muestra la Estructura en Trípode, que permite exponer sólo los servidores frontera de la denominada "Zona Desmilitarizada".
Ejercicio Principio 5 - En un mundo informatizado y con auge de la tecnología, hay que cifrar toda aquella información que se considere importante, confidencial o crítica. Procedimiento de cifrado asimétrico de la información, que permite garantizar la identidad del emisor de los datos y sólo los podrá descifrar la entidad autorizada.
Ejercicio Principio 6 - La complejidad de una contraseña no es algo insustancial. Resulta sorprendente cuando la clave de un portal, indica que sólo podrá tener 8 caracteres alfanuméricos, no pudiendo contener símbolos. Este simple mensaje reduce de golpe la combinatoria de claves posibles. Se mostrará la construcción de Diccionarios con Crunch basados en Ingeniería Social y se atacará un fichero cifrado utilizando John the Ripper, se comprobará la complicación del crackeo según la complejidad de las claves de cifrado.
Ejercicio Principio 10 - Los Sistemas de Detección de Intrusiones de código abierto, se benefician de actualizaciones de las reglas de detección, tanto por adición de nuevas reglas que alertan de nuevos ataques, como por retirada de reglas obsoletas. Localizar las reglas de la comunidad Snort en una instalación típica de este IDS e indicar dónde se deben configurar las reglas ad hoc.

2.- NORMATIVA DE PROTECCIÓN DEL PUESTO DE TRABAJO

La Extensión del Ámbito del Puesto de Trabajo

El principal activo de una empresa es su información, estos datos son los relativos al desarrollo habitual de su negocio en las aplicaciones de producción, además de los puros datos estructurales y administrativos (topología de red, plan de direcciones, máquinas, contabilidad, nómina, estrategia, logística, operaciones, inventario de activos y resto de datos de la empresa). La gestión de esta información se realiza desde el Puesto de Trabajo de cada empleado.

El ámbito del Puesto de Trabajo ha ido extendiéndose, tanto con la incorporación de dispositivos tecnológicos, como con la ampliación de su alcance físico y geográfico, tras la incorporación del concepto de teletrabajo.

Actualmente se utilizan dispositivos muy diversos, tales como ordenadores de sobremesa, portátiles, teléfonos móviles, tabletas, dispositivos de almacenamiento extraíbles, impresoras de red, escáneres, etc. Dentro de este escenario de riesgo es donde pueden producirse fugas de datos, pérdida de información confidencial o infecciones por malware.

Para mitigar estos riesgos, se deben establecer medidas de seguridad, adaptadas a las necesidades de cada tipo de puesto de trabajo, tanto de carácter organizativo como técnico. La aplicación de estas medidas, junto con un adecuado plan de formación y concienciación de los empleados que gestionan la información desde sus puestos de trabajo, ayudará a proteger de manera sólida cualquier empresa.

Para saber más El INCIBE publica periódicamente un Dossier sobre Protección del Puesto de Trabajo, dentro de su colección “Protege tu empresa”. En él se abordan de forma extensa y actualizada todos los aspectos de la ciberseguridad relativos a esta materia.

Ejercicio Ataque a un Inventario de Activos - El inventario de activos de una empresa contiene la información relativa a su entorno informático y productivo. Si un pirata informático accede a esta información, se llevará la empresa completa. Se construirá una maqueta de Inventario de Activos sobre una base de datos relacional, atacándola después con Medusa para mostrar cuán fácil es entrar fraudulentamente en este tipo de inventarios.

3.- PLAN DE FORMACIÓN Y CONCIENCIACIÓN EN MATERIA DE CIBERSEGURIDAD.

Los Riesgos asociados a las Nuevas Tecnologías

El creciente uso de las nuevas tecnologías en las empresas hace indispensable la concienciación sobre los riesgos asociados a las mismas. Es necesario que los empleados conozcan y apliquen buenas prácticas en el uso de todo tipo de dispositivos (de escritorio, portátiles, móviles, pendrives) y soluciones tecnológicas (páginas web, servicios en la nube, redes sociales, correo electrónico) para lo cual se les debe proporcionar formación en ciberseguridad adecuada a su puesto, ya que de este modo se pueden prevenir la mayoría de los incidentes.

Para alcanzar los objetivos fijados con esta política, será necesario el compromiso total por parte de la Dirección, que habrá de ser consciente de que la formación deberá ser una actividad continua que habrá de repetirse y revisarse periódicamente, para que surta su efecto de prevención de incidentes y esté adaptada a las nuevas tecnologías que inevitablemente se irán utilizando.

Los objetivos del Plan de Formación y Concienciación deberán asegurar que, en todo momento, los empleados conocen, entienden y cumplen las normas y las medidas de protección adoptadas en materia de ciberseguridad, advirtiéndoles de los riesgos que puede suponer un mal uso de los dispositivos y soluciones tecnológicas a su alcance.

Es importante resaltar que ciertas posiciones en las empresas llevan aparejada una gran responsabilidad sobre la información, con riesgos potenciales de aplicación de medidas disciplinarias en caso de pérdida o divulgación de datos sensibles, como pueden ser aquellos que afecten a la propiedad industrial.

Dicha responsabilidad puede llegar incluso a tener implicaciones legales si llegan a estar involucrados datos personales protegidos, pues las personas responsables de los mismos figurarán en una lista oficial declarada en las Administraciones Públicas (Responsables de Tratamiento de Datos y Delegados de Protección de Datos), por lo que en algunos casos puede que sean ellos mismos quienes tengan que responder directamente de una filtración de datos.

Ejercicio Ataque a un Servidor Empresarial - Se crearán diccionarios de credenciales de usuarios (login-password) y se usarán para atacar a un servidor empresarial con la herramienta Hydra, provocando Denegación de Servicio.

3.1.- CONTROLES

Se pueden definir una serie de controles para revisar el cumplimiento de la política de seguridad, en lo relativo a concienciación y formación en ciberseguridad.

Dichos controles se clasifican en dos niveles de complejidad:

- Básico. El esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- Avanzado. El esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Además, estos controles podrán tener el siguiente alcance:

- Procesos. Aplica a la dirección o al personal de gestión.
- Tecnología. Aplica al personal técnico especializado.
- Personas. Aplica a todo el personal.

Ejercicio Controles Básicos para Procesos - Se efectuará el ejercicio para el Nivel Básico, Alcance Procesos.

- Difusión de la política de seguridad. Documentar y difundir las normas de ciberseguridad de la empresa para que estén siempre accesibles.
- Concretar el plan de formación. Elaborar o revisar el plan de formación para elevar el nivel de seguridad de la plantilla.
- Programas de formación específicos. Desarrollar y aplicar programas de formación en ciberseguridad adecuados a los distintos puestos de trabajo.
- Periodicidad de la formación. Asegurar que los empleados realizan cursos o van a charlas de concienciación, cada período prefijado.
- Evaluar el aprendizaje obtenido. Comprobar la asimilación del conocimiento adquirido por los empleados.
- Promover una cultura de seguridad de la información que abarque a toda la cadena de suministro de la empresa y a los clientes.

3.2.- PUNTOS CLAVE

Los puntos clave de esta política son:

- Difusión de la política de seguridad. Las normas de seguridad de la información de la organización deben estar correctamente documentadas y al alcance de todo el personal en todo momento.
- Concretar el plan de formación. Se deben seleccionar los aspectos a cubrir para garantizar el éxito del programa formativo.
- Programas de formación específicos. Es conveniente analizar si se deben desarrollar programas de formación y concienciación especializados para ciertos perfiles de empleados, tales como técnicos de soporte y administradores de sistemas. Además, sería de gran utilidad elaborar una actividad formativa introductoria para los nuevos empleados (Paquete de Bienvenida o Welcome Pack).
- Periodicidad de la formación. Se debe establecer una periodicidad en las actividades formativas y de concienciación. De esta manera se conseguirá tener unos contenidos actualizados en materia de ciberseguridad y se reforzarán las debilidades detectadas o los mensajes de mayor importancia.
- Promover una cultura de seguridad de la información. Además de concienciar y formar a los empleados en ciberseguridad, es conveniente exigir a las entidades externas que interactúan con los sistemas de información que sus políticas de ciberseguridad estén alineadas con la de la empresa. Se intentará pues extender el plan de concienciación a la mayoría de los proveedores y clientes.
- Evaluar el aprendizaje obtenido. Se considerará la necesidad de realizar evaluaciones entre los empleados (assessment) para determinar el grado de concienciación y formación que éstos hayan alcanzado.

Ejercicio Concretar el Plan de Formación - Desarrollaremos el punto "Concretar el Plan de Formación".

- Procedimientos y controles de seguridad básicos.
- Necesidad de conocer y cumplir normas, leyes, contratos y acuerdos.
- Seguridad en el puesto de trabajo, aplicaciones permitidas, uso correcto de los recursos, propiedad intelectual, protección de datos personales, etc.
- Concienciar a los empleados sobre la existencia y peligros de la Ingeniería Social (espionaje humano o robótico).
- Responsabilidad personal por acción u omisión y posibles sanciones.

4.- MATERIALES DE FORMACIÓN Y CONCIENCIACIÓN

Los Riesgos de los Empleados y de la Organización

Los empleados son el motor de la empresa, los que hacen posible su funcionamiento. A diario se enfrentan a un entorno de trabajo cada vez más digitalizado, revisando y respondiendo al correo electrónico, procesando facturas, tramitando pedidos online, gestionando procesos a través de aplicaciones en la nube o en dispositivos móviles, o bien, realizando tareas de marketing y difusión en Redes Sociales o a través de la Página Web de la empresa. Los empleados utilizan la tecnología en su día a día, pero ¿son realmente conscientes de los riesgos a los que están expuestos y en qué medida éstos pueden poner en jaque a la organización?

La mayoría de las situaciones que afectan a la continuidad del negocio se deben de alguna forma a la falta de preparación en ciberseguridad de aquellos que tienen que manejar la tecnología. Para suplir esa debilidad las PYMEs y microempresas pueden utilizar un Kit de Concienciación como el propuesto por el INCIBE, que consiste en una herramienta didáctica para concienciar y entrenar a los empleados en el uso seguro de la tecnología.
Con este Kit de Concienciación los empleados podrán acceder a recursos didácticos y herramientas de entrenamiento para evitar los incidentes de ciberseguridad que afectan habitualmente a las empresas. Este kit ha sido diseñado para que su implantación puedan llevarla a cabo organizaciones de todos los sectores, sin necesidad de tener conocimientos técnicos previos.

5.- AUDITORÍAS INTERNAS DE CUMPLIMIENTO EN MATERIA DE PREVENCIÓN

El Concepto de Nivel de Seguridad

A la hora de implementar la ciberseguridad en una organización, primero hay que ser consciente del nivel de seguridad existente en la empresa, y posteriormente, establecer el nivel a conseguir para garantizar la seguridad de los procesos más críticos (escenarios de partida y de llegada, también conocidos como AS IS y TO BE).
Para la consecución de tal fin, será necesario realizar auditorías que permitan analizar y evaluar la situación de los distintos elementos que conforman la organización, ya sean tecnológicos (sistemas, ordenadores, routers), o físicos (salas de servidores, control de acceso a diferentes instalaciones).

Las Auditorías Internas de cumplimiento en materia de prevención deberán realizarse por parte de personal cualificado, lo que sin duda conlleva mejorar la eficacia y eficiencia de todos los procesos de una empresa y, por consiguiente, mejorar su seguridad, es decir, que en ciertos momentos será necesario contar con servicios especializados de auditoría o auditorías forenses, que se encarguen de investigar lo ocurrido tras un incidente grave de seguridad (brecha de datos, botnet, ransomware).
En cualquier caso, las auditorías de sistemas tendrán como finalidad obtener evidencias de cómo los sistemas de información de la organización cumplen con los requisitos de seguridad. Estas evidencias servirán para analizar el estado actual de una empresa en materia de seguridad, o como parte de un proceso de mejora continua o kaizen (que significa literalmente "el cambio es bueno" en japonés)

Ejercicio Servicios Especializados de Auditoría - Se detallarán algunos servicios especializados de auditoría. Se tratará en concreto de los relativos a la revisión de Cumplimiento Legal o Normativo.

- RGPD. Reglamento General de Protección de Datos. Reglamento Europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y su libre circulación.
- SGSI. Sistema de Gestión de la Seguridad de la Información (ISO/IEC 27001), que consiste en un conjunto de políticas de administración de la información.

5.1.- CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE UNA POLÍTICA DE AUDITORÍAS

A continuación, se detallan una serie de controles que deberán tenerse en cuenta en la política de seguridad de auditoría de sistemas.
En primer lugar, habrá que detallar los elementos clave que se desea auditar. Para poder llevar a cabo con éxito un proceso de auditoría es necesario identificar los elementos que son esenciales para el negocio y, por lo tanto, que necesariamente deberán comprobarse: ficheros, bases de datos, páginas web, equipos y programas.

Para cada uno de estos activos se revisará si disponen de las siguientes medidas de seguridad:

- Sistemas antimalware
- Procesos de gestión de permisos
- Procesos de cumplimiento legal (compliance)
- Políticas de prevención de fraude y de fuga de datos
- Sistema de actualizaciones
- Sistemas de monitorización de recursos

Es recomendable seleccionar un esquema de mejora continua o un modelo de madurez para garantizar que los resultados de las auditorías tengan como fin la implantación continua de mejoras en materia de ciberseguridad y la consecución de los diferentes niveles de seguridad.
Se deberá revisar si se tienen que realizar auditorías legales necesarias para garantizar que en la organización se cumplan los requerimientos legales, como por ejemplo el RGPD.
En el caso de que ocurra algún incidente de seguridad habrá que realizar auditorías forenses para identificar cuáles han sido sus causas. Con estas auditorías, se recabarán evidencias para su posterior análisis, cuyo fin será depurar responsabilidades y, según el caso, iniciar un proceso de denuncia.

Con todo lo anterior se establecerán los procedimientos adecuados en función del tipo de auditoría requerido:

- Test de penetración o de Hacking Ético
- Auditoría de red
- Auditoría de seguridad perimetral
- Auditoría web
- Auditoría forense
- Auditoría legal

Habrá que definir en detalle el procedimiento que se seguirá y el registro de logs. Además, habrá que concretar cómo registrar los resultados de las revisiones para realizar los correspondientes informes.

Se planificarán las auditorías de forma periódica. La finalidad de una auditoría es la revisión y evaluación de todos los aspectos relacionados con la seguridad de la información en la organización. Por tanto, se fijará la periodicidad de estas revisiones que deberán realizarse al menos cada seis meses. Además, será necesario repetir estas auditorías tras la implantación de algún cambio significativo en los sistemas de la empresa. Por tanto, si tras un proceso de auditoría se ha implantado una medida que tiene relevancia para el negocio, se establecerá un proceso que audite si esa medida cumple los objetivos y expectativas para los que fue tomada.

Finalmente, se analizará el resultado de la auditoría para buscar errores e identificar debilidades y puntos de mejora. Además, se deberán llevar a cabo las acciones necesarias a fin de corregir las vulnerabilidades detectadas y así:

- Identificar las causas y motivos del resultado desfavorable
- Evaluar las medidas de seguridad
- Implantar y revisar dichas medidas

Siempre existe la duda de si se cuenta con el nivel de seguridad adecuado para proteger la información que se maneja en la organización. Conocer este nivel de seguridad será el primer paso antes de diseñar e implantar cualquier medida de prevención o mitigación, y el método para obtener esta información será a través de una auditoría inicial, que permitirá conocer el estado de seguridad del negocio.
Si se piensa en la seguridad y en la protección de la empresa, resulta fundamental disponer de una política de auditoría de sistemas.

Autoevaluación I

¿Quién publica los Principios Generales en Materia de Ciberseguridad?

a) Instituto Nacional de Ciberseguridad
b) Esquema Nacional de Seguridad
c) Centro Criptológico Nacional

Autoevaluación II

¿Qué ha supuesto para las empresas la implantación del Teletrabajo?

a) Sólo Ampliación del Alcance Físico
b) Ampliación del Alcance Físico y Tecnológico

Autoevaluación III

¿Cuál es el punto más importante del Plan de Formación y Concienciación?

a) Implementar una serie de controles para revisar el cumplimiento de la política de seguridad
b) La Cultura de la Ciberseguridad

Autoevaluación IV

Indicar los requisitos necesarios para implantar el Kit de Concienciación del INCIBE

a) No será necesario disponer de conocimientos previos
b) La organización necesitará una base mínima de Ciberseguridad, que podrá adquirir a través de unos cursos básicos impartidos por el INCIBE.

Autoevaluación V

¿Cuál es el primer paso para implementar una política de auditorías?

a) Revisar si se dispone de las pertinentes medidas de seguridad
b) Detallar los elementos clave que se desea auditar
c) Seleccionar un esquema de mejora continua o un modelo de madurez

TEST I

1- ¿Qué es la Cibernética?

a) La ciencia que estudia la arquitectura de los ordenadores.
b) La ciencia que estudia los flujos de información en un sistema.
c) La ciencia que estudia los fundamentos de la robótica.

2- En el Cifrado Asimétrico:

a) Ambas claves se pueden descifrar.
b) Se cifra con la clave pública y se descifra con la clave privada.
c) Ambas claves pueden cifrar.
d) Se cifra con la clave privada y se descifra con la pública.

3- ¿Cuáles son las amenazas habituales de la información:

a) Hackers.
b) Intrusiones y Malware.
c) Todas las anteriores.
d) Ataques Físicos.

4- ¿Cuál es la clave de un SOC?:

a) El binomio IDS+SIEM.
b) El análisis de los incidentes en un entorno experto y con información de incidentes anteriores.
c) Las reglas de prevención de incidentes.

5- ¿Qué información recoge la norma ISO/IEC 270012:

a) La Ley Orgánica de Protección de Datos de Carácter Personal.
b) Las consideraciones de seguridad perimetral en una organización.
c) Los requisitos para los sistemas de gestión de la seguridad de la información.
d) El reglamento general de protección de datos.

6- ¿Qué organismo publica periódicamente el Dossier sobre Protección del Puesto de Trabajo?
   a) El CCN
   b) El CNI
   c) El CSIRT.
   d) El INCIBE.

7- Los Procesos de Compliance tienen que ver con:
   a) Fuga de Datos.
   b) Cumplimiento Legal.
   c) Prevención del Fraude.
   d) Gestión de Permisos.

8- Limitar la superficie de Exposición a las Amenazas consiste en:
   a) Todas las anteriores.
   b) Limitar el número de máquinas de la LAN que tienen conexión directa con la WAN.
   c) Implementar Medidas de Seguridad para Proteger el Acceso a la Información.
   d) Determinar los servicios que son estrictamente necesarios.

9- ¿En qué consiste la Ciberseguridad?:
   a) En proteger los sistemas de información de una empresa.
   b) En aplicar las estrategias de la seguridad clásica a la Cibernética.
   c) En desarrollar aplicaciones antimalware.

10- ¿Cuál es la mejor alternativa de recuperación en caso de infección por ransomware?:
   a) Realizar copias de seguridad periódicas.
   b) Activar los escudos antimalware.
   c) Para el rescate, pero sólo una vez.
   d) Ninguna de las anteriores.

Solución
Autoevaluación I: c)
Autoevaluación II: b)
Autoevaluación III: b)
Autoevaluación IV: a)
Autoevaluación V: b)
TEST: 1 b), 2 b), 3 c), 4 b), 5 c), 6 d), 7 b), 8 d), 9 b), 10 a)

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)

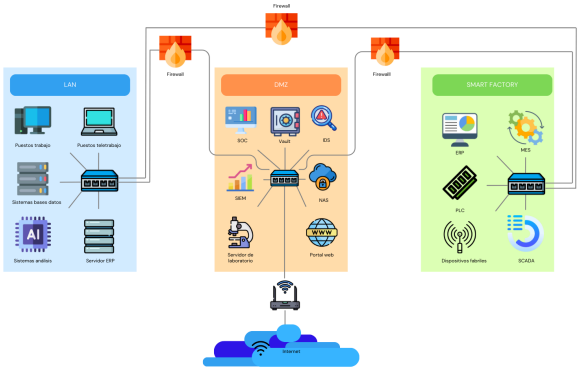
- Puestos de trabajo de los empleados, tanto locales como remotos
- Sistemas de bases de datos y almacenamiento
- ERP (Gestión recursos empresariales)
- Sistemas de análisis (Big Data, IA y Machine Learning)

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.