Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Incidentes de Ciberseguridad

UD01. Auditoría Interna de Prevención.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

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.

¿Qué te pedimos que hagas?

- ✓ **Apartado 1: Diseño del esquema de una Empresa Ficticia.**

  Información básica para diseñar el esquema de la empresa:

  - Para la definición de los elementos de la empresa consideraremos una joven PYME industrial que se dedica a la fabricación de repuestos para el automóvil. Esta empresa estará dotada pues de Tecnologías de Información para su Gestión Empresarial, y de Tecnologías de Operación para su Gestión Fabril.
  - Esta empresa cuenta con un esquema sencillo de Sistemas de Información. El diseño debe seguir las siguientes indicaciones:

    1. Estructura de red en trípode, con todas sus zonas a definir, como la red interna, DMZ, etc.
    2. Los elementos de red que contiene la empresa son: routers, switches, OLT/ONT de fibra, Firewalls, etc.
    3. Contiene los siguientes servicios expuestos al exterior: portal web, servidor NAS con Vault (AutoDesk), servidor laboratorio interno.
    4. Puestos de trabajo remotos.
    5. Puestos de trabajo locales estándar y otros puestos especializados como: SCADA+FIREWALL, sistema de control de inventario, dispositivos fabriles, PLC de control, base de datos económico financiera, entre otros posibles.
    6. Centro de operaciones de seguridad (Security Operations Center - SOC).

  Con la información proporcionada deberás efectuar las siguientes tareas:

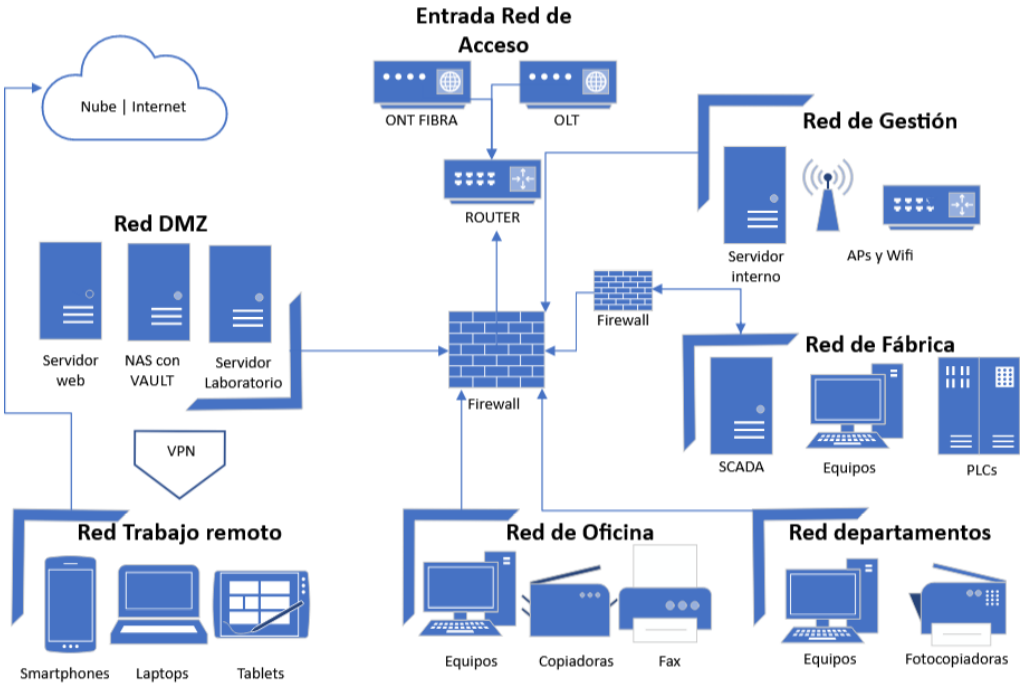
  - Crear un Diagrama de Bloques gráfico de la Empresa Ficticia según la estructura pedida en el que se distribuyan los activos anteriores y otros que consideres necesarios. Para la realización de este diseño se puede usar la herramienta que se considere más idónea. Algunas alternativas pueden ser: draw.io u otras alternativas integradas en suites ofimáticas.

    La estructura queda formada por:

    - ✓ **Red de Acceso**, con el punto de entrada, el ONT de fibra y el router.
    - ✓ La red interna distribuida en:
      Red de Gestión, SOC que incorpora un servidor, APs y controlador Wifi .
      Red de Fábrica, con el servidor SCADA, los equipos necesarios y los PLCs.

Red de Oficina, con los equipos de dirección, administración y contabilidad, Copiadoras/impresoras, Fax.
Red de departamentos: Equipos de áreas técnicas, impresoras/copiadoras.

- ✓ **La red DMZ** con los servidores web, Vault y de laboratorio.
- ✓ **Red de trabajo remoto.** Conectada por VPN a la anterior, con smartphones, laptops o tablets.



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

Deberás efectuar las siguientes tareas:

➢ Tomando el diseño del apartado anterior, efectuar una labor de inventariado de activos hardware y software que se desea auditar. Al menos, de estos activos se debe recoger: nombre o identificador, modelo de máquina, sistema operativo, función en la empresa, dirección IP o rangos de IP y observaciones.
**Nota: se debe definir los elementos según se estimen necesarios. Ejemplo de switch: 3COM 4500G 48puertos.*
Se recomienda la realización de una tabla con las características a definir de cada elemento. Las columnas podrían ser: nombre del activo (elemento), dirección/rango IP, Sistema Operativo, Marca y Modelo de máquina, función en la empresa, observaciones.

Nombre	Dirección IP	Sistema Operativo	Marca Modelo	Función	Observaciones
Router	192.168.0.1	RouterOS	Mikrotic C52Ig-5HaxD-TC	Conexión a red	ONT
Router	192.168.1.1	RouterOS	TP-LINK TL-SG1024	Switch-firewall	Red de Gestión

Servidor	192.168.1.2	Linux SUSE	DELL R720XD 12LF	Backup sistemas y SGBD	Red de Gestión
Control acceso	192.168.1.3	Windows11	TimeMoto TM-626	Acceso y control horario	Red Interna
Router	192.168.2.1	RouterOS	TP-LINK TL-SG1024	Switch-firewall	Red DMZ
Servidor	192.168.2.12	Linux SUSE	HP Proliant DL380	Servidor web	Red DMZ
Servidor	192.168.2.13	Windows Server 2019	HP Proliant DL380	Servidor Vault	Red DMZ
Servidor	192.168.2.14	Linux SUSE	HP Proliant DL380	Servidor Laboratorio	Red DMZ
Servidor	192.168.2.13	Windows Server 2019	HP Proliant DL380	Servidor SCADA	Red de fábrica
PLC	192.168.2.14	propio	SCHNEIDER ELECTRIC TM221C16R	Sensor	Red de fábrica
PLC	192.168.2.14	propio	SCHNEIDER ELECTRIC TM221C16R	Sensor	Red de fábrica
PLC	192.168.2.14	propio	SCHNEIDER ELECTRIC TM221C16R	Sensor	Red de fábrica
PC	192.168.2.14	Windows 11	Lenovo ThinkCentre M700	Pc sobremesa	Red de fábrica
PC	192.168.2.14	Windows 11	Lenovo ThinkCentre M700	Pc sobremesa	Red de fábrica
Servidor	192.168.3.21	Windows Server 2019	HP Proliant DL380	Servidor	Red Gestión
PC	192.168.3.22	Windows 11	Lenovo ThinkCentre M700	Pc sobremesa	Red de Gestión
Access Point	192.168.3.23	RouterOS	TP-Link EAP115	Wifi fábrica	Red de Gestión
Access Point	192.168.3.23	RouterOS	TP-Link EAP115	Wifi fábrica	Red de Gestión
PC	192.168.3.22	Windows 11	Lenovo ThinkCentre M700	Pc sobremesa	Red de Oficina

PC	192.168.3.22	Windows 11	Lenovo ThinkCentre M700	Pc sobremesa	Red de Oficina
PC	192.168.3.22	Windows 11	Lenovo ThinkCentre M700	Pc sobremesa	Red de Oficina
Impresora	192.168.4.31	propio	Canon Pixma TS7450a	Impresora	Red de Oficina
Impresora	192.168.4.32	propio	Canon Pixma TS7450a	Impresora	Red de Oficina
Impresora	192.168.4.33	propio	Xerox WorkCentre 7855	Impresora	Red de Oficina
PC	192.168.3.22	Windows 11	Lenovo ThinkCentre M700	Pc sobremesa	Red de Departamento
PC	192.168.3.22	Windows 11	Lenovo ThinkCentre M700	Pc sobremesa	Red de Departamento
PC	192.168.3.22	Windows 11	Lenovo ThinkCentre M700	Pc sobremesa	Red de Departamento
Impresora	192.168.4.33	propio	Xerox WorkCentre 7855	Impresora	Red de Departamento
Impresora	192.168.4.33	propio	Xerox WorkCentre 7855	Impresora	Red de Departamento
Impresora	192.168.4.31	propio	Canon Pixma TS7450a	Impresora	Red de Departamento

- Será menester identificar todos los elementos esenciales para el negocio y que precisarán comprobación, no sólo los infraestructurales, sino también ficheros, bases de datos, páginas web, equipos, programas, etc.

  Dentro de la estructura anterior, se encuentran los Sistemas operativos enumerados, de backup, las bases de datos de personal, proveedores, clientes, contabilidad y gestión, registro de piezas e inventario. También la plataforma de gestión empresarial integrada Indosgestión y los programas propietarios de Autodesk utilizados en la sección técnica: Mechanical, Inventor y Revit.

✓ **Apartado 3: Detalle de las Comprobaciones a efectuar para cada uno de los Activos.** 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.
- Protección de datos/Protección intelectual.

**Se recomienda usar un formato tabla con los activos y las diferentes comprobaciones a las que serían sometidos.*

Nombre	Marca	Sistemas antimalware	Procesos de Gestión de Permisos	Procesos de Compliance	Políticas de prevención de fraude y fuga de datos	Sistema de actualizaciones	Sistemas de monitorización de recursos	Protección de Datos
Router Acceso	Mikrotic C52Ig-5HaxD-TC		✓			✓		
Router gestión	TP-LINK TL-SG1024	✓	✓	✓	✓	✓		
Servidor	DELL R720XD 12LF	✓	✓	✓	✓	✓	✓	✓
Control Acceso	TimeMoto TM-626		✓	✓	✓	✓	✓	✓
Router Red DMZ	TP-LINK TL-SG1024	✓	✓	✓	✓	✓	✓	
Servidor web Red DMZ	HP Proliant DL380	✓	✓	✓	✓	✓	✓	✓
Servidor NAS Red DMZ	HP Proliant DL380	✓	✓	✓	✓	✓	✓	✓
Servidor Lab Red DMZ	HP Proliant DL380	✓	✓	✓	✓	✓		
Servidor SCADA Red Fábrica	HP Proliant DL380	✓	✓	✓	✓	✓		
PLC Red Fábrica	SCHNEIDER ELECTRIC TM221C16R					✓		
PLC Red Fábrica	SCHNEIDER ELECTRIC TM221C16R					✓		
PLC Red Fábrica	SCHNEIDER ELECTRIC TM221C16R					✓		

PC Red Fábrica	Lenovo ThinkCentre M700	✓	✓	✓	✓	✓	✓	✓
PC Red Fábrica	Lenovo ThinkCentre M700	✓	✓	✓	✓	✓	✓	✓
Servidor Red Gestión	HP Proliant DL380	✓	✓	✓	✓	✓	✓	✓
PC Red Gestión	Lenovo ThinkCentre M700	✓	✓	✓	✓	✓	✓	✓
Access Point Red Gestión	TP-Link EAP115		✓			✓		✓
Access Point Red Gestión	TP-Link EAP115		✓			✓		✓
PC Red Oficina	Lenovo ThinkCentre M700	✓	✓	✓	✓	✓	✓	✓
PC Red Oficina	Lenovo ThinkCentre M700	✓	✓	✓	✓	✓	✓	✓
PC Red Oficina	Lenovo ThinkCentre M700	✓	✓	✓	✓	✓	✓	✓
Impresora Red Oficina	Canon Pixma TS7450a		✓		✓	✓	✓	✓
Impresora Red Oficina	Canon Pixma TS7450a		✓		✓	✓	✓	✓
Impresora Red Oficina	Xerox WorkCentre 7855		✓		✓	✓	✓	✓
PC Red Departamento	Lenovo ThinkCentre M700	✓	✓	✓	✓	✓	✓	✓
PC Red Departamento	Lenovo ThinkCentre M700	✓	✓	✓	✓	✓	✓	✓
PC Red Departamento	Lenovo ThinkCentre M700	✓	✓	✓	✓	✓	✓	✓
Impresora Red Departamento	Xerox WorkCentre 7855		✓		✓	✓	✓	✓

Impresora Red Departamento	Xerox WorkCentre 7855		✓		✓	✓	✓	✓
Impresora Red Departamento	Canon Pixma TS7450a		✓		✓	✓	✓	✓

✓ **Apartado 4: Detallar los tipos de auditorías que aplican y sus procedimientos asociados.** Establecer 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.
- Registro Logs.

**Se recomienda usar un formato tabla con los activos y los procedimientos a los que se someterían.*

Nombre	Marca	Test de penetración o HE	Auditoría de Red	Auditoría de seguridad perimetral	Auditoría web	Auditoría forense	Auditoría legal	Registro de logs
Router Acceso	Mikrotic C52Ig-5HaxD-TC	✓	✓	✓		✓		✓
Router gestión	TP-LINK TL-SG1024	✓	✓	✓		✓		✓
Servidor	DELL R720XD 12LF	✓	✓	✓	✓	✓	✓	✓
Control Acceso	TimeMoto TM-626		✓				✓	✓
Router Red DMZ	TP-LINK TL-SG1024	✓	✓	✓		✓		✓
Servidor web Red DMZ	HP Proliant DL380	✓	✓	✓	✓	✓	✓	✓
Servidor NAS Red DMZ	HP Proliant DL380	✓	✓	✓	✓	✓	✓	✓
Servidor Lab Red DMZ	HP Proliant DL380	✓	✓	✓		✓	✓	✓
Servidor SCADA Red Fábrica	HP Proliant DL380	✓	✓	✓	✓	✓	✓	✓

PLC Red Fábrica	SCHNEIDER ELECTRIC TM221C16R		✓			✓		✓
PLC Red Fábrica	SCHNEIDER ELECTRIC TM221C16R		✓			✓		✓
PLC Red Fábrica	SCHNEIDER ELECTRIC TM221C16R		✓			✓		✓
PC Red Fábrica	Lenovo ThinkCentre M700	✓	✓			✓	✓	✓
PC Red Fábrica	Lenovo ThinkCentre M700	✓	✓			✓	✓	✓
Servidor Red Gestión	HP Proliant DL380	✓	✓	✓	✓	✓	✓	✓
PC Red Gestión	Lenovo ThinkCentre M700	✓	✓			✓	✓	✓
Access Point Red Gestión	TP-Link EAP115	✓	✓			✓	✓	✓
Access Point Red Gestión	TP-Link EAP115	✓	✓			✓	✓	✓
PC Red Oficina	Lenovo ThinkCentre M700	✓	✓	✓		✓	✓	✓
PC Red Oficina	Lenovo ThinkCentre M700	✓	✓	✓		✓	✓	✓
PC Red Oficina	Lenovo ThinkCentre M700	✓	✓	✓		✓	✓	✓
Impresora Red Oficina	Canon Pixma TS7450a	✓	✓	✓	✓	✓		✓
Impresora Red Oficina	Canon Pixma TS7450a	✓	✓	✓	✓	✓		✓
Impresora Red Oficina	Xerox WorkCentre 7855	✓	✓	✓	✓	✓		✓
PC Red Departamento	Lenovo ThinkCentre M700	✓	✓	✓		✓	✓	✓

PC Red Departamento	Lenovo ThinkCentre M700	✓	✓	✓		✓	✓	✓
PC Red Departamento	Lenovo ThinkCentre M700	✓	✓	✓		✓	✓	✓
Impresora Red Departamento	Xerox WorkCentre 7855	✓	✓	✓	✓	✓		✓
Impresora Red Departamento	Xerox WorkCentre 7855	✓	✓	✓	✓	✓		✓
Impresora Red Departamento	Canon Pixma TS7450a	✓	✓	✓	✓	✓		✓

✓ **Apartado 5: Detallar un Esquema de Mejora Continua o un Modelo de Madurez.**

Deberás efectuar las siguientes tareas:

➢ Analizar, al menos, un esquema de madurez existente en el ámbito empresarial.

Uno de los modelos de madurez por el que me decantaría, al estar muy presente en empresas del ámbito tecnológico y digital, es el CMMI.

Evalúa la madurez empresarial mediante áreas de proceso con objetivos y prácticas definidas, que según se cumplan pueden ser valorados en la siguiente escala de entre 1 y 5:

1. Inicial. Por procesos inmaduros, expuesto al riesgo e ineficiencia.
2. Gestionado. Los proyectos se ejecutan mediante procedimientos planificados, supervisados y medibles.
3. Definido. Mejora de proactividad con procesos documentados y estandarizados.
4. Gestionado cuantitativamente. La ejecución ahora es cuantitativa, y a través de los datos se detectan deficiencias, permitiendo anticiparse a nuevas necesidades.
5. Optimización. Con los procesos proactivos y estandarizados, el entorno empresarial es predecible y pueden desarrollar mejoras con las que aumentar el desempeño.

Al ser un proceso guiado, es más sencillo llegar a objetivos, ganar prestigio o completar normas y estándares con los que seguir mejorando nuestra imagen y presencia a todos los niveles.

➢ Analizar, al menos, un esquema de mejora continua.

El PDCA o ciclo de Deming, tiene como objetivo la mejora constante de los procesos. Es posiblemente la metodología de gestión que más se ha mantenido en el tiempo, al haber surgido hace ya un siglo.

Su acrónimo en inglés, Plan (planificar), Do (hacer), check (verificar) y Act-Adjust (actuar o ajustar), ya nos muestra su carácter cíclico -recursivo- que, mediante la repetición de dichos pasos, consigue acelerar y mejorar la calidad de productos y procesos.

Por ello, nos facilita la resolución de problemas, la correcta toma de decisiones o medidas preventivas, la mejora en la Innovación y la calidad, así como una mejor adaptación a los constantes cambios del mercado.

Decidir cuál de los tipos de esquemas se deberá aplicar para garantizar que los resultados de la auditoría tengan como fin la implantación continua de mejoras en materia de ciberseguridad y la consecución de los diferentes niveles de seguridad.

Aunque los dos esquemas ofrecen modelos claros y demostrados para la mejora de procesos empresariales (incluso en el ámbito de la ciberseguridad), el esquema CMMI creo que se ajusta mejor a la consecución de distintos niveles de seguridad.

Nos permite conseguir nuestros objetivos nivel a nivel, centrados en la madurez de cada etapa antes de pasar a la siguiente, y una mejora continua que permita encontrar debilidades, prevenirlas y alinear seguridad informática y objetivos comerciales.

Además, de forma similar a como podríamos hacer con el ciclo de Deming, se pueden aprovechar los procesos desarrollados para facilitar la adaptación y cumplimiento a estándares y regulaciones de la industria, mejorando de paso la imagen y competitividad de la empresa.

Webgrafía.

https://www.unir.net/empresa/revista/cmmi/

https://www.fguell.com/la-madurez-organizativa/

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwit65_-mpeDAxUcgP0HHdMjD4UQFnoECCsQAQ&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F7167687.pdf&usg=AOvVaw0qa5zHSPL58clhPdPofrHU&opi=89978449

https://asana.com/es/resources/continuous-improvement

https://www.sydle.com/es/blog/ciclo-pdca-61ba2a15876cf6271d556be9

https://tbsek.mx/blog/2023/marzo/39.CMMI.html

https://repositorio.usmp.edu.pe/handle/20.500.12727/7059?locale-attribute=es

https://riskonnect.com/es/business-continuity-resilience/plan-do-check-act-pdca-how-it-applies-to-business-continuity/