Tarea online IC01.

Título de la tarea: Auditoría Interna de Prevención.

Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Incidentes de Ciberseguridad.

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Resultados de aprendizaje

- **RA1.** Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.

Contenidos

1.- Principios Generales en Materia de Ciberseguridad.
2.- Normativa de Protección del Puesto de Trabajo.
3.- Plan de Formación y Concienciación en Materia de Ciberseguridad.
    3.1.- Controles.
    3.2.- Puntos Clave.
4.- Materiales de Formación y Concienciación.
5.- Auditorías Internas de Cumplimiento en Materia de Prevención.
    5.1.- Consideraciones para la Implementación de una Política de Auditorías.
6.- Bibliografía.

1.- Descripción de la tarea.

Auditorías Internas de Cumplimiento en Materia de Prevención.

Auditoría Interna (CC0)

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:

    - Estructura de red en trípode, con todas sus zonas a definir, como la red interna, DMZ, etc.
    - Los elementos de red que contiene la empresa son: routers, switches, OLT/ONT de fibra, Firewalls, etc.
    - Contiene los siguientes servicios expuestos al exterior: portal web, servidor NAS con Vault (AutoDesk), servidor laboratorio interno.
    - Puestos de trabajo remotos.

- 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.
- 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.

- **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.

  - 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.

- **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.*

- **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.*

- **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.
  - Analizar, al menos, un esquema de mejora continua.
  - 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.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

- Se trata de un ejercicio teórico, por lo que sólo hará falta:
  - un ordenador personal con Sistema Operativo Windows.
  - Herramientas ofimáticas, como: Microsoft Office, OpenOffice o herramientas ofimáticas del Workspace de Google.
  - Herramientas de creación de diagramas, como "draw.io". Viene incorporada en las herramientas de Google.

Recomendaciones

- Antes de abordar la tarea:
  - lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
  - Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- No olvides elaborar el documento explicativo.

Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_Nombre_IC01_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna Begoña Sánchez Mañas para la primera unidad del MP de IC, debería nombrar esta tarea como...

sanchez_manas_begona_IC01_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación implicados

Criterios de evaluación RA1

- a) Se han definido los principios generales de la organización en materia de ciberseguridad, que deben ser conocidos y apoyados por la dirección de la misma.
- b) Se ha establecido una normativa de protección del puesto de trabajo.
- c) Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados.
- d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados.
- **e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.**

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: Se valorará que se identifiquen y clasifiquen correctamente todos los activos en la estructura de la empresa. Se crea un diagrama de bloques con estructura en trípode en el que se reflejan los elementos correctamente clasificados en las diferentes áreas de la estructura.	1 punto (obligatorio)
Apartado 2. Criterio 1: Identfica una amplia variedad de activos. Deben haber de los siguientes tipos: estructurales, equipos, softwares, bbdd o ficheros.	0,5 puntos (obligatorio)
Apartado 2. Criterio 2: Número de activos: Identifica al menos 12 activos diferentes.	0,5 puntos (obligatorio)
Apartado 2. Criterio 3: Nombres y direcciones IP: recoge correctamente estos parámetros de los activos identificados.	0,5 puntos (obligatorio)
Apartado 2. Criterio 4: S.O., marca y modelo de máquina: recoge correctamente estos parámetros de los activos identificados.	0,5 puntos (obligatorio)
Apartado 2. Criterio 5: Función y observaciones: recoge correctamente estos parámetros de los activos identificados.	0,5 puntos (obligatorio)
Apartado 3. Criterio 1: Disposición de sistemas antimalware: determina la necesidad de este rasgo en los activos identificados.	0,4 puntos (obligatorio)
Apartado 3. Criterio 2: Disposición de gestión de permisos: determina la necesidad de este rasgo en los activos identificados.	0,35 puntos (obligatorio)

Apartado 3. Criterio 3: Disposición de cumplimiento legal: determina la necesidad de este rasgo en los activos identificados.	0,35 puntos (obligatorio)
Apartado 3. Criterio 4: Disposición de prevención de fraude y fuga de datos: determina la necesidad de este rasgo en los activos identificados.	0,35 puntos (obligatorio)
Apartado 3. Criterio 5: Disposición de actualizaciones: determina la necesidad de este rasgo en los activos identificados.	0,35 puntos (obligatorio)
Apartado 3. Criterio 6: Disposición de monitorización de recursos: determina la necesidad de este rasgo en los activos identificados.	0,35 puntos (obligatorio)
Apartado 3. Criterio 7: Disposición de P.D. y P.I.: determina la necesidad de este rasgo en los activos identificados.	0,35 puntos (obligatorio)
Apartado 4. Criterio 1: Auditoría de hacking ético: identifica si se debe realizar este tipo de auditoría en los activos identificados.	0,3 puntos (obligatorio)
Apartado 4. Criterio 2: Auditoría de red: identifica si se debe realizar este tipo de auditoría en los activos identificados.	0,3 puntos (obligatorio)
Apartado 4. Criterio 3: Auditoría de seguridad perimetral: identifica si se debe realizar este tipo de auditoría en los activos identificados.	0,3 puntos (obligatorio)
Apartado 4. Criterio 4: Auditoría web: identifica si se debe realizar este tipo de auditoría en los activos identificados.	0,3 puntos (obligatorio)
Apartado 4. Criterio 5: Auditoría forense: identifica si se debe realizar este tipo de auditoría en los activos identificados.	0,3 puntos (obligatorio)
Apartado 4. Criterio 6: Auditoría de seguridad legal: identifica si se debe realizar este tipo de auditoría en los activos identificados.	0,3 puntos (obligatorio)
Apartado 4. Criterio 7: Auditoría de registros o log: identifica si se debe realizar este tipo de auditoría en los activos identificados.	0,2 puntos (obligatorio)
Apartado 5. Criterio 1: Correcta y detallada definición de un modelo de madurez.	0,7 puntos (obligatorio)
Apartado 5. Criterio 2: Correcta y detallada definición de un esquema de mejora continua.	0,7 puntos (obligatorio)
Apartado 5. Criterio 3: Se valorará la decisión del sistema de implantación continua de mejoras seleccionado junto con los argumentos que justifiquen dicha decisión.	0,6 puntos (obligatorio)