**Incidentes de ciberseguridad**

# Auditoría Interna de Prevención

## 

## 

## Contenídos

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.
   1. Controles.
   2. Puntos Clave.
4. Materiales de Formación y Concienciación.
5. Auditorías Internas de Cumplimiento en Materia de Prevención.
   1. Consideraciones para la Implementación de una Política de Auditorías.
6. Bibliografía.

## Resultados de aprendizaje

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

### 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.**

**Rubrica**

| **Apartado** **1**: Se valorará que el diseño de la empresa ficticia sea imaginativo y cubra las cuestiones técnicas habituales en una Auditoría Interna de Cumplimiento en Materia de Prevención. | 2 puntos (obligatorio) |
| --- | --- |
| **Apartado** **2**: Se valorará el buen criterio a la hora de identificar los activos clave de la empresa. | 2 puntos (obligatorio) |
| **Apartado** **3**: Se valorará la selección de comprobaciones a efectuar para verificar las medidas de seguridad de cada uno de los activos clave. | 2 puntos (obligatorio) |
| **Apartado** **4**: Se valorará el establecimiento de procedimientos de trabajo en función del tipo de auditoría requerido en cada caso. | 2 puntos (obligatorio) |
| **Apartado** **5**: Se valorará la decisión del sistema de implantación continua de mejoras seleccionado junto con los argumentos que justifiquen dicha decisión. | 2 puntos (obligatorio) |

| Apartado 1: Diseño de una Empresa Ficticia |
| --- |
| Diseñar una empresa con un esquema sencillo de Sistemas de Información, en el que se reflejan los puntos habituales de vulnerabilidad: bases de datos, puestos de trabajo en local o en remoto, conmutadores, servidores, etc. |
| Descripción del negocio |
| Ca'Manolo es un bar y restaurante que ha conquistado el corazón de sus clientes gracias a su dedicación a proporcionar los mejores bocadillos y pizzas como muestran en su página [web](https://www.camanolo.com/).  PINO su sobrina abogada se dedica a mantener el negoció al día con los impuestos y la contabilidad. |
| Red |
|  |
| Router 1 : Este es el router central que conecta la red de Ca'Manolo. Es el punto de entrada a la red desde el proveedor de servicios de Internet. |
| Cada uno de los siguientes routers representa una subdivisión de la red en diferentes áreas o departamentos de la empresa. |
| **Router 1 :** Red Para administración, bajo este se encuentra una base de datos usada dentro de esta red y un servidor web. |
| **Router 2 :** Red para personal del restaurante, en donde trabaja Manolo. |
| **Router 3 :** Red para clientes. |
| Apartado 2: Detalle de los Activos Clave que se deberán auditar. |

| Inventario Hardware | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Id** | **Nombre** | **Descripción** | **Responsable** | **Tipo** | **Ubicación** | **Crítico** |
| 001 | R0 | Salida a internet | PINO | ROUTER | Sala administración | SI |
| 002 | R1 | Red administrativa | PINO | ROUTER | Sala administración | SI |
| 003 | R2 | Red personal | MANOLO | ROUTER | Zona Restauración | SI |
| 004 | R3 | Red clientes | MANOLO | ROUTER | Zona Restauración | NO |
| 005 | S0 | Base de datos administración | PINO | SERVER | Sala administración | SI |
| 006 | S1 | Server Web | PINO | SERVER | Sala adminstración | SI |
| 007 | PC1 | Pc PINO | PINO | PC | Sala administración | NO |
| 008 | PC2 | Pc caja | MANOLO | PC | Zona Restauración | NO |
| 009 | PC3 | Móvil  Manolo | MANOLO | PC | Zona Restauración | NO |

## 

### Inventario Software

| **Id** | **Nombre** | **Descripción** | **Id Hardware** | **Tipo** |
| --- | --- | --- | --- | --- |
| SO1 | Windows 11 pro |  | 007 | SO |
| AT1 | Norton 360 | Antivirus para pc | 007 | antivirus |
| AT2 | Kaspersky for web servers | Antivírus para servidor | 006 | Antivirus - firewall |
| SS1 | Apache 2.4.58 | Servidor página web | 006 | Servidor web |
| SO2 | Ubuntu 20.04 LTS |  | 006 | SO |
| SS2 | Mysql 8.0 LTS | Servidor de bases de datos local | 005 | Base de datos |
| SO3 | Ubuntu 20.04 LTS | So de base de datos | 005 | SO |
| SC1 |  | Copia de seguridad de base de datos | 007 | fichero |

### Recursos humanos

| **Nombre** | **Lugar de trabajo** | **Puesto** |
| --- | --- | --- |
| Manolo Pérez Gonzalez | Zona de restauración | Encargado de restauración |
| PINO Rojo Pérez | Sala administración | Jefa administrativa |
| Manolín Perez Cruz | Zona de restauración | Auyante de cocina |

| Apartado 3: Detalle de las Comprobaciones a efectuar para cada uno de los Activos. |
| --- |
| Para asegurar el manejo seguro de los activos propongo el siguiente protocolo al que someter los activos de manera periódica. |
| 1. Sistemas Anti Malware:Selección del Antimalware:  * + La solución antimalware es confiable y está actualizada.   + Configurar la solución según las necesidades específicas del puesto.  Escaneo y Detección:  * + Establecer un programa regular de escaneo de sistemas y archivos.   + Configurar alertas para la detección inmediata de amenazas.   + Realizar análisis heurísticos para detectar amenazas desconocidas.  Actualizaciones de Firmas:  * + Automatizar la actualización de firmas de manera regular.   + Verificar que todas las estaciones de trabajo estén actualizadas.  2. Procesos de Gestión de Permisos:Identificación de Usuarios:  * + Implementar un sistema de autenticación seguro.   + Mantener un registro de usuarios y sus privilegios.  Control de Acceso:  * + Definir roles y permisos para cada usuario.   + Revisar y actualizar regularmente los permisos de acceso.  Monitoreo de Actividad:  * + Establecer un sistema de registro de actividades de usuarios.   + Implementar alertas para actividades inusuales.  3. Procesos de Cumplimiento Legal (Compliance):Conformidad con Normativas:  * + Revisar y entender las normativas relevantes (GDPR, HIPAA, LOPD...).   + Asegurarse de que las políticas de seguridad cumplen con estas normativas.  Auditorías y Revisiones:  * + Programar auditorías periódicas para evaluar la conformidad.   + Mantener registros detallados para auditorías internas y externas.  4. Políticas de Prevención de Fraude y Fuga de Datos:Educación del Usuario:  * + Implementar programas de concientización sobre seguridad.   + Proporcionar pautas claras sobre la manipulación de información confidencial.  Control de Dispositivos:  * + Establecer políticas para el uso de dispositivos de almacenamiento externo.   + Monitorizar la transferencia de datos para detectar posibles fugas.  5. Sistema de Actualizaciones:Automatización de Actualizaciones:  * + Configurar sistemas para recibir actualizaciones automáticas.   + Realizar pruebas antes de implementar actualizaciones en entornos de producción.   Política de Actualizaciones:  * + Establecer una política para la aplicación oportuna de parches de seguridad.   + Mantener un inventario actualizado de software y sistemas.  6. Sistemas de Monitorización de Recursos:Monitorización Continua:  * + Implementar herramientas de monitorización para recursos del sistema.   + Establecer umbrales y alertas para recursos críticos.  Análisis de Rendimiento:  * + Realizar análisis regulares del rendimiento del sistema.   + Identificar y abordar cuellos de botella y problemas de rendimiento. |