Desarrollo de Planes de Prevención y Concienciación en Ciberseguridad.

Cibernética y Ciberseguridad

Francisco Artés - Elaboración Propia. *Protección y Amenazas de la Información* (CC0)

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 Incerticumbre.**

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.

Agile Corporation. *Logotipo de Agile Corporation* (CC0)

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 5021 del programa formativo, denominado “Incidentes de Seguridad”, 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.

Un Decálogo para la Ciberseguridad

CCN. *Logotipo CCN-CERT* (CC0)

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** que se revisará a continuación.

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 proactiva de un usuario en un sistema informático, por pequeña que sea, puede desencadenar la ejecución de un Vector, inyectando código malicioso en el sistema.

En este ejercicio se mostrará cuán fácil es instalar un Troyano de Acceso Remoto en un ordenador personal y en un móvil, 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.

Entre todas las herramientas protectoras, la más efectiva en primera instancia es el Cortafuegos, que se puede implementar mediante hardware o software indistintamente.

En este ejercicio se mostrará el uso del Cortafuegos software más utilizado, esto es, el UFW de la Comunidad Ubuntu.

Ejercicio - Principio 4

Además de la estrategia lógica a aplicar para reducir la superficie expuesta a los ataques, existen ciertas estructuras físicas y topologías de red que también suman para trabajar en este sentido.

En este ejercicio se mostrará al alumno la Estructura en Trípode, que permite exponer al mundo sólo los servidores frontera de la denominada "Zona Desmilitarizada".

Ejercicio - Principio 5

En un mundo altamente informatizado y en el que la tecnología va a más con el paso del tiempo, no hay más remedio que cifrar toda aquella información que se considere importante, confidencial o crítica.

En este ejercicio se revisará el procedimiento de cifrado asimétrico de la información, que permite garantizar la identidad del emisor de los datos, así como que sólo los podrá descifrar la entidad autorizada por dicho emisor.

Ejercicio - Principio 6

La complejidad de una contraseña no es algo baladí. Por ello resulta sorprendente cuando algún portal con información sensible o directamente relacionada con la economía o las finanzas, presenta mensajes del tipo: "la clave sólo podrá tener 8 caracteres alfanuméricos, no pudiendo contener símbolos". Este simple mensaje reduce de golpe la combinatoria de claves posibles desde el infinito hasta unos pocos cientos de millones.

En este ejercicio se construirán Diccionarios con Crunch basados en Ingeniería Social y se atacará un fichero cifrado utilizando John the Ripper. Se comprobará también cómo se complica exponencialmente el trabajo del pirata informático cuando aumenta progresivamente la complejidad de las claves de cifrado.

Ejercicio - Principio 10

Por lo general, todos aquellos Sistemas de Detección de Intrusiones de código abierto desarrollados por una comunidad en Internet, se benefician de actualizaciones constantes 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 el lugar en el que se deben configurar las reglas *ad hoc* de dicha instalación.

2.- Normativa de Protección del Puesto de Trabajo.

La Extensión del Ámbito del Puesto de Trabajo

EOI. *Puesto de Trabajo* (CC0)

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 los **nuevos dispositivos tecnológicos**, como con la ampliación de su **alcance físico y geográfico**, tras la incorporación generalizada del concepto de **teletrabajo** para aquellas actividades laborales que son susceptibles de aplicarlo.

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.

Dicho dossier se puede descargar desde el siguiente enlace: https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-puesto-trabajo

Ejercicio - Ataque a un Inventario de Activos

El inventario de activos de una empresa contiene prácticamente toda la información relativa a su entorno informático y productivo. Si un pirata informático accede a esta información, se llevará mucho más que los datos relativos a las instalaciones, **se llevará la empresa completa.**

En este ejercicio se construirá una pequeña maqueta de Inventario de Activos sobre una base de datos relacional, atacándola después con Medusa para mostrar al alumno 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

INCIBE. *La Ciberseguridad empieza por ti* (CC0)

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

El presente ejercicio pretende concienciar al alumno de la potencial vulnerabilidad de cualquier servidor informático.

Para ello se crearán diccionarios de credenciales de usuarios (*login* y *password*) y se usarán para atacar a un servidor empresarial con la herramienta Hydra, provocando Denegación de Servicio.

3.1.- Controles.

EOI. *Controles de la Información* (CC0)

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 clasificarán 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

A continuación se detallará un ejemplo de dichos controles.

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.

EOI. *Puntos Clave* (CC0)

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

En este ejercicio desarrollaremos el punto "Concretar el Plan de Formación".

Para garantizar el éxito del Programa Formativo, seleccionar los aspectos que se desea cubrir.

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.

Ejercicio - Boletín Interno de Ciberseguridad y Newsletter Externa

Una de las estrategias más sencillas y efectivas a la hora de formar y concienciar de forma recurrente es divulgar las novedades de un tema mediante una publicación periódica.

En este ejercicio se planteará la estructura que debería tener un Boletín Interno de Ciberseguridad, o una *Newsletter* externa acerca del mismo tema.

Un Boletín Interno y una Newsletter Externa de Ciberseguridad tienen esencialmente la misma estructura. La diferencia entre ambos es que la información que se publica en ellos tiene carácter interno si se dirige a la organización y carácter externo si se dirige a la comunidad global, filtrándose la información adecuadamente en cada caso.

Un planteamiento estructural para dichas circulares podría tener la forma siguiente, alineada con los principios pragmáticos de la Ciberseguridad (protegerse de lo conocido, alertar de lo desconocido, preparar planes de respuesta):

•Última Hora. Nuevas amenazas y malware detectados y contrastados.

•Noticias del Sector. Nuevas herramientas antimalware, estrategias de protección y técnicas de pentesting.

•Amenazas Potenciales en Estudio. Análisis de indicios sospechosos, correlación de pruebas entre entornos y entre empresas.

•Análisis Forense. Estudio de ataques ya consumados y revisión de daños sufridos.

•Prevención y Respaldo. Nuevas propuestas técnicas y operativas para contención de amenazas e incidentes.

•Cartas Técnicas y Consultas. Comunicaciones de los miembros de la comunidad y empleados, detallando problemas acaecidos o planteando dudas técnicas.

•Información de Contacto. Detalle de los canales de comunicación con los editores de la circular

4.- Materiales de Formación y Concienciación.

Los Riesgos de los Empleados y de la Organización

INCIBE. *Kit de Concienciación* (CC0)

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

EOI. *Auditoría Interna* (CC0)

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 qué nivel se ha de 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

En este ejercicio 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 a la libre circulación de estos datos.

- 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.

INCIBE. *Implementación de Política de Auditorías* (CC0)

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.**

Para saber más

En el siguiente enlace el alumno se podrá descargar el documento de recomendaciones del INCIBE, en lo relativo a Políticas de Seguridad para las PYMEs, fundamentadas en las Auditorías de Seguridad de Sistemas.