Incidentes de ciberseguridad

Módulo 1 – Concienciación en ciberseguridad

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
Plan de Recuperación, Transformación y Resiliencia
Junta de Andalucía
Consejería de Desarrollo Educativo y Formación Profesional
Unión Europea-NextGenerationEU.
Junta de Andalucía

Índice

Contenidos

Contenidos

GOBIERNO DE ESPAÑA MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL Plan de Recuperación, Transformación y Resiliencia
Junta de Andalucía Consejería de Desarrollo Educativo y Formación Profesional
Unión Europea- NextGenerationEU.

Índice

Contenidos

Contenidos

1. Incidentes de ciberseguridad

Antes de comenzar con el contenido, analicemos el módulo profesional. Este módulo profesional tiene 5 RA, que son los siguientes:

- RA 1 - Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.
- RA 2 - Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.
- RA 3 - Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.

1. Incidentes de ciberseguridad

Antes de comenzar con el contenido, analicemos el módulo profesional. Este módulo profesional tiene 5 RA, que son los siguientes:

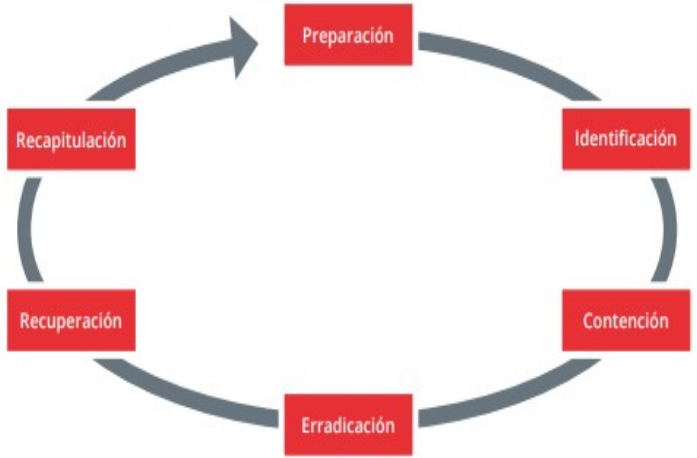
- RA 4 - Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.
- RA 5 - Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.

GOBIERNO DE ESPAÑA MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL Plan de Recuperación, Transformación y Resiliencia
Junta de Andalucía Consejería de Desarrollo Educativo y Formación Profesional
Unión Europea-NextGenerationEU.

1. Incidentes de ciberseguridad

Si además revisamos los criterios de evaluación, nos damos cuenta que el módulo profesional, no es meramente explicar cómo realizar una respuesta a incidentes, sino que abarca más contenidos generales.

Esto puede resultar confuso en los inicios, pues puede parecer que falte cohesión en su estructura, pero esto es debido a que este módulo tiene una función transversal, de enseñar ciberseguridad “general”, abarcando distintos aspectos en los que se profundizan más en el resto de módulos profesionales.



Fuente: incibe

1. Incidentes de ciberseguridad

El objetivo de este curso es lograr que comprendan el fundamento de cada uno de los resultados de aprendizaje, tengan bases teóricas y ejercicios para explicar cada criterio de evaluación, así como un ejemplo de controles tipo tests.

En definitiva, comprendan el módulo profesional a la vez que obtienen material para impartirlo.

Índice

Contenidos

Contenidos

2. Introducción a la ciberseguridad

2.1 Seguridad en sistemas en red

Comencemos por el primer resultado de aprendizaje, que se centra en planes de prevención y concienciación de Ciberseguridad.

Para ello, lo primero que debemos reflexionar es: ¿qué es la ciberseguridad? ¿Cuáles son sus principios generales?

Este primer punto no está relacionado con ningún criterio de evaluación, pero nos sirve como punto de partida para establecer ciertos conceptos de ciberseguridad.

2. Introducción a la ciberseguridad

2.1 Seguridad en sistemas en red

El constante avance tecnológico nos ha derivado en la necesidad de comunicar, compartir y divulgar la información, así como ofrecer productos y servicios de forma telemática.

Para ello se han desarrollado las redes de sistemas informáticos: conjunto de hardware, software y protocolos que hacen que se pueda dar comunicación entre varios sistemas.

Este intercambio de datos, y la información resultante, así como los sistemas que la propagan se han convertido en los objetivos de cibercriminales.

2. Introducción a la ciberseguridad

2.1 Seguridad en sistemas en red

Pentágono, CIA, Unicef, ONU o empresas privadas, como los ejemplos de abajo, han sido víctimas de ciberataques.

2. Introducción a la ciberseguridad

2.1 Seguridad en sistemas en red

La seguridad es una característica que nos indica que un sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible.

Como esta características es muy difícil de conseguir (y de hecho, para algunos expertos, imposible), se suaviza definición a fiabilidad: probabilidad de que un sistema se comporte tal y como se espera de él.

En muchos casos se habla de sistemas fiables en lugar de seguros.

2. Introducción a la ciberseguridad

2.1 Seguridad en sistemas en red

Uno de los problemas de la gestión de incidentes de ciberseguridad es el siguiente:

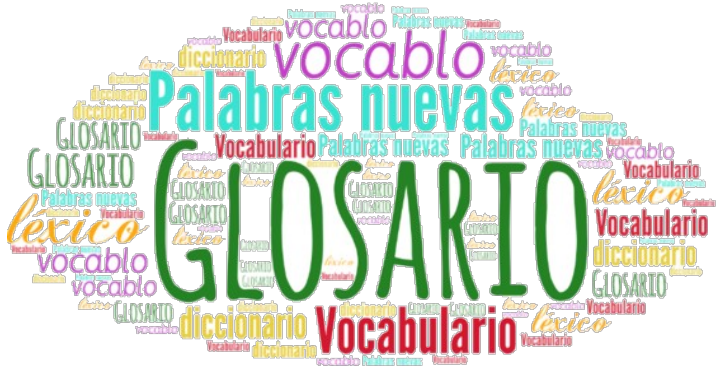
- Si no pasa nada, ¿para qué te pago?
- Si pasa algo, ¿para qué te pago?

Debemos tener presente que nuestro sistema, si está abierto al exterior, es visible y por tanto expuesto a ataques. La seguridad por ocultación no es una solución válida.

2. Introducción a la ciberseguridad

2.2 Glosario de términos de ciberseguridad

Durante el curso emplearemos muchos términos técnicos propios de la jerga de la ciberseguridad. Para facilitar la comprensión de los mismos se proporciona el siguiente glosario de términos, realizado por INCIBE:
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf



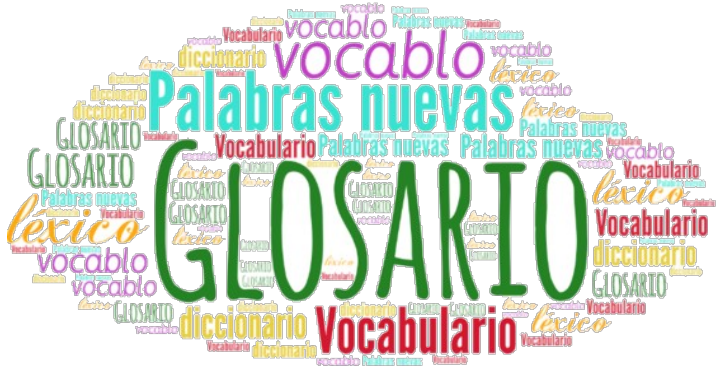
Algunos interesantes son: amenaza, activo, riesgo, vulnerabilidad, etc...

2. Introducción a la ciberseguridad

2.2 Glosario de términos de ciberseguridad

El Centro Criptológico Nacional (CCN-CERT) también nos ofrece un glosario de términos en el siguiente enlace:

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html



2. Introducción a la ciberseguridad

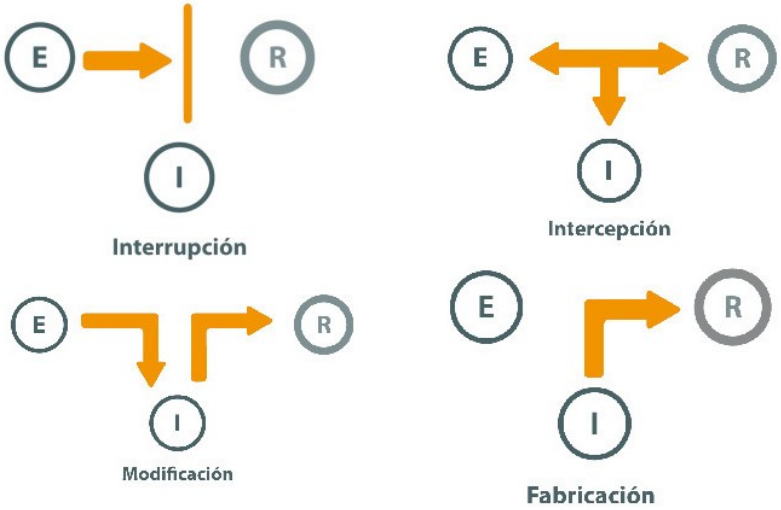
2.3 Elementos a proteger

- Hardware: conjunto de todos los elementos físicos de un sistema informático, como CPUs, cableado, discos duros, etc...
- Software: conjunto de programas lógicos que hacen al hardware funcionar, ya sean sistemas operativos, firmware o aplicaciones.
- Datos: conjunto de información lógica. Principal elemento a proteger. Es el más amenazado y difícil de recuperar. La información se obtiene a través del procesado de datos.

2. Introducción a la ciberseguridad

2.4 Amenazas de seguridad

Cualquier elemento está expuesto. Especialmente los datos, ya que son los más valiosos. Las taxonomías elementales de amenazas muestran cuatro tipos: interrupción, interceptación, modificación y fabricación.

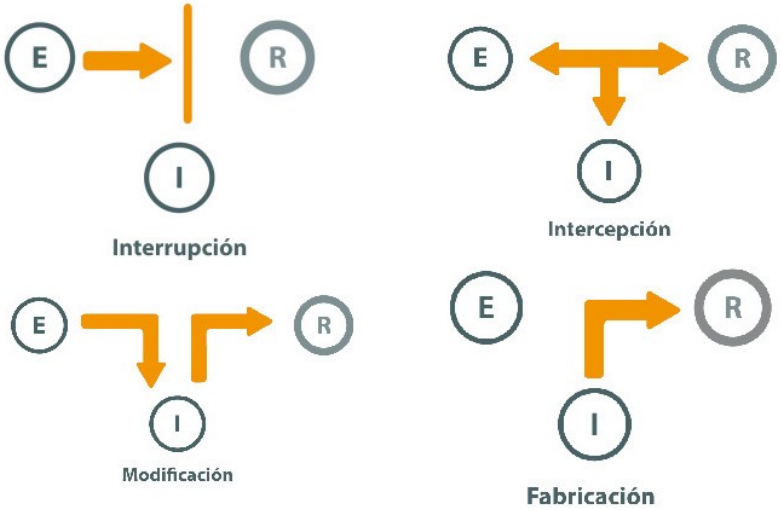


2. Introducción a la ciberseguridad

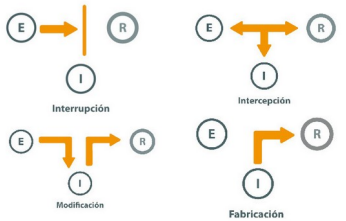
2.4 Amenazas de seguridad

Tipos de amenazas

- Interrupción del servicio: una entidad situada entre el emisor y el receptor evita la comunicación.
- Intercepción: una entidad obtiene mensajes cuyo destinatario era otra entidad.
- Modificación: los mensajes obtenidos por el receptor son diferentes a los emitidos por el emisor originalmente.
- Fabricación: una entidad tercera suplanta al emisor original.



2. Introducción a la ciberseguridad

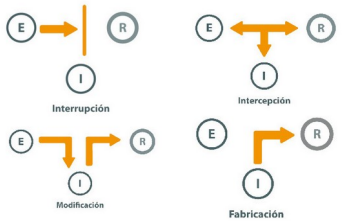


2.4 Amenazas de seguridad

Un proceso típico de un intento de penetración en un sistema puede ser el siguiente:

- Escaneo de puertos (portscan): detectar qué servicios ofrece una máquina. Abiertos, cerrados o protegidos (cortafuegos).
- Interceptación lógica (sniffing): analizar los paquetes que circulan por el medio compartido (dominio de colisión).
- Fabricación (spoofing): distintos tipos: IP, ARP (MitM), DNS, Web, Email (phishing).
- Denegación de servicio (DoS). Distribuido (DDoS): se consume todo el ancho de banda/procesamiento de un servidor.

2. Introducción a la ciberseguridad



2.4 Amenazas de seguridad

Centrándonos ahora en los orígenes de las amenazas de ciberseguridad o de los posibles incidentes, encontramos:

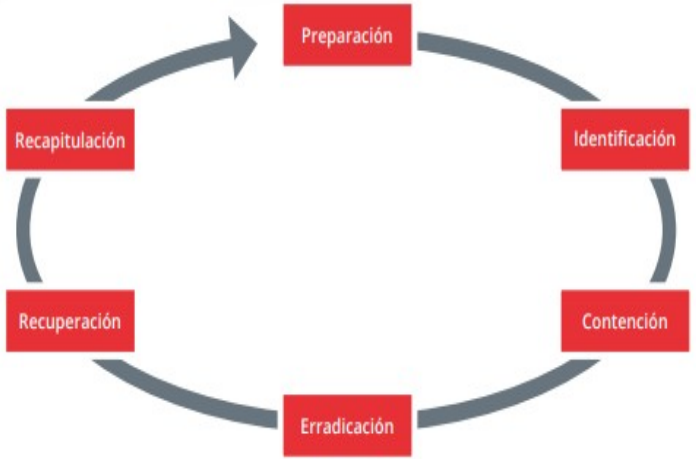
- Personas: personal, ex-empleados, curiosos, crackers, terroristas, hackers, intrusos remunerados, etc...
- Amenazas lógicas: programas, ya sea mediante errores de programación inesperados (*bugs)* o malware.
  - Ej: virus, bombas lógicas, gusanos, caballos de troya, programas conejo/bacteria o ransomware.
  - Los últimos son muy populares.
- Catástrofes naturales: incendios, inundaciones, terremotos...

2. Introducción a la ciberseguridad

2.5 Mecanismos de seguridad

Tres grupos de mecanismos:

- Prevención: aumentan la fiabilidad durante el funcionamiento normal, previniendo la ocurrencia de violaciones de seguridad.
  - Ejemplo: servicio de cifrado en la transmisión de datos, cortafuegos, WAF, firma digital, etc...
  - Se aplican técnicas de bastionado, así como los test de penetración (hacking ético).

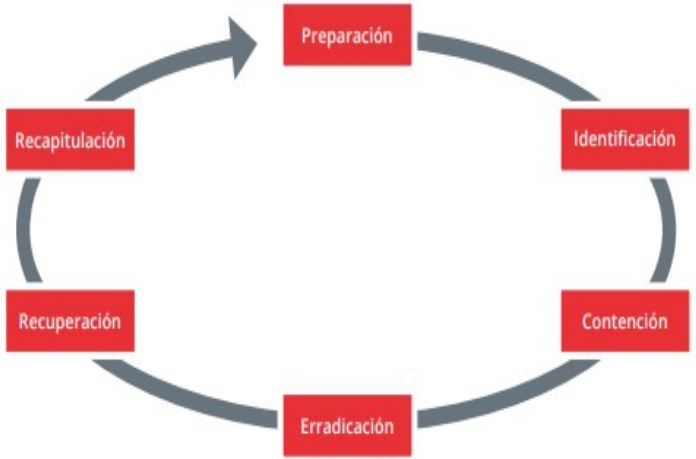


2. Introducción a la ciberseguridad

2.5 Mecanismos de seguridad

Tres grupos de mecanismos:

- Detección: aquellos que se utilizan para revelar violaciones de seguridad o intentos.
  - Ejemplo: servicios de alarma tras un número de intentos de inicio de sesión fallidos, inicio de sesión desde nuevos dispositivos, SIEM, IDS, etc...

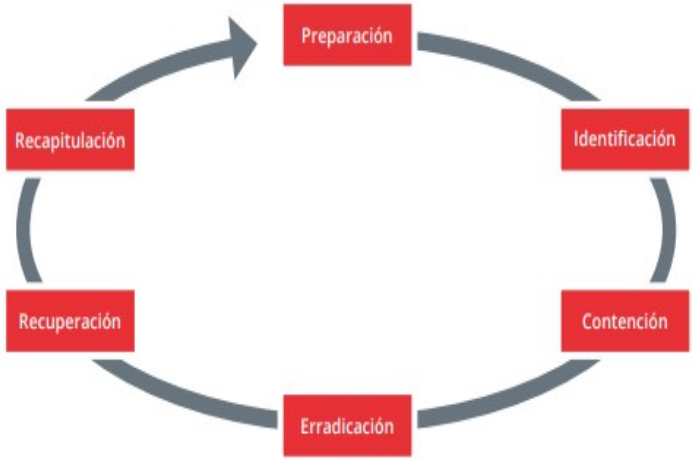


2. Introducción a la ciberseguridad

2.5 Mecanismos de seguridad

Tres grupos de mecanismos:

- Recuperación: se aplican cuando el incidente se ha detectado. Deben devolver el sistema a su funcionamiento normal.
  - Ejemplo: uso de copias de seguridad de datos (sistema 3-2-1), hardware adicional (redundante)...
  - Una tarea que se suele dar durante esta fase es el análisis forense: averiguar desde dónde se realizó el ataque, qué puerta se usó para entrar, de qué forma se puede prevenir para el futuro, etc...



Índice

Contenidos

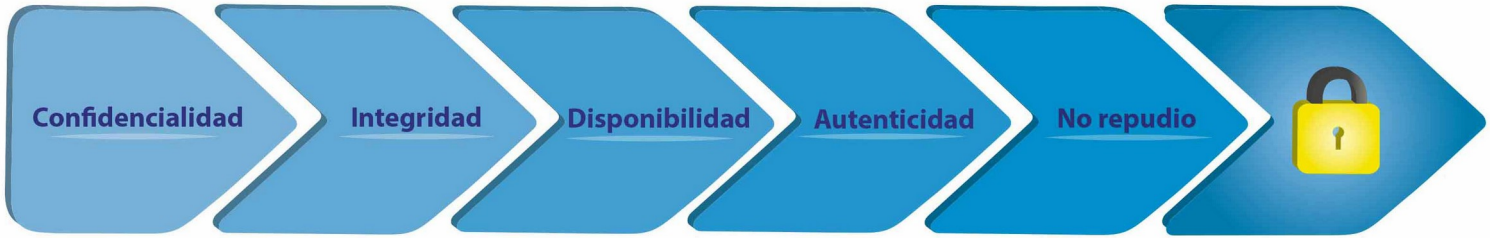
Contenidos

3. Principios generales de ciberseguridad

3.1 Principios básicos

Desde la empresa, al ofrecer nuestros servicios relacionados con la tecnologías de la información (ya sea un sistema web de información, una app, consultoría...) debemos garantizar la confidencialidad, la disponibilidad y la integridad de la información que gestionamos. Estos son los principios generales básicos de ciberseguridad, a los que se les añade la autenticidad y no repudio.

Veamos cada una de ellas por separado.



3. Principios generales de ciberseguridad

3.1 Principios básicos

Disponibilidad de la información: Se refiere a que la información debe estar accesible siempre para las personas autorizadas para hacerlo, y además puede recuperarse en caso de que ocurra un incidente de seguridad que cause su pérdida o corrupción.

- Es decir; permite que la información esté accesible cuando sea necesario.
- Ello nos obliga a generar los planes de prevención, actuación y recuperación necesarios para que un incidente no interrumpa el acceso al servicio.

3. Principios generales de ciberseguridad

3.1 Principios básicos

Confidencialidad de la información: relacionada con la privacidad, hace referencia a que la información sólo debe ser conocida por las personas que necesitan conocerla y que han sido autorizadas para ello.

- Este principio asegura que la información no va a ser divulgada de manera fortuita o intencionada.
- Debemos tener en cuenta que solo los usuarios adecuados pueden acceder al sistema (**autenticación**) y que cada uno de ellos debe ver solo su información y no la del resto de usuarios (**autorización**).

3. Principios generales de ciberseguridad

3.1 Principios básicos

En relación con la privacidad, multitud de servicios recopilan gran cantidad de información sobre nosotros. Esa información es obtenida bajo nuestro consentimiento, aceptando los términos y condiciones.

- Los datos recopilados por las empresas deben ser almacenados de forma segura, evitando las filtraciones de información (leaks).
- Existe cierto compromiso, en ocasiones, entre las ventajas de ceder los datos a estas empresas y el peligro que conlleva dicha cesión.

3. Principios generales de ciberseguridad

3.1 Principios básicos

Integridad de la información: Hace referencia a que la información que se encuentra almacenada en los dispositivos o la que se ha transmitido por cualquier canal de comunicación no ha sido manipulada por terceros de manera malintencionada.

- Esto garantiza que la información no será modificada por personas no autorizadas.
- La criptografía hoy en día nos permite garantizar la integridad de la información.

3. Principios generales de ciberseguridad

3.2 Principios generales extendidos

La autenticidad es una característica de la seguridad informática que se refiere a la comprobación y confirmación de la identidad real de los activos (procesos, sistemas, información) y/o actores (usuarios).

Esta autenticidad se puede realizar mediante un usuario y contraseña, aunque actualmente también se emplean datos biométricos (ojo, huella, rostro), u objetos (móvil, llaves 2FA, etc.).

3. Principios generales de ciberseguridad

3.2 Principios generales extendidos

No repudio: Servicio de seguridad (OSI ISO-7498-2) que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

En el primer caso el no repudio se denomina en origen y en el segundo en destino.

3. Principios generales de ciberseguridad

3.3 Principios generales del CCN-CERT

La siguiente información está recogida de la fuente: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2473-ccn-cert-bp-01-principios-y-recomendaciones-basicas-en-ciberseguridad/file.html

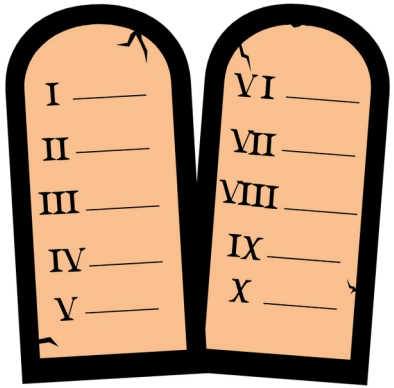
El Centro Criptológico Nacional publica y actualiza un informe en el que se detallan tanto los Principios Generales en Materia de Ciberseguridad, como recomendaciones, medidas fundamentales y buenas prácticas para concienciar y facilitar el uso seguro de las Tecnologías de la Información y la Comunicación.

Dicho informe incluye un Decálogo Básico de Ciberseguridad que resume su contenido en diez principios generales.

3. Principios generales de ciberseguridad

3.3 Principios generales del CCN-CERT

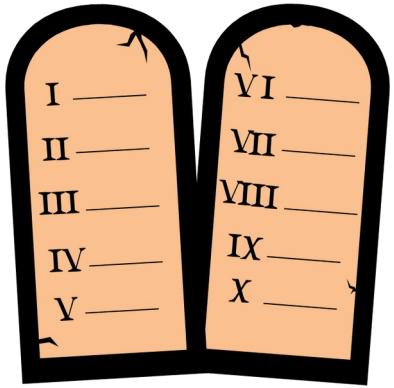
1. La cultura de la ciberseguridad, la concienciación del empleado, debe ser uno de los pilares en los que se asiente la ciberseguridad de cualquier organización.
2. No abrir ningún enlace ni descargar ningún fichero adjunto procedente de un correo electrónico que presente cualquier indicio o patrón fuera de lo habitual.
3. Utilizar software de seguridad, herramientas antivirus y antimalware, cortafuegos personales, herramientas de borrado seguro, etc.



3. Principios generales de ciberseguridad

3.3 Principios generales del CCN-CERT

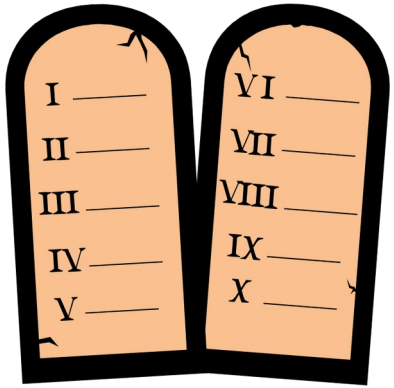
4. Limitar la superficie de exposición a las amenazas, pues no sólo hay que implementar medidas de seguridad que protejan el acceso a la información, sino que hay que determinar los servicios que son estrictamente necesarios.
5. Cifrar la información sensible, no hay otra alternativa.
6. Utilizar contraseñas adaptadas a la funcionalidad, siendo conscientes de que la múltiple autenticación ya es una necesidad.



3. Principios generales de ciberseguridad

3.2 Principios generales del CCN-CERT

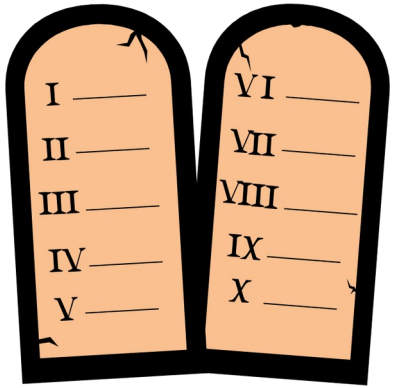
7. Efectuar un borrado seguro de la información una vez que ésta ya no sea necesaria o se vaya a retirar de uso el soporte en cuestión.
8. Realizar copias de seguridad periódicas, pues no existe otra alternativa de recuperación en caso de infecciones que cursen con pérdida de datos o avería de los recursos de almacenamiento. Estas copias de seguridad deberán ser frecuentes y cuidadosas, asegurando que no se esté respaldando también el malware en ellas.



3. Principios generales de ciberseguridad

3.3 Principios generales del CCN-CERT

9. Mantener actualizadas las aplicaciones y el sistema operativo es la mejor manera de evitar dar facilidades a la potencial amenaza.
10. Revisar regularmente la configuración de seguridad aplicada, los permisos de las aplicaciones y las opciones de seguridad.



3. Principios generales de ciberseguridad

3.4 Ejercicios recomendados

Para este apartado se pueden realizar los ejercicios 1 y 2 del documento de ejercicios propuestos.

Índice

Contenidos

Contenidos

4. Normativa de protección del puesto de trabajo

4.1 Qué es la normativa de protección del puesto de trabajo

La siguiente información ha sido obtenida del Esquema Nacional de Seguridad, que puede ser encontrado en la siguiente fuente: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file.html

La normativa de protección del puesto de trabajo es un conjunto o serie de documentos, que detallan la forma de enfrentarse a un problema. Cada uno de estos documentos expone una política de seguridad respecto a un asunto concreto.

Es decir, la normativa define el conjunto de posiciones del organismo en aspectos concretos y sirven para indicar cómo se debe actuar en caso de que una cierta circunstancia no esté recogida en un procedimiento explícito de la empresa, o que el procedimiento pueda ser impreciso, o contradictorio en sus términos.

4. Normativa de protección del puesto de trabajo

4.1 Qué es la normativa de protección del puesto de trabajo

Las normas deben centrarse en los objetivos que se desean alcanzar, antes que en la forma de lograrlo. Los detalles los proporcionarán los procedimientos. Las normas ayudan a tomar la decisión correcta en caso de duda.

Deben describir lo que se considera uso correcto, así como lo que se considera uso incorrecto.

La normativa tiene carácter de obligado cumplimiento. Esto debe destacarse, así como las consecuencias derivadas de su incumplimiento (medidas disciplinarias).

4. Normativa de protección del puesto de trabajo

4.1 Qué es la normativa de protección del puesto de trabajo

Las normas deben ser realistas y viables. Deben ser concisas (sin perder precisión) y sin ambigüedades. Deben estar motivadas, ser descriptivas y definir puntos de contacto para su interpretación correcta.

Se dispondrá de una serie de documentos que describan:

a) El uso correcto de equipos, servicios e instalaciones.
b) Lo que se considerará uso indebido.
c) La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente

4. Normativa de protección del puesto de trabajo

4.1 Qué es la normativa de protección del puesto de trabajo

Una recomendación personal, más allá de lo que nos indica el Esquema Nacional de Seguridad, es la siguiente.

Una forma en la que se pueden desarrollar las políticas es emplear un documento por cada una a implementar dentro de la normativa de protección del puesto de trabajo.

De esta manera es más sencillo realizar modificaciones, controlar las versiones, etc...

4. Normativa de protección del puesto de trabajo

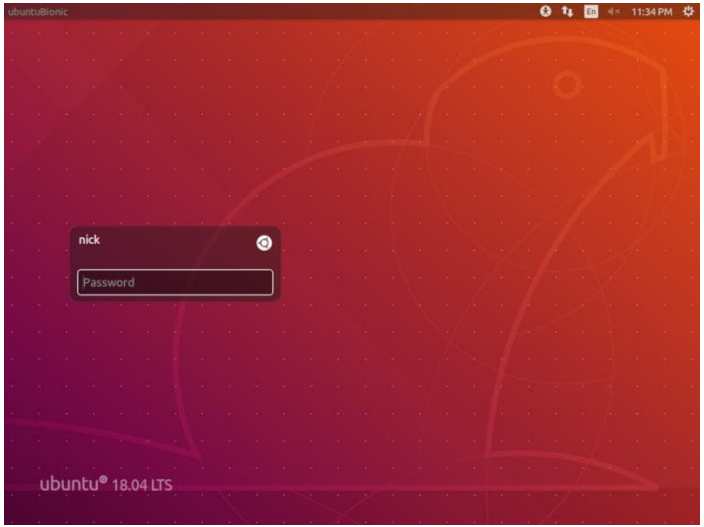
4.2 Ejemplos de normativas a considerar

- Equipos informáticos propios (bring your own device)
  - ¿Se puede poner una cuenta del trabajo en el ordenador o móvil personal? ¿Se puede conectar un móvil o un portátil personal a la red de la empresa?
- Sobre seguridad en autenticación
  - ¿Se obliga al uso de 2FA? ¿Se implanta una política de contraseñas seguras? ¿Se hace necesario cambiar la contraseña cada cierto tiempo?
- Política de mesas limpias.

4. Normativa de protección del puesto de trabajo

4.2 Ejemplos de normativas a considerar

- Proteger la información confidencial con mobiliario con cierres, cajas fuertes, armarios ignífugos...
- Transporte seguro de la información:
  - ¿Se permite transportar el portátil de la oficina fuera de ella? ¿Se puede copiar información a un disco duro externo o pen drive? ¿Se pueden introducir pen drive en los equipos de la empresa?
- Bloqueo de los equipos inactivos.
- No permitir modificar las configuraciones por defecto de los equipos empresariales.



4. Normativa de protección del puesto de trabajo

4.2 Ejemplos de normativas a considerar

- Destrucción de la información en papel. Si es confidencial, emplear máquinas destructoras.

4. Normativa de protección del puesto de trabajo

4.1 Ejercicios recomendados

Para este apartado se pueden realizar el ejercicio 3 del documento de ejercicios propuestos.

Índice

Contenidos

Contenidos

5. Plan de concienciación

5.1 Qué es el plan de concienciación en ciberseguridad

Una serie de políticas de ciberseguridad no son suficientes para proteger a una empresa o un empleado. De nada sirve tener una buena protección hacia el exterior si, de repente, un empleado envía sus claves de acceso a través de un email, víctima de un phishing. O si se instala un malware pensando que es un programa lícito. O si hace clic en enlaces peligrosos...

Es decir, la normativa de protección del puesto de trabajo debe venir acompañada de una formación en aspectos de ciberseguridad, para que evitar que un empleado no formado caiga víctima de ataques (como los de ingeniería social).

5. Plan de concienciación

5.1 Qué es el plan de concienciación en ciberseguridad

El plan de concienciación en ciberseguridad deberá alcanzar a todo el equipo de la organización, y por tanto todas las personas del equipo son destinatarias del mismo.

El plan, eso sí, debe tener en cuenta el perfil del empleado. Por ejemplo, un empleado de atención telefónica no maneja información tan relevante como el directivo encargado del departamento de finanzas.

5. Plan de concienciación

5.1 Qué es el plan de concienciación en ciberseguridad

Se deben establecer, por tanto, diferentes grupos de interés dentro del equipo para abordar las diversas necesidades de formación, y poder adecuarla a sus concretas responsabilidades, funciones y procesos de trabajo.

5. Plan de concienciación

5.2 Elementos a concienciar

Para ver este punto en profundidad, INCIBE nos proporciona una guía de ciberamenazas contra entornos empresariales:

https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberamenazas_contra_entornos_empresariales.pdf

En esta guía aparecen los ataques más habituales contra las empresas, por lo que se puede emplear de índice base para nuestro plan de concienciación.

5. Plan de concienciación

5.2 Elementos a concienciar

Además, otra guía de la que podemos obtener contenido para la realización de la concienciación en ciberseguridad es la guía de la Oficina de Seguridad del Internauta:

https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

5. Plan de concienciación

5.2 Elementos a concienciar

Aquí se van a exponer algunos ejemplos de elementos a concienciar, de manera que los empleados tengan unas buenas prácticas de ciberseguridad:

- Cumplimiento de las políticas de la normativa interna.
- Phishing, smishing, vishing, spear phishing…
- Leaks o fugas de información.
- Contraseñas seguras: de ciertos caracteres y con variedad de letras, números, mayúsculas o símbolos. Además debería ser única.

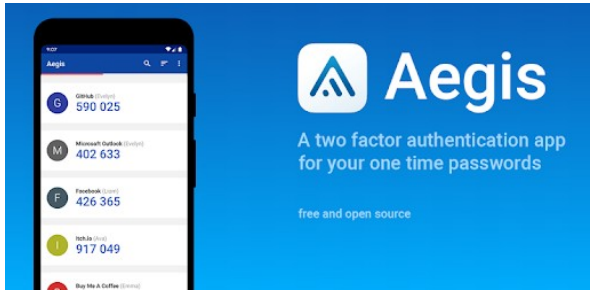
CONTRASEÑA	Tiempo estimado de descifrado
murcielago	4 minutos
MuRCieLaGo	2 días
1MuRCieLaGo!	4 años
EuldIMCd2019!	2 siglos

5. Plan de concienciación

5.2 Elementos a concienciar

Más ejemplos:

- Usar un gestor de contraseñas.
- No usar el email del trabajo para registrarse en webs de uso personal (por ejemplo: redes sociales).
- MFA o 2FA.
- Cifrado de teléfono móvil, disco duro del ordenador o de dispositivos extraíbles.



5. Plan de concienciación

5.2 Elementos a concienciar

Más ejemplos

- Ataques de ingeniería social: por teléfono, email, servicios de mensajería instantánea…
- Evitar introducir pen drive u otros soportes de datos si son desconocidos.
- Evitar ejecutar archivos con origen desconocido (por ejemplo, que vengan de un email extraño, de un pen drive desconocido, etc…).

Se pueden encontrar más ejemplos en: https://www.incibe.es/aprendeciberseguridad

5. Plan de concienciación

5.3 Apartados que puede contener

Hemos visto que hay muchos aspectos relevantes para proteger el puesto de trabajo, así como para concienciar al empleado, de forma que evitemos posibles incidentes de ciberseguridad.

Para poder concienciar a los empleados en estos aspectos se debe diseñar un plan para formar a los empleados en la cultura de la ciberseguridad. Cómo ejecutar esa formación es el plan de concienciación.

5. Plan de concienciación

5.3 Apartados que puede contener

Aunque cada organización puede y debe adaptar un programa de concienciación a sus necesidades y a la composición y ubicación de su fuerza laboral, hay algunos aspectos que siempre deben tenerse en cuenta para crear un programa que sea efectivo:

- Realizar una evaluación de ciberseguridad para identificar el riesgos e impacto de los ciberataques.
- Métodos de capacitación preferidos.
- Estrategias de refuerzo y medición para garantizar que se cumplan los objetivos de seguridad de la empresa.
- Evaluación periódica del programa.

5. Plan de concienciación

5.3 Apartados que puede contener

Veamos a continuación un ejemplo de los puntos que puede tener el programa:

1. Planificación del plan de concienciación.
    - 1.1 Identificar las necesidades.
    - 1.2 Destacar las debilidades.
    - 1.3 Adaptar el programa.
    - 1.4 Aplicar metodologías educativas.
2. Implementación.
    - 2.1 Estrategia y enfoque.
    - 2.2 Involucrar a todo el personal.
    - 2.3 Establecer responsabilidades.

Fuente: https://ciberseguridad.com/normativa/espana/medidas/plan-concienciacion/

5. Plan de concienciación

5.3 Apartados que puede contener

Veamos a continuación un ejemplo de los puntos que puede tener el programa:

3. Operar y mantener.
4. Monitorear y evaluar.
    - 4.1 Inspecciones (auditorías, punto 7).
    - 4.2 Métricas para supervisar.
    - 4.3 Actividades y comentarios.

Esto es solo un ejemplo de plan de concienciación, no un estándar de un organismo que indique cómo hacer un plan de concienciación. Cualquier otra variante, de cualquier otra fuente, puede ser válida.

5. Plan de concienciación

5.4 Ejercicios recomendados

Para este apartado se pueden realizar los ejercicios 4, 5 y 6 del documento de ejercicios propuestos.

5. Plan de concienciación

5.5 Plan director de seguridad

De forma adicional, se puede desarrollar un plan director de seguridad.

Cuando las empresas se quieren adentrar en el mundo de la ciberseguridad, se pueden preguntar: ¿Por dónde empezar?

A la hora de introducir la ciberseguridad, es importante tener una planificación de las actividades a realizar que cuente con el compromiso de la dirección. Este plan va a marcar las prioridades, los responsables y los recursos que se van a emplear para mejorar nuestro nivel seguridad en el mundo digital.

5. Plan de concienciación

5.5 Plan director de seguridad

El Plan Director de Seguridad contendrá los proyectos que vamos a abordar tanto técnicos como de contenido legal y organizativos. Así, habrá proyectos de instalación de productos o de contratación de servicios, pero otros serán para cumplir con las leyes de privacidad y comercio electrónico, formar a los empleados o para poner en marcha procedimientos y políticas internas.

Se puede ampliar información en el siguiente enlace de INCIBE:

https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad

DESCARGA EL DOSIER DEL PLAN DIRECTOR DE SEGURIDAD

Índice

Contenidos

Contenidos

6. Desarrollo de material para concienciación

6.1 Materiales de concienciación

Como parte del plan de concienciación, y para que los empleados se mantenga pendientes de los posibles riesgos en materia de ciberseguridad, se recomienda el desarrollo de materiales que les recuerden medidas vistas.

Por ejemplo, se puede proponer el colgar unos carteles con consejos de ciberseguridad, el uso de trípticos, el envío de emails recordando algunos ataques, tests de autoevaluación, etc...

6. Desarrollo de material para concienciación

6.1 Materiales de concienciación

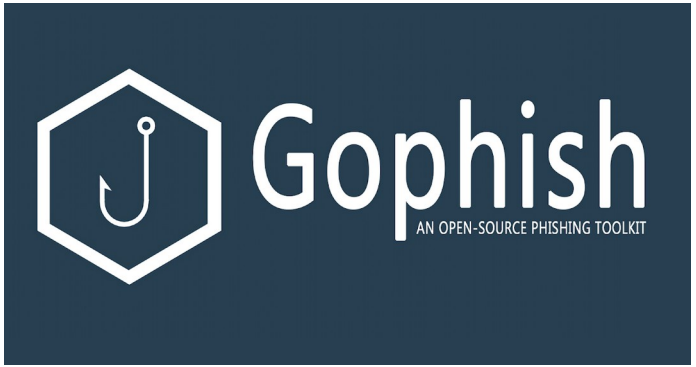
El Instituto Nacional de Ciberseguridad (INCIBE) nos ofrece en su página web un kit de ejemplo de materiales de concienciación: https://www.incibe.es/protege-tu-empresa/kit-concienciacion

6. Desarrollo de material para concienciación

6.2 Campaña de concienciación con gophish

Para realizar la concienciación respecto a aspectos de ingeniería social, phishing, y similares (spear phishing), podemos emplear la herramienta gophish.

Nota: Desde el cambio de las políticas de seguridad de Google, usar este tipo aplicaciones para enviar emails se ha vuelto algo más complejo. Debemos activar el 2FA y crear una contraseña de aplicación.



6. Desarrollo de material para concienciación

INSTITUTO NACIONAL DE CIBERSEGURIDAD

6.3 Ejemplos de emails enviados por bancos

6. Desarrollo de material para concienciación

6.3 Ejercicios recomendados

Para este apartado se pueden realizar los ejercicios 7, 8 y 9 del documento de ejercicios propuestos.

Índice

Contenidos

Contenidos

7. Auditorías para verificar cumplimiento y prevención

7.1 La necesidad de una auditoría

A la hora de implementar 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.

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, etc.), o físicos (salas de servidores, control de acceso a diferentes instalaciones, etc.).

7. Auditorías para verificar cumplimiento y prevención

7.1 La necesidad de una auditoría

En nuestro caso, acabamos de generar un plan de protección del puesto de trabajo, así como un plan de concienciación de ciberseguridad.

Los empleados deben tener entornos seguros de trabajo y operar en ellos bajo las medidas que hemos implementado en nuestro plan de protección del puesto de trabajo.

No obstante, uno de los puntos más débiles de la cadena es el propio empleado, y para ello debemos verificar periódicamente que se siguen cumpliendo los elementos anteriormente descritos.

7. Auditorías para verificar cumplimiento y prevención

7.2 Qué es una auditoría

Una auditoría es una inspección o verificación. En este caso hablamos de auditorías internas en una organización.

Se deben preparar un conjunto de acciones que comprueben, tras haber pasado un tiempo desde su implementación, la continuidad de las medidas de ciberseguridad implantadas. Concretamente la verificación de la normativa de protección del puesto de trabajo y la concienciación del empleado.

7. Auditorías para verificar cumplimiento y prevención

7.2 Qué es una auditoría

Dentro del objetivo de revisar que las medidas siguen siendo cumplidas, se debe considerar el caso en el que no. Es decir, se deben proponer una serie de acciones para reeducar a los empleados que no cumple o bien la normativa, o bien carece de la conciencia de ciberseguridad necesaria.

7. Auditorías para verificar cumplimiento y prevención

7.3 Cómo realizar una auditoría

El punto inicial en su realización suele ser detallar los elementos que se desean auditar. El criterio para estos elementos puede ser, por ejemplo, cuáles son los esenciales para que el negocio pueda funcionar.

Una vez se tengan los aspectos a revisar, se deben comprobar si estos disponen de las medidas de seguridad necesarias y además estas medidas están informadas a los empleados.

7. Auditorías para verificar cumplimiento y prevención

7.4 Qué elementos auditar

Los elementos a revisar en una auditoría son muy diversos. Consultando en internet se pueden encontrar desde las típicas checklist, hasta formas automatizadas a través de recursos informáticos. Aquí se proponen algunos elementos habituales.

- Uso de formularios (como los formularios de Google) para revisar qué nivel de conocimiento de la normativa siguen manteniendo los empleados.

7. Auditorías para verificar cumplimiento y prevención

7.4 Qué elementos auditar

- Revisión de las papeleras de la oficina, para verificar que se cumple la destrucción de los documentos confidenciales.
- Revisión de las mesas de los empleados para verificar el cumplimiento de las políticas de mesas limpias, comprobar que no tienen post-it con información confidencial (contraseñas, información interna…).
- Revisar en momentos de ausencia de los empleados (por ejemplo, durante el desayuno o el almuerzo) que todos los equipos están apagados o bloqueados. Ninguno accesible a terceros.

7. Auditorías para verificar cumplimiento y prevención

7.4 Qué elementos auditar

- Comprobar que los equipos piden usuario y contraseña al encenderse.
- Realizar una simulación de phishing para verificar que el entrenamiento de los empleados sigue siendo efectivo.
- Verificación que no se haya cambiado la configuración de los equipos (antivirus activo, firewall activo, equipos actualizados según las políticas internas…).
- Verificar que los empleados no introducen memorias USB desconocidas.

7. Auditorías para verificar cumplimiento y prevención

7.4 Qué elementos auditar

- Cifrado de datos en discos duros.
- Uso de contraseñas seguras, 2FA sigue activo, etc.
- Y uno de los aspectos más importantes, que trataremos a continuación en las siguientes unidades, y es que los eventos de seguridad (posibles incidentes) se notifican al personal adecuado.

7. Auditorías para verificar cumplimiento y prevención

7.5 Mejora de resultados

Es posible que revisando los anteriores puntos te hayas dado cuenta que hay ciertas revisiones de la auditoría que deben ser realizadas por personal cualificado.

Es posible que para determinados aspectos sea necesario contar con servicios especializados de auditoría, como por ejemplo, a la hora de realizar auditorías de revisión de cumplimiento legal o normativo (RGPD, por ejemplo), o auditorías forenses, que se encargan de investigar lo ocurrido tras un incidente de grave de seguridad (brecha de datos, botnet, ransomware, etc.).

7. Auditorías para verificar cumplimiento y prevención

7.5 Mejora de resultados

El objetivo de las auditorías es que se pueda mejorar a lo largo del tiempo. Para ello se pueden emplear métricas para ello (por ejemplo: comprobaciones falladas/total de comprobaciones), o sistemas más avanzados, como el sistema Kaizen de mejora continua.

7. Auditorías para verificar cumplimiento y prevención

7.5 Mejora de resultados

Se debe fijar la periodicidad de estas revisiones, las cuales se recomiendan que deberán realizarse al menos con carácter bianual.

Además, es necesario repetir estas auditorías tras la implantación de algún cambio significativo en los sistemas de la empresa. Esto significa que, si tras un proceso de auditoría se ha implantado una medida que tiene relevancia para nuestro negocio (por ejemplo, en el plan de protección del puesto de trabajo), estableceremos un proceso que audite si esa medida cumple los objetivos y expectativas para los que fue impuesta.

7. Auditorías para verificar cumplimiento y prevención

7.6 Otras consideraciones

En esta unidad, igual que en el curso, nos estamos centrando desde el punto de vista de la gestión de incidentes, obviando otros aspectos.

Por ejemplo, si nuestro sistema almacena información personal, debemos comprobar que se cumple la RGPD (europea) y la LOPDGDD (española). Estos otros aspectos, aunque siguen siendo esenciales de auditar, se encuentran más cercanos a lo que se conoce como una auditoría legal.

7. Auditorías para verificar cumplimiento y prevención

7.6 Otras consideraciones

Por otra parte, otras auditorías necesarias, más allá de la protección del puesto de trabajo y de la concienciación en ciberseguridad, son las siguientes:

- Test de penetración.
- Auditoría de redes y sistemas.
- Auditoría de seguridad perimetral.
- Auditorías de los sistemas web de la empresa.
- Auditorías forense.

Desde INCIBE se recomiendan, pero debemos tener en cuenta que se enmarcan fuera del contenido de este módulo profesional.

7. Auditorías para verificar cumplimiento y prevención

7.7 Ejercicios recomendados

Para este apartado se pueden realizar el ejercicio 10 del documento de ejercicios propuestos.

Índice

Contenidos

Contenidos

8. Bibliografía

- https://www.incibe.es/protege-tu-empresa/blog/has-revisado-tu-nivel-seguridad-utiliza-las-auditorias-sistemas
- https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/auditoria-sistemas.pdf
- https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2473-ccn-cert-bp-01-principios-y-recomendaciones-basicas-en-ciberseguridad/file.html
- https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-puesto-trabajo
- https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion_del_puesto_de_trabajo.pdf

8. Bibliografía

- https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/concienciacion-y-formacion.pdf
- https://www.incibe.es/protege-tu-empresa/kit-concienciacion
- https://files.incibe.es/incibe/kit_concienciacion/kit_concienciacion.zip
- https://www.incibe.es/protege-tu-empresa/blog/has-revisado-tu-nivel-seguridad-utiliza-las-auditorias-sistemas
- https://www.incibe.es/protege-tu-empresa/herramientas/politicas

8. Bibliografía

- https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file.html
- https://ciberseguridad.com/normativa/espana/medidas/plan-concienciacion/