

# Diseño de planes de securización.

## Caso práctico

El  
CEO  
de la



[Direct Media \(CCO\)](#)

empresa ha decidido modernizar la clínica para ello se han marcado los siguientes hitos:

- ✓ Desarrollar una herramienta informática que gestione:
  - ↳ o Historiales de los pacientes.
  - ↳ o Nóminas.
  - ↳ o Relaciones con proveedores.
- ✓ Informatizar todos los historiales.
- ✓ Adquirir nuevos equipos con los que poder utilizar la herramienta.
- ✓ Crear una página web corporativa de carácter informativo.
- ✓ Adquirir un nuevo servidor para alojar la herramienta.
- ✓ Reducir al máximo posible los costes y plazos de entrega.

Debido a que el presupuesto es reducido varias empresas con las que se han puesto en contacto se han negado a realizar el desarrollo pero finalmente una empresa local acepta los términos además garantizar costes y plazos. Transcurrido no más de un mes la empresa desarrolladora ha terminado y deciden presentar al CEO de Venus SA. los resultados de su trabajo.

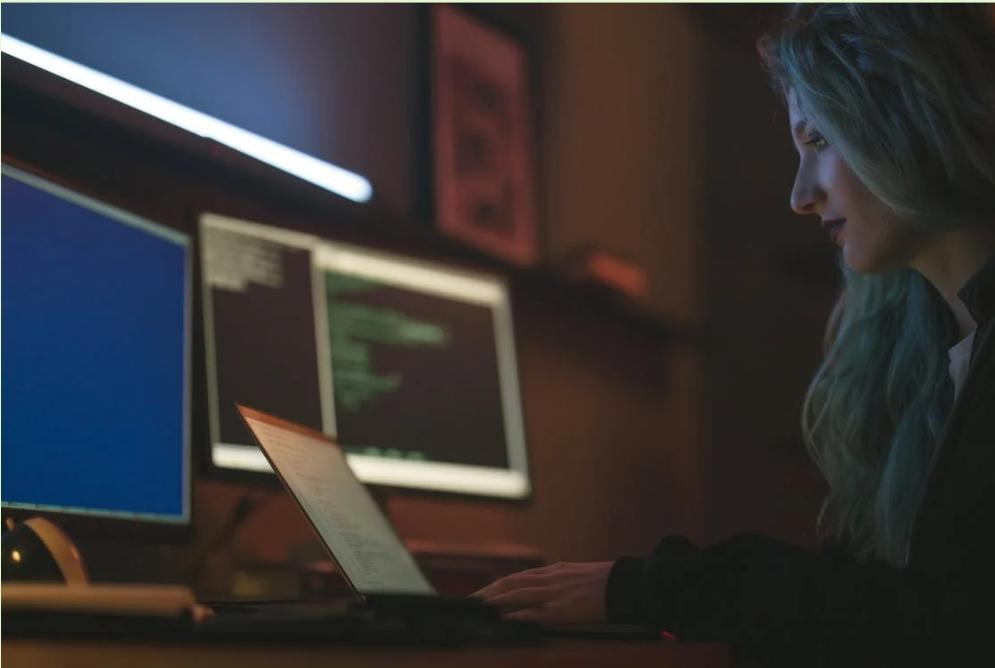
**Objetivos:**

En esta unidad de trabajo estudiarás los conceptos básicos sobre el desarrollo de planes de seguridad asociados a las tareas de bastionado de redes y sistemas. Comenzando por un análisis de riesgos hasta la implementación de un plan director de seguridad. Para ellos se darán a conocer cuáles son las medidas técnicas, las políticas de seguridad más usadas así como las guías de buenas prácticas más populares sin dejar de lado la caracterización de procesos.

Además también conocerá los principios de la economía circular y su importancia en la actualidad.

# 1.- Análisis de riesgos.

## Caso práctico



Una  
óptica  
que  
tiene  
dos

[Cottonbro \(CC0\)](#)

ordenadores, se ha visto afectada por una infección por ransomware. El empresario consideró que por su actividad no debería llevar a cabo un análisis de riesgos. Nada más lejos de la realidad. La óptica usaba una versión desactualizada de soluciones antivirus y ello provocó la infección. Como consecuencia han perdido todos los datos. Si hubieran llevado a cabo un pequeño análisis de riesgos, no hubieran tenido ese problema

Tal y como se introdujo en la unidad uno, para poder conocer a qué amenazas se encuentran sujetos los activos de una organización, el primer paso es llevar a cabo una evaluación de cuál es la situación inicial, en términos de ciberseguridad, de la organización. Esta fase conlleva una serie de actividades que describiremos a continuación.

## 1.- Conocer la situación actual del sistema/organización

Sin duda es indispensable conocer la situación actual en términos de ciberseguridad de la organización o sistema sobre el que vamos a hacer el análisis. Nunca podremos estar seguros de si realmente estamos elevando el nivel de seguridad si no conocemos la situación de partida.

Para llevar a cabo este primer análisis, tendremos en cuenta los aspectos esenciales sobre los que hemos de realizarlo como por ejemplo:

- Nivel de madurez de la empresa
- Elementos técnicos
- Aspectos organizativos
- Cumplimiento o normativa vigente
- Criticidad de la información

Como se puede inferir, este primer análisis, es necesario implicar a toda la organización, pues debemos realizar una serie de actividades como entrevistas, cuestionarios, etc. para recopilar la información necesaria de cara a llevar a cabo el análisis. En este punto podríamos encontrar dificultades o problemas como que no se nos facilitara toda la información, de manera intencionada o no, no contar con el apoyo de áreas críticas, como el área de TI, etc. Además será necesario contar con el apoyo de la dirección o la parte estratégica de la organización para esta cuestión ya que, por ejemplo, si no creen en las bondades de la ciberseguridad, difícilmente podremos incrementar el nivel de seguridad ya que no se facilitará presupuesto y se demorarán los plazos establecidos priorizando otras cuestiones.

## 2.- Limitar el alcance

En la unidad 1 ya avanzamos esta cuestión. Para poder implementar ciberseguridad desde un punto de vista efectivo y eficiente, se ha de limitar el alcance del proyecto y este además ha de ser realista. Por un lado para conocer el tamaño de las tareas que tendremos que llevar a cabo, y por otro para concretar sobre qué áreas o procesos se llevará a cabo. Por ejemplo, en una empresa dedicada a la investigación, una de las áreas más importantes a proteger será la relativa a I+D+i.

Atendiendo a lo anterior, tendremos que realizar una identificación de activos que serán los objetivos donde se aplicarán los controles de seguridad que implementemos, tanto a nivel técnico como organizativo sin olvidar los de carácter normativo. Lo habitual es que una vez determinados los más críticos, las tareas de protección comiencen por estos. Un buen punto de partida para determinar qué controles se han de implementar, podría estar basado en el listado de la norma ISO/IEC 27001 introducida en la unidad 1. Estos controles han de estar dirigidos por los que se denominan escalas o modelos de madurez que pueden tener distintos valores en función de cómo se encuentre implementado en la organización. Tomando como ejemplo los basados en CMM y considerando el control relativo a las copias de seguridad, este podría ser:

- Inexistente: carecen de política de copias de seguridad.
- Inicial: disponen de un sistema, pero nadie las controla ni se planifican.
- Repetible: se lleva a cabo la política pero sin ningún tipo de normalización, habitualmente bajo demanda.
- Definido: existe un procedimiento claro, pero no está aprobado por la dirección.
- Administrado: existe un procedimiento formal que ha sido aprobado.
- Optimizado: existe un procedimiento formal que ha sido aprobado y se verifica su eficacia periódicamente mediante indicadores.



## 1.1.- Fases del análisis.

Paralelamente a las cuestiones previas, llevaremos a cabo el análisis propiamente dicho en todas sus fases para obtener el listado de posibles amenazas que podrían afectar al sistema analizado. En la unidad uno ya introducimos las diferentes metodologías y estándares existentes para llevar a cabo esta tarea y estas presentan aspectos comunes. Sin duda el que confluye en todas, es el valorar cada activo para establecer posteriormente la priorización.

Entre las fases para llevar a cabo esta tarea destacamos:

### Fase inicial: reconocimiento

1. Identificación de activos: para identificar las amenazas a las que podrían estar sujetos.
2. Identificación del riesgo intrínseco: resultante de la fase previa y que, nos dará el nivel de riesgo del activo sin la aplicación de los controles que mejorarán la seguridad.
3. Probabilidad de ocurrencia: estableceremos la posibilidad de que se materialice la amenaza sobre el activo y que pueda generar un impacto y las consecuencias derivadas. En este punto podremos calcular el nivel de riesgo siguiendo la fórmula:  
Riesgo= Impacto (€) x probabilidad. En este sentido y usando un ejemplo, si para nuestra empresa, la falta de acceso a la información de los servidores físicos a causa de un incendio en las instalaciones podría costarnos 1000€ al día y eso se puede prorrogar durante un mes, y considerando una probabilidad baja en una escala del 1 al 10, la fórmula podría quedar de la siguiente manera: Riesgo=(1000x30)x2, resultando una cantidad de 60000€ en posibles pérdidas. Esto evidentemente indica que se requiere establecer un control para esta cuestión.
4. Riesgos no aceptables: tras el paso previo, hemos de identificar aquellos riesgos que no son aceptables. Estos serían aquellos que pueden afectar muy negativamente al negocio hasta el punto de dejar la organización sin servicio. El tipo de control a implementar, será siempre proporcional al activo que se quiere proteger.
5. Riesgo residual: determinará el nivel de riesgo tras su reducción considerando este con un valor “aceptable”.



[Intef \(CC BY-NC-SA\)](#)

### Mitigación de los riesgos

Tras la fase previa, en esta será donde se establecerán los mecanismos y controles que permitirán definir un nivel de riesgo aceptable y asumible. ¿Con qué mecanismos contamos para llevar a cabo esta tarea? Podemos implementar los siguientes:

1. Implementar controles para su mitigación: suele ser la más habitual cuando se trata de problemas que pueden interferir en el correcto funcionamiento de los procesos de una organización.
2. Eliminando el riesgo: cuando se trata de un proceso que no es necesario pero que podría poner en peligro otros activos de la organización.
3. Tercerizar o transferir el riesgo: a través por ejemplo de un ciberseguro o una póliza de [ciberriesgos](#).

## Establecimiento de indicadores y verificación del proceso

Tras definir los controles, se han de establecer [cuadros de mando](#) que nos permitan medir el correcto funcionamiento de los controles. Si no tenemos en cuenta esta cuestión, es decir si no medimos, nunca sabremos si realmente el control está funcionando. Por ejemplo, en una política de copias de seguridad, si no comprobamos la frecuencia con que se hacen y si no verificamos su posible restauración, no podremos estar seguros de si realmente la misma está funcionando de manera correcta. De esta manera verificaremos que la medida que se ha implementado es efectiva contra el riesgo que queremos reducir.

Por último, es importante indicar, que el análisis de riesgos es un proceso continuo y que se debe llevar a cabo de manera periódica pues las tecnologías, servicios e infraestructuras de las organizaciones cambian frecuentemente en el mundo TI. Se trata como indicamos en la unidad 1, de un proceso de mejora continua.

### Debes conocer

En el siguiente enlace podrás conocer lo sencillo que es llevar a cabo un análisis de riesgos en una pyme:

[Análisis de riesgos](#)



## AUTOEVALUACIÓN

La fase inicial de un análisis de riesgos es:

- Implementación de medidas
- Reconocimiento inicial
- Reconocer el riesgo residual

## 2.- Principios de la economía circular.

### Caso práctico



[Intef \(CC BY-NC-SA\)](#)

Es importante disponer de sistemas productivos que permitan el reciclaje y la sostenibilidad. Por ejemplo, aquellas organizaciones que producen con materias tipo monocomponente, en el futuro serán sostenibles. Imaginemos una empresa que mezcla muchos tejidos en sus prendas. Será prácticamente imposible reciclar esa ropa ya que el proceso de separación sería muy complejo.

El proceso productivo actual, no es sostenible. Se trata de un proceso lineal donde se usa demasiada materia prima que luego no es posible reciclar o reutilizar, o al menos en un porcentaje que garantice unos niveles de sostenibilidad adecuados.

¿En qué consiste la economía circular en la industria 4.0? básicamente en un sistema que permita aprovechar los recursos, reduciendo elementos innecesarios que por su naturaleza no pueden volver al medio ambiente.

Algunos de sus principios fundamentales (Fuente [Corponet](#)):

- El residuo se convierte en recurso. Todo el material biodegradable vuelve a la naturaleza y el no biodegradable se reutiliza.
- Reintroducir en el circuito económico aquellos productos que ya no corresponden a las necesidades iniciales de los consumidores.
- Reutilizar ciertos residuos o partes de ellos que todavía pueden funcionar para elaborar nuevos productos.
- Reparar y encontrar una segunda vida para los productos estropeados o defectuosos.
- Reciclar los materiales que se encuentran en los residuos.
- Aprovechar energéticamente los residuos que no se pueden reciclar.
- Eliminar la venta de ciertos productos para implantar un sistema de alquiler de bienes. Cuando el producto cumple su función principal, vuelve a la empresa y esta lo desmonta para reutilizar las piezas que pueden ser utilizadas nuevamente.
- Eliminar los combustibles fósiles para producir el producto, reutilizar y reciclar.
- Considerar los impactos medioambientales a lo largo del ciclo de vida de un producto y los integra desde su concepción.
- Establecer un método de organización industrial en un mismo territorio caracterizado por una gestión optimizada de los stocks y de los flujos de materiales, energía y servicios.

En el mundo TI por ejemplo, se busca poner fin a la obsolescencia programada y diseñar productos que sean sostenibles y eficaces en el tiempo, pero no sólo eso, si no que los avances tecnológicos como la inteligencia artificial, el Big Data y otras tecnologías, mejoras los procesos aunque no es ninguna panacea. En cualquier caso, aún estamos comenzando con este proceso y será esencial en los próximos años para garantizar la buena salud del medio ambiente.

Esta cita del Dr. Edmond Locard es conocida como el **Principio de Locard**, y del mismo se deduce que, a la hora de realizar el propio análisis forense, hay que ser especialmente cuidadoso para que el sistema se vea afectado en la menor medida posible y que las evidencias adquiridas no se vean alteradas, debido a que el uso de cualquier dispositivo informático siempre puede dejar algún tipo de rastro.

## Debes conocer

Amplia información acerca de la economía circular: [Economía circular 4.0](#)

### 3.- Medidas técnicas de seguridad.

#### Caso práctico



[Clker-Free-Vector-Images](#) (Dominio público)

Para implementar seguridad, además del factor humano, hay que considerar las tecnologías. Imaginemos que una persona tiene que encargarse de comprobar uno a uno los archivos para ver si contienen virus o no. Sería una tarea titánica y que estaría sujeta a fallos debido al cansancio que provocaría. De este modo mediante una medida técnica como un antivirus, servirá para llevar a cabo dicha tarea de manera más eficiente y eficaz.

En este punto entraremos a describir diferentes medidas técnicas de seguridad adecuadas para reforzar la seguridad de los sistemas. No entraremos en detalles pormenorizados si no que lo haremos a alto nivel.

Es obvio que cuando hablamos de ciberseguridad, lo primero que nos suele venir a la cabeza, es lo relativo a tecnologías y herramientas. Evidentemente estas tienen gran importancia, pero no son lo único que hemos de tener en cuenta a la hora de bastionar una infraestructura, aunque sí será lo que trataremos en este apartado.

Podemos definir como medida técnica de seguridad “aquella que ha sido diseñada en base a una tecnología o varias, cuyo propósito es proteger un activo o servicio de alguna amenaza o riesgo y que habitualmente ha de proteger las tres dimensiones de la seguridad de la información: la confidencialidad, la integridad y la disponibilidad”. En este sentido podemos contener dichas medidas en dos grupos fundamentales:

- Medidas preventivas
- Medidas reactivas

#### Preventivas

Dentro de este grupo, enumeraremos algunas de las principales herramientas o grupos de herramientas destinadas a evitar que se materialice una amenaza en un activo. Habitualmente siempre se suele decir que “es mejor prevenir que lamentar” y en el mundo de las TI podríamos suscribir dicha frase. Podemos ilustrarlo con un ejemplo clásico, ¿Qué es más recomendable. Usar un equipo con una herramienta antimalware o pensar que somos lo suficientemente precavidos como para no necesitarla? Evidentemente si un día nos infectamos con un ransomware, nos acordaremos de que deberíamos haber instalado una aplicación de esas características.

Aunque las veremos el funcionamiento de algunas herramientas con mayor detalle en unidades posteriores, en esta ocasión describiremos de manera somera algunos grupos de controles:

- Herramientas antimalware: se trata de la solución más básica. Los comúnmente conocidos como antivirus aunque desde hace unos años, disponen de otras funcionalidades integradas como cortafuegos.
- EDR y XDR: se trata de soluciones antimalware más modernas que las anteriores y que además disponen de medidas o funciones reactivas. EDR (Endpoint Detection and Response) se puede considerar la primera generación de este tipo de soluciones, y XDR (Extended Detection and Response) como la segunda. Ambas usan inteligencia artificial y otras técnicas para prever posibles ataques y patrones.
- Firewalls o cortafuegos: se trata de herramientas que van a poder configurarse para permitir o impedir el tráfico entre las redes en base a las reglas que se establezcan.
- Copias de seguridad: sin duda la estrella de las medidas preventivas y reina de los planes de contingencia. En caso de pérdida de la información, nos permitirá recuperarla.
- DLP: Data Loss Prevention, son un conjunto de herramientas que velan por que la información de una compañía no se exfiltre o se envíe sin disponer de autorización, lo que también se conoce como una fuga de datos. Estas herramientas permiten mantener el control de la información sin perder productividad.
- Verificación de integridad: mediante este tipo de soluciones, será posible controlar la integridad de los archivos que forman parte de un sistema o arquitectura. A través de la construcción de una base de datos, si se produce algún cambio como por ejemplo un binario, la herramienta generará una alerta. Habitualmente se usan funciones de [hash](#).
- Conexiones seguras: algo esencial para proteger las comunicaciones, es mantener la confidencialidad de los datos que discurren por ellas. Existen numerosas herramientas pero destaca la implementación de VPNs (Virtual Private Networks) y otro tipo de soluciones de encapsulado. Si algún atacante intercepta el tráfico, en principio no podrá leerlo.
- IDS: los sistemas de detección de intrusos, son herramientas de carácter preventivo que informan ante un comportamiento anómalo en la red o en un host, para llevar a cabo algún tipo de acción.
- Virtual patching: se trata de un conjunto de soluciones diseñadas sobre todo para aquellos sistemas de producción que están soportados por sistemas obsoletos y que no es posible cambiar.
- SIEMs: los sistemas de identificación de eventos de seguridad, son sin duda una de las herramientas más populares de los últimos años que ayudará a identificar comportamientos anómalos tanto en una red como en un host.

## Reactivas

En este grupo se encuentran las herramientas que en caso de identificación o en el peor de los casos, se materialice un incidente, puedan llevar a cabo alguna acción que permita contenerlo, eliminarlo o corregir la situación. Indicar que algunas herramientas de carácter reactivo, también se encuentran en el grupo previo.

Quizás podamos considerar que si disponemos de un buen conjunto de medidas técnicas de carácter preventivo, no tenga demasiado sentido contar con medidas reactivas. Sin duda estaríamos ante un gran error de contexto ya que suelen complementarse. Algunas de estas herramientas pasarían por:

-  EDR y  XDR: la función reactiva de estas herramientas pasa por contener, bloquear o eliminar la amenaza detectada. Los sistemas de inferencia que usan son muy avanzados y efectivos.
- IPS: se trata de un IDS pero con capacidad reactiva, es decir, si identifica un evento no autorizado, además de avisar, llevará a cabo algún tipo de acción como un bloqueo.
- Plan de contingencia: más que de una herramienta, se trata de una política que recoge varias herramientas o soluciones que permitirán restaurar la actividad de una organización a través de un procedimiento específico. Suelen involucrar herramientas de copia de seguridad, de gestión de incidentes, etc.
- Verificación de integridad: esta herramienta, además de prevenir, puede llevar a cabo acciones como la restauración de un archivo en caso de modificación no autorizada o similar.
- Virtual patching: como con otras soluciones que también tienen un carácter preventivo, el virtual patching va a poder bloquear o parar ciertas amenazas que puedan afectar al activo que protege.

## Debes conocer

INCIBE cuenta con un extenso [catálogo ciberseguridad](#), en el que se recogen más de 5000 soluciones y servicios de ciberseguridad.

## 4.- Políticas de securización.

### Caso práctico



[Mediamodifier](#) (Dominio público)

Los análisis de riesgos son fundamentales para una empresa. Por ejemplo, una organización que no haya llevado a cabo la identificación de sus procesos más críticos, como por ejemplo aquella que se dedica al ecommerce y no vela por la seguridad de su portal web, tendrá severos problemas para mantener la actividad. En este caso

y de manera mínima, tendrá que disponer de una política de copias de seguridad para los datos así como una política de actualizaciones.

Existen numerosas formas de agrupar las políticas en base a diversos criterios. La clasificación más común podemos decir que es la que distingue a la parte técnica y a la parte organizativa. No obstante, antes de entrar en ese aspecto, es importante conocer la diferencia entre una política y una buena práctica. A menudo se confunden o se asocian dichos conceptos a la misma cuestión, algo que es incorrecto. De manera somera podemos decir que:

- Buena práctica: recomendación que no es de obligado cumplimiento.
- Política: instrucción de obligado cumplimiento y que, en caso de no proceder como se indica, es posible amonestar o llevar algún tipo de acción sancionadora.

Una vez hecha la distinción pertinente, pasaremos a describir los dos grupos de políticas así como las más habituales que conforman dichos grupos.

Las políticas son una herramienta que permitirá implementar ciberseguridad en los distintos procesos que forman parte del negocio de una organización. Tal y como avanzamos al comienzo del punto podemos distinguir dos grupos: organizativas y técnicas. Las primeras hacen referencia a cuestiones relacionadas con el comportamiento que deben tener por ejemplo, los empleados ante determinadas cuestiones y que normalmente no pueden ser protegidas mediante medidas técnicas. Por ejemplo, "Está prohibido compartir contraseñas", o "será obligatorio destruir la documentación en papel". En cambio las técnicas, permiten implementar medidas que automatizan el control que se quiere implementar. Por ejemplo, la necesidad de cambiar la contraseña cada "x" meses, su complejidad y tamaño se puede configurar a través de una directiva en el servidor.

Habitualmente, las políticas son de aplicación sobre tres elementos, los procesos, las personas y las tecnologías. En función de a quién se dirija tendrán unas características concretas que servirán para el diseño de la propia política.

En relación a las políticas, es importante también, considerar que deben estar equilibradas y alineadas por un lado con el negocio, y por otro con la usabilidad de los sistemas. No será nunca recomendable implementar políticas tan restrictivas que impidan que los procesos del negocio se desarrollen con normalidad, es decir, la ciberseguridad ha de apoyar al negocio y no al contrario.

A continuación se ofrecerá un listado de las políticas más comunes tanto a nivel organizativo como técnico.

## Organizativas

- Continuidad del negocio: esta política permitirá implementar los controles necesarios para que en caso de desastre, se pueda recuperar la actividad del negocio lo más rápido posible de manera que las consecuencias no sean muy negativas.
- Cumplimiento legal: a día de hoy y al menos en el Espacio Europeo, las empresas con independencia de si son públicas o de ámbito privado, han de cumplir una serie de leyes que en caso contrario, acarrearían duras sanciones. Algunas destacadas son el [RGPD](#) o la [LOPDGDD](#). Esta política se implementa para garantizar el cumplimiento.
- Relación con proveedores: a día de hoy, no se concibe la actividad de una empresa sin múltiples colaboradores. En ocasiones, la falta de controles entre las transacciones que se realizan, podrían provocar un incidente. Esta política vela por que se haga de manera correcta sin poner en riesgo a la empresa.
- Concienciación y formación: sin duda de las más importantes de cara a permitir que los empleados puedan elevar el nivel de ciberseguridad. Una política de este tipo garantizará la existencia de un “firewall humano” que será capaz de identificar los incidentes y eliminarlos o reportarlos.
- Uso del correo electrónico: a pesar de que se asocia el uso de una tecnología, como un cliente, es importante conocer cómo se debe hacer. Habitualmente esto se relaciona con el uso corporativo eliminando el derecho relativo al uso personal.
- Uso de dispositivos corporativos: similar a la anterior, esta política regula las directrices que un empleado ha de asumir cuando usa un equipo corporativo, sea un PC, portátil o dispositivo móvil.
- Uso de contraseñas: en este caso, el control se refiere a todo lo que no puede ser controlado por una directiva o política técnica. Tal y como adelantamos en el punto previo, se refiere a la no compartición de contraseñas, a no apuntarlas en post-it, etc.
- Protección del puesto de trabajo: también dirigida a los empleados para hacer un uso correcto del entorno. Por ejemplo el bloqueo de sesión, no dejar información confidencial a la vista, etc.

## Técnicas

- Auditoría de sistemas: se trata de una medida técnica que permitirá identificar cualquier problema ante la evolución de las infraestructuras. Será un proceso que se ejecutará cada cierto tiempo. Sirva como ejemplo, que una auditoría realizada hace un año, poco o nada tendrá que ver con la situación actual de la empresa ya que los sistemas y aplicaciones pueden haber evolucionado.
  - Antimalware: política que obliga a disponer de una solución individual o centralizada para combatir este tipo de amenazas.
  - Uso de dispositivos móviles y equipos corporativos: medida que a través de diversas directivas técnicas, tiene como propósito la protección del hardware enumerado.
  - Control de acceso: en una empresa u organización, todos los empleados no tienen que tener acceso a “todo”, de hecho, tal y como vimos en la unidad 1, ahora se apuesta por el paradigma “Zero Trust”. En base a esto, la política establecerá los roles y permisos para poder garantizar los dominios de la seguridad de la información.
  - Copias de seguridad: se ha repetido un millón de veces que la información es el activo más importante de una empresa. Este activo está sujeto a una serie de amenazas que pueden afectar a su disponibilidad, integridad o confidencialidad. Las políticas de copias de seguridad deben estar diseñadas para hacer frente a dichos problemas y además debe de estar incardinada en la política de continuidad de negocio.
  - Gestión de logs: la monitorización de los sistemas es esencial para garantizar que ante un incidente, podemos dar la respuesta más ágil. Esta política está diseñada para conocer las alertas que se pueden dar, llevar a cabo un análisis que permita identificar el problema y detectar cualquier tipo de error.
  - Respuesta a incidentes: con independencia de que hayamos diseñado un excelente plan director de seguridad, es un hecho que los incidentes van a poder materializarse. Una política de este tipo permitirá diseñar un plan de acción y un sistema de escalado para mitigar el problema de una manera ágil. Es muy importante que esta política esté muy bien detallada.
  - Actualizaciones: puesto que la entrega o el “delivery” de actualizaciones puede ser muy complejo en organizaciones muy grandes, es vital contar con un plan que impida que un atacante pueda aprovecharse de una vulnerabilidad en un sistema operativo o una aplicación. A través de esta política se diseñará como llevar a cabo el despliegue.
  - Borrado seguro: en ocasiones por necesidad, otras por cumplimiento legal (eliminación de datos tras retención obligatoria), será necesario diseñar e implementar un control que permita a la organización destruir la información con total garantía de que no es posible recuperarla.
  - Teletrabajo: se trata de una política que tras la aparición de la pandemia se ha hecho muy popular. Básicamente contendrá las directrices necesarias para desempeñar esta modalidad de manera segura. Por ejemplo, conectarse siempre a través de una VPN, usar 2FA, etc.
-

## Debes conocer

Existen tantas políticas de seguridad como necesidades identifiquemos en nuestro negocio pero en cualquier caso, es importante que se priorice en función de qué es lo que deseamos proteger. En INCIBE, disponen de una [serie de políticas](#) de carácter generalista para desplegar en cualquier tipo de organización.



## AUTOEVALUACIÓN

Una política es equivalente a una buena práctica:

- Verdadero     Falso

## 5.- Guías buenas prácticas.

### Caso práctico



[OpenClipart-Vectors](#) (Dominio público)

Un técnico de una empresa necesita implementar varias medidas de seguridad en algunos de los servicios de la empresa para la que trabaja. Navegando por Internet, se encuentra que en INCIBE, existen numerosas referencias que le pueden servir. Para ello, toma varios de los documentos que consultará para securizar la red wifi, destruir la información de manera segura y crear políticas de seguridad. La existencia de este tipo de guías puede facilitar el trabajo de los técnicos de TI.

Tal y como distinguimos en el punto previo, es importante distinguir entre una buena práctica y una política. En el caso de las guías, ocurre algo similar. Las empresas van a poder contar con documentos elaborados por diversas organizaciones dedicadas a la ciberseguridad, tanto de ámbito nacional como el [INCIBE](#) o el [CCN-CERT](#), como internacional con la [ENISA](#) o [ECSO](#), que facilitan numerosas guías de buenas prácticas con muy diversos propósitos. Recordamos que estas no son de obligado cumplimiento pero sí muy recomendables para la implementación de controles específicos sobre los sistemas o redes que queramos proteger.

Las temáticas que ofrecen son muy diversas, desde el uso seguro de las redes wifi hasta recomendaciones específicas para sectores concretos como por ejemplo los fabricantes de juguetes conectados.

Puesto que no es objetivo de este punto enumerar y explicar el propósito de cada una de las guías disponibles, se facilitan las referencias a los listados más interesantes para que el alumno pueda escoger.

- [Guías de ciberseguridad del INCIBE](#)
- [Guías STIC del CCN](#)
- [Guías de la ENISA](#)
- [Guías de ECSO](#)

Mencionar que si llevamos a cabo una búsqueda, encontraremos miles de referencias a guías de buenas prácticas. Se han escogido las previas por tratarse de organizaciones que no atienden a intereses particulares ni están sujetas a cuestiones económicas dependientes de grandes corporaciones.

## **6.- Estándares de securización en sistemas y redes.**

---

### **Caso práctico**



Inlef (CC BY-NC-SA)

La implementación de un estándar de seguridad tiene muchas ventajas. Por un lado, la organización que lo implemente, estará alienada con las mejores prácticas desarrolladas por conjuntos de expertos, lo que tendrá más garantías de que los procedimientos funcionen adecuadamente. Además, también podrá certificarse en alguno de estos estándares como por ejemplo la ISO27000.

Si en el punto anterior, hablábamos de medidas que aunque no son obligatorias es recomendable implementar, cuando nos referimos a un estándar o un marco específico de securización para las redes y los sistemas, nos encontramos ante un modelo de obligado cumplimiento siempre y cuando, la empresa que lo implemente, quiera certificarse en ese estándar. Como ejemplo sirva una empresa que toma el cuadro de controles de la [ISO 27001](#), para implementar alguno de ellos pero sin certificarse, obviamente lo podrá hacer sin ningún problema, pero en el momento en que quiera certificar su [SGSI](#) (Sistema de gestión de la seguridad de la información), deberá cumplir todos aquellos controles que le apliquen.

Partamos mencionando la definición de estándar: "La legislación (Artículo 8 de la Ley 21/1992 de Industria) define norma como "la especificación técnica de aplicación repetitiva o continuada cuya observancia no es obligatoria, establecida con participación de todas las partes interesadas, que aprueba un Organismo reconocido, a nivel nacional o internacional, por su actividad normativa". Este concepto cuyo origen parte del ámbito industrial, se ha llevado también a otros contextos, como es el caso de la ciberseguridad y ha venido manteniendo el orden de aprobación a través de organismos conocidos como UNE, ISA, NIST, IEC, entre otras.

Mencionar que también es cierto que existen corrientes que no están demasiado a favor de estas cuestiones pues la implementación de una norma, lleva asociados una serie de costes que no todas las organizaciones pueden asumir. De hecho, la certificación de un SGSI cuenta con unos períodos de revisión en los que hay que desembolsar, además de cumplir los requisitos, una suma de dinero para mantener la certificación.

Algunos de los estándares más relevantes en el mundo de la ciberseguridad que cubrirían los aspectos más importantes serían:

## ISO

A continuación las más relevantes relativas a la [International Standards Organization](#):

- ISO/IEC 27000: Gestión de la seguridad de la información (SGSI).
- ISO/IEC 27032: Directrices para la ciberseguridad.
- ISO/IEC 27033: Seguridad de las redes.
- ISO/IEC 27034: Seguridad de las aplicaciones.
- ISO/IEC 27035: Gestión de incidentes de seguridad de TI.
- ISO/IEC 27036: Gestión de la seguridad de la información en relaciones con terceros.

## NIST

- [Cybersecurity Framework](#)

## Debes conocer

El [ENS](#), a pesar de que no es un estándar, si no un marco normativo de aplicación en la Administración Pública de España, cada vez es más común que en las licitaciones públicas se exija a los contratistas estar certificados en el Esquema Nacional de Seguridad. Si se medita, tiene todo el sentido, pues una empresa que va a ofrecer servicios a una Administración, deberá contar con al menos, las mismas medidas de seguridad que esa administración.

## 7.- Caracterización de procedimientos, instrucciones y recomendaciones.

### Caso práctico



[SusanLesch](#) (Dominio público)

Una empresa de seguridad, quiere desarrollar un servicio de SOC. Para ello necesita caracterizar el proceso de gestión de incidentes. Eso le va a permitir transformar los datos de entrada en un valor o producto final. En el proceso de

caracterización, determina que sus inputs son los propios incidentes que se transformarán en función de los procesos a los que estén sometidos para finalizar en un resultado.

A continuación, y tomando como ejemplo la gestión de incidentes, se va a proponer un modelo de caracterización pero hay decenas de alternativas. En primer lugar hemos de determinar los elementos esenciales:

- Nombre del proceso/procedimiento: gestión de incidentes
- Propietario: jefe de seguridad (CISO). En este caso, será el que tenga la responsabilidad.
- Cliente/destinatario del proceso: usuarios, personal, clientes, etc. El público al que se dirige.
- Objetivo del proceso: gestionar los incidentes que lleguen a través de la cuenta de correo y procesarlos a través de RTIR. Aunque la descripción es sencilla en este caso, se ha de tener en cuenta cuestiones como la idoneidad del mismo, la obtención de indicadores para medir la eficacia y eficiencia y ver cómo satisfacen las necesidades de los destinatarios.
- Elementos de entrada: colas de correo, llamadas telefónicas y formulario web. Se han de indicar desde dónde llegan los input.
- Elementos de salida: elementos resultantes del proceso como informes, estadísticas, etc.
- Recursos humanos: responsable, tres técnicos de nivel 1 y un técnico de nivel 2. Será el “músculo” para que el procedimiento se lleve a cabo.
- Recursos tecnológicos:  cola [RTIR](#), máquinas de pruebas, sandboxes y cuadros de mando Kibana.
- Mecanismos de control: informes de seguimiento y tiempo de respuesta.
- Indicadores: número de incidentes resueltos por día, media de resolución de incidentes, etc. Es importante contar con herramientas de medición ya que lo que no se puede medir, no se puede mejorar.

El formato de presentación de la información puede ser muy diverso. Lo que tenemos que considerar a la hora de establecer un modelo, es que tendremos elementos de entrada, procesado y posterior salida. Un posible ejemplo sería:

Nombre del Proceso					
Misión del Proceso					
Responsable					
DESCRIPCIÓN DEL PROCESO					
Proveedores	Entradas	Actividades realizadas (consignar solo las principales)	Medidas de control	Salidas	Clientes

Elaboración propia (Dominio público)



## AUTOEVALUACIÓN

Los indicadores son un elemento fundamental en la caracterización:

- Verdadero
- Falso

## 8.- Niveles, escalado y protocolos de atención a incidencias

### Caso práctico



# CSIRT

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

[Gobierno de Chile \(CCO\)](#)

Como en otros procedimientos, en la gestión de incidentes es necesario llevar a cabo procesos de escalado. Estos se realizan en función de la importancia del incidente o del impacto que este pueda tener. Por ejemplo una infección convencional de un virus que es fácil de contener, no será escalado al equipo más especializado. Por el contrario si se trata de una amenaza que puede provocar grandes daños, se elevará al equipo más preparado para contenerla.

Aunque este tema se trata con mayor detalle en el módulo 2 y el módulo 7, haremos una pequeña incursión a través de este punto. Comenzaremos mencionando que no existe un método específico para esta cuestión. Puesto que la tipología de incidentes varía a medida que las tecnologías evolucionan, los procedimientos avanzan en pro de estas.

En primer lugar es preciso distinguir entre:

- Evento: cambio de estado de “algo” dentro de la infraestructura TIC, que es significativo. También se puede denominar notificación o alerta.
- Evento de seguridad: se trata de un evento que genera una notificación a raíz de la violación de una política o directiva de seguridad implementada.
- Incidente de seguridad: es un evento o una serie de eventos de seguridad no deseados o no previstos que pueden poner en riesgo a los sistemas de la organización y a la información que almacenan o contienen.

Por lo tanto, identificamos tres tipos de eventos que presumiblemente derivarán en tres tipo de gestión o de escalado. No obstante, antes de proceder a dicha cuestión, será necesario categorizar el tipo de incidente que variará en función de los sistemas que afecte, la criticidad de los mismos, la información que puede comprometer, etc. De hecho, para la clasificación de incidentes, existe una taxonomía común muy interesante que se puede consultar en la [página del CERT de INCIBE](#).

Una vez clasificado el incidente y su nivel de criticidad, se procederá a escalarlo a dónde el procedimiento indique. Por ejemplo, considerando la información y el equipo del punto anterior, los incidentes de tipo bajo, medio y alto, serán resueltos por el nivel 1, mientras que los incidentes de tipo muy alto y crítico, serán resueltos por nivel 2.

Tras esta acción, comenzará la fase de procesado del incidente que podría incluir las fases de seguimiento y cierre. Hay que mencionar que el cierre de un incidente, no significa que este se haya resuelto favorablemente. Pongamos como ejemplo un ataque de ransomware para el que no hay herramienta de descifrado y donde la empresa afectada no dispone de copia de seguridad. En ese supuesto se cerraría el incidente sin haberse solucionado el problema y el acceder al pago del atacante, no sería parte de la solución.

Para finalizar, en el proceso de gestión de incidentes, es necesario obtener indicadores acerca del servicio para redimensionarlo, para reducir su tiempo de respuesta o para mejorar el servicio.

## Debes conocer

Para obtener más información acerca de la gestión de incidentes, puedes consultar [la guía de INCIBE](#).

# Condiciones y términos de uso de los materiales

Materiales desarrollados inicialmente por el Ministerio de Educación, Cultura y Deporte y actualizados por el profesorado de la Junta de Andalucía bajo licencia Creative Commons BY-NC-SA.



MINISTERIO  
DE EDUCACIÓN  
Y FORMACIÓN PROFESIONAL



Antes de cualquier uso leer detenidamente el siguiente [Aviso legal](#)

## Historial de actualizaciones

Versión: 01.00.00

Fecha de actualización: 28/06/23

Versión inicial de los materiales.