

# Introducción al Bastionado.

## Caso práctico

La empresa “Venus SA”, dedicada a la cirugía estética y con sede en Ibiza. El grado de dependencia tecnológica es bajo ya que la mayor parte de la información que gestionan como los historiales de los pacientes se encuentran en formato físico. La empresa cuenta con 10 empleados distribuidos de la siguiente manera:

- ✓ Un CEO.
- ✓ Un empleado del departamento de RR.HH..
- ✓ Cinco doctores en cirugía estética.
- ✓ Dos empleados encargados de la limpieza y saneamiento de la clínica.
- ✓ Un recepcionista.



[Direct Media](#) (Dominio público)

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.

Para esta unidad, el alumno ha de buscar información acerca del nuevo paradigma denominado “Zero Trust” e identificar modelos y servicios entre los diferentes proveedores que lo soporten y describir las características más representativas de dicho modelo.

Para la resolución del ejercicio, además deberá describir o interpretar cómo se pueden implementar dicho servicio e indicar cuáles son las ventajas e inconvenientes con respecto a modelos de bastionado anteriores o “clásicos”.

# 1.- Orígenes.

## Caso práctico

En la empresa de Juan han empezado a tener problemas desde hace poco tiempo con caídas del servicio, comportamientos sospechosos del sistema, el sistema funciona más lento,...La gota que ha colmado el vaso es que el mes pasado varios ordenadores quedaron inoperativos a causa de un " ransomware". Por suerte había copia de seguridad del mes pasado para algunos equipos afectados, y otros se configuraron de nuevo. Pero la red no mejora al nivel de operatividad esperado.



[Persona gritando ante el error en su portátil \(CC0\)](#)

Para tener un mayor control sobre el sistema se han empezado a revisar la configuración de los dispositivos de red, equipos y servidores para saber qué opciones de configuración segura existen y poder aplicarlas para tener un mayor control sobre la seguridad y disminuir los riesgos. Ya que están empezando a crecer el número de incidentes y el impacto que tienen sobre la empresa.

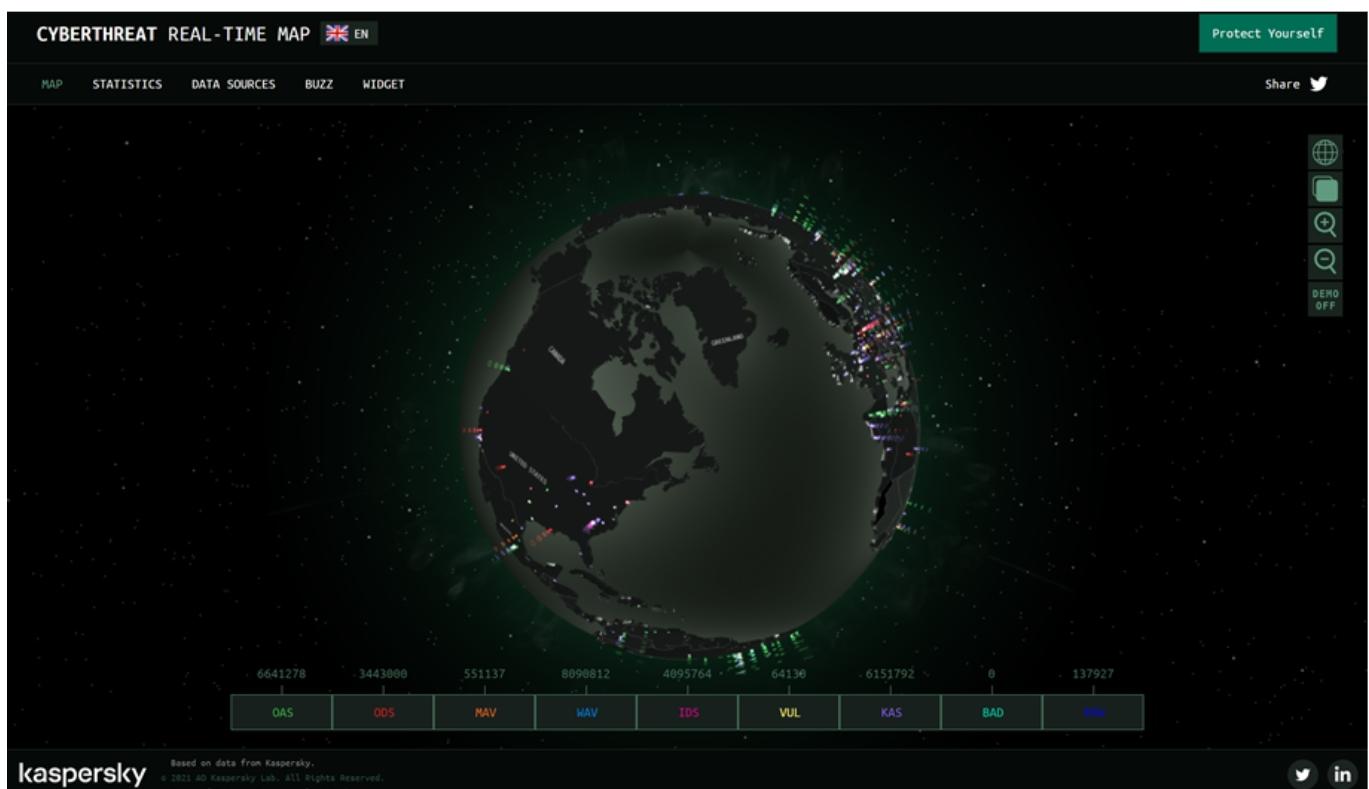
A lo largo de las últimas cinco décadas la informática ha experimentado prácticamente la totalidad de la evolución que conocemos hasta nuestros días. Desde sus orígenes en los que las cuestiones de seguridad eran inexistentes hasta nuestros días en los que mantener los sistemas protegidos se ha convertido en todo un reto. ¿Quién diría a los [creadores del correo electrónico](#) es uno de los servicios más utilizados tras la expansión de Internet. Y que este sería el vector de acceso más utilizado por los ciberdelincuentes? Esto es algo que ocurre en la actualidad con la mayor parte de servicios y sobre todo, con las arquitecturas que los soportan. No debemos olvidar que cuando alguien crea un servicio web, este estará gestionado y proporcionado por una serie de tecnologías que van desde el propio Sistema operativo, así como las infraestructuras de red necesarias para servirlo.



[freepik.com](https://www.freepik.com) (Dominio público)

Durante las décadas de los 70 y 80, apenas existía la preocupación por las amenazas que fueran más allá de las físicas. A pesar de que comenzaban a popularizarse los ordenadores, los problemas derivados del  malware, por ejemplo, no eran ni por asomo tan populares como lo son hoy, aunque si buscamos en la hemeroteca, Podemos encontrar algún que otro hecho reseñable como el Famoso [gusano de Morris](#), creado por el hijo de quien diseñaría uno de los primeros virus de la historia, [Creeper](#). Una parte muy interesante derivada del incidente del gusano, fue que a partir de ahí se creó el primer CERT (Computer Emergency Response Team) con el propósito de contener amenazas similares que pudieran aparecer en el futuro. Comentaremos en otro punto qué son y para qué sirve un [CERT](#) o también denominados [CSIRT](#) (Computer Security Information Response Team).

A partir de finales de los años 80 y con otros riesgos en el horizonte como la externalización de servicios o la expansión de internet, las posibilidades de que un incidente se materializara en un sistema o en una red, crecían de manera exponencial. Ahora los problemas no eran únicamente físicos, la parte lógica cobraba gran importancia y era necesario proteger los sistemas y las redes. Aparecen los primeros servicios de asistencia en ciberseguridad, por aquel entonces, “seguridad informática”. A partir de la década del 2000 la cosa podemos decir que empieza a “descontrolarse”. Se crean numerosos servicios de carácter colaborativo, las redes comienzan a estar más integradas, se inventan los smartphones, aparece el paradigma del cloud, y un largo etc. que con independencia de evolucionar hacia un sistema más competitivo gracias a las ventajas de la digitalización, y derivado de la gran exposición a la que las organizaciones y usuarios se ven expuestos, también se convierte en un estupendo frente de batalla para la lucha contra el cibercrimen y otros problemas de ciberseguridad.



[Kaspersky](#) (Dominio público)

## **1.1.- Necesidad.**

---

### **Necesidad**

Tras la pequeña introducción del punto previo, huelga decir por qué es necesario llevar a cabo labores o tareas de bastionado de sistemas y redes. En primer lugar, por la necesidad de mantener las famosas 3 dimensiones de la seguridad de la información: confidencialidad, integridad y disponibilidad; y en segundo, porque existen, aunque no a nivel global, numerosos requerimientos legales que precisan de la protección de las infraestructuras tecnológicas que almacenan la información, como por ejemplo los datos de carácter personal. El [Reglamento General de Protección de Datos](#), en su parte técnica (considerando 83) indica que para el tratamiento de los datos de carácter personal se utilizarán mecanismos de cifrado que doten de mayor seguridad. En segundo lugar, por todas las amenazas a las que están sujetos tanto los servicios como las tecnologías. En este sentido estamos hablando de los siguientes:

**Malware** (popularmente conocido como virus), o software malicioso cuyos subtipos más populares serían:

- Ransomware: Malware capaz de secuestrar nuestro dispositivo mediante el cifrado de los archivos principalmente. Se solicita un secuestro para volver a la actividad normal. Más información sobre [ransomware](#).
- Spyware: o programa espía, son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas para luego enviarla a través de Internet. Se pueden catalogar en dos tipos. El primero y más peligroso, aquel que recopila información, mensajes, datos, contraseñas, etc. de cualquier dispositivo para enviarla a algún atacante que lo controla remotamente. El segundo más inocuo, aquel que envía información sobre nuestros hábitos de navegación y similar y que generalmente lo manda a alguna empresa de publicidad. El primero de los tipos fue muy popular en el año 2022 por el escándalo asociado al software [Pegasus](#) que espió a varios miembros del Gobierno de España.
- Troyanos: es una pieza de software dañino disfrazado de software legítimo. Este malware no es capaz de replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software.
- Gusanos (worms): similares a los virus, pero no dependen de archivos portadores para poder contaminar otros sistemas. Pueden modificar el sistema operativo con el fin de auto ejecutarse como parte del proceso de inicialización del sistema.
- Bots: son programas que a través de órdenes enviadas desde otra computadora controlan el equipo personal de la víctima, es decir convirtiéndola en un "Zombi". Forman redes de ordenadores "Zombis" llamadas BotNets que pueden ser usadas para propósitos como realizar ataques de denegación de servicio distribuída (DDoS), robo de credenciales, envío de SPAM, etc.
- Keylogger: que una vez infectado el equipo, roba información registrando las pulsaciones del teclado o clics de ratón, para robar todo tipo de información.
- Rootkit: programas que son insertados en una computadora después de que algún atacante ha ganado el control de un sistema. Los rootkit generalmente incluyen funciones para ocultar los rastros del ataque, como es borrar los log de entradas o encubrir los procesos del atacante.
- Fileless malware: en este caso el atacante se aprovecha de funcionalidad del sistema operativo para llevar a cabo la infección. Por ejemplo mediante scripts programados para interpretarse con la herramienta PowerShell de Windows, se podría llevar a cabo un ataque de estas características.



[protegermpc.net](http://protegermpc.net) (CC0)

**Vulnerabilidades:** podemos definir este concepto como “*un fallo en el código o en la configuración de un software o en el diseño e implementación de un sistema hardware o físico, que permite a un atacante comprometer la seguridad del activo y hacer que muestre y realice funciones anti productivas y para el que no está autorizado*”. Es importante destacar que **no es lo mismo una amenaza que una vulnerabilidad**, más tarde entraremos en dicha distinción. En este sentido, se podría decir que todo el software es susceptible de contener o de adolecer de fallos de seguridad. Si bien es cierto, no todas las aplicaciones y servicios están bajo los ojos de los investigadores o de los ciberdelincuentes. Habitualmente las aplicaciones, sistemas operativos o tecnologías más usadas o populares, son las más escrutadas por el impacto que la explotación de un fallo tendrían sobre estas. Por ejemplo, Windows tiene más vulnerabilidades reportadas que Debian. En cualquier caso, y por fortuna, los fabricantes suelen publicar periódicamente actualizaciones de seguridad o parches para corregir las vulnerabilidades. Volviendo al caso de Microsoft, cada segundo martes de mes realizan la publicación, pero en caso de vulnerabilidad grave, lo harían fuera de dicho ciclo. También encontramos en este grupo, cuestiones relativas a configuraciones incorrectas, el uso de credenciales por defecto y otras cuestiones que trataremos a lo largo de este módulo.



[truedataconsultores \(CC0\)](#)

**Fraude:** sin duda uno de los problemas más recurrentes. En esencia porque la motivación de los ciberdelincuentes es básicamente la económica. Evidencia de esto, es que en los balances de ciberseguridad de INCIBE tanto del [2020](#) como del [2021](#), se encuentra en el “top 3” de los incidentes gestionados. Los fraudes pueden llegar de varias maneras y pueden poner en compromiso sistemas y arquitecturas ya que dentro de este tipo de incidente, también se contemplan las suplantaciones de correo electrónico o web también conocidas como phishing.

**Insiders:** se trata de una amenaza que aunque no reciente, en la actualidad se ha puesto gran interés en mitigar. Básicamente se trata de un ataque generalmente interno, llevado a cabo por un empleado o alguien dentro o con acceso a los sistemas de la organización que, con un propósito trata de realizar alguna acción que podría perjudicarla como el robo de información, la deshabilitación de servicios, etc. para evitar estos riesgos, en el módulo referenciaremos sistemas de protección como por ejemplo los sistemas para evitar la pérdida o robo de información ([DLP -Data Loss Prevention-](#)) entre otros.

**Ataques externos:** que podrían ser intencionados o no. Algunos que entrarían dentro de esta tipología podrían ser los escaneos indiscriminados con herramientas de enumeración como [NMAP](#) ; la identificación de vulnerabilidades con herramientas como [Nessus](#) o [Acunetix](#), etc

Aunque no es tema principal de este módulo ni de esta unidad, si se desea obtener más información acerca de los diferentes tipos de incidentes, se puede consultar la [Taxonomía de Referencia](#) definida en la [Guía Nacional de Notificación y Gestión de Ciberincidentes](#).

En el siguiente punto, entraremos en mayor detalle de a qué se refiere el concepto de bastionado o también denominado “Hardening”.



## Autoevaluación

¿Cuál de lo siguiente no es un motivo para implementar bastionado o configuración segura?

- Por normativa legal
- La seguridad es un requisito indispensable del sistema
- RGPD
- Los técnicos lo consideran necesario

## 2.- Bastionado o "Hardening".



### Caso práctico

El aumento de número de dispositivos y de interconexiones que tienen los sistemas, ha hecho que sea difícil confiar en los sistemas de nuestros proveedores con los que trabajamos habitualmente o con partes propias del sistema, pero que se encuentran albergados en servicios en la nube. Por lo que hay que enfocarlos como si fueran sistemas no confiables. Porque como dicen un refrán "dónde hay confianza da asco" haciendo referencia a que la confianza hay que renovarla para que no se convierta en un abuso y en un problema. En la seguridad pasa lo mismo es necesario renovar esa confianza hasta con los elementos que forman parte del nuestro círculo, como sucede en el modelo Zero Trust.



[Guillermo Colons \(CC0\)](#)

Indica los requisitos de seguridad que le pondrías a la conexión de un proveedor que te envía datos de tus pedidos

Requisitos

Este concepto se refiere a todo lo que tiene que ver con la protección de los activos que soportan los sistemas de información, es decir, dotar de las defensas necesarias a los sistemas y redes para evitar que las amenazas que les afectan, se puedan materializar. También es posible que encontremos este término en referencia a los propios usuarios. En este caso se trataría de dotar de las capacidades a los mismos para que sean capaces de identificar amenazas, reportar incidentes, etc.

Es en este punto donde hemos de diferenciar los conceptos de amenaza y vulnerabilidad. El primero hace referencia a algo que podría representar un daño potencial sobre un activo, mientras que el segundo, es un estado o condición que tiene el activo y que podría hacer que el daño se materializara. Trasladándolo a un ejemplo, en un sistema Windows con el servicio de escritorio remoto habilitado, tendríamos la potencial amenaza de que un atacante que conozca la IP, podría llevar a cabo intentos de conexión para intentar acceder. Una vulnerabilidad en este sentido, sería que el servicio utilizara credenciales por defecto o credenciales poco robustas donde un ataque de fuerza bruta podría tener éxito.



<https://nodenet.es/> (CC0)

Es en un contexto de este tipo donde el concepto de bastionado cobra todo el sentido. De manera somera, podemos referirnos al bastionado de un sistema o de una red como “el proceso que se lleva a cabo para reducir o mitigar las vulnerabilidades a través de políticas, medidas técnicas de seguridad, o cualquier otro mecanismo que lo consiga”. Algunos modelos propugnan que limitar las funciones de un sistema a una única función, proporcionan más seguridad que aquellos que disponen de multitud de servicios. El propósito del bastionado, es conseguir lo que también se denomina “defensa en profundidad” (DiD – Defense in Depth), término originariamente del ámbito militar y que ha evolucionado para integrarse en el mundo de las tecnologías de la información (TI).

De manera inicial, algunas de las características que contempla el bastionado pasarían por:

- Eliminación de cuentas innecesarias.
- Eliminación de contraseñas por defecto.
- Instalación de tecnologías de seguridad como firewalls, WAFs (Web Application Firewalls, etc.)
- Implementar política de actualizaciones para mantener los sistemas seguros.
- Deshabilitación de puertos y servicios que no se usen y elevar la seguridad al máximo de los que sí se utilizan.
- Desarrollar planes de contingencia que incluyan políticas de copia de seguridad y recuperación de sistemas.
- Elevar la seguridad en redes inalámbricas y usarlas únicamente si es necesario.

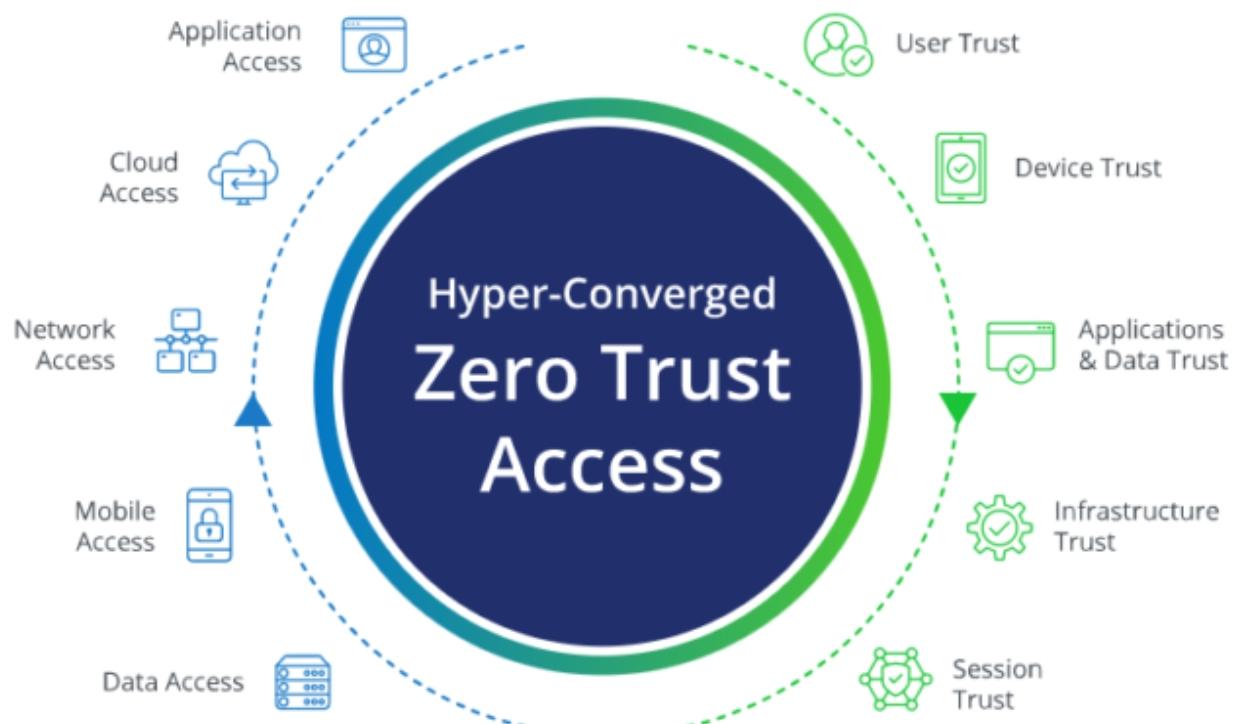
Estas cuestiones y otras, las veremos a lo largo de las unidades de este módulo.

## **2.1.- Zero trust.**

---

Un nuevo paradigma que se está extendiendo que se podría considerar la evolución del “mínimo privilegio”, es lo que se conoce como “Zero Trust Security”. A grandes rasgos, este nuevo modelo representa un nuevo modo de proteger la información. En algunas referencias encontramos que esto pasaría por disponer de una red interna confiable y una red externa no confiable. ¿Por qué surgió todo esto? Esencialmente porque con la implementación de la movilidad de muchos empleados, y más derivado de la pandemia, el perímetro de seguridad de las compañías se extendía más allá de sus firewalls, VPNs y otras tecnologías que bajo las directivas y políticas de la compañía, eran entonces suficientes. Si a esto le sumamos la existencia de las infraestructuras híbridas (on premise y Cloud) y la “iotización” (del IoT - Internet of Things-), el perímetro se vuelve aún más “incontrolable”, cuestión conocida por los cibercriminales y que en muchos casos han sabido aprovechar para sacar tajada de sus víctimas. ¿En qué se traduce esto? Básicamente en que por defecto, no se ha de confiar incluso en los usuarios confiables. Algunas de las cuestiones que aborda este paradigma y que veremos en el módulo con mayor detalle:

- Doble factor de autenticación ( 2FA) o multifactor de autenticación ( MFA): minimizando el posible compromiso de la barrera clásica formada por usuario/contraseña.
- Control del flujo de red entre los activos.
- Acceso discrección a aplicaciones frente a la red completa.
- Acceso por parte de los usuarios con mínimos privilegios.
- Mejora de las estrategias existentes en ciberseguridad con mecanismos avanzados de detección de amenazas incluidas vulnerabilidades “zero day”.
- Implementación de VPNs transparentes para el usuario



## **2.2.- ¿Por dónde empiezo?.**

---

Aunque suene a respuesta típica, antes de comenzar a implementar acciones que permitan reforzar la seguridad de una organización, es necesario llevar a cabo un análisis de riesgos. Esta tarea nos dará la información necesaria para identificar dónde tenemos que poner atención para conseguir elevar el nivel de ciberseguridad de aquellos procesos más importantes para la organización o empresa. Un principio que no debemos olvidar en este punto, es que la ciberseguridad se ha de alinear con el negocio, nunca se debe priorizar las medidas de seguridad frente a la operativa o la actividad de la empresa. La ciberseguridad ha de acompañar a la estrategia de la organización. Teniendo esto claro, existen numerosas metodologías, normas y estándares para llevar a cabo esta tarea, pero una cosa está clara, “si no sé dónde me encuentro, difícilmente voy a poder mejorar”.



### **Herramienta de autodiagnóstico de INCIBE**

De manera básica y para aproximarnos a esta actividad, podríamos utilizar la [herramienta de autodiagnóstico de INCIBE](#). Se trata de una herramienta muy sencilla que considera tres elementos: personas, procesos y tecnologías sobre cinco aspectos que la mayor parte de organizaciones tiene como una página web, el trabajo en movilidad, servidores propios, correo electrónico y posibilidad de teletrabajar.

Dependencia tecnológica

Reiniciar

¿Qué tecnologías utiliza en su empresa?

Tecnología sí pero con seguridad  
Seleccione las tecnologías que utiliza en su negocio o aquellas para las que quiera calcular el riesgo.

Correo electrónico  
Página web  
Servidor(es) propio(s)  
Teletrabajo  
Dispositivos móviles (tablet / smartphone / portátiles) con información de empresa

INCIBE (CC0)

Mediante las respuestas a las preguntas del cuestionario interactivo, iremos conociendo el apetito de riesgo que tiene la organización en relación a los tres elementos mencionados anteriormente. Al finalizar el análisis, obtendremos ayuda para saber cómo reducir el nivel de riesgo en relación a las personas, los procesos o las tecnologías.

### Resumen del diagnóstico

Aún no considera que la seguridad de la información es importante para su empresa o bien cree que la información no es muy esencial para su actividad.

- Analice y clasifique la información que maneja en su empresa (facturas, bases de datos de clientes, contratos, etc.) en función de su confidencialidad, integridad y disponibilidad. Consulte la sección de [Protección de la información](#).
- Revise si la información que maneja está sujeta al RGPD y si en su web tiene que cumplir con la LSSI según el apartado de [Cumplimiento Legal](#).
- Considere empezar a formar a supreg\_99\_1s empleados, como indica el apartado de [Desarrollar una cultura de seguridad](#).

Ahora que ya conoce el nivel de riesgo de su empresa, ¿quiere conocer el estado de seguridad de sus datos? Puede hacerlo con la [herramienta FACILITA](#) de la Agencia Española de Protección de Datos.

¿Qué le ha parecido la Herramienta de Autodiagnóstico? Su opinión nos importa, ayúdenos a mejorarlo completando la siguiente [Encuesta de Valoración](#)

El resultado de la encuesta concluye que el riesgo en su empresa es:

! 68.8%

Este porcentaje está considerado como  
RIESGO ALTO

Niveles de riesgo

Personas	70.6%	Riesgo ALTO	<input type="checkbox"/> ¿Quiere reducirlo?
Procesos	67.0%	Riesgo ALTO	<input type="checkbox"/> ¿Quiere reducirlo?
Tecnología	68.8%	Riesgo ALTO	<input type="checkbox"/> ¿Quiere reducirlo?

Comparta esta herramienta en las redes sociales

Permita que sus contactos y amigos evalúen los riesgos de seguridad de su negocio en tan solo cinco minutos.

Pulse para descargar el resultado en PDF



Volver a la página principal

INCIBE (CC0)



## Autoevaluación

Para aplicar seguridad a un sistema por dónde empiezo.

- Configurando los firewall
- Análisis de riesgos
- Tener el presupuesto de los equipos que protegen el sistema.

### **3.- Plan director de seguridad.**



#### **Caso práctico**

Todos han quedado encantados en el departamento de tecnologías cuando se ha implementado un nivel de seguridad aceptable en el nuevo sistema que han instalado y es mejor que otros que sistemas que no tienen ninguna medida de protección relativa a la seguridad. Se han quitado un peso de encima, por fin nos hemos librado de esa actividad de cuidar la seguridad.



[INCIBE](#) (Dominio público)

Hemos de determinar un plan de gestión de Seguridad de la información para que la seguridad del sistema siga manteniendo su nivel de seguridad o aumente, pero que nunca decaiga. Hay muchos marcos de referencia. Investiga sobre ellos.

**Dame un Plan**

#### **Plan director de seguridad**

Un plan director de seguridad es un conjunto de actividades direccionalas a elevar el nivel de ciberseguridad. Las acciones que se han de llevar a cabo tienen el propósito de reducir los riesgos a los que se pueda exponer una organización. Esta reducción se considerará adecuada cuando tras los análisis, se consideren que los riesgos se han minimizado hasta un nivel aceptable. Como se ha mencionado previamente, cualquier proyecto de ciberseguridad ha de estar alineado con el negocio de la organización y nunca discurrir por un camino fuera de la estrategia. **La ciberseguridad apoya al negocio.**

Un plan director, ha de incluir tanto **medidas técnicas como medidas organizativas** en su ejecución y como otros planes, tiene que contener una definición y alcance concreto que permita incrementar la seguridad en los **procesos considerados como críticos de la organización**. Uno de los errores más comunes es diseñar planes que no son realistas, esto son aquellos que tratan de abarcar cuestiones que no son críticas o que implementan soluciones sobredimensionadas.

No existe una manera única de llevar a cabo o implementar un plan director, de hecho, variará en función de varias características de la organización donde se desee implementar como por ejemplo la dependencia tecnológica, el sector al que pertenece la organización o la criticidad de la información que se maneje, entre otros. Por ejemplo, no tendrán los mismos requerimientos una empresa dedicada a cuestiones agrícolas que una que ofrece servicios tecnológicos.

Los planes directores de seguridad, así como la certificación en estándares que veremos a continuación, se basan en lo que se denominan, **ciclos de mejora continua**. Esto supone que tras la implementación, el ciclo continua para iterar de nuevo, pues las tecnologías, la situación de las empresas y otros factores, cambian a lo largo del tiempo.



# 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.



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE EDUCACIÓN  
Y FORMACIÓN PROFESIONAL



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

## Historial de actualizaciones

Versión: 01.00.01

Fecha de actualización: 02/10/23

Actualización de materiales y correcciones menores.

Versión: 01.00.00

Fecha de actualización: 28/06/23

Versión inicial de los materiales.