GUÍA DE CIBERSEGURIDAD

Ciberseguridad para empresas.

PREVENSYSTEM®

info@iprevensystem.com | www.prevensystem.com

Edición mayo 2022

PREVENSYSTEM®

“LÍDERES EN SOLUCIONES PARA EL CUMPLIMIENTO”

Somos una compañía especializada en el diseño y desarrollo de soluciones para el cumplimiento legal.

“LÍDERES EN SOLUCIONES PARA EL CUMPLIMIENTO”, es el concepto que mejor define la filosofía y los valores de nuestra entidad, capaz de diseñar las soluciones más vanguardistas y eficaces para nuestra clientela.

Operamos con presencia directa en más de 16 países con una red internacional de más de 80 oficinas que prestan servicio a más de 20.000 organizaciones clientes en todo el mundo.

Misión

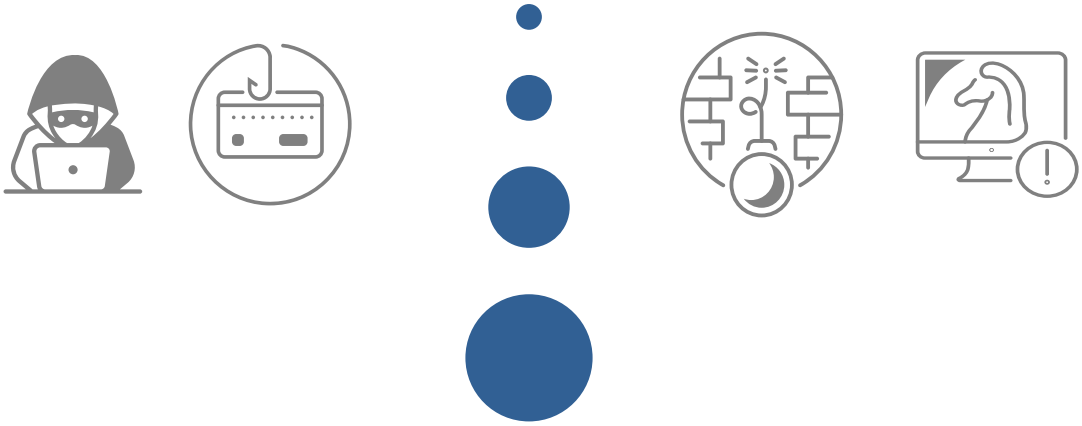
Ser la entidad más vanguardista y avanzada en el asesoramiento a empresas y organizaciones en el cumplimiento de la normativa de aplicación.
Todo ello en beneficio de nuestros clientes, de sus personas trabajadoras y de la sociedad en general.

Estrategia

Nuestra máxima es ser líderes en la innovación especializada de sistemas de gestión para el cumplimiento normativo, mediante la combinación de experiencia técnica, vanguardia tecnológica y el máximo nivel de cercanía para asistir a nuestros clientes.

Compromisos

Nos cuestionamos las bases del sistema actual de trabajo desde su origen, con el fin de construir desde los cimientos, los procedimientos y herramientas de trabajo más avanzados e innovadores.



Guía de Ciberseguridad PREVENSYSTEM

La información es el activo más importante de una organización

¡¡APRENDAMOS A PROTEGERLA!!

Las personas trabajadoras de una organización son la primera línea de defensa contra las ciberamenazas, resulta imprescindible que dispongan de los conocimientos y habilidades necesarios para proteger a la organización de incidentes que comprometan la seguridad de su información.

"El 94% de las empresas ha sufrido al menos un incidente grave de ciberseguridad a lo largo de 2021"

* Deloitte: El estado de la ciberseguridad en España

"El 95% de los incidentes de ciberseguridad son producidos por un error humano"

* Fuente: World Economic Forum – The Global Risk Report 2022

"Junto al cambio climático y la desigualdad social, la ciberseguridad es uno de los principales desafíos que enfrenta la humanidad"

* Fuente: World Economic Forum – The Global Risk Report 2022

"Los incidentes de ciberseguridad son el riesgo de negocio más importante para 2022 por delante de las pandemias, el cambio climático o los desastres naturales"

* Fuente: Allianz – Barómetro de riesgos 2022

Fuerza bruta

Consiste en adivinar nuestra contraseña mediante ensayo y error. Se comienza probando diferentes combinaciones con nuestros datos personales (conocidos por otras fuentes) y se continúa haciendo combinaciones de palabras al azar, conjugando nombres, letras y números, hasta que se identifica el patrón correcto.

Ataque por diccionario

Se utiliza un software para averiguar nuestra contraseña de manera automática. Este software realiza diferentes comprobaciones, empezando con letras simples como "a", "AA" o "AAA" y, progresivamente, va generando combinaciones más complejas.

Objetivos.

El objetivo es acceder a la información almacenada en nuestras cuentas. En función de que sea el correo electrónico, con el que obtener datos personales y contactos, una red social, con la que poder suplantar nuestra identidad, o datos bancarios con los que llevar a cabo transferencias o realizar compras sin nuestro consentimiento.

¿Qué tenemos que hacer?

01| Utilizar contraseñas robustas

02| No utilizar la misma contraseña para diferentes servicios

03| No utilizar información personal a modo de contraseña (ej. fecha de nacimiento,...)

04| No apuntar las contraseñas en notas o archivos sin cifrar

05| No guardar las contraseñas en webs o navegadores

06| Utilizar gestores de contraseñas

¿Cuánto tiempo tarda un software automático en averiguar nuestra CONTRASEÑA en función de la longitud y de los tipos de caracteres utilizados?

Longitud	Combinación de todos los tipos de caracteres	Sólo letras minúsculas
3 caracteres	0,86 segundos	0,02 segundos
4 caracteres	1,36 minutos	0,46 segundos
5 caracteres	2,15 horas	11,9 segundos
6 caracteres	8,51 días	5,15 minutos
7 caracteres	2,21 años	2,23 horas
8 caracteres	2,10 siglos	2,42 días
9 caracteres	20 milenios	2,07 meses
10 caracteres	1.899 milenios	4,48 años
11 caracteres	180.365 milenios	1,16 siglos
12 caracteres	17.184.705 milenios	3,03 milenios
13 caracteres	1.627.797.068 milenios	78,7 milenios
14 caracteres	154.640.721.434 milenios	2.046 milenios

Una contraseña
ROBUSTA.

Longitud mínima de **8** caracteres.

Mayúsculas:
A, U, P, T, M, …..

Minúsculas:
y, g, s, o, u, …..

Números:
3, 8, 9, 4, 7, …..

Símbolos:
], /, :, =, +, &, ……

Password
m@r25Z0#70

El DOBLE FACTOR DE AUTENTICACIÓN (o múltiple) es una capa adicional de seguridad que complementa el uso de las contraseñas. Su objetivo es asegurarse de que el/la usuario/a no solo conoce la contraseña para acceder al servicio, sino que además es quien dice ser aportando otra información en el proceso.

Un ejemplo SENCILLO.

01| Accedemos a la pantalla de inicio de sesión del servicio.

02| Insertamos nuestro usuario y contraseña (algo que conocemos).

03| Se nos pide confirmación de autenticación por medio de un código que recibimos, por ejemplo, a través de nuestro smartphone (algo que tenemos).

04| Y finalmente, también pueden pedirnos un tercer factor a través de un dispositivo biométrico, por ejemplo, nuestra huella dactilar (algo que somos).

Los ataques por ingeniería social se basan en un conjunto de técnicas dirigidas a los/as usuarios/as, con el objetivo de conseguir que revelemos información personal o de permitir al atacante tomar control de nuestros dispositivos (frecuentemente se utiliza como paso previo a un ataque por malware).

Phishing, Vishing y Smishing

Se envía un mensaje suplantando a una entidad legítima, por ejemplo un banco, una red social, un servicio técnico o una entidad pública, con la que nos sintamos vinculados, para lograr su objetivo. Estos mensajes suelen ser de carácter urgente o atractivo, evitando que se aplique el sentido común y nos lo pensemos dos veces.

Pueden incluir enlace a una web fraudulenta fingiendo ser un enlace legítimo, o bien se trata de un archivo adjunto malicioso para infectarnos con malware.

Dirigido a una persona en concreto se conoce como Spear phishing, recabando información previa sobre ella para maximizar las probabilidades de éxito.

Objetivos.

El objetivo es acceder a la información almacenada en nuestras cuentas. En función de que sea el correo electrónico, con el que obtener datos personales y contactos, una red social, con la que poder suplantar nuestra identidad, o datos bancarios con los que llevar a cabo transferencias o realizar compras sin nuestro consentimiento.

¿Qué tenemos que hacer?

01| Debemos ser precavidos y leer el mensaje detenidamente, especialmente si se trata de entidades con peticiones urgentes, promociones o chollos demasiado atractivos.

02| Detectar errores gramaticales en el mensaje.

03| Revisar que el enlace coincide con la dirección a la que apunta. En cualquier caso, debemos ingresar la url nosotros directamente en el navegador, sin copiar y pegar.

04| Comprobar el remitente del mensaje, o asegurarnos de que se trata de un teléfono legítimo.

05| No descargar ningún archivo adjunto y analizarlo previamente con el antivirus.

06| En caso de vishing, no debemos descargar ningún archivo que nos haya solicitado el atacante, ni ceder el control de nuestro equipo por medio de ningún software de control remoto.

07| No contestar nunca al mensaje y eliminarlo.

Phishing.

Correo electrónico, RRSS, mensajería instantánea,...

Vishing.

Llamadas telefónicas.

Smishing.

SMS.

¿CORREO SOSPECHOSO?

01| Asunto
¿Llamativo para captar tu atención?

02| Remitente
¿Esperabas un correo de esta persona/entidad y coincide la dirección?

03| Objetivos
Un banco nunca te pedirá datos por correo

04| Redacción
¿Contiene errores ortográficos o parece una mala traducción de otro idioma?

05| Enlaces
¿Es una página legítima y segura (https://)? Sitúa el cursor encima del enlace y podrás ver la URL real a la que te redirige.

06| Adjuntos
¿Contiene archivos adjuntos sospechosos?

Baiting o Gancho

El Baiting se sirve de un medio físico y de nuestra curiosidad. Utilizando un cebo, los/as atacantes consiguen que infectemos nuestros equipos o compartamos información personal.

El medio más utilizado son los dispositivos USB infectados que los/as atacantes colocan en sitios estratégicos, como lugares públicos con mucha afluencia de personas o en la entrada de las empresas.

Objetivos.

Conseguir que los/as usuarios/as conectemos estos dispositivos infectados en nuestros equipos para ejecutar malware con el que robar nuestros datos personales y/o tomar control del equipo, infectar la red y llegar al resto de dispositivos.

¿Qué tenemos que hacer?

La mejor defensa para este tipo de ataques es evitar conectar dispositivos desconocidos de almacenamiento externo o con conexión USB a nuestros equipos. Además, debemos mantener nuestro sistema actualizado y las herramientas de protección, como el antivirus, activadas y actualizadas.

Como en todos los ataques por ingeniería social, debemos desconfiar de cualquier promoción demasiado atractiva o de promesas de webs poco fiables.

Shoulder surfing

El/la ciberdelincuente consigue información mirando "por encima del hombro" desde una posición cercana, mientras que utilizamos los dispositivos sin darnos cuenta.

Es habitual que se de en lugares públicos, como cafeterías o centros comerciales, y en transportes, mientras utilizamos nuestro equipo, o en cajeros automáticos.

Objetivos.

El objetivo es, como en otros ataques por ingeniería social, el robo de información: documentos confidenciales, credenciales, contactos, códigos de desbloqueo, etc.

¿Qué tenemos que hacer?

01| La opción más segura es evitar que terceros tengan visión de nuestra actividad y, en sitios públicos, eludir compartir información personal o acceder a nuestras cuentas. También se recomienda utilizar gestores de contraseñas y la verificación en dos pasos para añadir una capa extra de seguridad a las credenciales.

02| Finalmente, debemos cerciorarnos de que no hay terceras personas observando nuestro dispositivo, especialmente a la hora de ingresar datos personales. Podemos utilizar medidas físicas, como los filtros "anti-espía". Se trata de una lámina fina que podemos colocar sobre la pantalla de nuestro dispositivo para evitar que terceros puedan ver su contenido desde distintos ángulos.

Dumpster Diving

Se conoce como "buscar en nuestra basura" para obtener información útil sobre nosotros/as o nuestra empresa que después pueda utilizarse para otro tipo de ataques.

Objetivos.

El objetivo son documentos, anotaciones y demás información que hayamos tirado a la papelera por descuido (claves de acceso, contactos,...).

También buscan dispositivos electrónicos desechados a los que acceder y extraer toda la información que no haya sido borrada correctamente.

¿Qué tenemos que hacer?

La única medida de protección que debemos seguir es la eliminación segura de información. Desde una trituradora de papel para el formato físico, hasta seguir los pasos para la eliminación segura de información digital:

01| **Formatear o resetear** a valores de fábrica para que los datos sensibles que puedan estar fuera de nuestro conocimiento se borren por completo (recuerda hacer **copia de seguridad** de tus datos antes de restaurar o formatear el dispositivo).

02| **Borrar la información de los navegadores** (favoritos, cookies, historial, credenciales autoguardadas,...) (Ccleaner, ...), incluyendo el caso de utilizar un terminal público.

03| **Eliminar las cuentas de los servicios** que pueden ser consultadas por terceros si no se han desactivado antes.

04| En el caso de equipos de sobremesa no es suficiente con formatear, debemos recurrir a **herramientas de borrado seguro** (Eraser, ...).

Spam

Consiste en el envío de grandes cantidades de mensajes o envíos publicitarios a través de Internet sin haber sido solicitados, es decir, se trata de mensajes no deseados (email, mensajería instantánea, RRSS, ...). La mayoría tienen una finalidad comercial, aunque los puede haber que contengan algún tipo de malware.

Objetivos.

Los objetivos pueden ir desde el envío masivo de mensajes publicitarios, hasta maximizar las opciones de éxito de un ataque de tipo phishing a una gran población, o tratar de infectar el mayor número posible de equipos mediante malware.

¿Qué tenemos que hacer?

Se recomienda no utilizar la cuenta de correo electrónico principal para registrarnos en ofertas o promociones, además de configurar el filtro antiSpam para evitar la recepción de este tipo de mensajes e ignorar y eliminar los mismos.

01| No publicar la dirección de correo en foros, blogs o páginas web, evitando que se recopile al rastrear una web. Si tenemos que hacerlo, publicar así: nombredeusuario[espacio]arroba[espacio]dominio[punto]com.

02| No reenviar cadenas de emails o utilizar listas de correos con las direcciones de los destinatarios a la vista. Si reenvías un correo, hazlo siempre con Copia Oculta (CCO).

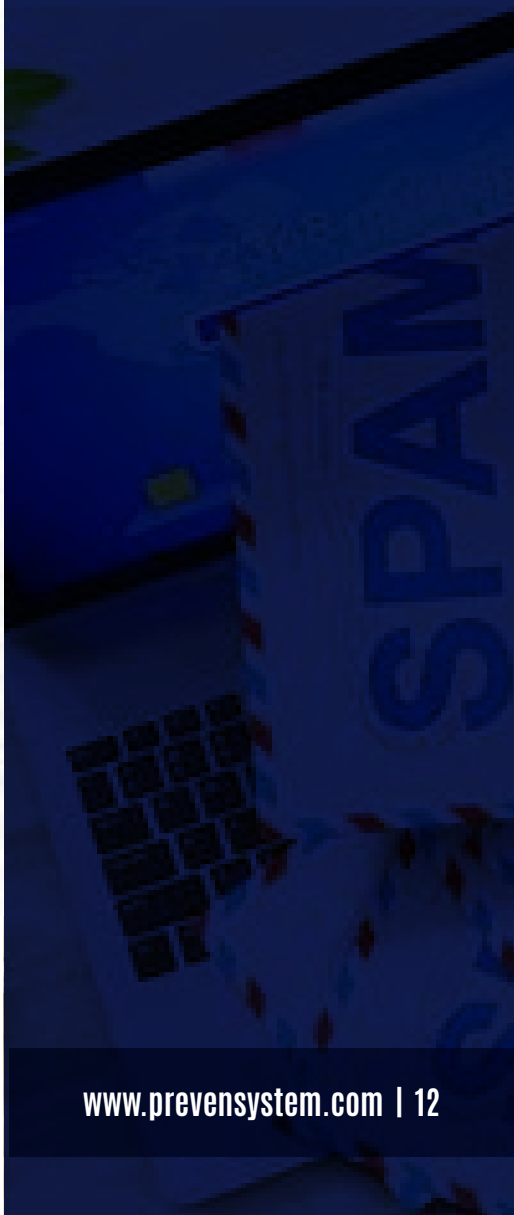
03| No intentar dar de baja del correo basura, se usa para detectar si la cuenta está activa, y seguir enviando.

04| Usar una dirección de correo alternativa para registrarse en foros o blogs.

05| Al registrar en un servicio, infórmate del tratamiento que realiza de tus datos (¿compartir con terceros?).

06| No descargar archivos adjuntos de remitentes desconocidos, si es conocido analizar con antivirus.

07| Mantener actualizado el sistema operativo, el software y apps que utilicemos así como el antivirus.



Son ataques muy comunes, los/as ciberdelincuentes se sirven de diversas herramientas con las que saltarse las medidas de seguridad e infectar o tomar control de nuestros dispositivos. Generalmente, este tipo de ataques consisten en interponerse en el intercambio de información entre nosotros/as y el servicio web, para monitorizar y robar datos personales, bancarios, contraseñas, etc.

Redes trampa

La creación de redes wifi falsas es una práctica muy utilizada por los/as ciberdelincuentes, creando una red wifi gemela a otra legítima y segura, con un nombre igual o muy similar a la original. Después, se configura con los mismos parámetros que la original, esperando la conexión a esta segunda red. Este mecanismo es generalmente utilizado en lugares con red wifi pública, con gran afluencia de usuarios/as.

Objetivos.

El objetivo es conseguir robar nuestros datos cuando accedemos a nuestra cuenta bancaria, redes sociales o correo electrónico, pensando que estamos llevando a cabo una conexión segura. Se puede llegar a tomar control sobre nuestra navegación, accediendo a webs fraudulentas similares a la original y preparadas para el engaño o para la infección por malware.

Redes trampa

¿Qué tenemos que hacer?

Aprender a identificar redes wifi falsas:

01| Dos redes con nombres iguales o muy similares o, por ejemplo, que añadan la palabra "gratis".

02| Si las webs a las que accedes tras conectarte solo utilizan el protocolo http, detén tu actividad y desconéctate.

03| Es probable que estas redes sean abiertas o permitan cualquier contraseña.

04| Desconectar la función de conectarse automáticamente a redes abiertas.

05| Nunca utilizar este tipo de redes cuando vamos a intercambiar información sensible, como nuestros datos bancarios. En caso de necesidad, podemos recurrir a una VPN.

Una Red Privada Virtual es un servicio mediante el cual nuestro equipo se conecta a otro que hace de intermediario (servidor VPN) entre nosotros/as y los servicios y páginas web de Internet a los que accedemos.

La conexión entre nuestro equipo y el servidor VPN siempre está cifrada por lo que si alguien interceptara nuestras comunicaciones, sería incapaz de leer la información.

Las Redes Privadas Virtuales, dividen la conexión en dos partes o zonas, la primera va desde nuestro equipo hasta el servidor VPN y la segunda desde el servidor VPN hasta el servidor o servicio al que nos vamos a conectar.

Spoofing

Consiste en el empleo de técnicas de hacking de forma maliciosa para suplantar nuestra identidad, la de una web o una entidad. El objetivo es disponer de un acceso a nuestros datos. Como protección, es fundamental que nos mantengamos alerta y sigamos las recomendaciones para una navegación segura.

1. IP Spoofing

El/la ciberdelincuente consigue falsear su dirección IP y hacerla pasar por una dirección distinta. De este modo, consigue saltarse las restricciones del router del servidor o del nuestro y, por ejemplo, hacernos llegar un paquete con malware.

Objetivos.

Robar las credenciales o los datos que intercambiemos con dicho servicio web falso. Generalmente, se utilizan para hacerse con nuestras credenciales al tratar de ingresarlos en la web falsa.

¿Qué tenemos que hacer?

Al ser un ataque que suele llegar en forma de enlace se debe revisar con mucho cuidado la URL para identificar diferencias con la original. También debemos desconfiar de webs sin https ni certificados digitales y, en caso de tenerlo, comprobar que se trata de la web que dice ser.

Spoofing

2. Web Spoofing

Consiste en la suplantación de una página web real por otra falsa. La web falsa es una copia del diseño de la original, llegando incluso a utilizar una URL muy similar. El/la atacante trata de hacernos creer que la web falsa es la original. El/la atacante se sirve de otro tipo de ataques, como la ingeniería social o anuncios maliciosos, para intentar que accedamos al enlace de la web falsa pensando que se trata de la página web legítima.

Objetivos.

Robar las credenciales o los datos que intercambiemos con dicho servicio web falso. Generalmente, se utilizan para hacerse con nuestras credenciales al tratar de ingresarlos en la web falsa.

¿Qué tenemos que hacer?

Al ser un ataque que suele llegar en forma de enlace se debe revisar con mucho cuidado la URL para identificar diferencias con la original. También debemos desconfiar de webs sin https ni certificados digitales y, en caso de tenerlo, comprobar que se trata de la web que dice ser.

Spoofing

2. Web Spoofing

Siempre que proporciones información privada a través de Internet como nombre, apellidos, DNI, tarjeta de crédito, etc. comprueba que la página envía la información utilizando el protocolo de comunicación seguro HTTPS.

Spoofing

3. Email Spoofing

Consiste en suplantar la dirección de correo de una persona o entidad de confianza. Suele ser utilizado para enviar de forma masiva correos de spam o cadenas de bulos u otros fraudes. Se ha podido obtener el email suplantado a partir de otro tipo de ataques, como ingeniería social. Es muy utilizado en otros ataques, como el phishing o el spam, para aumentar sus probabilidades de éxito.

Objetivos.

Conseguir información personal sirviéndose de la confianza que transmita la identidad suplantada o engañarnos para conseguir que descarguemos malware en nuestro equipo.

¿Qué tenemos que hacer?

Utilizar firma digital o cifrado a la hora de enviar emails nos permitirá autenticar los mensajes y prevenir suplantaciones. Si la organización con la que nos comunicamos dispone de firma digital, también será más sencillo identificar este tipo de ataques.

Finalmente, analizando el contenido como si de un phishing se tratase, bastará para identificar el engaño.

Spoofing

4. DNS Spoofing

A través de programas maliciosos específicos y aprovechando vulnerabilidades en las medidas de protección, los/as atacantes consiguen infectar y acceder a nuestro router. Así, cuando tratemos de acceder a una determinada web desde el navegador, este nos llevará a otra web elegida por el/la atacante. Para ello, los/as atacantes suplantan la DNS (domain name system), es decir, la tecnología utilizada para conocer la dirección IP del servidor donde está alojado el dominio al que queremos acceder.

Objetivos.

El objetivo del/de la atacante es modificar los DNS para redirigirnos cada vez que intentemos acceder a una página web, a una web fraudulenta preparada por el/la atacante.

¿Qué tenemos que hacer?

La mejor forma de prevenir este ataque es blindar la seguridad del router, restringiendo las conexiones remotas, cambiando las contraseñas por defecto, además de seguir las pautas para identificar webs fraudulentas.

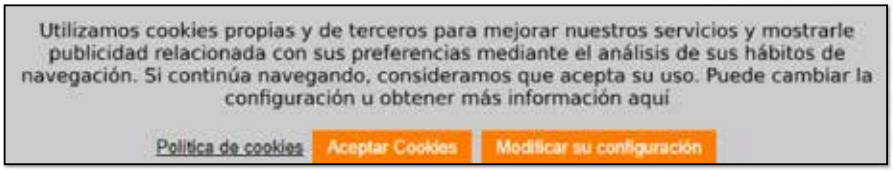
Ataques a Cookies

Las cookies son pequeños ficheros que contienen información de las páginas webs que hemos visitado, así como otros datos de navegación, como pueden ser los anuncios vistos, el idioma, la zona horaria, si hemos proporcionado una dirección de correo electrónico, etc. Su función es ayudarnos a navegar de forma más rápida, recordando esta información para no tener que volver a procesarla.

En paginas con protocolos http puede ser visible para los/as ciberdelincuentes el intercambio de cookies que se realiza entre el servidor de la web y nuestro equipo. Los ataques a las cookies consisten en el robo o modificación de la información almacenada en una cookie.

Objetivos.

El robo de identidad y credenciales, obtener información personal sin nuestra autorización o modificar datos.



Ataques a Cookies

¿Qué tenemos que hacer?

01| Configurar correctamente las cookies dentro de nuestro navegador.

02| Mantener actualizado el navegador, así como los complementos o plugins instalados, y siempre descargarlos desde sitios oficiales.

03| Eliminar cada cierto tiempo los datos de navegación, como cookies, historial y caché.

04| Revisar detenidamente las notificaciones o mensajes que aparezcan al acceder a una web antes de aceptarlos.

05| A la hora de intercambiar información sensible o datos confidenciales o muy personales, es mejor utilizar el modo incógnito.

06| No guardar contraseñas en el navegador y utilizar gestores de contraseñas.

Ataque DDoS

DDoS son las siglas en inglés de "ataque distribuido denegación de servicio" y consiste en atacar un servidor web al mismo tiempo desde muchos equipos diferentes para que deje de funcionar al no poder soportar tantas peticiones.

Objetivos.

Su objetivo es provocar la caída de la web. Las consecuencias son una pérdida de reputación, suspensión del servicio, así como pérdidas económicas, además de las consecuencias de una brecha en su seguridad, como el robo de datos. Los/as usuarios/as no pueden acceder al servicio al estar caído debido al ataque. También podemos ser cómplices del ataque sin saberlo si nuestros equipos han sido infectados para formar parte de una botnet, por ejemplo.

¿Qué tenemos que hacer?

Disponemos de diferentes servicios de protección de nuestro servicio web:

01| **Monitorización continua,** existen herramientas para analizar la actividad del sitio web y detectar posibles ataques DDoS antes de que se conviertan en un problema. El firewall puede ayudarnos a detectar posibles intrusos/as o una actividad fuera de lo normal.

02| **Proveedor fiable,** que nos ofrezca garantías, como un servicio de prevención o una infraestructura sólida para aguantar un intento de ataque.

03| **Actualizaciones** de seguridad nos protegerán de vulnerabilidades en el software.

04| **Conexión sólida** con buen ancho de banda que nos ayude a reducir los efectos de un ataque DDoS y a reponernos antes.

05| **Reducir la superficie afectada,** es útil limitar la infraestructura del servicio web que puede ser atacada, por ej. redirigiendo tráfico directo de Internet.

Inyección SQL

Las páginas webs suelen estar vinculadas a bases de datos, basadas en un lenguaje de programación conocido como SQL. Estos ataques permiten a los/as ciberdelincuentes insertar líneas de código SQL maliciosas en la propia aplicación web, obteniendo acceso parcial o completo a los datos, pudiendo ser monitorizados, modificados o robados por el/la atacante.

Objetivos.

Tener acceso a los datos sensibles recogidos en la base de datos del servicio o aplicación web para robarlos o destruirlos.

¿Qué tenemos que hacer?

Como usuarios/as, no podemos hacer mucho para prevenir este tipo de ataques, pues depende de la seguridad implantada por el servicio web. En el caso de los desarrolladores web, es fundamental que sigan las recomendaciones basadas en el diseño seguro y en el desarrollo de código seguro, que priorice la privacidad de las comunicaciones y la protección de nuestros datos.

Escaneo de puertos

El ataque de escaneo de puertos, o portscan, es el proceso en el que se analizan automáticamente los puertos de una máquina conectada a la red para identificar cuáles están abiertos, cerrados o cuentan con algún protocolo de seguridad.

Objetivos.

El objetivo suele ser el robo de nuestra información, como credenciales o datos bancarios, pero también ofrecen una entrada para controlar dispositivos conectados a una red.

¿Qué tenemos que hacer?

El router tiene el papel protagonista a la hora de proteger los sistemas de la mayoría de los ataques a las conexiones. Es fundamental configurarlo correctamente, controlar las conexiones entrantes y los dispositivos conectados por medio de un filtrado MAC, mantener el firewall activado y controlar los puertos que tenemos abiertos. Y siempre mantenerlo actualizado para protegerlo de posibles brechas de seguridad.

Man in the middle

Este tipo de ataque requiere que el atacante se sitúe entre nosotros/as y el servidor con el que nos estamos comunicando.

Son habituales en redes públicas o en redes wifi falsas localizadas en sitios públicos, como centros comerciales, aeropuertos u hoteles. El/la atacante consigue monitorizar la actividad online dentro de la red infectada.

Objetivos.

Interceptar, leer o manipular los datos intercambiados, como mensajes, credenciales, transferencias económicas, etc. Generalmente, el/la atacante monitoriza nuestra actividad online y registra la información que más le interese.

¿Qué tenemos que hacer?

01| NO CONECTARNOS A REDES PÚBLICAS (hoteles, centros comerciales, aeropuertos,...).

02| Mantener actualizados los dispositivos, programas y aplicaciones.

03| Utilizar contraseñas robustas y, si es posible, una capa extra de seguridad con verificación en dos pasos.

04| Navegar por páginas https y comprobar su certificado digital.

05| Usar aplicaciones con cifrado extremo a extremo, cifrar documentos y correos.

06| Utilizar VPN.

Sniffing

Se trata de una técnica utilizada para escuchar todo lo que ocurre dentro de una red. Los/as atacantes utilizan herramientas de hacking, conocidas como sniffers, para monitorizar el tráfico de una red.

Objetivos.

Mediante el uso de diferentes herramientas, los/as atacantes buscan capturar, interpretar y robar paquetes de datos lanzados por la red, para analizarlos y hacerse con nuestros datos.

¿Qué tenemos que hacer?

Existen herramientas de protección antimalware que pueden detectar y eliminar los sniffers instalados en un equipo, pero al no ser considerados como malware, no siempre son detectados y deben ser eliminados de forma manual.

Para evitarlo, se deben seguir todas las pautas para prevenir la descarga de software malicioso cuando navegamos por la red, como no descargar adjuntos sospechosos, no navegar por webs fraudulentas, evitar conectar dispositivos USB desconocidos, etc.

Los ataques por malware se sirven de programas maliciosos cuya función es llevar a cabo acciones dañinas en un sistema informático y contra nuestra privacidad.

Generalmente buscan robar información, causar daños en el equipo, obtener un beneficio económico a nuestra costa o tomar el control del equipo.

Existen diferentes tipos de malware, pero las medidas de protección son muy similares para todos ellos y se basan en mantener activas y actualizadas las herramientas de protección antimalware.

Troyanos

Suelen camuflarse como un software legítimo para infectar nuestro equipo, o a través de ataques de ingeniería social.

Objetivos.

La mayoría de troyanos tienen como objetivo controlar nuestro equipo, robar datos, introducir más software malicioso en el equipo y propagarse a otros dispositivos.

Acostumbran a propagarse por medio de archivos adjuntos en correos electrónicos o desde páginas webs poco fiables, escondiéndose tras descargas de juegos, películas o aplicaciones no legítimas.

No somos conscientes de que nuestros equipos han sido infectados hasta que es demasiado tarde.

Backdoors

Una vez instalado en el sistema, permitirá el/la ciberdelincuente tomar el control del equipo de forma remota. Suelen utilizarse para infectar a varios dispositivos y formar una red zombi o Botnet.

Keyloggers

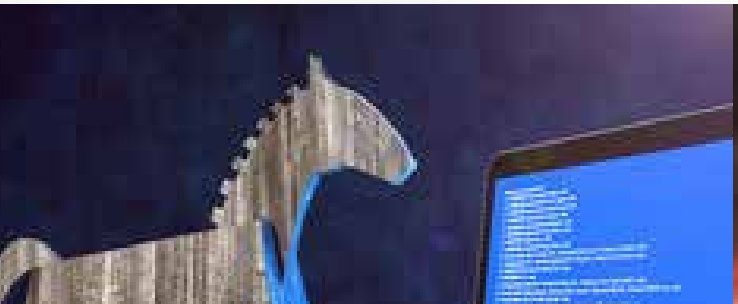
Los Keyloggers realizan un seguimiento y registran cada tecla que se pulsa en un equipo sin nuestro consentimiento. Pueden estar basados en un software o en un hardware, como por ejemplo un dispositivo USB.

Stealers

Este tipo de troyano accede a la información privada almacenada en el equipo. Al ejecutarse, analiza los programas instalados y las credenciales almacenadas para compartirlas con el/la atacante.

Ransomware

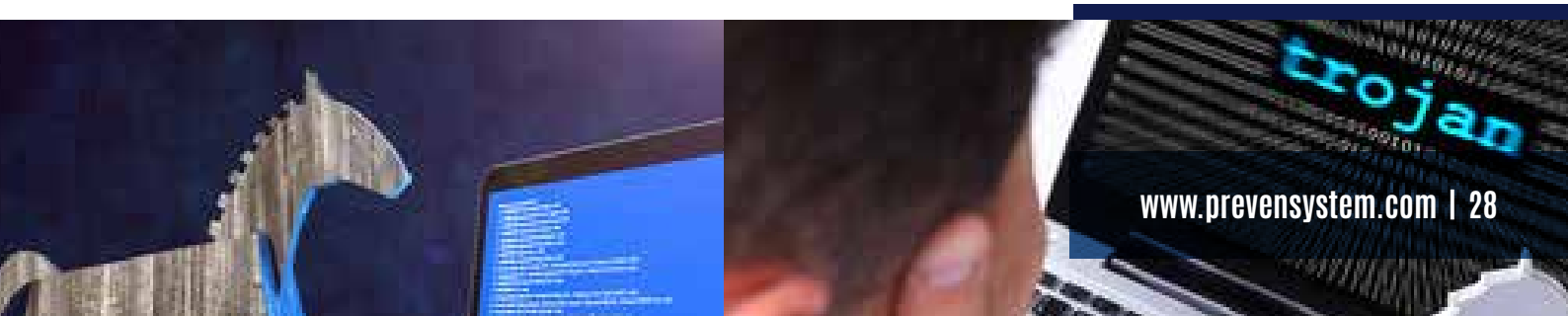
Malware que consigue tomar el control del dispositivo para cifrar el acceso al mismo y/o nuestros archivos o discos duros. A cambio de recuperar el control y la información, nos exigirá el pago de un rescate.



Troyanos

¿Qué tenemos que hacer?

Las medidas de protección son comunes con otro tipo de malware, como mantener el equipo actualizado y las medidas de protección activadas (antivirus). También evitar ejecutar archivos, links o utilizar dispositivos USB de dudosa procedencia.



Virus

Los virus se encuentran dentro de la categoría de malware y están diseñados para copiarse a sí mismos y propagarse a tantos dispositivos como les sea posible.

Proliferan infectando aplicaciones a través del correo electrónico u otros servicios web, y pueden transmitirse por medio de dispositivos extraíbles, como memorias USB, o archivos adjuntos e incluso a través de conexiones de red.

Objetivos.

Modificar o eliminar los archivos almacenados en un equipo. Son capaces de dañar un sistema, eliminando o corrompiendo datos esenciales para su correcto funcionamiento.

¿Qué tenemos que hacer?

01| Instalar un antivirus y un cortafuegos y mantenerlos actualizados.

02| Mantener el equipo constantemente actualizado.

03| No ejecutar nunca un programa o seguir un enlace que llegue por correo y parezca extraño.

04| No ejecutar ficheros de dudoso origen.

05| No conectar al equipo un USB cuya procedencia no conocemos.

06| Utilizar el sentido común, siendo precavidos ante cualquier cosa que parezca sospechosa.

Adware

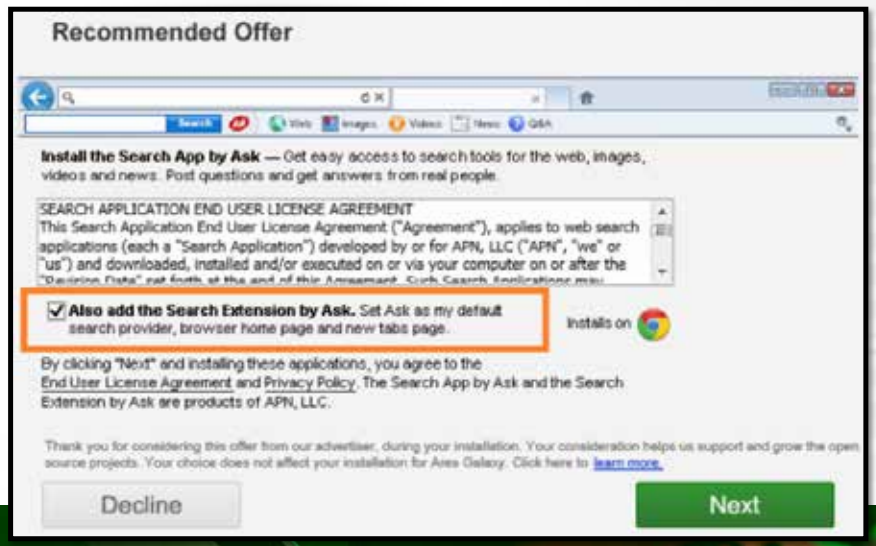
Se trata de un software malicioso diseñado para mostrarnos anuncios no deseados de forma masiva. Suelen instalarse junto a otros programas legítimos que aceptamos e instalamos sin percatarnos.

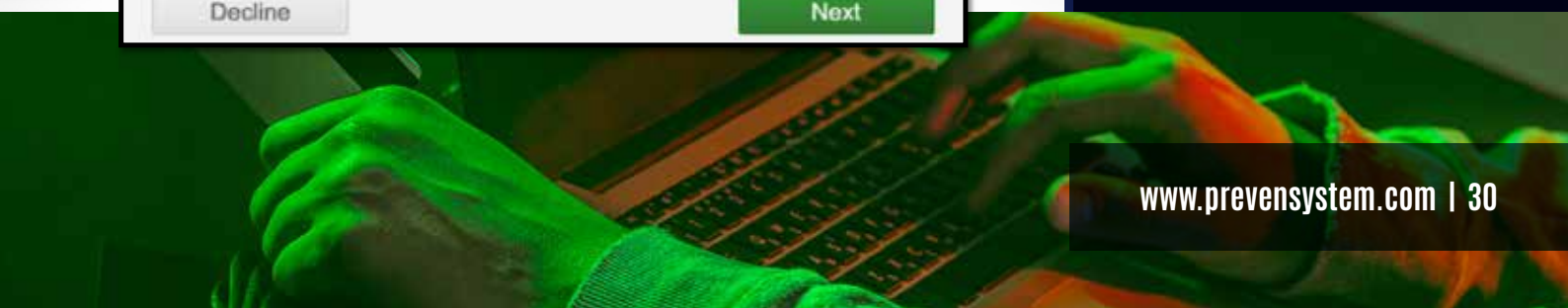
Objetivos.

Su objetivo es recopilar información sobre nuestra actividad para mostrarnos anuncios dirigidos. Supone molestia e incordio y su instalación puede suponer una bajada de rendimiento y un mal funcionamiento del dispositivo. También acostumbran a servir de enlace a sitios web maliciosos.

¿Qué tenemos que hacer?

Como protección, es fundamental evitar la descarga de aplicaciones de sitios no oficiales o software pirata. Se debe prestar atención a los pasos de la instalación para evitar seleccionar casillas con las que instalar programas adicionales.





Spyware

Este malware se instala en nuestros equipos y comienza a recopilar información, supervisando toda la actividad para luego compartirlo con un usuario remoto. También es capaz de descargar otros malware e instalarlos en el equipo.

Al navegar por páginas webs no seguras, pueden aparecer mensajes en forma de anuncios o pop-ups que, al hacer clic, descargan este tipo de malware. También es común que se ejecuten como programas adicionales durante la instalación de un software.

Objetivos.

Una vez que el malware se instala en el dispositivo, puede llevar a cabo numerosas acciones, como controlar el dispositivo de forma remota, realizar capturas del contenido de aplicaciones y servicios como el correo electrónico o redes sociales. También es capaz de registrar y capturar el historial de navegación y llevar a cabo grabaciones utilizando la cámara o el micrófono.

¿Qué tenemos que hacer?

Descargar software desde el sitio oficial y prestar atención durante el proceso de instalación es fundamental. Además, es recomendable ignorar los anuncios y ventanas emergentes que aparezcan durante la navegación, y no hacer clic en archivos o enlaces que provengan de un sitio poco fiable. Finalmente, mantener el sistema y las herramientas de protección siempre activas y actualizadas minimizará los riesgos.

Gusano

Es un tipo de malware que, una vez ejecutado en un sistema, puede modificar el código o las características de este. Suelen pasar inadvertidos hasta que su proceso de reproducción se hace evidente, afectando al rendimiento de nuestro equipo.

Generalmente se propaga a través de archivos adjuntos, redes de intercambio de archivos y enlaces a sitios web maliciosos. También pueden infectar otros dispositivos al conectar dispositivos USB infectados con el gusano.

Objetivos.

El objetivo es replicarse e infectar otros dispositivos. La propagación de este tipo de malware ocasiona un consumo de los recursos del sistema infectado que puede traducirse en una disminución del rendimiento o una peor conexión al estar consumiendo parte de nuestro ancho de banda.

¿Qué tenemos que hacer?

Las medidas de protección son comunes a otro tipo de ataques por malware. Se basan en mantener activos y actualizados los programas de protección, como el antivirus y el firewall, así como mantener nuestro sistema actualizado para evitar vulnerabilidades. Se recomienda evitar la descargar de archivos maliciosos y navegar por sitios webs fraudulentos.

Botnets

Red compuesta por diversos dispositivos infectados y controlados de forma remota por uno/a o varios/as ciberdelincuentes.

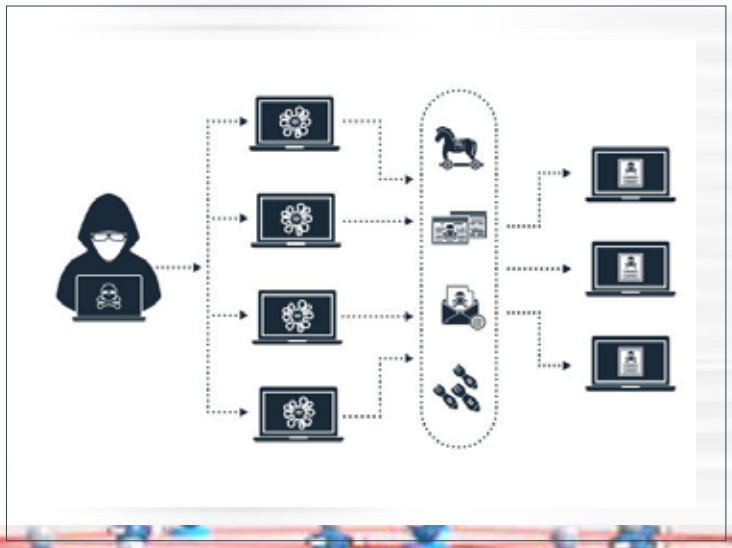
Para infectar un equipo, los/as atacantes suelen recurrir a códigos maliciosos en páginas webs tras explotar una vulnerabilidad o al envío de archivos maliciosos a través de correo electrónico. Una vez que accedemos, nuestro equipo queda infectado sin ser conscientes de ello.

Objetivos.

El/la atacante busca controlar el mayor número de dispositivos posible con los que llevar a cabo sus actividades ilícitas con mayor probabilidad de éxito.

¿Qué tenemos que hacer?

Mantener activos y actualizados los programas de protección, como el antivirus y el firewall, así como mantener nuestro sistema actualizado para evitar vulnerabilidades. Es recomendable evitar la descarga de archivos maliciosos y la utilización de contraseñas robustas.



Rogueware

Es un software malicioso que simula ser un antivirus o herramienta de seguridad y alerta sobre la presencia de un malware, una amenaza o un problema en nuestro dispositivo que hay que corregir. A continuación, nos invitará a hacer clic en un enlace para descargar un supuesto software con el que solucionar el problema.

Se propaga a través de archivos maliciosos que podríamos haber descargado a través de Internet, por ejemplo, al navegar por sitios webs poco fiables.

Objetivos.

El objetivo del/de la atacante es conseguir que hagamos clic en los enlaces que aparecen en las supuestas alertas de seguridad. Una vez hacemos clic, se descargará algún tipo de malware, o accederemos a una página web maliciosa.

¿Qué tenemos que hacer?

Dado que el/la atacante requiere que hagamos clic en sus alertas, la mejor protección es aplicar el sentido común y confiar solo en las herramientas de seguridad legítimas. También es importante que el sistema y las herramientas de protección se encuentren debidamente actualizadas.

Criptojacking

Los/as ciberdelincuentes utilizan nuestros dispositivos sin consentimiento para llevar a cabo "extracciones" de criptomonedas, utilizando los recursos del sistema durante el proceso.

Un equipo puede infectarse al descargar este malware a través de un archivo malicioso o a través de páginas webs maliciosas que utilizan el ancho de banda de nuestra conexión para llevar a cabo los procesos de extracción.

Objetivos.

El interés no está en acceder a nuestros datos personales, sino en utilizar nuestros recursos para el minado de criptomonedas y obtener un beneficio económico. La principal amenaza reside en el consumo de recursos que puede paralizar otros procesos e impedirnos utilizar el equipo con normalidad, incrementando además las facturas de luz y reduciendo la vida útil del dispositivo.

¿Qué tenemos que hacer?

Instalación y actualización de un antivirus, así como llevar a cabo inspecciones regulares en busca de malware. Es recomendable evitar la descarga de archivos maliciosos y la conexión a redes wifi públicas o a páginas webs poco fiables. Finalmente, existen diversos complementos para el navegador que actúan como bloqueadores de scripts de Criptojacking.

Las criptomonedas son un tipo de dinero digital que existe solo en el mundo digital, sin una forma física. Se crearon como una alternativa al dinero tradicional y se hicieron populares por su diseño avanzado, su potencial de crecimiento y su anonimato.

Todas las criptomonedas existen como unidades monetarias descentralizadas y cifradas que pueden transferirse libremente entre los participantes de la red.

El proceso de minería consiste en convertir los recursos informáticos en coins de criptomoneda, resolviendo independientemente los complejos rompecabezas matemáticos de encriptación que demuestran la legitimidad de la transacción para su registro en el libro de contabilidad digital público descentralizado.

El cryptojacking surge cuando en lugar de pagar un ordenador caro dedicado a la minería, los hackers empezaron a infectar ordenadores normales y a utilizarlos como una red a su antojo.

Apps maliciosas

Las Apps maliciosas se hacen pasar por aplicaciones legítimas o tratan de emular a otras aplicaciones de éxito. Una vez instaladas en el dispositivo, nos pedirán una serie de permisos abusivos o, por el contrario, harán un uso fraudulento de dichos permisos.

Suelen estar disponibles para su descarga fuera de las tiendas oficiales de aplicaciones, aunque en ocasiones pueden saltarse los filtros de seguridad de estos sitios oficiales.

Objetivos.

El objetivo de una App maliciosa es aprovecharse de los permisos concedidos para el robo de información y la toma de control del dispositivo. Las consecuencias dependerán del tipo de permiso que se conceda a la App. Pueden ir desde una reducción en el rendimiento del dispositivo o el robo de datos hasta la toma de control por parte del/de la atacante debido a la concesión de permisos.

¿Qué tenemos que hacer?

Como protección, lo primero si se sospecha de la instalación de una App maliciosa es desinstalarla del dispositivo. Para prevenir consecuencias más graves, es conveniente cifrar el dispositivo, así como hacer copias de seguridad de la información almacenada. Finalmente, es imprescindible descargar aplicaciones de los sitios oficiales, como Google Play o la App Store.

DECÁLOGO BÁSICO DE CIBERSEGURIDAD.

01 **Utilizar un antivirus** para analizar todas las descargas y archivos sospechosos y mantenerlo siempre activo y actualizado.

02 **Mantener el sistema operativo, navegador y aplicaciones siempre actualizados** en su última versión para evitar vulnerabilidades.

03 **Utilizar contraseñas robustas y diferentes** para proteger todas las cuentas. Si es posible, utilizar la verificación en dos pasos u otro factor de autenticación.

04 **Desconfiar de los adjuntos sospechosos, enlaces o promociones demasiado atractivas.** La mayoría de los fraudes se basan en ataques de ingeniería social que pueden ser detectados aplicando el sentido común.

05 **Tener cuidado por dónde se navega.** Utilizar solo webs seguras con https y certificado digital y utilizar el modo incógnito cuando no se quiera dejar rastro.

06 **Descargar solo de sitios oficiales** aplicaciones o software legítimo para evitar la infección por malware. En el caso de las aplicaciones, dar solo los permisos imprescindibles para su funcionamiento.

07 **Evitar la conexión a redes wifi públicas o a conexiones inalámbricas desconocidas,** especialmente cuando se vaya a intercambiar información sensible como los datos bancarios. Y, en caso de tener que conectarse por una emergencia, tratar de utilizar una VPN.

08 **No compartir información personal** con desconocidos ni publicarla o guardarla en páginas o servicios web no fiables.

09 **Hacer copias de seguridad** para minimizar el impacto de un posible ciberataque.

10 La **CULTURA DE CIBERSEGURIDAD** y la concienciación de las personas trabajadoras debe ser el pilar fundamental sobre el que se apoye la ciberseguridad de cualquier organización.

SEGURIDAD EN LA INFORMACION

FORMACIÓN

- Curso Universitario de Especialización en Sistemas de Gestión de la Seguridad de la Información. ISO 27001
- Auditor Interno en Sistemas de Gestión de la Seguridad de la Información ISO 27001:2013
- Auditor Líder/jefe en Sistemas de Gestión de la Seguridad de la Información. ISO 27001
- Sistemas de Gestión de la Seguridad de la Información. ISO 27001
- Experto en Sistemas de Gestión de la Seguridad de la Información. ISO 27001
- Auditor Interno en Sistemas de Gestión de la Continuidad de Negocio. ISO 22301:2019
- Sistemas de Gestión de la Continuidad de Negocio. Requisitos ISO 22301:2019
- Experto en Ciberseguridad
- Delegado de Protección de Datos - DPO (100 horas)
- Delegado de Protección de Datos - DPO (60 horas)
- Protección a la información de las personas físicas. LOPDGDD 2019
- Auditor Interno en Sistemas de Gestión del Servicio ISO/IEC 20000-1:2018
- Sistemas de Gestión del Servicio. Requisitos ISO 20000-1
- Sistemas de Gestión de Información de Privacidad (PIMS). Requisitos ISO 27701:2019
- Esquema Nacional de Seguridad

CONSULTORÍA

- Delegado de protección de datos (DPD)
- Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- Esquema Nacional de Seguridad (ENS)

GUÍA DE CIBERSEGURIDAD

Ciberseguridad para empresas.

PREVENSYSTEM®

info@iprevensystem.com | www.prevensystem.com

Edición mayo 2022