

TITULARES

Lo que la ciberseguridad corporativa puede aprender del fútbol

La ciberseguridad y el fútbol comparten más similitudes de las que podríamos imaginar. Los equipos de fútbol deben planificar sus partidos dependiendo del rival y del juego. Lo mismo ocurre con las empresas, que viven en un contexto de ciberataques cada vez más complejos.

[Pág. 2](#)**Razones por las que hacer copias de seguridad en casa**

Las copias de seguridad son una forma de proteger la información que guardas en tu ordenador, móvil o tablet. Consiste en hacer una copia de los archivos más importantes y guardarlos en otro lugar, como puede ser un disco duro externo o un servicio de almacenamiento en la nube (servicio cloud).

[Pág. 3](#)**Sistemas de verificación de edad**

La AEPD (Agencia Española Protección Datos) dispone de un sistema de verificación de edad para proteger a los menores de edad ante el acceso a contenidos de adultos en Internet.

[Pág. 4](#)**Compras seguras en Black Friday y Cyber Monday**

Se acercan dos días muy esperados para quienes quieren aprovechar grandes ofertas online.

El problema: ¡también son fechas señaladas para los ciberdelincuentes!

Como el Black Friday y el Cyber Monday están a la vuelta de la esquina, queremos compartirte cinco consejos para que tus compras online no acaben en un susto:

- Revisa las valoraciones de otros usuarios antes de comprar.
- Compra sólo en tiendas y plataformas oficiales o de confianza.
- Desconfía de ofertas demasiado buenas o urgentes: podrían ser un gancho.
- Verifica que la tienda online sea segura ("https" en la barra del navegador).
- Evita hacer pagos desde redes Wi-Fi públicas o compartidas.



Es preferible perder una oferta que precipitarse y ser víctima de un fraude. Ante todo, ¡compra con seguridad!

EI POST-IT**LA PELÍCULA****CONTRAPORTADA**

123456, la contraseña más usada



Atención: los ciberdelincuentes han desarrollado nuevas técnicas para robar dinero en cajeros sin tarjeta



"Hemos encontrado tu iPhone": la trampa para robar tus credenciales de Apple



Booking vuelve a ser un reclamo para el phishing



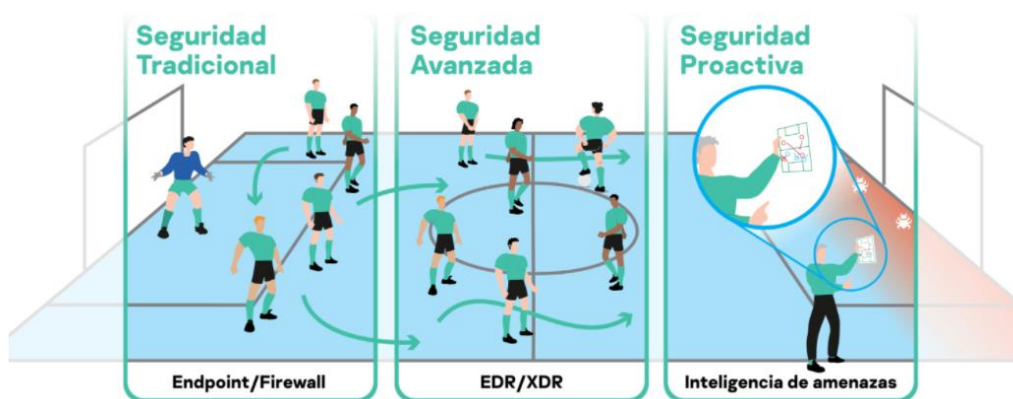
Comprueba si tu cuenta de correo está comprometida, <https://haveibeenpwned.com/>. Si es así, **cambia la contraseña**.

TITULARES

Lo que la ciberseguridad corporativa puede aprender del fútbol

Replegarse para adoptar una posición defensiva en fútbol puede tener inconvenientes. Lo mismo ocurre en entornos empresariales cuando se trata de ciberseguridad.

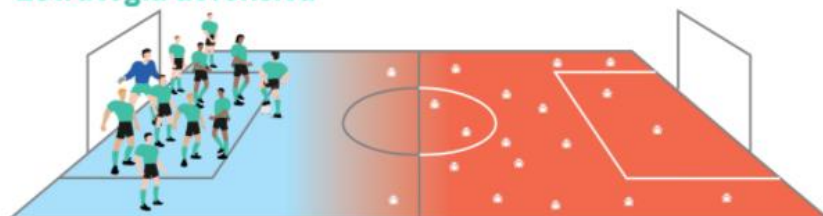
Otra similitud entre el fútbol y la ciberseguridad empresarial es la forma en la que cada equipo y compañía deciden “jugar”. Puedes jugar a presionar alto, o poner el “autobús” en tu portería y esperar que no te metan gol.



¿Encerrarse atrás es la mejor estrategia?

Aunque una postura defensiva pueda parecer una estrategia ideal, esa decisión puede dejar vulnerables tanto al equipo como a la empresa y no brinda el tiempo necesario para reaccionar ante una amenaza.

Estrategia defensiva



Puntos positivos:

- Sensación de seguridad
- Concentrarse en no perder

Puntos negativos:

- Los adversarios aprovechan los puntos débiles
- No hay tiempo para reaccionar ante un ataque
- Sólo puedes ver el ataque cuando está en el área de defensa (endpoint/firewall)

Una defensa proactiva

La primera línea de defensa de cualquier empresa será el famoso antivirus y el firewall -y aquí ya incluye la protección en entornos de nube y el EDR-. Todos son básicamente reactivos, ya que solo se activan cuando los ordenadores o servidores son atacados, y es solo en ese escenario donde se sabrá si funcionan bien o no.

Estrategia proactiva

Puntos positivos:

- Anticipa la identificación de los ataques
- Posibilidad de bloqueo en diferentes momentos (más protección)
- Puede ver el ataque desde su origen (a través de endpoint, red, accesos + datos de campo extras con Threat Intelligence)

Puntos negativos:

- 1. Requiere que la empresa tenga un equipo de seguridad interno o externo

Razones por las que hacer copias de seguridad en casa

5 Razones

por las que hacer copias de seguridad

COPIANDO 75%

Todos tenemos información que queremos **proteger, guardar y preservar en el tiempo**. Para ello, lo mejor es crear copias de seguridad.

1 Estás prevenido en caso de deterioro del dispositivo

El paso del tiempo y el uso constante del dispositivo pueden provocar que no funcione correctamente. Haz copias de seguridad para salvar la información más importante.

2 Proteges la información

Utilizamos muchos dispositivos y ninguno está exento de un robo, pérdida o infección por malware. En casos como estos, desearás disponer de una copia de seguridad.

3 La preservas en el tiempo

Para disponer de la información en el tiempo es recomendable generar copias de seguridad en diferentes soportes y que estos estén soportados por las tecnologías actuales. ¿Recuerdas cómo pasamos del VHS al CD/DVD? ¿Y del CD/DVD a los discos duros externos?

4 Liberas espacio

La información que almacenamos acaba por ocupar gran parte del espacio en disco de nuestros dispositivos. Realizar copias de seguridad ayudará a liberar espacio y mejorar su uso y rendimiento.

5 La proteges de ti mismo

¿Alguna vez has borrado algo por equivocación? Para evitar el susto, mejor contar con una capa extra de seguridad en forma de copia de seguridad.

DISCO EXTERNO (F:)

1,2 GB disponibles de 100 GB

¿ESTÁ SEGURO?
BORRAR TODO
ACEPTAR

No lo dejes para más adelante, haz copias de seguridad y evitarás disgustos en el futuro.

Elaborado por el SOC de la Junta de Andalucía

¡Síguenos en X: @CentroCiberAND!
Consulta las alertas de seguridad que publicamos en el SOC.

Junta de Andalucía

Agencia Digital de Andalucía

OSI Oficina de Seguridad del Internauta

Sistemas de verificación de edad

La AEPD propone diferentes métodos para verificar la edad en Internet, pero todos presentan riesgos que conviene conocer.

SISTEMAS DE VERIFICACIÓN DE EDAD



Autodeclaración de la edad ante el proveedor de contenidos



Compartición de credenciales o atributos con el proveedor de contenidos



Estimación de la edad realizada por el proveedor de contenidos



Entidades terceras como intermediarias entre la persona usuaria y el proveedor de contenidos



AMENAZAS

FALTA DE IDONEIDAD

No existe certidumbre acerca de la edad verificada.



IDENTIFICACIÓN

El proveedor podría llegar a inferir la identidad real de la persona usuaria.



NO REPUDIO/VINCULACIÓN DE ACTIVIDADES EN DIFERENTES SERVICIOS

La persona no puede negar su actividad en uno o varios servicios.



DETECCIÓN

Una entidad tercera (proveedor o no) puede localizar menores de edad.



REVELACION, APROPIACIÓN O TRANSFERENCIA

Se recopilan datos no necesarios, se realizan tratamientos o transferencias adicionales.



PÉRDIDA DE CONTROL

Falta de transparencia hacia la persona usuaria o de control por parte de los que ejercen la patria potestad para tomar decisiones informadas.



RIESGOS PARA LOS DERECHOS Y LIBERTADES



FALTA DE IDONEIDAD

Riesgos para el interés superior del menor (acceso de menores a contenido inadecuado: impactos en salud mental, desarrollo emocional, etc.) o riesgos para el derecho a la comunicación libre, a la libertad de información y de expresión en adultos (limitación de acceso a contenidos para adultos)

IDENTIFICACIÓN. NO REPUDIO. VINCULACIÓN

Riesgos para el derecho al honor y a la intimidad (prestigio, reputación), a la comunicación libre, a la libertad de información y de expresión (autocensura), libertad ideológica y derecho de a la participación (manipulación y propaganda), derecho a la seguridad y derecho al trabajo (estigmatización, discriminación)

DETECCIÓN

Riesgos para el interés superior del menor (derecho a seguridad)

REVELACIÓN, APROPIACIÓN, TRANSFERENCIA, PERDIDA DE CONTROL

Riesgos para los derechos asociados al RGPD (acceso, rectificación, etc.), riesgos para la libertad de quienes ejercen la patria potestad para tener decisiones informadas.

EL POST-IT

Acceso a equipamiento, aplicaciones y sistemas

[Código de conducta](#) en el uso de las tecnologías de la información y la comunicación para profesionales públicos de la administración de la Junta de Andalucía.



Se utilizarán los mecanismos de acceso implantados para el equipamiento, las aplicaciones y los sistemas.

Si sospechas que tus credenciales de acceso están siendo utilizadas por otra persona, procede inmediatamente a su cambio y notificar la incidencia de seguridad.



Custodiarás diligentemente tus credenciales de acceso, sin proceder a su revelación o puesta al alcance de terceros. Serás responsable de toda la actividad realizada con tus credenciales.

Nunca se intentará obtener, por medios ilícitos, derechos de acceso superiores a los que te correspondan, ni utilizar las credenciales de otras personas.



Cumple con las obligaciones de secreto y confidencialidad, y por supuesto con la normativa vigente en protección de datos.



El incumplimiento de estas medidas puede ocasionar serias brechas de seguridad, que deriven en sanciones administrativas, multas, inhabilitaciones y, en caso de daños graves, hasta penas de prisión. ¡Debemos ser muy cuidadosos en cuestiones de acceso y custodia de la información!

LA PELÍCULA



Pesadilla antes de Navidad

Se acercan las ofertas de Black Friday, Cyber Monday y Navidad, y es un hecho que cada vez compramos más por Internet. Para que tus compras no se conviertan en una "Pesadilla antes de Navidad", te dejamos unos consejos básicos para realizarlas de forma segura, extraídos de [esta completa guía de INCIBE](#).

 Compra en webs de confianza (reconocidas, seguras, con reputación, etc.).

Asegúrate que está identificado el responsable de la tienda y su ubicación.



 La web debe ofrecerte toda la información que necesitas sobre consumo y tratamiento de datos personales.

Te recomendamos usar tarjeta de pagos solo para Internet.



 Desconfía de las ofertas demasiado atractivas (smartphones a 10 euros, etc.).

Cuida tu dispositivo y tu conexión. Evita comprar usando redes wifi públicas, ya que puede haber otras personas monitorizando el tráfico de tus datos.



 Evita las transferencias y envíos de efectivo. Solo tarjeta.

Tienes como mínimo 14 días de garantía: puedes desistir de una compra o contrato sin tener que dar explicaciones en los 14 días posteriores.



Cómo evitar fraudes

El día que aprendí sobre compras seguras

¿Cuánto sabes sobre compras seguras online?



Oficina
de Seguridad
del Internauta

CONTRAPORTADA

123456, la contraseña más usada

Según un reciente estudio, elaborado sobre más de 2.000 millones de contraseñas filtradas en 2025, casi 7,6 millones de cuentas utilizaban la “clásica” 123456. Recuerda que para que una contraseña sea considerada segura debería tener al menos 12 caracteres, combinando mayúsculas, minúsculas, símbolos y números. [Más info aquí.](#)



Atención: los ciberdelincuentes han desarrollado nuevas técnicas para robar dinero en cajeros sin tarjeta

El uso del contactless en los cajeros automáticos podría no ser tan seguro como creen muchos clientes, un nuevo malware para móviles permite hackear la tecnología NFC para pagar o utilizar tarjetas de crédito en cajeros automáticos. [Más información.](#)



“Hemos encontrado tu iPhone”: la trampa para robar tus credenciales de Apple

El Centro Nacional de Ciberseguridad de Suiza alertó recientemente de una elaborada estafa de phishing, que intenta suplantar a Apple. A través de este timo, los ciberdelincuentes buscan hacerse con el Apple ID de usuarios que han perdido o a los que les han robado sus iPhone. [Te dejamos más info aquí.](#)



Booking vuelve a ser un reclamo para el phishing

La plataforma de reserva de hoteles y apartamentos turísticos lleva tiempo siendo un blanco para los ciberdelincuentes. Y con la llegada de la IA, estas amenazas se perfeccionan. Recientemente, se ha detectado una nueva campaña que explota cuentas comprometidas de hoteles, con el fin de estafar a los viajeros. [Más información.](#)



¿Has observado un comportamiento digital sospechoso? ¿Estás recibiendo intentos de phishing?
¿Has sufrido un incidente de seguridad? ¡Notifícalo de inmediato por correo o teléfono!

incidentes.soc@juntadeandalucia.es / 955 060 974 (Corporativo 360974)