BOLESTIC

Nº 10 febrero 2025

Boletín de concienciación en ciberseguridad

Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.

incidentes.soc@juntadeandalucia.es

TITULARES

La importancia de las actualizaciones de seguridad

Los sistemas operativos, navegadores web, programas y aplicaciones son susceptibles de tener fallos de seguridad. Por este motivo, pueden necesitar ser actualizados, independientemente del dispositivo en el que se encuentren instalados.

Pág. 2

¿Cuánto sabe de ti tu smartphone?

Este conocimiento deriva en una técnica utilizada para descubrir y difundir información personal de un individuo sin su consentimiento. Se utiliza a menudo con fines maliciosos, como acoso, amenazas, extorsión, y otros delitos cibernéticos.

Pág. 3

Escenarios de riesgo en el puesto de trabajo

Fuga de datos, pérdida de información confidencial, infecciones por malware o deslices en el uso del correo electrónico o las redes sociales son algunos riesgos a los que nos enfrentamos en el puesto de trabajo.

Pág. 4

4º CONGRESO DE CIBERSEGURIDAD DE ANDALUCÍA

Tras el éxito alcanzado en ediciones anteriores, este año se celebrará la cuarta edición del Congreso de Ciberseguridad de Andalucía.

La cita, organizada por la Agencia Digital de Andalucía a través del Centro de Ciberseguridad de Andalucía, CIAN, abordará la importancia de la ciberseguridad en todos los sectores y su papel clave en la transformación digital de la región.

Tendrá lugar los días 2 y 3 abril de 2025 en el Palacio de Ferias y Congresos de Málaga, FYCMA.

La Junta destaca que el Centro de Operaciones de Seguridad frenó 11.203 ciberataques en 2024, un 43,6% más que en 2023

Se han puesto en marcha herramientas como el EDR y el SIEM corporativos y se ha mejorado la plataforma de caza de amenazas, basada en la herramienta 'Carmen' del CCN-CERT.

Se han creado nuevos servicios de ciberseguridad, como los de vigilancia digital, alerta temprana de vulnerabilidades, análisis mejorado de la superficie de exposición o análisis de vulnerabilidades.

Para más información, pulsa Aquí.

El POST-IT

LA PELÍCULA

CONTRAPORTADA

Una maniobra de La Liga bloquea miles de webs legales para frenar el fútbol pirata.

La Guardia Civil advierte de la estafa de moda: "Nunca envíes dinero"

Usuarios de Gmail en peligro por una estafa que amenaza las cuentas bancarias

cómo puedes proteger a tus padres de las estafas más peligrosas: "No les hagas sentir culpables"

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

BOLESTIC
Nº 10 febrero 2025
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.
incidentes.soc@juntadeandalucia.es

TITULARES

La importancia de las actualizaciones de seguridad

Los sistemas operativos, navegadores web, programas y aplicaciones son susceptibles de tener fallos de seguridad. Por este motivo, pueden necesitar ser actualizados, independientemente del dispositivo en el que se encuentren instalados. Esto incluye los programas y sistemas operativos de ordenadores, tablets, smartphones, consolas de videojuegos e incluso televisiones inteligentes.

Una actualización es un añadido o modificación realizada sobre los sistemas operativos o aplicaciones que tenemos instaladas en nuestros dispositivos, cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad.

Por tanto, si queremos mantener la seguridad de nuestros dispositivos, debemos:

- Vigilar el estado de actualización de todos nuestros dispositivos y aplicaciones.
- Elegir la opción de actualizaciones automáticas siempre que esté disponible.
- Instalar las actualizaciones tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores y programas antivirus.
- Ser cuidadosos con las aplicaciones que instalamos, huyendo de fuentes no confiables y vigilando los privilegios que les concedemos.
- Evitar usar aplicaciones y sistemas antiguos que ya no dispongan de actualizaciones de seguridad.

Es importante no confundir tener una aplicación actualizada con tener la última versión. Podemos tener instalado y actualizado Windows 10, a pesar de no tratarse de la última versión de este sistema operativo. Los fabricantes no solo comercializan nuevas versiones que incorporan mejoras, sino que mantienen un largo periodo de tiempo las antiguas versiones a través de actualizaciones.

¿Quién se encarga de publicarlas?

Los propios desarrolladores y fabricantes elaboran las actualizaciones. En algunas ocasiones, ante un fallo de seguridad detectado publican con muchísima rapidez parches (actualizaciones de seguridad), que solucionan los problemas identificados. No obstante, ante esta circunstancia poco podemos hacer más allá de ser conscientes del riesgo y no realizar acciones que nos puedan comprometer hasta que la actualización esté disponible.

¿Qué debemos hacer ante una nueva actualización?

Mantener un dispositivo sin actualizar es un riesgo del que debemos ser conscientes. Por ese motivo, una vez se hace público un fallo de seguridad, cualquiera con los conocimientos adecuados puede utilizarlo para causarnos un daño (acceso no autorizado a nuestros dispositivos, robo de información, perjuicio económico, suplantación de identidad, etc.). Por tanto, todos hemos de adoptar el hábito de mantener nuestros dispositivos al día.

En muchos casos, las aplicaciones y dispositivos disponen de opciones de actualización automática, de manera que las instalan, de forma transparente para nosotros, tan pronto el fabricante o desarrollador las publican. Esta es la opción más recomendada, ya que evita que tengamos que estar nosotros pendientes de esta tarea, que en ocasiones resulta un poco tediosa.

Algunas precauciones

Debemos huir de sitios "pirata", especialmente de aquellos que ofrecen aplicaciones o servicios gratuitos o extremadamente baratos. No debemos instalar nada que no provenga de los canales oficiales, que proporcionan los fabricantes y desarrolladores de los dispositivos o el software.

Es recomendable revisar los privilegios que se solicitan para evitar que individuos maliciosos, que buscan tomar control de nuestro dispositivo, puedan usarlos. En cualquier caso, instalemos aplicaciones solo de fuentes de confianza y revisemos siempre los privilegios, por si fuesen excesivos o innecesarios para el propósito al que están destinados.

BOLESTIC
Nº 10 febrero 2025
Boletín de concienciación en ciberseguridad

incidentes.soc@juntadeandalucia.es

¿Cuánto sabe de ti tu smartphone?

BOLESTIC
Nº 10 febrero 2025
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.
incidentes.soc@juntadeandalucia.es

Escenarios de riesgo en el puesto de trabajo

El concepto de puesto de trabajo va más allá de la ubicación «física» donde una persona desempeña sus funciones diarias. Dentro de este entorno podemos identificar elementos con relación directa con la seguridad de la información: equipos de trabajo, smartphones, tabletas, dispositivos de almacenamiento extraíbles, impresoras, escáneres, documentación, archivadores, etc.

A continuación, os mostramos algunos ejemplos de estos posibles escenarios de riesgo.

No siempre una fuga o pérdida de datos se produce por un usuario malintencionado. A menudo se trata de usuarios que llevan a cabo prácticas no recomendables, que pueden ser aprovechadas por un atacante externo o interno, o simplemente llevar asociadas consecuencias indeseables.

Muchas fugas de información que se producen tienen como origen el puesto de un empleado. Pueden ser fruto tanto de actos malintencionados por parte de empleados descontentos, como de errores al utilizar los sistemas con los que gestionamos la información.

Las aplicaciones para gestionar el correo electrónico, suelen tener la función de autocompletar la dirección del destino. Un descuido, puede provocar el envío accidental de información confidencial a un destinatario inadecuado.

En redes sociales corporativas, es habitual que algunos usuarios incluyan información sobre clientes o proyectos en los que están trabajando, proporcionando valiosa información que puede ser utilizada para organizar un ataque de ingeniería social entre otros.

Actualmente existen soluciones informáticas, cuyo objetivo principal es reducir el riesgo de las fugas de información, sin embargo, debemos tener en cuenta que ninguna herramienta es capaz de sustituir al sentido común a la hora de gestionar la información.

Un puesto de trabajo sin las correctas medidas de seguridad, aunque no disponga de acceso a información, puede ser la puerta de entrada a la red corporativa para un atacante.

Aunque el robo o fuga de información es una de las principales amenazas, existen otras como la infección por virus, que puede llevar a interrupción de las actividades del servicio y a la pérdida de información.

La ingeniería social, tiene como objetivo a los empleados de nuestra organización y permite obtener información confidencial de las víctimas y su organización. Debemos aprender a detectar los ataques de ingeniería social.

El malware/virus no puede discriminar entre "objetivos" y "accidentes". Aunque nuestra sede no sea objetivo directo de los atacantes, el malware que existe en Internet puede hacer que nuestros sistemas estén afectados sólo porque tienen ciertas vulnerabilidades.

La extensión del lugar de trabajo a los dispositivos portátiles, ha llevado a la utilización en muchos casos de los dispositivos personales como si fuesen profesionales. No obstante, éstos carecen a menudo de los controles y protecciones de un entorno corporativo.

La información no es el único elemento valioso del puesto de trabajo. La capacidad de procesamiento o la conexión a Internet, son características que pueden ser explotadas como vías para cometer ataques sobre otras organizaciones.

BOLESTIC
Nº 10 febrero 2025
Boletín de concienciación en ciberseguridad

incidentes.soc@juntadeandalucia.es

EL POST-IT

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.

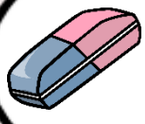
Las contraseñas son de carácter secreto

¿Quién debe responder por la falta de negligencia?

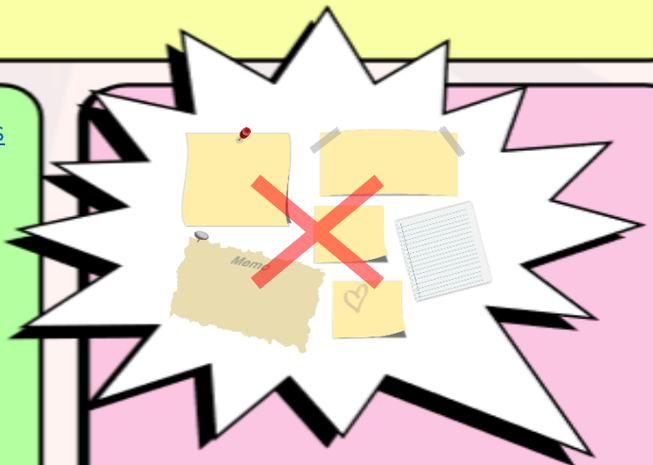
Se mantendrá la privacidad y custodia de los soportes en los cuales, guarden las contraseñas.

Se respetarán las políticas de cambio de contraseñas, procediendo a su cambio a la mayor brevedad posible cuando sea requerido y respetando las reglas de fortaleza establecidas por el responsable del recurso correspondiente.

El peligro de guardar todas nuestras claves en un mismo sitio



Se prestará especial cuidado en que no quede su contraseña guardada en un dispositivo que no vaya a utilizar.



No se revelarán por ningún medio

BOLESTIC
Nº 10 febrero 2025
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.
incidentes.soc@juntadeandalucia.es

LA PELÍCULA

¿De verdad quieres usar tu webcam?

Las webcam son una ventana al exterior donde cualquiera puede colarse.

En muchas ocasiones no somos concientes de toda la información que podemos llegar a facilitar al usar estos dispositivos inadecuandamente.

01. Información

La webcam ofrece información muy detallada del interlocutor, como la edad aproximada, el estado de ánimo, el lenguaje corporal y la expresividad, el tipo de ropa y de hogar, si existen personas cerca, datos de contextos como fotografías, posters, artículos de recuerdos...

02. Suplantación

No es recomendable usar el intercambio de imágenes, para conocer la identidad de la otra persona. Las imágenes que creemos que vienen de la webcam de la otra persona, pueden estar trucadas por ésta.

03. Grabación

Lo que envía la webcam puede ser grabado desde el otro lado.

04. Manipulación

Tu webcam puede ser activada de forma remota, sin que te des cuenta usando un malware.

BOLESTIC
Nº 10 febrero 2025
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.
incidentes.soc@juntadeandalucia.es

CONTRAPORTADA

Una maniobra de La Liga bloquea miles de webs legales para frenar el fútbol pirata.

La nueva táctica de La Liga para acabar con las retransmisiones pirata tiene como objetivo a Cloudflare y se basa en culpar al mensajero de los contenidos. Aprovechar un cuello de botella de Internet para cortarlo, caiga quien caiga. Para más información, pulsa aquí.

La Guardia Civil advierte de la estafa de moda: "Nunca envíes dinero"

Las autoridades han advertido por medio de TikTok cómo evitar caer en las trampas de los ciberdelincuentes, y que te dejen la cuenta a cero. Para más información, pulsa aquí.

Usuarios de Gmail en peligro por una estafa que amenaza las cuentas bancarias

El FBI ha lanzado una alerta a los 1800 millones de usuarios que utilizan Gmail, para no caer en una estafa que está haciendo uso de inteligencia artificial para crear llamadas automáticas y posteriormente el envío de correos electrónicos maliciosos. Para más información, pulsa aquí.

cómo puedes proteger a tus padres de las estafas más peligrosas: "No les hagas sentir culpables"

El uso de smartphones por parte de las personas mayores es un tema importante, especialmente en lo que respecta a la ciberseguridad y la prevención de estafas. Para más información, pulsa aquí.