BOLESTIC

N.º 6 Octubre 2024

Boletín de concienciación en ciberseguridad

Junta de Andalucía | Agencia Digital de Andalucía

incidentes.soc@juntadeandalucia.es

TITULARES

Ciberseguridad en casa: crea un espacio de trabajo seguro

Cuando te toque trabajar desde casa no olvides seguir nuestros consejos para crear un espacio de trabajo seguro. ¿Los cumples todos?

Pág. 2

Cómo compartir de forma segura tu DNI

Una copia de un DNI puede facilitar que un delincuente llegue a suplantar la identidad. Por esto mismo, cuerpos de seguridad del estado como Guardia Civil o Policía Nacional, nos advierten del riesgo que supone.

Pág. 3

IoT, los riesgos de un mundo hiperconectado

El término Internet de las cosas o Internet of Things (IoT) hace referencia a la digitalización de todo tipo de dispositivos comunes, como vehículos, cámaras de grabación, implantes médicos, ropa, etc. ¿Qué ventajas nos aporta? ¿A qué riesgos estamos expuestos?

Pág. 4

Guía de control parental

Las herramientas de control parental son un apoyo en el aprendizaje digital de los menores, limitando las funciones y el alcance de sus dispositivos cuando se conectan a Internet.

DE INTERÉS

Tiempo que tarda un hacker en descifrar tu contraseña

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

El POST-IT

Tratamiento de datos personales

LA PELÍCULA

ESPECIAL MES EUROPEO DE LA CIBERSEGURIDAD

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

BOLESTIC
N.º 6 Octubre 2024
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

Ciberseguridad en casa: crea un espacio de trabajo seguro

Abrir el correo para estar al día de las últimas notificaciones recibidas, realizar un pedido a uno de nuestros proveedores o actualizar la lista de clientes son solo algunas de las tareas corporativas que podemos realizar cómodamente desde nuestro hogar.

Hasta aquí todo parecen ventajas pero ¿y si hablamos de la seguridad? ¿Tomamos en casa las mismas precauciones que en la oficina? ¿Realmente conocemos todas las medidas de seguridad que necesitamos?

1 Webcam
Tapa tu webcam cuando no la estés utilizando.

2 Bloqueo del dispositivo
Cuando abandones tu equipo, bloquéalo para que nadie lo utilice sin tu permiso.

3 Instala las actualizaciones
Mantén el software de tu equipo, programas y aplicaciones actualizados.

4 Copias de seguridad
Haz copias de tu información en dispositivos externos o en la nube, para no perderla.

5 Router
Revisa las configuraciones que trae por defecto: el nombre de la Wi-Fi, la contraseña, etc.

6 Conexiones inalámbricas públicas/gratuitas
Evita conectarte a estas redes ya que no conoces sus medidas de seguridad, quién está conectado a ellas ni con qué intenciones.

7 Antivirus y cortafuegos
Actívalos para hacer frente a posibles amenazas, como virus y fraudes.

8 Información a la vista
No dejes papeles a la vista con información relevante, como contraseñas.

9 Dispositivos extraíbles (USB)
Cuando termines de usarlos, no los dejes a la vista. Guárdalos en un sitio seguro.

10 Asistentes virtuales
Configura adecuadamente las opciones de privacidad para que no registren información confidencial.

11 Dispositivos IoT
Revisa las configuraciones que ofrecen a través de sus aplicaciones móviles y mantén su software actualizado.

BOLESTIC
N.º 6 Octubre 2024
Boletín de concienciación en ciberseguridad

incidentes.soc@juntadeandalucia.es

Cómo compartir de forma segura tu DNI

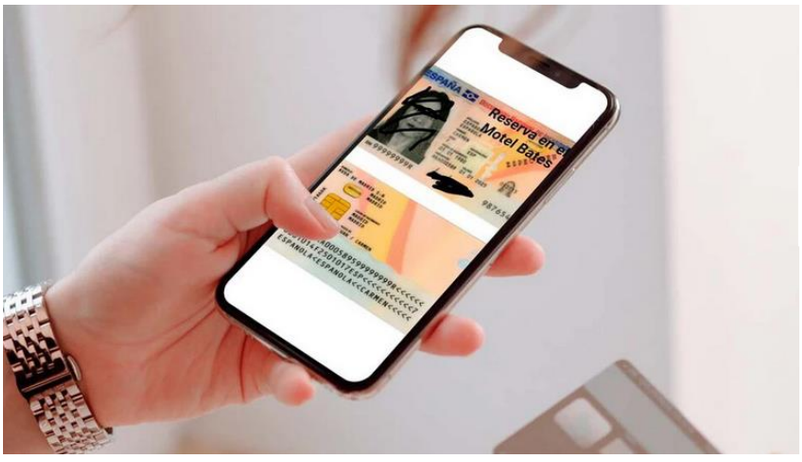
Una copia de un DNI puede facilitar que un delincuente llegue a suplantar la identidad. Por esto mismo, cuerpos de seguridad del estado como Guardia Civil o Policía Nacional, nos advierten del riesgo que supone. Sin embargo, hay determinados momentos en los que necesitaremos entregar una copia, para firmar el alquiler del piso, comprar un vehículo, etc.

Debes saber que está prohibido que nos pidan fotocopia del DNI desde el Real Decreto 522/2006, de 28 de abril, por el que se suprime la aportación de fotocopias de documentos de identidad en los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes, por lo que si algún órgano de la Administración General del Estado nos la estuviera pidiendo tendríamos que desconfiar automáticamente porque quizá se trate un de un caso de phishing".

Antes de enviarlo, asegúrate fehacientemente de que es necesario que esa persona lo tenga. De lo contrario, no envíes en ningún momento tu **carné de identidad**. Después de esto, si no tienes más remedio que enviarlo a otra persona, deberás tener una copia digitalizada a la que haremos una serie de modificaciones con un editor de imagen, ya sea escaneando el DNI o realizando una foto con calidad.

Ahora que ya lo tenemos en nuestro poder, necesitaremos cualquier editor de imágenes, ya sea una app para Android o iOS, o desde un ordenador. Incluso, los móviles ya vienen con un editor para fotos predeterminado que podemos utilizar. Lo importante son los retoques que realizaremos en la **copia del DNI** que vamos a compartir:

- Uno de los primeros cambios que deberemos realizar será **poner la copia del DNI en blanco y negro**.
- Colocar una **marca de agua**: podemos incluir un texto que indique que únicamente se autoriza el uso de la fotocopia de nuestro carné para ese uso en particular, para determinar que no se puede utilizar para otro fin.
- También podemos difuminar, borrar o colocar una banda negra en datos relevantes como: **fecha de emisión, validez y equipo**.
- Si no es necesaria que aparezca la firma, podemos ocultarla para que no puedan falsificarla.
- La **foto del DNI**: en algunos casos podemos añadir una banda negra en los ojos.



BOLESTIC
N.º 6 Octubre 2024
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

IoT, los riesgos de un mundo hiperconectado

Estamos hiperconectados

El Internet de las cosas se refiere a las tecnologías y dispositivos que detectan información y la comparten a través de Internet y, en algunos casos, actúan en función de ella.

Ejemplos de IoT en la Sociedad

Suministros
Regular suministros como el agua, electricidad o gas bajo demanda.

Tráfico
Mostrar información del tráfico en tiempo real.

Domótica
Intercambiar información entre dispositivos.

Comercios
Conocer hábitos de consumo de los clientes.

Salud
Monitorizar las constantes y la actividad física.

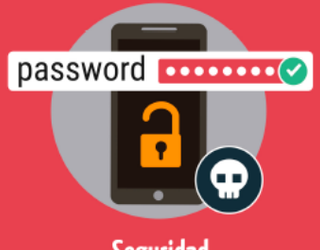
¿Qué **ventajas** nos aporta?

Ahorro económico
Nos permiten **monitorizar y controlar el funcionamiento** de los distintos dispositivos.
Ej: Las luces se apagan cuando no hay nadie.

Personalización
La información que reciben estos dispositivos **les permite ajustarse a nuestras necesidades** y reaccionar en consecuencia.
Ej: Mostrar ofertas de productos en función de nuestras búsquedas.

Interacción
Los distintos dispositivos **pueden comunicarse entre ellos** para facilitar el día a día del usuario.
Ej: El GPS del coche, a cierta distancia de casa, manda una señal al termostato para que encienda la calefacción.

¿A qué **riesgos** estamos expuestos?



Seguridad
La principal vulnerabilidad de este tipo de dispositivos es su **falta de medidas de seguridad** que lo protejan de accesos no autorizados.

Pérdida de Privacidad
Los dispositivos IoT almacenan una **gran cantidad de información personal**. Si estos datos cayesen en malas manos, nuestra privacidad quedaría expuesta.

Pérdida de Control
Si acceden a nuestros dispositivos, podrían inutilizarlos, **provocar un mal funcionamiento** o incluso realizar actividades ilícitas con ellos.

BOLESTIC

N.º 6 Octubre 2024

Boletín de concienciación en ciberseguridad

incidentes.soc@juntadeandalucia.es

EL POST-IT

Tratamiento de datos personales

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.

La Junta dispone de un canal para denuncias anónimas de los empleados públicos sobre irregularidades.

Prisión para un funcionario público por usar información reservada en su propio beneficio.

Todos los profesionales deberán conocer los datos de contacto del delegado/a de protección de datos de su organización.

La revelación de secretos y de información confidencial, se considera un delito.

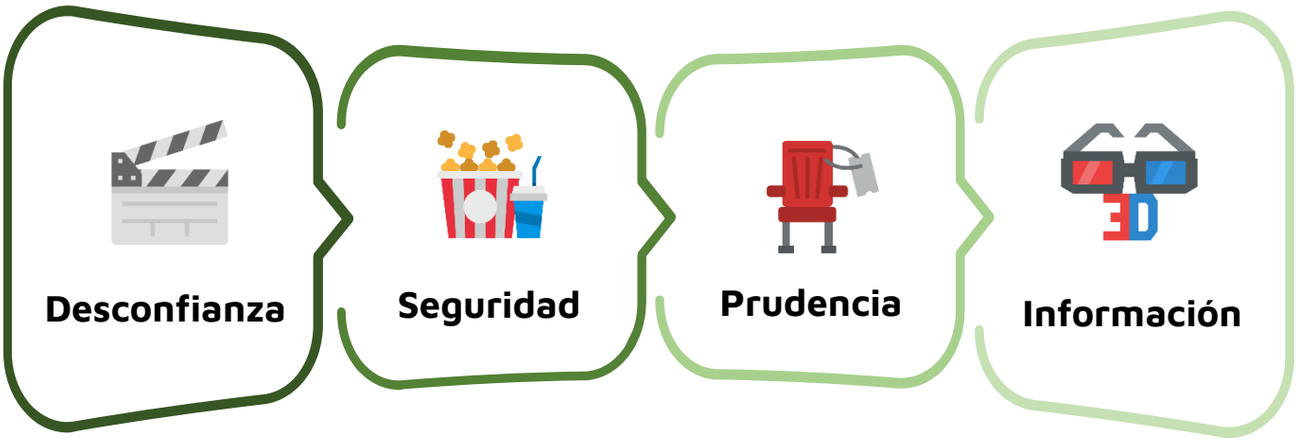
BOLESTIC
N.º 6 Octubre 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.
incidentes.soc@juntadeandalucia.es

LA PELÍCULA

La Amenaza Fantasma

Todas las acciones que aprovechan una vulnerabilidad para atentar contra nuestra seguridad son una amenaza, éstas suelen surgir cuando un ciberataque establece como objetivo los datos, sistemas informáticos, redes o dispositivos de una organización.

Las amenazas del lado oscuro están ahí, pero no las vemos.



01. DesconfianzaLa

Desconfía, los bancos y entidades oficiales nunca solicitan datos personales por correo o sms.Todas las acciones que aprovechan una vulnerabilidad para atentar contra nuestra

02. Seguridad

Debes estar seguro donde cliqueas, muchos enlaces son fraudulentos.

03. Prudencia

No utilices el móvil en aglomeraciones donde cualquiera pueda ver lo que haces.

04. Información

Informa siempre y bloquea las cuentas sospechosas.

BOLESTIC
N.º 6 Octubre 2024
Boletín de concienciación en ciberseguridad

incidentes.soc@juntadeandalucia.es

ESPECIAL MES EUROPEO DE LA CIBERSEGURIDAD

La Unión Europea promueve cada año la celebración del Mes Europeo de la Ciberseguridad, que dedica octubre a sensibilizar y difundir acciones que destaquen la importancia de la ciberseguridad en un mundo hiperconectado.

La Agencia Digital de Andalucía, **ADA** ha realizado durante el mes de octubre numerosas actividades formativas y de sensibilización en seguridad digital, en el marco del Mes Europeo de la Ciberseguridad. A través de RRSS y bajo el hashtag **#CiberseguridadAND24** puedes volver a ver las diversas actividades de sensibilización y formación puestas en marcha desde las distintas iniciativas que integran la **ADA**.

Para más información, pulsa aquí.

Guía de ciberseguridad y webinars a la carta

Desde la plataforma Andalucía Vuela, que ofrece formación digital 'online' y gratuita destinada a la ciudadanía, emprendedores y empresas, se han difundido contenidos específicos de concienciación y sensibilización sobre ciberseguridad en su blog y sus perfiles en redes sociales.

Destaca la guía disponible para consulta: ¡Navega hacia una Internet segura!

Y los webinars a la carta:

- Cómo trabaja el Blue Team en ciberseguridad
- Gestión de incidentes de ciberseguridad paso a paso
- Ciberseguridad en Infraestructuras Criticas

Charlas virtuales organizadas por el SOC de la Junta de Andalucía.

El 25 de octubre tuvo lugar una cápsula digital que trató las principales amenazas y contramedidas en el ámbito de la gestión económica y contratación para la protección del fraude de facturas.
Durante la charla, Eloy R. Sanz, del Servicio de Ciberseguridad de la Agencia Digital de Andalucía ha estado acompañado por Gabriel de la Cuesta, del Servicio de Ciberseguridad de la Agencia Digital de Andalucía y por José Luís García, del Servicio de Central de Compras de la Agencia Digital de Andalucía.

Puedes acceder aquí.

El viernes, 11 de octubre tuvo lugar la charla virtual "La Ciberseguridad y tú: consejos prácticos para una vida digital segura", impartida por Enrique Rando, Consejero Técnico del Centro de Ciberseguridad de Andalucía.

Puedes acceder aquí.

Sé más inteligente que un Hacker

BOLESTIC
N.º 6 Octubre 2024
Boletín de concienciación en ciberseguridad

incidentes.soc@juntadeandalucia.es

Cualquiera de nosotros puedes ser víctima de un ciberataque

¿Quiénes son los más vulnerables ante los ciberataques? Cualquiera de nosotros puede ser víctima, ya que todos tenemos información valiosa para un ciberdelincuente.

Qué debemos hacer para protegernos

- Actúa con precaución, especialmente al recibir correos electrónicos o llamadas sospechosas.
- Sé consciente de la información que compartes, prestando especial atención a los datos financieros, bancarios, confidenciales o personales.
- Usa contraseñas fuertes y únicas para cada servicio, y evita compartirlas.
- Evita usar conexiones Wi-Fi públicas en bares, así como establecimientos similares, para protegerte de los ciberdelitos.

¿Sabías que la mayoría de las brechas de seguridad se producen por errores humanos?

Un simple clic en un enlace sospechoso o una contraseña débil pueden poner en riesgo la información confidencial de toda la Junta de Andalucía.

Súmate a las iniciativas de Formación y Concienciación que implante la Junta de Andalucía en materia de Ciberseguridad.

- Aprenderás a identificar las amenazas más comunes, como el phishing, el ransomware y las estafas online.
- Pondrás a prueba tus conocimientos en escenarios simulados para fortalecer tus habilidades.
- Estarás al día de las últimas amenazas y mejores prácticas.

Notifica siempre los correos electrónicos sospechosos y comportamientos inusuales que observes.

Puedes usar los siguientes canales de notificación:

- Correo: incidentes.soc@juntadeandalucia.es
- Teléfono: 955 060 974

¡Tu participación es clave!

Entre todos podemos forjar una cultura de ciberseguridad robusta.