BoleSTIC
Boletín de concienciación en ciberseguridad
Enero de 2026
Nº 20
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Alerta prioritaria

¡Ojo con las estafas de enero!

¡Mantén la guardia alta! Los ciberdelincuentes aprovechan el inicio de año para lanzar campañas masivas. Estas son las amenazas activas este mes.

- **Brecha de datos masiva en Endesa:** la compañía ha informado a sus clientes sobre que se ha accedido de forma no autorizada e ilegítima a datos personales de sus clientes como datos identificativos, de contacto, DNIs y datos relativos a su contrato y medios de pago (IBAN). Es previsible que lleguen campañas de fraude masivas empleando estos datos.
- **Fraudes en suscripciones de streaming:** se han detectado correos y SMS falsos suplantando a plataformas como Netflix o Disney+. Avisan de un supuesto problema con el pago para que introduzcas tus datos bancarios en una web fraudulenta.
- **"Chollos" de rebajas:** cuidado con las ofertas demasiado buenas para ser ciertas en redes sociales o anuncios. Si el descuento es excesivo, probablemente sea una tienda falsa diseñada para robar tus datos.
- **Falsas renovaciones:** hace meses se identificó una campaña fraudulenta que comunicaba la falsa sustitución de la tarjeta sanitaria. Al igual que con este caso, desconfía siempre de cualquier mensaje urgente que pida datos personales.

¡Recuerda!

- **La Administración** o las compañías nunca solicitan contraseñas, códigos o datos personales por correo o SMS.
- **Coincidiendo con periodos de descuentos,** aumentan los fraudes en tiendas falsas que imitan comercios conocidos para robar datos bancarios.

¿Qué debes hacer?

1. **Duda de la urgencia:** los mensajes que meten prisa suelen ser estafas.
2. **No cliques:** accede siempre desde la aplicación oficial o la URL real escribiéndola en el navegador.
3. **Nunca compartas credenciales** ni códigos de verificación.
4. **Reporta:** si recibes algo sospechoso en tu cuenta corporativa, avisa de inmediato al SOC.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía · Agencia Digital de Andalucía

BoleSTIC
Boletín de concienciación en ciberseguridad
Enero de 2026
Nº 20
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Tema del mes

Refuerza la seguridad en tu puesto de trabajo

Tras el descanso navideño, es vital recuperar nuestros buenos hábitos digitales. La seguridad de la Administración depende del comportamiento de cada uno de nosotros.

Un pequeño descuido puede convertirse en la puerta de entrada a un incidente que afecte no solo a tu equipo, sino a toda la organización y a las personas que dependen de ella.

¿Por qué es tan importante la seguridad en el puesto de trabajo?

Cuando hablamos de ciberseguridad, muchas veces pensamos en grandes ataques informáticos, hackers sofisticados o problemas lejanos a nuestro día a día. Sin embargo, la realidad es que la seguridad empieza en cada puesto de trabajo, en las pequeñas decisiones que tomamos a diario frente al ordenador o el móvil.

El equipo, las aplicaciones y los sistemas que utilizamos forman parte de una red común. Una acción insegura en un solo puesto puede afectar a muchas personas, a servicios públicos esenciales y, en algunos casos, a la ciudadanía en general.

El puesto de trabajo es la primera línea de defensa

Los sistemas de la Administración cuentan con medidas técnicas de seguridad, pero ninguna herramienta es eficaz si el uso diario no es responsable. El factor humano sigue siendo uno de los principales objetivos de los ciberdelincuentes, porque es más fácil engañar a una persona que vulnerar un sistema bien protegido.

Correos fraudulentos, enlaces engañosos o mensajes que simulan ser urgentes buscan provocar una reacción rápida: que se pulse un enlace, se descargue un archivo o se facilite información sin verificar. En ese momento, el puesto de trabajo se convierte en la puerta de entrada del incidente.

Un descuido puede tener consecuencias reales

A veces se piensa que “no pasa nada” por un pequeño error, pero las consecuencias pueden ser importantes:

- **Acceso no autorizado a información sensible**
- **Bloqueo de sistemas y aplicaciones**
- **Pérdida o alteración de datos**
- **Interrupción de servicios públicos**
- **Uso fraudulento de credenciales corporativas**

Además del impacto técnico, estos incidentes pueden afectar a la confianza de la ciudadanía y generar costes económicos y de tiempo para su resolución.

SIGUE >>

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía · Agencia Digital de Andalucía

BoleSTIC
Boletín de concienciación en ciberseguridad
Enero de 2026
Nº 20
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

≪ VIENE DE LA ANTERIOR

Seguridad también es proteger la información que gestionamos

En el puesto de trabajo se manejan datos personales, documentos internos, expedientes y comunicaciones que deben protegerse adecuadamente. No se trata solo de cumplir una normativa, sino de garantizar la confidencialidad, integridad y disponibilidad de la información.

Hábitos de oro para tu día a día:

- **Contraseñas robustas y únicas:** siempre que la aplicación lo permita, utiliza frases largas con mayúsculas, minúsculas, números y símbolos, almacenándolas en gestores de contraseñas. Si el sistema lo permite, activa la doble autenticación (MFA).
- **Bloqueo de sesión:** siempre que te levantes de tu puesto, aunque sea un minuto para ir a por agua, bloquea la pantalla. Un equipo desatendido es una puerta abierta a actores malintencionados.
- **Mesa limpia:** no dejes notas con contraseñas o documentos con datos sensibles a la vista. Al finalizar la jornada, guarda todo bajo llave o al menos, que no quede a la vista.
- **Cuidado con el USB:** los pendrives y discos externos pueden contener virus. Usa preferiblemente las herramientas de almacenamiento corporativo en la nube.
- **Eliminación segura:** no tires documentos confidenciales a la papelera normal; utiliza las destructoras de papel o los contenedores específicos.

Checklist de vuelta al puesto

- ☑ He actualizado mi equipo y aplicaciones.
- ☑ Mi mesa está libre de notas con claves o información sensible.
- ☑ No estoy reutilizando claves y todas son complejas.
- ☑ Bloqueo mi equipo cuando me ausento de mi puesto.
- ☑ Conozco cómo reportar un incidente al SOC.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
INSTITUTO NACIONAL DE CIBERSEGURIDAD

BoleSTIC
Boletín de concienciación en ciberseguridad
Enero de 2026
Nº 20
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Guía rápida

Refuerza la seguridad en tu puesto de trabajo

- **¿Debo fiarme de un correo urgente?**
  No. La urgencia es una técnica habitual de fraude.
- **¿Es seguro usar la misma contraseña?**
  No. Usa contraseñas únicas y robustas.
- **¿Tengo que cambiar mis contraseñas aunque sean robustas?**
  Sí. Es recomendable cambiar las claves periódicamente.
- **¿Puedo abrir archivos de remitentes conocidos?**
  Con precaución. Si no esperabas el archivo, confirma antes.
- **Si detecto algo sospechoso, ¿cómo procedo?**
  No interactúes con el correo o SMS. Notifícalo al SOC para que puedan investigarlo y sigue sus indicaciones.
- **Si he hecho clic y/o proporcionado información, ¿qué debo hacer?**
  Notifícalo inmediatamente al SOC para que te informen de cómo proceder.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía · Agencia Digital de Andalucía

BoleSTIC
Boletín de concienciación en ciberseguridad
Enero de 2026
Nº 20
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Zona interactiva

En esta nueva sección te presentamos algunas dudas comunes en materia de ciberseguridad, y una situación real que todos podríamos encontrarnos. Te invitamos a reflexionar sobre ello. ¡Encontrarás las respuestas más adelante!

Quiz del mes

1. ¿Cuál es la forma más segura de crear una contraseña?

- **A** Usar mi fecha de nacimiento, o alguna otra que sea fácil de recordar.
- **B** Crear una frase combinando mayúsculas, minúsculas, números y símbolos.
- **C** Utilizar la misma que ya uso en mi correo personal u otro servicio.

2. Recibes un correo de "Soporte Técnico" pidiendo tu clave para "mantenimiento". ¿Qué haces?

- **A** Se la doy. Para eso es el servicio de soporte de mi área/departamento.
- **B** No hago nada. No me fío de estos correos y lo mejor es ignorarlos.
- **C** Desconfío y reporto al SOC. Así puedo ayudar a detectar amenazas.

3. ¿Qué significa la política de "mesa limpia"?

- **A** Que el servicio de limpieza ha pasado por nuestro puesto.
- **B** Que no debemos dejar información sensible a la vista.
- **C** Que los usuarios/claves deben guardarse ordenadamente en papel.

4. Encuentras un USB tirado en el aparcamiento de la oficina. ¿Qué deberías hacer?

- **A** Llevártelo y conectarlo para ver de quién puede ser y dárselo.
- **B** Quedártelo. Total, lo puedes enchufar a tu equipo y borrarlo.
- **C** Entregarlo al área de informática o seguridad, sin conectarlo.

5. ¿Cuál de estas contraseñas es más segura?

- **A** 123456
- **B** Contraseña$egura
- **C** GaT0-VeRd3*C0rR3/2o24.

6. Tu ordenador se bloquea y aparece un mensaje raro pidiendo dinero. ¿Qué haces?

- **A** Pago rápido, que tengo prisa, y le paso el ticket al área/departamento.
- **B** Aviso al SOC de que mi equipo parece haberse infectado por ransomware.
- **C** Intento arreglarlo como sea para que nadie se entere de lo que me ha pasado.

SIGUE >>

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

CONTENIDOS

Alerta prioritaria
Tema del mes
Guía rápida
Zona interactiva
Radar de amenazas
Normativa al día
Respuestas correctas
Canal directo

≪ VIENE DE LA ANTERIOR

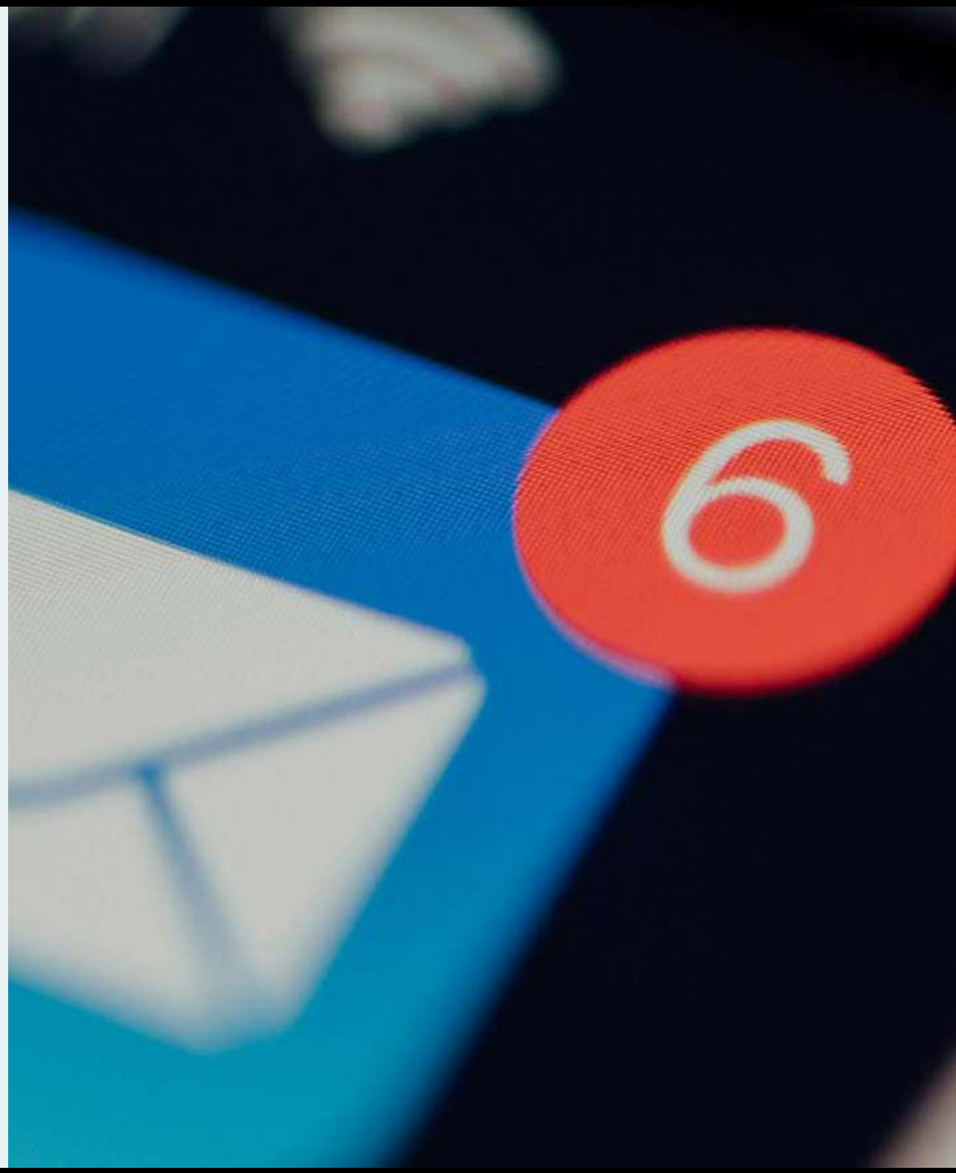
Caso práctico

Recibes un correo electrónico que, a primera vista, parece legítimo, proveniente de tu compañía de suministro eléctrico (luz, gas, etc.). El asunto es urgente, notificando la existencia de una factura adjunta con un importe excepcionalmente elevado que no esperabas.

Lo más alarmante es que el mensaje contiene todos tus datos personales de manera correcta (nombre completo, dirección de suministro, quizás incluso tu número de contrato), lo que le da bastante credibilidad.

Se te insta a descargar o abrir el archivo adjunto (que suele ser un PDF o un ZIP), o a hacer clic en un enlace, para “consultar el detalle” o “proceder al pago inmediato” para evitar un corte de servicio o cargos adicionales.

¿Qué haces?



Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía · Agencia Digital de Andalucía

BoleSTIC
Boletín de concienciación en ciberseguridad
Enero de 2026
Nº 20
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Radar de amenazas

El panorama de la ciberseguridad evoluciona rápido y debemos estar informados. Compartimos contigo algunas noticias destacadas de este mes.

Alerta sobre la estafa de las “grúas pirata” y recomendaciones para protegernos

La baliza V16, el nuevo sistema de señalización de vehículos inmovilizados obligatorio desde el 1 de enero, podría entrañar un riesgo para los conductores en caso de avería en carretera.

Esto es debido a la creación de sistemas de geolocalización de incidencias y mapas públicos de tráfico, que aunque tienen como objetivo mejorar la seguridad vial, podrían ser usados por operadores maliciosos para localizar situaciones de vulnerabilidad.

La estafa consiste en la utilización de estos mapas para enviar a los vehículos recién accidentados servicios de asistencia ilegítimos, que llegando antes que los oficiales buscan aprovechar la situación de estrés de los conductores para exigir pagos desproporcionados por su actuación.

> Enlace a la noticia

Apple alerta sobre ciberataques avanzados en iPhone

Apple ha lanzado una alerta sobre ciberataques sofisticados que están afectando a usuarios de iPhone. Estas amenazas utilizan spyware avanzado y no se mitigan completamente con las actualizaciones de software rutinarias.

A diferencia del phishing común, se trata de ataques altamente dirigidos y complejos que explotan vulnerabilidades “cero clic”. Esto significa que el spyware puede comprometer un iPhone sin necesidad de que el usuario realice ninguna acción (como hacer clic en enlaces o abrir archivos), similar al caso conocido del software Pegasus.

La acción más crítica es instalar de inmediato la actualización a iOS 26, si tu dispositivo es compatible. Para ello, accede a Ajustes, General y luego a Actualización de software.

> Enlace a la noticia

SIGUE >>

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
INSTITUTO NACIONAL DE CIBERSEGURIDAD

BoleSTIC
Boletín de concienciación en ciberseguridad
Enero de 2026
Nº 20
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

≪ VIENE DE LA ANTERIOR

Así es la estafa de la multa con código QR en el parabrisas de tu coche

Encontrar una supuesta multa en el parabrisas puede generar una reacción inmediata de prisa por ver los detalles y resolver el pago. Los estafadores están aprovechando precisamente esta urgencia. Diversos cuerpos policiales en España han emitido una alerta sobre una nueva modalidad de fraude que utiliza un elemento cada vez más común: el código QR.

El método es sencillo y busca ser creíble: se coloca en el vehículo una hoja de papel que simula ser una notificación administrativa por una infracción de estacionamiento. Este documento insta al conductor a "consultar" la multa escaneando un código QR, a menudo con frases como "para ver su multa, escanee el código".

Sin embargo, el código QR no conduce a una multa real, sino a una página web falsa que suplanta a un organismo oficial o a una plataforma de pago. A partir de ahí, la estafa puede variar: desde solicitar los datos de la tarjeta de crédito para un supuesto abono de la sanción, hasta recolectar información personal que será utilizada para cometer otros delitos.

> Enlace a la noticia

Suplantan comunicaciones del gestor de claves LastPass

LastPass, reconocido gestor de contraseñas en la nube, ha alertado de una campaña activa de phishing dirigida a sus usuarios mediante correos electrónicos fraudulentos que simulan avisos oficiales de la compañía. Los mensajes advierten de supuestas tareas urgentes de mantenimiento o de la necesidad de realizar una copia de seguridad del almacén de contraseñas, con el objetivo de generar sensación de urgencia y provocar que el usuario actúe sin comprobar la legitimidad del aviso.

Al hacer clic en los enlaces incluidos en estos correos, las víctimas son redirigidas a páginas web falsas que imitan el portal de LastPass y solicitan la contraseña maestra, algo que la empresa nunca pide por correo electrónico. El fin del ataque es obtener acceso completo a las cuentas y a todas las credenciales almacenadas. LastPass recuerda a los usuarios que verifiquen cuidadosamente el remitente y los enlaces de cualquier comunicación, y que desconfíen de mensajes que presionen para actuar con urgencia.

> Enlace a la noticia

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
INSTITUTO NACIONAL DE CIBERSEGURIDAD

BoleSTIC
Boletín de concienciación en ciberseguridad
Enero de 2026
Nº 20
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Normativa al día

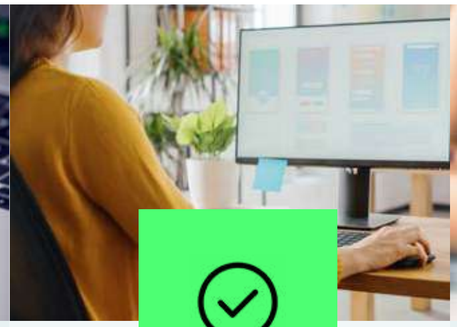
Debemos hacer un buen uso de las tecnologías de la información y la comunicación en nuestros puestos de trabajo. Te recordamos varios puntos importantes.

Usa las TIC siempre con orientación al servicio público

El uso de las tecnologías debe contribuir a mejorar la atención a la ciudadanía y la calidad de los servicios públicos. Cada herramienta TIC es un medio para prestar un servicio eficaz, accesible y cercano, no un fin en sí mismo.

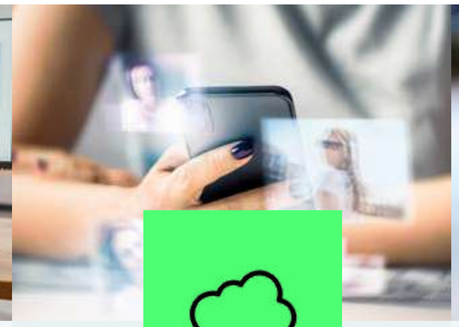
No prestes tu ordenador ni tus dispositivos a terceros

No está permitido facilitar el uso del equipamiento TIC a personas no autorizadas, aunque se trate de compañeros, familiares o personas de confianza.



Usa solo las aplicaciones autorizadas para tu trabajo

Debes utilizar exclusivamente las aplicaciones y sistemas que la Junta de Andalucía haya habilitado para el desempeño de tus funciones, siguiendo las guías y manuales establecidos.



No utilices nubes personales para trabajar

Está prohibido utilizar cuentas personales en servicios externos de almacenamiento en la nube para el desarrollo de funciones profesionales.

Verifica siempre destinatarios y copias

Antes de enviar un correo, revisa cuidadosamente los destinatarios y valora el uso de copia oculta para evitar revelar datos personales.

> **Código de Conducta en el uso de las TIC para profesionales de la Administración de la Junta de Andalucía**

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

BoleSTIC
Boletín de concienciación en ciberseguridad
Enero de 2026
Nº 20
Elaborado por el SOC de la Junta de Andalucía.

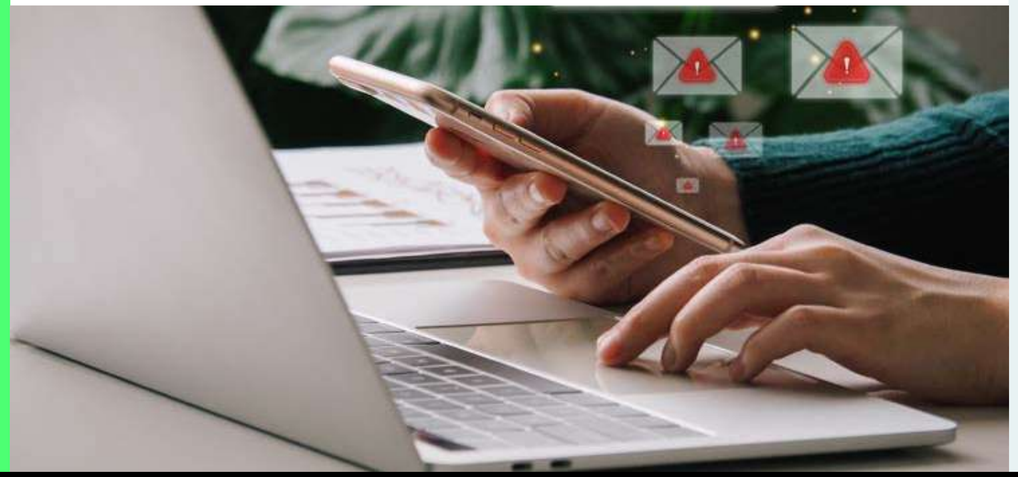
CONTENIDOS

Respuestas correctas

Aquí tienes las respuestas a la ZONA INTERACTIVA de este mes.

Quiz del mes

1. **B** Crear una frase combinando mayúsculas, minúsculas, números y símbolos.
2. **C** Desconfío y reporto al SOC. Así puedo ayudar a detectar amenazas.
3. **B** Que no debemos dejar información sensible a la vista.
4. **C** Entregarlo al área de informática o seguridad, sin conectarlo.
5. **C** GaT0-VeRd3*C0rR3/2o24.
6. **B** Aviso al SOC de que mi equipo parece haberse infectado por ransomware.



Caso práctico

Lo primero es mantener la calma y no actuar impulsivamente. El factor sorpresa y la urgencia son tácticas de phishing para forzar una reacción irreflexiva.

Fíjate en el archivo adjunto y en su formato, no lo descargues ni lo abras. Tampoco pinches en ningún enlace. Los adjuntos pueden contener malware (.exe es un ejecutable, no un documento), y los enlaces dirigir a páginas fraudulentas (mira la URL de destino, si coincide o no con la web oficial).

Que el correo contenga tus datos correctos no valida la factura: los ciberdelincuentes pueden haberlos obtenido de una brecha de seguridad o base de datos robada, y usarlos para generar confianza y urgencia.

Llama al número de atención al cliente oficial de la compañía (el que aparece en tus facturas físicas o en su web, no en el correo sospechoso). Pregunta si existe alguna factura pendiente con ese importe, o si han enviado un email con esas características.

Si prefieres comprobarlo mediante tu área de cliente en la web de la compañía, abre tu navegador y accede tecleando manualmente la dirección web oficial de la empresa, nunca pinchando en el enlace que aparezca en el email.

Los ataques de phishing son cada vez más elaborados y profesionales, pero con atención, precaución y calma podemos detectarlos para no caer en la trampa.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía · Agencia Digital de Andalucía

BoleSTIC
Boletín de concienciación en ciberseguridad
Enero de 2026
Nº 20
Elaborado por el SOC de la Junta de Andalucía.

CONTENIDOS

Canal directo

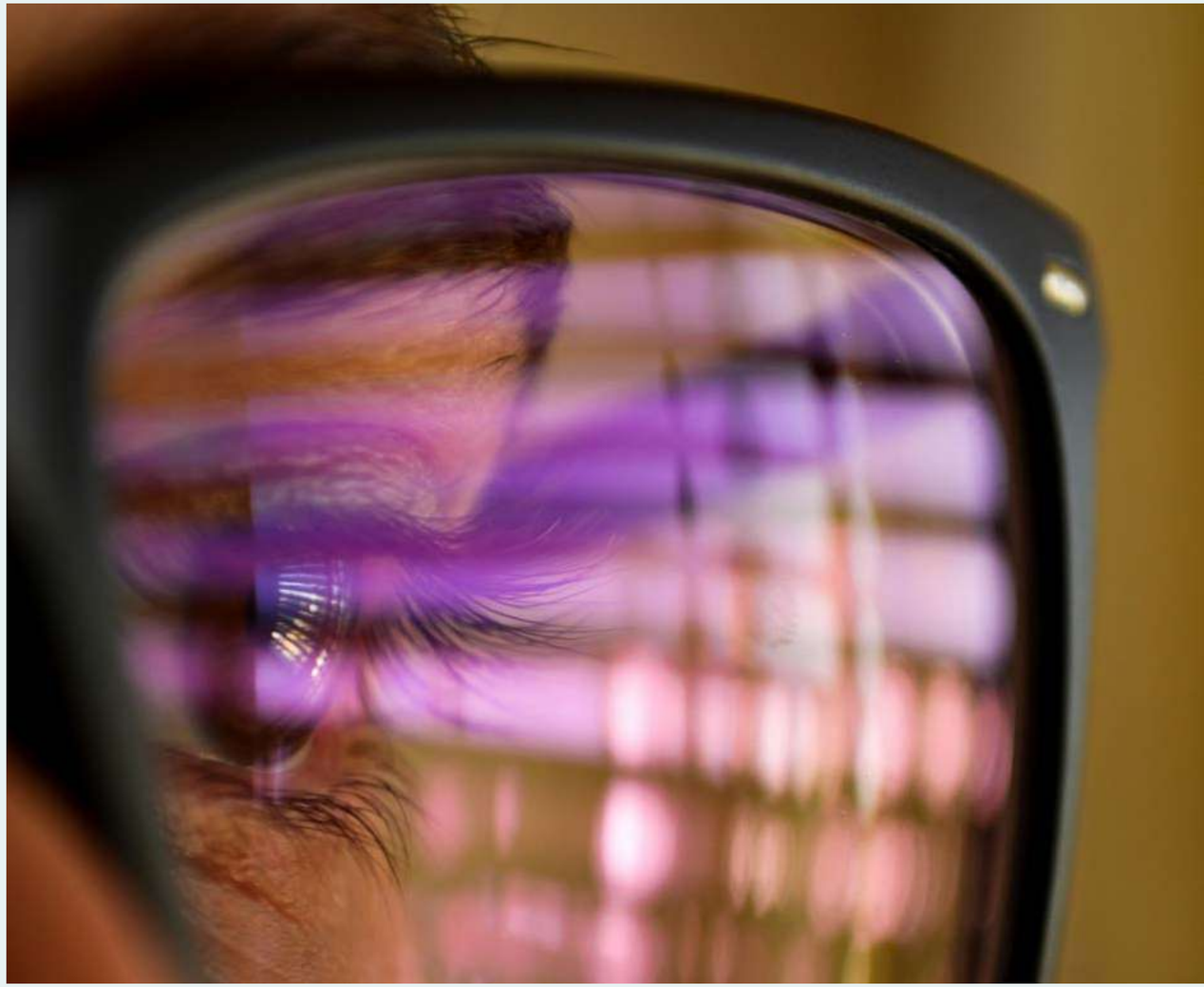
La seguridad es una tarea compartida. Si tienes cualquier duda o sospechas de un incidente, ¡contacta con nosotros!

Email
incidentes.soc@juntadeandalucia.es

Teléfono
955 060 974
360 974 (corporativo)

Alertas de seguridad y campañas activas
> Consúltalas aquí.

Síguenos en X
@CentroCiberAND



Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia