Tips de Ciberseguridad

ashotel
ASOCIACIÓN HOTELERA Y EXTRAHOTELERA DE TENERIFE, LA PALMA, LA GOMERA Y EL HIERRO

HD Abogados

¡Ashotel HUELLA POSITIVA!

Introducción

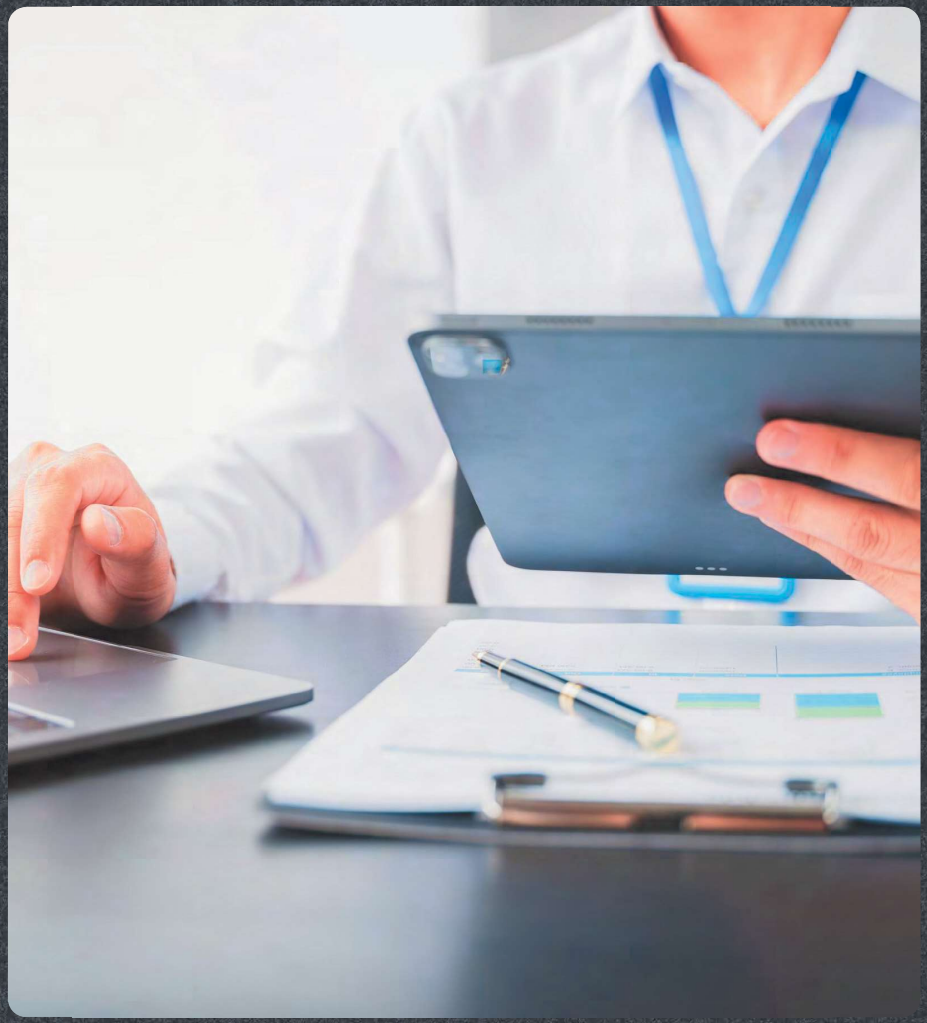
La ciberseguridad ya no es solo una cuestión técnica: es una condición esencial para la competitividad, la confianza y la sostenibilidad del sector empresarial.

En el marco del programa Ashotel Huella Positiva, se busca formar y sensibilizar a todas las personas, promoviendo una cultura de seguridad digital basada en la responsabilidad y la transparencia.

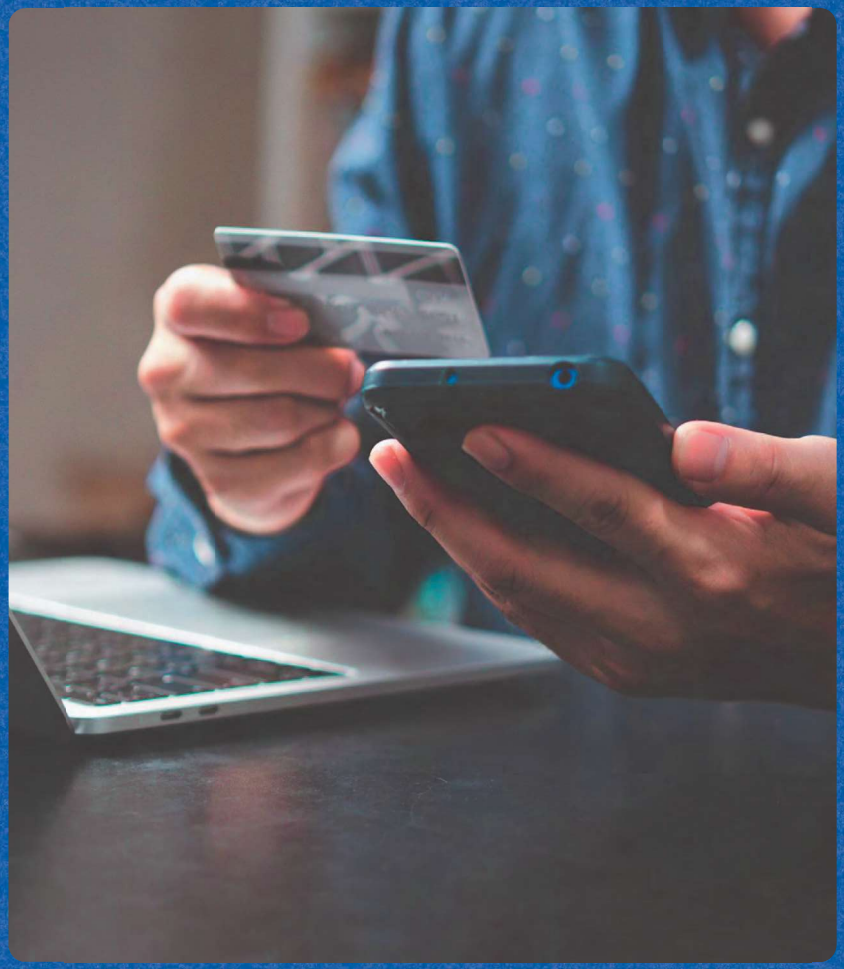
Esta charla busca precisamente eso: sensibilizar y ofrecer pautas prácticas para fortalecer la seguridad digital en el día a día.

Caso Real

Envío de correo con apariencia real.
Esto es lo que se conoce como **phishing o suplantación de identidad**, y es una de las formas más comunes de ataque hoy en día.
Los ciberdelincuentes buscan **ganarse nuestra confianza** para que hagamos algo: abrir un archivo, pulsar en un enlace o compartir una información sensible. Y lo logran porque el correo parece venir de alguien que conocemos.
Lo importante de este caso es que **no fue un fallo técnico**, sino una **maniobra psicológica**, una técnica de manipulación que aprovecha la confianza y la rutina diaria. Por eso, lo más importante es **reconocer las señales de alerta** antes de caer en la trampa.



Detectar: pensar antes de hacer clic



La primera defensa es **la atención**.

INCIBE (Instituto Nacional de Ciberseguridad de España) – En sus campañas menciona que la mayoría de los incidentes comienzan con un mensaje que simula ser legítimo.

Para detectarlos, basta con aplicar el principio de **duda razonable digital**:

- ¿Conozco realmente al remitente?
- ¿El tono o el tipo de solicitud encajan con lo habitual?
- ¿Me pide hacer algo urgente, confidencial o inusual?
- Si algo no encaja, **detente**. Antes de abrir, responder o reenviar, verifica.

Pensar 10 segundos puede evitar 10 días de consecuencias.

Revisa el remitente.
Desconfía de la urgencia.
Confirma por otra vía.
Si dudas, no hagas clic.

Proteger: 5 tips para estar seguros

Una vez desarrollamos la atención, toca **protegernos**.

Aquí van cinco acciones sencillas que todos podemos aplicar desde hoy:

1. 🔒 **Usar contraseñas seguras y únicas.** Usar contraseñas robustas. No utilizar la misma contraseña en el correo, la WiFi y el sistema interno.

2. 📱 **Activar la verificación en dos pasos.** App doble factor.

3. 🚫 **Evitar reenviar correos sospechosos.** Ejemplo:
Si recibes un correo extraño que dice “mira este documento urgente” o “factura pendiente”, no lo reenvíes a otros para preguntar.
Haz una captura o reenvíalo únicamente al área de soporte o al contacto de seguridad.
Esto evita que más personas hagan clic por error.

4. 💾 **Mantener los equipos y móviles actualizados.** Cuando el ordenador pide “actualizar sistema”, no es molestia, es **una barrera de seguridad**.
Las actualizaciones corrigen fallos que los ciberdelincuentes aprovechan.

5. 🗣️ **Avisar ante cualquier sospecha, no actuar solo.**

Son medidas simples, pero muy efectivas para reducir riesgos en el día a día.

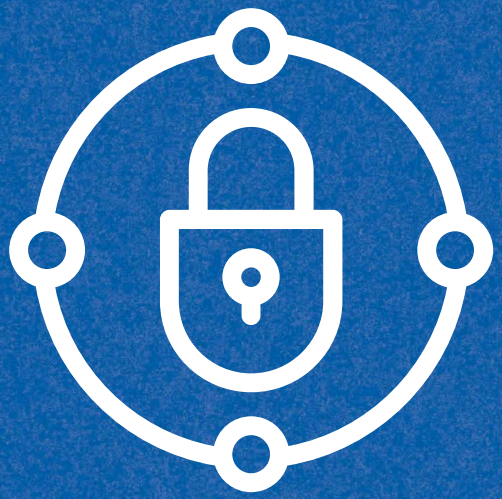
Recomendaciones

Generales

- Integrar la ciberseguridad en la estrategia de sostenibilidad y digitalización de la entidad.
- Definir roles y responsabilidades claras en la gestión de incidentes y protección de datos.
- Establecer protocolos internos de actuación ante ciberataques o brechas de seguridad.
- Revisar y actualizar políticas de seguridad y confidencialidad al menos una vez al año.
- Formar periódicamente al personal en materia de ciberseguridad y protección de datos.
- Impulsar una cultura preventiva basada en la comunicación y la transparencia.

Normativa de referencia

- Reglamento (UE) 2016/679 (RGPD) – Seguridad, confidencialidad y responsabilidad proactiva en el tratamiento de datos personales.
- Ley Orgánica 3/2018 (LOPDGDD) – Adaptación nacional del RGPD y deberes de las entidades en materia de protección de datos de carácter personal.
- Ley 2/2023, de protección del informante – Obliga a disponer de canales seguros y confidenciales para la comunicación de irregularidades.
- ISO/IEC 27001 estándar internacional para la gestión de la seguridad de la información, basado en la evaluación del riesgo y la mejora continua.



Gracias por la atención