Boletín 04/20

LOPD EN LA EMPRESA

DESIGNAR A UN DPD: LA CLAVE PARA EVITAR SANCIONES Y RESOLVER RECLAMACIONES

En el ámbito del cumplimiento de la normativa existe siempre un profesional que acompaña, guía y aconseja a las entidades para que pueda desarrollar su actividad profesional con las mejores garantías de cumplimiento y evitar así ser sancionados. De entre ellos, podemos mencionar a los asesores fiscales, laborales, y, en la materia que nos ocupa en este post, al consultor especialista en protección de datos y, en concreto, nos referiremos al Delegado de Protección de Datos.

¿Por qué tienen las entidades que nombrar un dpd?

En primer lugar, para dar respuesta a esta pregunta acudiremos al artículo 37 del RGPD y al artículo 34 de nuestra Ley Orgánica (LOPDGDD). En estos artículos encontramos supuestos en los que resulta obligatorio su nombramiento por Ley:

En el art.37del RGPD:

- Cuando el tratamiento de datos personales los lleve a cabo una autoridad u organismo público.
- Las actividades principales del responsable o encargado, consisten en una observación habitual y sistemática de interesados a gran escala.
- Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales.

La AEPD sancionó con 25.000 euros a la entidad GLOVOAPP23 S.L. por incumplimiento de este artículo, ya que no habían designado un DPD, siendo éste obligatorio debido al número tan elevado de clientes y el tratamiento de datos personales identificadores básicos.

En el art. 34 de LOPDGDD:
Encontramos un listado con entidades obligadas a nombrar un DPD. Aún son muchos los responsable y encargados del tratamiento que encontrándose incluida su actividad en este listado no tienen designado a un Delegado de Protección de Datos. Este es el caso de la reciente multa impuesta por la AEPD a la empresa de seguridad privada CONSEGURIDAD S.L. La sanción alcanzó los 50.000 euros.
En segundo lugar, la normativa también da la opción de un nombramiento voluntario de DPD, éste aportaría a la entidad sus conocimientos especializados del Derecho y la práctica en materia de protección de datos, para apoyar al responsable y al encargado del tratamiento en el cumplimiento de todos los requisitos exigidos por la Ley.

Dpd figura esencial en la remisión de las reclamaciones

El DPD se convierte en una figura esencial para apoyar, guiar y aconsejar al responsable y encargado del tratamiento para llevar a cabo una de las exigencias contenidas en la LOPDGDD. Una de las novedades reguladas en nuestra Ley Orgánica es la inclusión del mecanismo previo a la admisión a trámite de las reclamaciones que se formulen ante la AEPD, esta puede trasladarlas a los Delegados de Protección de Datos designados o a los responsables y encargados del tratamiento. En el plazo de un mes se tiene que dar contestación al reclamante y a la AEPD, por lo que el apoyo del DPD resulta imprescindible en este tipo de actuaciones para resolverlas eficazmente.

Por tanto, la figura del DPD va a ser clave para las empresas. Puedes convertirte en DPD con nuestro curso online de Delegado de Protección de Datos.

NUEVA GUÍA DE CIBERATAQUES PARA USUARIOS PUBLICADA POR INCIBE

La semana pasada el Instituto Nacional de Ciberseguridad (INCIBE) publicaba, a través de la Oficina de Seguridad del Internauta, Guía de ciberataques. Todo lo que debes saber a nivel usuario. Es un sencillo manual para que los usuarios conozcan más de 30 tipos de intrusiones y sepan cómo actuar frente a ellas.

¿Qué debes saber a nivel de usuario?

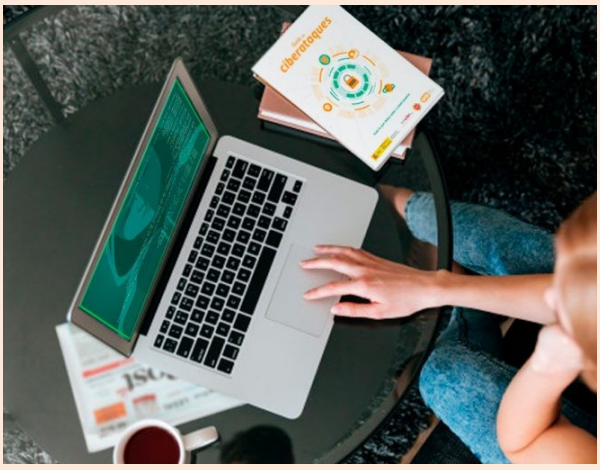
La guía recoge las características de las principales intrusiones a las que un usuario puede enfrentarse cuando navega por Internet, detallándo cómo los ciberdelincuentes realizan los ciberataques y qué les motiva a hacerlos. Este manual destaca porque pone a disposición del usuario qué debe hacer para estar protegido específicamente de cada uno de ellos y cómo combatirlos sin necesidad de tener grandes conocimientos técnicos.

Su objetivo es que el usuario no acabe siendo una víctima de la ciberdelincuencia.

Categorías de ataques

Divide los ciberataques en 4 categorías:

- **Ataques a las contraseñas**: Cómo pueden sustraernos nuestras contraseñas.
- **Ataques por ingeniería social**: Cómo pueden engañarnos para que hagamos, descarguemos o instalemos algo malicioso.
- **Ataques a las conexiones**: Cómo los ciberdelincuentes nos pueden robar información personal, controlar nuestro equipo de forma remota, suplantar una cuenta de correo electrónico o efectuar un ataque de DoS, entre otros.
- **Ataques por malware**: Donde explica qué es un virus, un troyano, un spyware o las botnets, entre otros.
-



La nueva guía destaca porque todo su contenido está explicado en un lenguaje sencillo para que todos los usuarios que no tengan conocimientos técnicos puedan protegerse y actuar ante ellos.

Consejos que proporciona la guía para mejorar la protección de los dispositivos

- Mantener el S.O., el navegador y las aplicaciones siempre actualizadas.
- Utilizar contraseñas robustas y diferentes para proteger todas tus cuentas. Si es posible, utiliza la verificación en dos pasos u otro factor de autenticación.
- Siempre utilizar un software anti-malware.
- Descargar solo de sitios oficiales aplicaciones o software legítimo.
- Desconfiar de los adjuntos sospechosos y enlaces de los correos.
- Tener cuidado por dónde navegas. Si vas a proporcionar datos, utiliza solo webs seguras con https.
- Evitar conectarse a redes wifi públicas o a conexiones inalámbricas desconocidas.
- No compartir información personal con cualquier desconocido ni publicarla o guardarla en páginas o servicios webs no fiables
- Hacer copias de seguridad frecuentes en un medio que no esté conectado al equipo.

Otras vías para protegerse de los ciberataques

Si tenemos alguna duda en cuanto a ciberseguridad, privacidad, confianza digital y uso seguro y responsable de Internet, podemos llamar al 017, teléfono que puso a disposición de los usuarios el INCIBE, el pasado mes de mayo.

También es importante formarse en ciberseguridad. La Guía de Ciberataques es un gran apoyo para tener conocimientos sobre los posibles ataques y conocer cómo protegerse de ellos.

BRECHAS DE SEGURIDAD DE DATOS PERSONALES

¿Qué son?

Según la Agencia Española de Protección de Datos, una brecha de seguridad es un incidente de seguridad que afecta a datos de carácter personal. El origen de dicho incidente puede ser accidental o intencionado y, puede afectar tanto a datos en formato digital como en papel. Este hecho suele ocasionar la destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales.

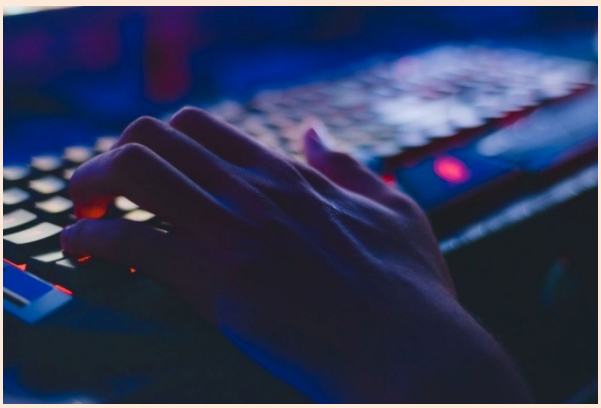
¿Cómo evitar una brecha de seguridad?

Para evitar una brecha de seguridad debemos incorporar medidas de seguridad adecuadas que abarquen:

Seguridad informática en el puesto de trabajo: uso de contraseñas seguras y doble factor de autenticación.

Seguridad informática en la red: sistemas actualizados para así evitar las posibles vulnerabilidades y la exposición de servicios de Internet. Los accesos remotos siempre deben realizarse a través de sistemas VPN, proxy inverso o medidas igualmente eficaces.

Seguridad informática en los datos: se debe realizar copias de seguridad periódicas para así, si somos víctimas de secuestros de información, poder acceder a ella sin necesidad de pagar un rescate. También, debemos cifrar todos los dispositivos para asegurar la confidencialidad de la información, no solo los ordenadores portátiles, sino también los USB, teléfonos móviles, tabletas, entre otros.



Formación en ciberseguridad: es necesario que todos los usuarios de dispositivos tecnológicos conectados o no a Internet dispongan de unos conocimientos básicos para poder realizar un uso ciberseguro de los dispositivos. Todos estos conocimientos puedes aprenderlos en el curso online de Ciberseguridad Laboral y Personal.

Seguridad de los documentos en formato papel. aquellos que contengan datos personales deberán ser guardados bajo llave. En caso de que ya no sean útiles, ser destruidos de una manera segura, como por ejemplo con una destructora de papel o una empresa especializada en destruir datos.

¿Cuándo se debe notificar una brecha de seguridad?

Para saber si se debe o no notificar una brecha de seguridad, el responsable de tratamiento de datos debe valorar las consecuencias de dicha brecha sobre los usuarios afectados.

A fin de conocer estas consecuencias se debe tener previamente elaborado y actualizado el registro de actividades de tratamiento y el análisis de riesgo de la entidad.

El Reglamento General de Protección de Datos establece que si la brecha de seguridad es un riesgo para los derechos y las libertades de las personas se debe notificar ante la AEPD. El plazo máximo para notificar una brecha de seguridad es de 72 horas desde que se tenga constancia de que ha ocurrido una brecha de seguridad. Aunque la AEPD recomienda siempre notificarla.

Si ésta conlleva un alto riesgo se deberá comunicar sin mayor dilación a los usuarios afectados. La comunicación se realizará a través del medio que se suela utilizar para comunicarse. Se explicará de manera clara y concisa qué es lo que ha ocurrido y qué medidas deben hacer al respecto.

Si la brecha la sufre un encargado del tratamiento, este debe informar al responsable del tratamiento, sin dilación, para que decida si notifica o no la brecha de seguridad y si es necesario comunicar dicho incidente a los afectados.

Se notifique o no a la AEPD o si se ha informado o no a los afectados, cada entidad o persona física debe llevar siempre un registro con las brechas de seguridad que le ocurran. Este control puede ser exigible por parte de la AEPD en cualquier momento.
Esta información está recogida en los artículos 33 y 34 del RGPD.

Conclusión

Debemos utilizar las herramientas necesarias para evitar una brecha de seguridad. También debemos aprender los conocimientos básicos para estar ciberseguros y aplicarlos no solo en nuestro ámbito laboral, sino también personal. Estas medidas pueden fallar, por lo que debemos de conocer cuál es el mejor protocolo de actuación ante una brecha de seguridad.

COMERCIO ONLINE: VENTAJAS DE IMPULSAR TU NEGOCIO CON UNA E-COMMERCE O TIENDA ONLINE

Las ventas a través de internet aumentan un 11,6% en España
El comercio electrónico en España crece a pasos agigantados. Gracias a la transformación digital, la experiencia de compra del consumidor ha cambiado. Las ventas realizadas a través de internet en España superan ya los 12.200 millones de euros, según los últimos datos publicados por la Comisión Nacional de los Mercados y la Competencia (CNMC).

Las cifras se refieren al primer trimestre de 2020 (el último disponible), y destacan que el crecimiento del e-Commerce en España ha aumentado un 11,6% respecto al mismo periodo del año anterior.

Concretamente, las webs de comercio electrónico en España se han llevado el 49,2% de los ingresos; y el porcentaje restante corresponde a las compras realizadas desde España a webs extranjeras.

Los datos del informe indican que los sectores que aportan mayores ingresos a nuestro país son las agencias de viajes y operadores turísticos, el transporte aéreo, y la moda.

¿Qué facilidades ofrece el e-Commerce?

El éxito de la compra desde casa viene dado por las grandes ventajas que aporta al cliente, y más en tiempos de pandemia, este método que ha revolucionado el consumo mundial.

En primer lugar, por el alcance global. El e-Commerce permite que una empresa llegue a las demandas del mercado nacional e internacional, ya que no hay límites geográficos.

Otra facilidad de la compra en línea es la inexistencia de horarios. El consumidor puede realizar transacciones las 24 horas del día, incluso en festivos y fines de semana.

Con el amplio mercado online, los clientes también pueden buscar los productos a su gusto, analizando los más baratos y los de mayor calidad.

Fórmate en e-Commerce y dale un giro a tu empresa

El comercio online no solo acerca tu empresa a clientes de todo el mundo, sino que reduce significativamente los costes y permite invertir de forma más rentable, según la demanda.

CONSEJOS PARA MEJORAR LA SEGURIDAD DE CONSUMIDORES Y EMPRESAS

“No existe la seguridad al 100% en el mundo digital”, asegura Lozano, del Incibe. Ante ello hay que tomar algunas precauciones si se compra o se vende por Internet.

1. **Router**: Unas de las primeras recomendaciones, tanto para consumidores como para empresas, es poner al día el router. Ese aparato relegado a una esquina de la casa o del negocio puede ser la puerta de entrada para los delincuentes. Para evitar sorpresas hay que seguir dos pasos muy básicos: actualizar el software del dispositivo a la última versión disponible y cambiar las credenciales predefinidas por defecto (usuario y contraseña), destacan los expertos del Incibe.

2. **Antivirus**. Instalar un antivirus puede contribuir a evitar los ataques, pero no lo es todo. “Hay que contar con la última actualización”, dice Lozano.

3. **Ofertas**. Desconfíe de las gangas sospechosas, “El Black Friday y el Cyber Monday presentan muchas ofertas legítimas ofrecidas por comercios de confianza y de buena reputación. Sin embargo, los ciberdelincuentes se aprovechan de ello replicando y difundiendo muchas ofertas falsas”, advierte. El especialista indica que puede ser difícil distinguir entre una oferta real y una estafa, por lo que es mejor asegurarse de que un sitio web es auténtico y seguro.

“Comprar en tiendas de confianza y con buena reputación, que sean de confianza o que alguien las haya recomendado. Hay que huir del comercio electrónico de desconocidos o de aquel que ofrece descuentos dudosos difíciles de creer”, recomienda.

4. **Códigos QR**. Las nuevas medidas de seguridad sanitaria han traído un cambio en la hostelería y el turismo. Hoy, los menús en los bares y restaurantes o los trípticos informativos en museos u oficinas de turismo vienen a través de códigos QR. Esta tecnología puede ser también la entrada para recibir un ataque.

Si tu negocio usa estos códigos, comprueba de forma frecuente que redirigen a la página indicada. Para los usuarios, lo recomendable es deshabilitar la apertura automática de enlaces al escanear un código QR, afirma el Incibe.

5. **Contraseña**. Aún existen personas que utilizan “1234”, “contraseña” o “iloveyou” como claves de acceso a la red o en algún dispositivo, según la firma NordPass. El Incibe recomienda crear una que sea robusta y complicada e ir cambiándola. Para ello, lo único que debe hacer es agregar varios elementos como una mayúscula o un número.
Por ejemplo, si se utiliza “murcielago” como clave de acceso, un delincuente tardará cuatro minutos en descubrir la contraseña. Si se cambia a “MuRCieLaGo” tardaría dos días y si optará por “1MuRCieLaGo” le tomaría cuatro años en descubrirla, según explican desde el Incibe.

6. **Tarjeta de crédito**. Desactivar la tarjeta después de una compra por Internet. Para máxima seguridad, recomendamos que se active la opción de compra en línea solo cuando se quiera efectuar un pago. De esta manera, habrá un mayor control de las tarjetas porque el usuario decide cuándo se pueden hacer compras con ella. Este servicio que ofrecen las entidades bancarias también permite recibir notificaciones de los pagos y denunciar compras fraudulentas.

7. **Páginas web seguras**. Asegurarse de que la dirección web del comercio es segura. El primer paso es seleccionar la URL y comprobar la validez de la dirección web. Debe buscarse el símbolo de un candado (verde o blanco) en la barra de direcciones y comprobar que la URL comienza con 'https://' o 'shttp://'.

La **s** indica que la dirección web ha sido encriptada. "Si no se detecta que empieza por HTTPS, cualquier dato que se comparta con el sitio podría ser interceptado por terceros y darle usos fraudulentos", destaca el experto del banco. Si el candado es amarillo o rojo, la recomendación es que no se compre en esa web.

8. **Wifi público**. Este tipo de conexión no requiere autentificación para activarse, permitiendo a los delincuentes el acceso directo a cualquier dispositivo no protegido en la misma Red. Esto facilita el robo de información valiosa como contraseñas de acceso, datos de tarjetas de crédito y otros detalles personales y financieros.

9. **Copias de seguridad**. Son imprescindibles. Este es un proceso mediante el cual se duplica la información existente de un soporte a otro (del ordenador a una memoria externa, por ejemplo), con el fin de poder recuperarlos en caso de fallo del primer alojamiento de los datos.

En el ámbito empresarial, la copia de seguridad es una salvaguarda para la continuidad de la compañía. La información de clientes, proveedores y los propios datos de la empresa son lo más importante. Por ello, dice el experto, hay que hacerla con regularidad. Si es posible habría que realizarla diariamente.