DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 19| Enero 2022

LA PROTECCIÓN DE DATOS COMO GARANTÍA EN LAS POLÍTICAS DE PREVENCIÓN DE ACOSO

Í N D I C E

LA PROTECCIÓN DE DATOS COMO GARANTÍA EN LAS POLÍTICAS DE PREVENCIÓN DE ACOSO

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN

La evolución de las tecnologías de la información y la comunicación y la extensión de su uso a través de los servicios y aplicaciones de Internet, como redes sociales, mensajería instantánea o correo electrónico en dispositivos *smart*, ha llevado a que se utilicen con maldad. Expresiones como ciberacoso, ciberbullying, sexting, grooming, phising, pharming o carding, que nos van resultando cada vez más familiares, son términos en inglés que identifican situaciones de acoso, amenazas, coacciones, revelación de secretos, delitos sexuales, violencia de género o estafas.

El uso de información o datos de carácter personal, junto al de las tecnologías de la información y comunicación como las que se desarrollan en Internet, puede dar lugar, aunque no seamos conscientes, a la comisión de infracciones de privacidad o delitos.

Muchas de estas conductas tienen en la utilización de información personal, sin cumplir la normativa de protección de datos, uno de sus elementos sin el cual no se hubieran producido, por ejemplo, accediendo de manera ilegítima, o cuando se utilizan o modifican datos de carácter personal que pueden perjudicar a otra persona sin su consentimiento.

De hecho, aunque muchas de las conductas que nos afecten no llegasen a constituir delito, sí que constituirían una infracción a la normativa de protección de datos. El Reglamento General de Protección de Datos (RGPD) y por consiguiente la Ley Orgánica de Protección de Datos y garantía de derechos digitales (LOPDGDD) amplía los derechos de las personas afectadas, siendo relevante el derecho de supresión (olvido) y la retirada del consentimiento.

El trabajo es un escenario donde también se producen y reproducen estas formas de violencia digital, por ello la Ley Orgánica 3/2007, para la igualdad efectiva de mujeres y hombres y el RDL 6/2019 promueve la elaboración de Planes de Igualdad y la elaboración del Protocolo de Prevención del Acoso Sexual o por razón de sexo regulado en el artículo 48 de la Ley Orgánica de Igualdad (LOI).

"MUCHAS DE ESTAS CONDUCTAS DELICTIVAS TIENEN EN LA UTILIZACIÓN DE INFORMACIÓN PERSONAL, SIN CUMPLIR LA NORMATIVA DE PROTECCIÓN DE DATOS, UNO DE SUS ELEMENTOS SIN EL CUAL NO SE HUBIERAN PRODUCIDO".

ENTRE PRIVACIDAD Y CIBERACOSO: ¿DE QUÉ ESTAMOS HABLANDO?

A modo de ejemplo, son conductas constitutivas de acoso a través de un tratamiento ilícito de datos personales:

La **grabación de imágenes** degradantes que afecten a la intimidad de los trabajadores, en particular -pero no solo- cuando estas afecten a la vida y libertad sexual de las personas

La difusión de imágenes o videos de **contenido sexual** entre los trabajadores, ya se trate del envío por quien las haya recibido de forma legítima – el llamado 'porno vengativo', o de la mera difusión en redes sociales o de comunicación (Telegram, WhatsApp) de imágenes o videos de terceras personas.

La publicación o difusión de mensajes o contenido audiovisual (imágenes,memes, etc.) que tenga por objeto menoscabar la dignidad de un trabajador y **crear un entorno hostil**, especialmente -pero no solo- cuando estos supongan insinuaciones relativas a la vida sexual del trabajador.

La publicación o difusión de **comentarios despectivos**, chistes ofensivos o demérito de la valía profesional de un trabajador en redes de mensajería instantánea o redes sociales ya tengan un carácter sexual (constitutivos de acoso sexual), ya estén relacionados con el sexo del trabajador (acoso por razón desexo) o su orientación o identidad sexual, ya tengan un carácter general (acoso laboral).

El envío de mensajes o **insinuaciones ofensivas** de carácter sexual realizadas por redes de mensajería instantánea o redes sociales.

La difusión de insultos o de **rumores falsos** empleando redes de mensajería instantánea o redes sociales.

LA CARACTERÍSTICA DE ESTE TIPO DE ACOSO ES EL USO DE INTERNET Y DE LAS SOLUCIONES TECNOLÓGICAS PARA EL ACCESO Y/O DIFUSIÓN DE CONTENIDOS, BASADOS EN DATOS PERSONALES EN FORMATO ELECTRÓNICO

¿CÓMO SE CASTIGA EL CIBERACOSO?

Las consecuencias jurídicas para un empleado que cometa estos actos pueden acarrear una serie de responsabilidades.

RESPONSABILIDAD EN MATERIA DE PROTECCIÓN DE DATOS

La difusión de datos de una persona física (en contenidos tales como imágenes, audios o vídeos que permitan identificarla), publicados en diferentes servicios de internet sin consentimiento, se considera una infracción de la normativa de protección dedatos personales. La AEPD es competente para sancionar estas conductas con multas.

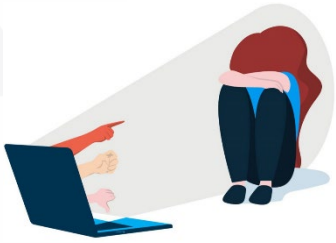
RESPONSABILIDAD EN EL ÁMBITO LABORAL

Los trabajadores que lleven a cabo estas conductas incurrirán en responsabilidad disciplinaria que, en el caso de faltas muy graves, podrá acarrear el despido. Igualmente, para el caso del personal funcionario estas conductas están tipificadas como faltas disciplinarias graves o muy graves que podrían ser sancionadas con traslados, suspensión de funciones o incluso separación del servicio.

Asimismo, la organización también podría ser sancionada vía prevención de riesgos laborales.

RESPONSABILIDAD PENAL

La difusión y la cesión a terceros de imágenes o vídeos sin consentimiento, incluso si se han obtenido con la anuencia de la persona afectada en cualquier lugar fuera de la mirada de terceros, cuando menoscaben la intimidad de una persona física, pueden ser constitutivas de diferentes delitos. Todos estos delitos contra la integridad moral, descubrimiento de secretos o incluso, de acoso sexual si fueran un medio para la obtención de favores sexuales, pueden ser castigados con penas de prisión.



RESPONSABILIDAD CIVIL

Se deberá responder por los daños y perjuicios causadosa la persona afectada, tanto los de carácter patrimonial como los de carácter moral.

LAS CONSECUENCIAS JURÍDICAS PARA UN EMPLEADO QUE COMETA ESTOS ACTOS PUEDEN ACARREAR NO SOLO RESPONSABILIDADES ADMINISTRATIVAS VÍA AEPD, SINO TAMBIÉN LABORALES (FUNCIONARIALES), PENALES Y, EN SU CASO, CIVILES.

INFORMACIÓN RELEVANTE

RECUERDA:

La Diputación de Valencia cuenta con un **protocolo** frente al acoso sexual y discriminatorio en el ámbito laboral y **canal de quejas** (véase apartado de noticias de esta boletín o intranet DIVAL).

En resumen: la protección de datos es una garantía en la prevención de acoso, siempre que recordemos también estas **prohibiciones**:

1. Conseguir los datos personales de una persona de manera ilícita, de forma engañosa y fraudulenta.
2. Utilizar los datos de carácter personal de una persona o comunicarlos a terceros sin su consentimiento, en particular si se trata de datos sensibles como la ideología, religión, creencias, origen étnico, salud, vida y orientación sexual.
3. Utilizar los datos de carácter personal de una persona para fines incompatibles para los que fueron recogidos sin contar con su consentimiento.

En todo caso, hay que tener presente:

- No utilizar la información personal de terceros en Internet, sin su consentimiento. Si se quiere utilizar hay que pedir permiso antes a su titular, diciéndole qué es lo que se va a hacer con la información.
- El que se haya obtenido información de otras personas con su consentimiento, por ejemplo, mediante fotografías o vídeos en las que aparecen, no significa que podamos hacer con esos datos personales lo que queramos.
- Lo que se publica en Internet, como fotografías, videos o audios de personas, queda fuera del control de quien lo publica.
- Todo lo que se publica en Internet deja rastro, aunque te parezca que es anónimo. La información que damos de nosotros y la que las demás personas dan de nosotros va creando una identidad digital.
- El uso de Internet puede agravar las penas de los delitos cometidos.
- Las actividades que se realizan en Internet y la información que se sube crea una huella digital.

A LA PREVENCIÓN DEL CIBERACOSO SON TAMBIÉN APLICABLES LOS CONSEJOS DE PONER EN PRÁCTICA LA "CIBERHIGIENE"

MATERIAL COMPLEMENTARIO

- La protección de datos como garantía en las políticas de prevención del acoso: recomendaciones de la AEPD. Consulta este enlace.
- Guía de Protección de Datos y prevención de delitos (AEPD). Consulta este enlace.
- Protocolo de actuación frente al acoso sexual y por razón de sexo en la AEPD. Consulta este enlace.
- Protocolo de actuación frente al acoso laboral digital en la AEPD. Consulta este enlace.
- Canal específico para comunicar, con carácter prioritario, la difusión ilegítima de imágenes sensibles (AEPD). Consulta este enlace.
- Guía de privacidad y seguridad en Internet (AEPD, INCIBE, OSI). Consulta este enlace.

NOTICIAS

- **La Diputació de València presenta su protocolo frente al acoso sexual y discriminatorio en el ámbito laboral.**
  El protocolo contempla medidas de formación, sensibilización y de protección a las víctimas de acoso, garantizando confidencialidad, diligencia y celeridad.
  Así, con el fin de desarrollar los mecanismos para eliminar cualquier comportamiento relacionado con situaciones de acoso sexual laboral que se pudiera dar en el ámbito de la corporación, la medida establece la puesta a disposición de recursos humanos y materiales para atender, tramitar y resolver quejas.
  El protocolo se encuentra a disposición en la intranet de la página web de la Diputació, junto con un díptico informativo y una solicitud de queja.
  Sigue leyendo en este enlace.

- **De 3 a 32 millones: Protección de Datos multa un 1.000% más y convierte a España en el sexto país europeo en sanciones por vulnerar el RGPD**
  2021 ha sido un año de récord para la AEPD. El organismo de control español ha propuesto 47% sanciones más que en 2020 (más de 180 frente a unas 120 en el año pasado), lo que se ha traducido en más de 32 millones de euros en sanciones, casi un 1.000% más que los 3 millones de euros que propuso en 2020.
  Consulta la noticia a través de este enlace.

- **Programa RNE: ciberseguridad y protección de datos.**
  La pandemia ha dado un impulso a la revolución digital y cada vez más esferas de nuestras vidas dependen del código binario. Esto ha planteado grandes dilemas en materia de ciberseguridad y protección de datos. Desde que en 2018 entró en vigor en la Unión Europea el RGPD, el cumplimiento de esta normativa una prioridad para las instituciones europeas. Ahora bien, ¿cómo funciona esto en los países de fuera de la Unión?
  Para esuchar el programa consulta este enlace.