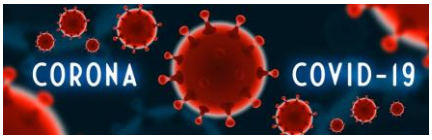
FORLOPD®
seguridad en la información



Y

LA PROTECCIÓN DE DATOS PERSONALES

Informe elaborado por el Departamento Jurídico de
SEGURIDAD Y PRIVACIDAD DE DATOS S.L.

Tabla de contenido

INTRODUCCIÓN.

La propagación del Coronavirus (en adelante, "*COVID*-19") a finales del año 2019 ha obligado al planeta entero en mayor o menor medida, a paralizar su actividad y realizar cambios drásticos en los extractos económicos y sociales de las distintas Sociedades, Territorios y Zonas Geográficas.

Un evento tan inesperado e imprevisible nos ha obligado a todos emplear medidas nuca vistas en las democracias cercanas, medidas cuyas consecuencias finales aun son desconocidas.

Sentimos que es nuestra labor participar en la disminución de los efectos negativos de estas consecuencias y pretendemos sin ser demasiado pretenciosos aportar nuestro granito de arena en la continuidad de vuestro negocio, así como, la superación exitosa de este evento tan pernicioso.

ANÁLISIS O ALCANCE.

Tal y como acabamos de indicar, como consecuencia del reciente brote de Covid-19 y la situación de Estado de Alarma en la que nos encontramos, varios de los extractos de nuestra sociedad se han visto duramente afectados.

Por todo ello, varios son los objetos del presente informe, que para una mejor comprensión, procederemos a enunciarlos en orden correlativo.

En primer lugar, el Estado de Alarma ha impuesto el cierre temporal de todos los sectores económicos no esenciales. Ante ello, algunas de las empresas obligadas al cierre de su negocio al público han encontrado una solución en la venta On-line de sus productos o la prestación de sus servicios a través de medios telemáticos. Nuestra primera labor, será determinar cuáles son las precauciones que deben adoptar, y en particular, las obligaciones legales del E- commerce.

En segundo lugar, también hay muchos sectores que han decidido prestar sus servicios de forma telemática, tales como, consultas médicas, actividades educativas, etc., e incluso han apostado por el teletrabajo. A tal efecto, prestaremos algunas recomendaciones al respecto, enfocadas a preservar la seguridad y privacidad de los datos tratados por parte de las empresas y demás profesionales.

En tercer lugar, trataremos, el ámbito laboral, donde se han aplicado medidas tendentes a la contención de la propagación del virus en los centros de trabajo, provocando nuevos tratamientos de datos de los empleados, como aquellos relacionados con su salud o el de la unidad familiar.

Por último, la extensión por todo el planeta del virus Covid-19 ha provocado un aumento de los ciberataques. También el Tele-trabajo o el acceso remoto a los dispositivos por parte de los empleados son situación que los ciberdelincuentes aprovechan para atacar.

En relación con esta situación, más adelante procederemos a realizar algunas recomendaciones para evitar o en su caso disminuir, el impacto que puedan causas los ciberataques.

Por último, debemos especificar que a pesar de que nos encontramos ante una emergencia sanitaria de alcance general,

la normativa en protección de datos, no limita o impide el tratamiento de datos se salud, sino que al contrario, lo regula de manera expresa en el Considerando (46) del R.G.P.D. donde reconoce que en situaciones excepcionales, como una epidemia, la base jurídica de los tratamientos puede ser múltiple, basada tanto en el **interés público, como en el interés vital del interesado u otra persona física.**

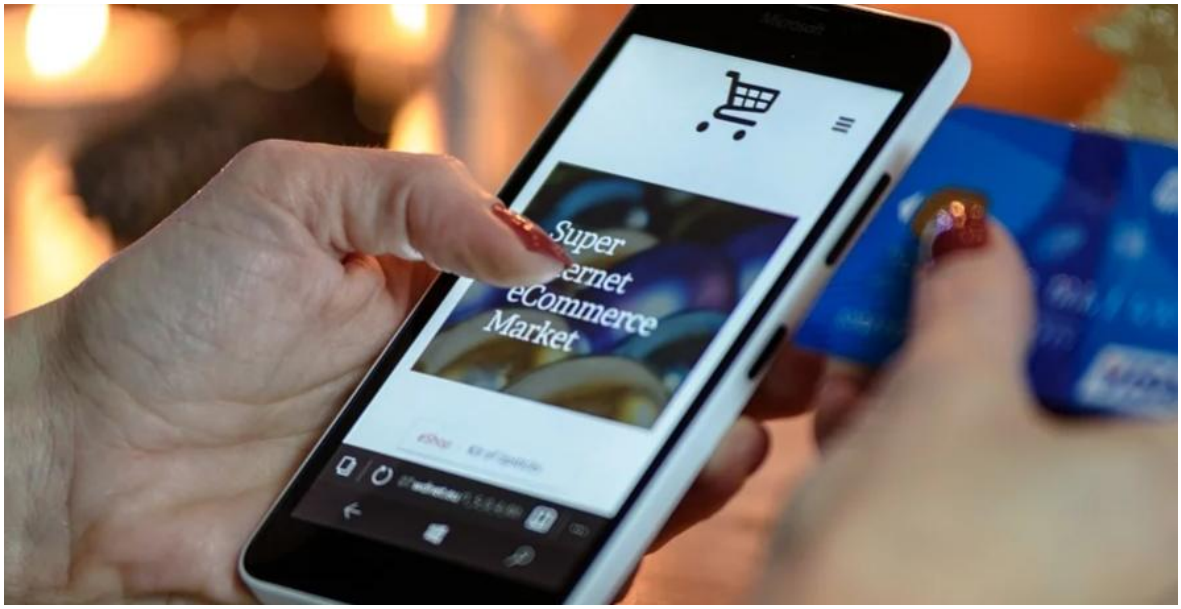
> *"El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano."*

LEGISLACIÓN

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 *(R.G.P.D.)*.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (*L.O.P.D.G.D.D.*).
- Real Decreto-ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente al COVID-19.
- Ley 34/2002 de servicios de las sociedad de la información y del comercio electrónico
- Ley de Ordenación del Comercio Minorista.
- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias
- Informe del Gabinete Jurídico de la AEPD. N/REF: 0017/2020.
- FAQ sobre el COVID-19 publicado por la AEPD.

DESARROLLO.

VENTA POR INTERNET.



El E-commerce parece cobrar especial relevancia durante el Estado de Alarma provocado por el Covid- 19, de tal forma, que la venta On-line resulta ser una medida eficaz que permite la continuidad de un negocio que de otra manera estaría obligado ya no solo a bajar su persiana, sino a suspender su actividad durante el periodo de confinamiento.

Para poder empezar a vender de esta forma, muchos se estarán preguntando por dónde empezar o cuales son las distintas obligaciones con las deben cumplir.

Pues bien, es irrelevante lo cual grande o pequeño sea tu empresa o la cantidad de productos que vayan a venderse o el tipo deservicio que desea prestarse, todos deben cumplir con las obligaciones legales.

En cuanto a la implantación de la tienda On-line hay tener en cuenta, la siguiente normativa, de la cual procederemos a informar con carácter general en las siguientes líneas:

- **Ley 34/2002 de servicios de las sociedad de la información y del comercio electrónico (LSSI).**

  Una de las normativas más importantes a las que hay que prestar especial atención es la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI), que regula determinadas obligaciones a la hora de vender por Internet.

- **Ley de Ordenación del Comercio Minorista.**

  Las tiendas On-line deben cumplir una serie de condiciones legales específicas, ya que la relación entre proveedor y cliente se realizan sin la presencia física simultánea, por lo que

los artículos que afectan especialmente a las tiendas virtuales son los correspondientes a las Ventas a Distancia.

- **Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios.**

  Básicamente, cualquier tienda virtual que venda sus productos o preste servicios a personas físicas debe cumplir con determinadas obligaciones recogidas en la normativa mencionada.

Estas son algunas de las obligaciones legales con las que hay que cumplir, si quieren vender por internet.

Ley 34/2002 de servicios de las sociedad de la información y del comercio electrónico	Deber de Información	Se aplica a empresas y profesionales que desarrollan una actividad económica de comercio electrónico por Internet y establece la necesidad de que la plataforma de ecommerce albergue en un lugar visible y accesible a cualquier usuario los datos básicos del negocio Si realizas contratos de carácter electrónico, tendrás el deber de facilitar al cliente, información referente al proceso de contratación electrónica, en los instantes anterior y posterior a la celebración del contrato
	Condiciones de uso	Las condiciones del servicio recogen los derechos y obligaciones de los clientes y usuarios y deben ser aceptadas de previa y expresamente por el usuario antes de adquirir cualquier producto o servicio de nuestra plataforma de ecommerce. De la misma forma que los datos básicos de la empresa, deben colocarse en un lugar visible y de fácil y acceso y estar redactadas de manera clara, concisa.

Ley de Ordenación del Comercio Minorista	Plazo de ejecución y pago	De no indicarse en la oferta el plazo de envío del pedido, la entrega deberá realizarse en un máximo de 30 días desde la celebración del contrato.
	Derecho de desistimiento	El comprador podrá desistir libremente del contrato, sin necesidad de alegar ninguna causa, dentro del plazo de 14 días naturales contados desde la fecha de recepción del producto. El importe ha de ser devuelto en un plazo máximo de 14 días naturales tras el desistimiento. (En caso de que esta información no aparezca expresa durante la compra el plazo de devolución se amplía a un año).
	Pago mediante tarjeta de crédito	Cuando el importe de una compra sea cargado utilizando el número de una tarjeta de crédito sin que ésta hubiese sido presentada directamente o identificada electrónicamente, su titular podrá exigir la inmediata anulación del cargo y el reabono se deberá efectuar a la mayor brevedad. En el caso de que la compra hubiese sido efectivamente realizada por el titular de la tarjeta y éste hubiese exigido indebidamente la anulación, quedará obligado frente al vendedor al resarcimiento de los daños y perjuicios ocasionados como consecuencia de dicha anulación.

Ley General para la Defensa de los Consumidores y Usuarios	Se deberá mostrar de forma clara e inequívoca el precio final del producto o servicio	En caso de que el cliente no tenga acceso al precio definitivo desde el comienzo de la transacción, podrá recuperar la diferencia entre el coste inicial y el final.
	El plazo de devolución de productos actual es de14 días naturales	En caso de que el consumidor no sea informado, el plazo podría ampliarse a 12 meses, contados desde la fecha de expiración del periodo inicial.
		Será obligatorio poner a disposición del comprador un formulario de desistimiento, común en toda Europa y que deberá ser facilitado junto con la información previa al contrato de compra
	Información hasta el último paso de la transacción o proceso de compra, de que la aceptación de la oferta obliga al pago por su parte.	
	El empresario o vendedor será el encargado de asumir los riesgos que pudiera sufrir el producto durante el transporte hasta que sea entregado al consumidor.	

En relación a este punto, otros pasos igual de importantes a tener en cuenta son:

- Registrar el nombre del dominio.
- Contratar un hosting y suscribir el contrato de acceso a datos por terceros.
- Configurar la web y su estructura, insertando los textos legales en protección de datos así como, el resto de políticas para la tienda On-line.
- Buscar una plataforma para el E-commerce y suscribir el contrato de acceso a datos por terceros.
- Insertar una pasarela de pago.
- Implantar un certificado de seguridad.

Prestación de servicios vía On-line.

Algunos de los empresarios y profesionales cuyo negocio está siendo afectado por el Covid-19 han decidido hacer uso de otros canales o medios para seguir prestando sus servicios a los clientes, alumnos, pacientes y demás usuarios. Esta fórmula está siendo utilizada por entidades del sector sanitario, realizando consultas de forma On-line, por el sector de la educación, impartiendo clases a los alumnos de forma telemática. En estos casos, no siempre están utilizando aplicación o plataformas seguras.

En estos casos, hay que prestar especial atención al tipo de canal que se ha escogido, proteger de forma adicional aquella información sensible y que revele en especial datos salud o afecte a menores o colectivos especialmente vulnerables

El cumplimiento de la normativa en protección de datos puede pasar a un segundo y tercer plano e incluso desaparecer de la lista de prioridades y preocupaciones

Desde el punto de vista legal, resulta especialmente relevante destacar el hecho de que la normativa actual en materia de protección de datos, se aplica en su integridad a pesar del Estado de Alarma. Este derecho fundamental no ha sido limitado, y tal y como establece la AEPD la en uno de sus informes “no existe razón alguna que determine la suspensión de derechos fundamentales, como es el derecho a la protección de datos, ni dicha medida ha sido adoptada.”

Por lo tanto, cualquier tipo de actuación contraria o que vulnere la normativa en protección de datos podrá ser objeto de sanción por parte de las Autoridades Competentes.

Consultas médicas/ psicológicas y demás actividades realizadas vía On-line.

En el caso de las consultas médicas o terapias, el tratamiento de datos viene legitimado por el artículo 9 del R.G.P.D. , en la letra h, siempre que el tratamiento sea necesario para realizar un diagnóstico médico, o cualquier otro tipo de asistencia de tipo sanitario o para la gestión de los sistemas y servicios de asistencia sanitaria y social.

Por otra parte, al realizar la terapia por videollamada, es recomendable utilizar Webcams, o cotejar los datos facilitados con la Base de Datos de forma que no haya duda alguna de la identidad del paciente.

En aquellos casos en que sea la primera vez que se trata al paciente y la recogida de datos se realice en la misma videollamada, se debe facilitar la información en protección de datos. Para que quede constancia de este hecho, así como del contenido de la información trasladada, es necesario enviar un correo que contenga la información en protección de datos facilitada.

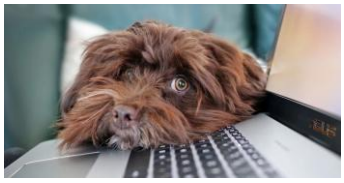
*"[…]h) el tratamiento es necesario para **fines de medicina preventiva** o laboral, evaluación de la capacidad laboral del trabajador, **diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social,** o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;[…]"*

Recomendaciones:

Algunas de las precauciones que recomendamos tomar en caso de impartir las clases de forma On-line o tratara un paciente de manera telemática o incluso hacer alguna actividad en común como clases de baile o ejercicio físico, son las siguientes:

1. Realizar las videoconferencias desde un lugar seguro, donde pueda asegurarse de que no puedan escuchar la llamada o videollamada terceros ajenos, que provoque un acceso a datos sensibles por su parte.
2. No confiar y utilizar versiones gratuitas de aplicaciones o plataformas como Skype, Team, Zoom, Youtube, etc.
3. En caso de hacer uso de estas aplicaciones, hay que leer detenidamente las políticas de privacidad y solo conceder aquellos permisos que sean estrictamente necesarios para la prestación del servicio.
4. Utilizar contraseñas fuertes, no almacenarlas, compartirlas o dejarlas expuestas a terceros.
5. **En caso de que se deba enviar información sensible por correo electrónico, tanto por parte del cliente, como por parte del profesional, por ejemplo, fotografías, informes, historial clínico, la información deberá ser cifrada.**

Tele-trabajo



El Tele-trabajo es otra solución eficaz adoptada por gran parte de las empresas a la hora de seguir adelante con su actividad. El Tele-trabajo supone que los equipos de información y comunicación son utilizados para permitir que los empleados realicen su trabajo fuera de la organización.

Para aquellas empresas que permitan a sus empleados teletrabajar, y/o extraer fuera de las instalaciones dispositivos corporativos capacees de almacenar, transferir o procesar cualquier tipo de información (portátiles, teléfonos móviles (inteligentes o no), tabletas, tarjetas de memoria, pen drives, discos duros externos, CD, DVD y cualquier otro equipo utilizado para almacenamiento, procesamiento y/o transferencia de datos), resulta primordial establecer las siguientes medidas de seguridad:

Recomendaciones:

- Implantar, publicar y difundir entre el personal laboral, la política o teletrabajo, y en su caso, la Bring Your Own Device (BYOD).
- Gestionar, controlar y documentar la entrega de sopores.
- Facilitar el acceso remoto para minimizar los daños causados por la pérdida o robo de Dispositivos corporativos.
- Cifrar la información para evitar el acceso no autorizado.
- Realizar copias de seguridad en un soporte externo.
- Establecer contraseñas robustas de bloqueo de pantalla.
- Uso de malware, uso y supervisión de cortafuegos o firewall.
- Actualización de ordenadores y dispositivos.
- Auditorías en protección de datos y seguridad de la información.
- Evaluaciones de Impacto y Análisis de Riesgos, siempre que sean necesarias.
- Formar al personal en materia de protección de datos y seguridad de la información.
- Contar con el asesoramiento de un Delegado en Protección de Datos.

RELACIONES LABORALES

Según las Autoridades, el Covid- 19 es un virus altamente contagioso que se propaga sobre todo mediante gotículas respiratorias que se producen cuando una persona infectada tose o estornuda. Este virus también permanece en diferentes superficies y objetos, que al tocarlos se pueden incorporar a las manos, lo que es potencialmente infeccioso si la persona luego con esa misma mano se toca la boca, la nariz y posiblemente los ojos.

Por todo ello, las empresas se han visto obligadas tomar medidas excepcionales dentro de los diferentes centros de trabajo con la finalidad principal de garantizar la salud de todo el personal, y evitar contagios en el seno de la empresa y/o centros de trabajo.

Estas medidas deben ser aprobadas teniendo en cuenta en todo momento las disposiciones establecidas tanto por la normativa de trabajo y prevención de riesgos laborales como la normativa de protección de datos (R.G.P.D. y L.O.P.D.G.D.D.).

Algunos de los tratamientos de datos de los trabajadores realizados por parte de las empresas, pueden ampararse en lo dispuesto en el artículo 9.2 R.G.P.D. en tanto que resulten necesarios para el cumplimiento de obligaciones y el ejercicio de derechos específicos del empleador o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social.

En este caso, el empleador está sujeto o a la normativa de prevención de riesgos laborales (Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales) y en virtud del artículo 14 del mismo cuerpo legal, el empresario tiene el deber de proteger a los trabajadores frente a los riesgos laborales, para lo cual el empresario deberá garantizar la seguridad y salud de todos los trabajadores a su servicio en los aspectos relacionados con el trabajo.

Para poder determinar los planes de actuación, hay que tener en cuenta las directrices publicadas recientemente en esta materia por nuestra Autoridad de Control (A.E.P.D.).

En concreto, la empresas y demás organizaciones están legitimadas para tratar de acuerdo con dicha normativa y con las garantías que dichas normas establecen, los datos necesarios para garantizar la salud de los trabajadores.

No obstante, dichas medidas deberán aplicarse teniendo en cuenta los principios de licitud, lealtad y transparencia, limitación de la finalidad, principio de exactitud, y el principio de minimización de datos.

Sobre esto último, los datos tratados deben ser los necesarios para garantizar la salud de los trabajadores, sin que las organizaciones o los responsables designados puedan extender dicho tratamiento a otros datos personales no estrictamente necesarios para conseguir dicho fin. Por ejemplo, preguntar sobre síntomas no relacionados con el virus, o acerca de otras enfermedades.

Del mismo modo, el conocimiento de dicha información, por ejemplo, si el trabajador ha contraído el virus, o tiene síntomas, debe centrarse exclusivamente en aquellas personas responsables en la organización de adoptar e implantar las medidas der seguridad, sin que se releve la identidad de los afectados cuando ya se hayan adoptado otras medidas más eficaces para prevenir el contagio de la organización y/o centros de trabajo.

A continuación, procedemos a exponer algunas dudas relacionadas con el protocolo de actuación por parte de la empresa respecto de los datos de salud del personal para la prevención y contención del virus Covid- 19.

- **¿Puede la empresa preguntar a los empleados si estos o sus familiares presentan sintomatología relacionada con el Covid- 19?**

  Sí. Aunque en todo caso, de conformidad con lo indicado anteriormente, la empresa y/o el personal autorizado por esta, deberá limitarse a indagar sobre la existencia de síntomas del Covid-19, o si la persona trabajadora ha sido diagnosticada como contagiada, o sujeto en cuarentena.

- **¿Puede la empresa preguntar si las personas trabajadoras y visitantes ajenos a la empresa han visitado recientemente países afectados por el Covid?**

  Sí. Aunque en línea con lo que venimos diciendo, la información deberá ser proporcionada y limitarse exclusivamente a preguntar por visitas a zonas de alta prevalencia del virus en las últimas 2 semanas.

- **¿En caso de que presente síntomas, o uno de los miembros de la unidad familiar haya sido contagiado, el trabajador está obligado a informar a la empresa sobre ello?**

  Sí. Es muy necesario que el trabajador informe a la entidad o al personal autorizado, sobre esta circunstancia, para tomar las precauciones necesarias con el resto de compañeros que han estado en contacto con el empleado afectado por el virus.

- **¿El personal de seguridad puede tomar la temperatura a los trabajadores con el fin de detectar posibles casos de coronavirus?**

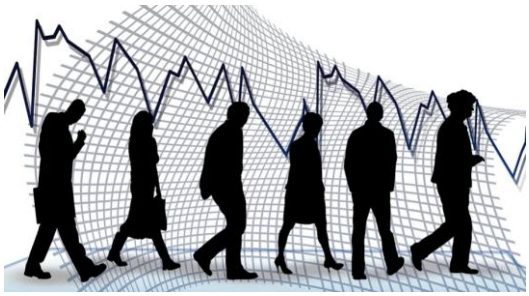
  Sí, pero el tratamiento de los datos obtenidos a partir de las tomas de temperatura debe hacerse respetando la normativa de protección de datos y, por ello debe obedecer a la

finalidad específica de contener la propagación del coronavirus, y no extenderse a otras distintas.

Recomendaciones:

1. No realizar cuestionarios de salud extensos y detallados, o que incluyan preguntas no relacionadas con la enfermedad al personal.
2. Mantener el más estricto secreto sobre la información trasladada por parte de los trabajadores afectados, así como, sobre aquella información recopilada a través de las medidas aplicadas.
3. En caso de externalizar el servicio de control de la temperatura del personal, firmar el contrato de acceso a datos con el tercero.
4. Vigilar que los trabajadores autorizados a recabar esta información hayan suscrito el deber de confidencialidad. También sería correcto hacer especial hincapié y recordar dicha obligación.

ERTES y cesión de datos al SEPE.



Respecto de los expedientes de regulación temporal de empleo (**ERTE**), el tratamiento de datos consistente en la comunicación de estos por parte del empleador empresario al SEPE está justificada.

Si bien la gestión de estos trámites correspondía en un primer momento a la empresa y al trabajador de forma conjunta, debido al elevado volumen de ERTES que se han producido hasta la fecha, el SEPE publicó en su web un aviso mediante el cual estableció que dicho trámite deberá ser efectuado en todo caso por parte de las empresas http://www.sepe.es/HomeSepe

Por ello, dichos trámites efectuados por las empresas no se realizan sobre la base del consentimiento del trabajador.

Sin perjuicio de lo anterior, si los empleadores o el personal autorizado, recaban datos diferentes a los recopilados inicialmente por parte de la empresa para la ejecución del contrato laboral, como por ejemplo, correo electrónico personal, si sería necesario informar previamente sobre ello a los empleados. **También hay que tener en cuenta, la instrucción provisional publicada por parte del Ministerio de Trabajo y de Economía Social, donde establece la necesidad de suscribir una declaración responsable por parte de la empresa donde conste haber obtenido la autorización de los trabajadores para el reconocimiento de la prestación contributiva por desempleo y la presentación de los empleados afectados para presentar en su nombre la solicitud.**

ÁMBITO DE LA CIBERSEGURIDAD.

Desde el Instituto Nacional de Ciberseguridad se han facilitado algunas recomendaciones para protegerse ante el elevado número de ataques cibernéticos que se están produciendo como consecuencia de la expansión del Coronavirus. A tal efecto, se recomienda:

- Formar a los empleados.
- Utilizar contraseñas complicadas.
- Mantener el software actualizado.
- Cerrar sesión siempre.
- Realizar copias de seguridad.
- Utilizar Protocolo HTTPs.
- Contar con medidas de seguridad actualizadas para tele-trabajar.
- Utilizar distintos métodos de autenticación.
- Establecer comunicaciones seguras mediante email.

DERECHOS DE LOS CONSUMIDORES Y USUARIOS, DURANTE EL ESTADO DE ALARMA POR EL CORONAVIRUS.

Para poder salvaguardar la salud de los consumidores y usuarios, así como, garantizar la efectividad de sus derechos, en el Real Decreto-ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente al COVID-19 se han establecido medida tendente a conseguir la protección de este colectivo.

Derecho de desistimiento / devolución de pedido.

A tal efecto, los consumidores y usuarios podrán ejercer el derecho a resolver el contrato, es decir, desistir de su compra, durante un plazo de 14 días. No obstante, en consonancia con la interrupción de plazos procesales y administrativos, el Ejecutivo también suspendió **el plazo legal de devoluciones para que los consumidores puedan ejercer sus derechos** sin quebrantar el Estado de Alarma.

En tal caso, el plazo que se da a los clientes para devolver sus pedidos será reanudado en el momento en el que el Estado de Alarma pierda su vigencia.

Contratos con consumidores.

Respecto de los contratos de tracto sucesivo, también se ha visto paralizado el cobro de nuevas cuotas hasta que el servicio pueda volver a prestarse con normalidad; no obstante, en este caso, el contrato no queda rescindido.

En el caso de los servicios que incluyan a varios proveedores, como por ejemplo, los viajes combinados, el consumidor o usuario podrá:

- Optar por solicitar el reembolso, o bien,
- Hacer uso del bono que le entregará el organizador o, en su caso, el minorista.

Se establece un plazo mínimo para utilizar el abono en un año desde la conclusión del Estado de Alarma. En caso de que el consumidor no haga uso del mismo en este plazo, podrá ejercer el derecho de reembolso.

Otras medidas de protección.

En el ámbito de la ordenación del juego, para proteger a los menores de edad, adultos jóvenes o personas con trastornos de juego, especialmente en esta situación de confinamiento, se han limitado las comunicaciones comerciales realizadas por los operadores de juego de ámbito estatal. Esta limitación, también afecta a los juegos de lotería.

Otro ámbito importante a destacar es la gran desinformación que está generando entre estos colectivos, la rápida difusión de bulos a través de las Redes Sociales.

Hace pocos días, la Policía Nacional presentó la primera guía para evitar ser manipulados por las fake news.

Para que los ciudadanos puedan identificar los bulos que circulan por internet, se recomienda:

- **Conoce la fuente de la noticia**: "googlear" el contenido publicado, fijándose en las cuentas o perfiles que han difundido la noticia, así como la fecha de la publicación.
- **Contrasta la noticia:** acudir a otros medios para cotejar la veracidad de la información.
- **Hay que prestar atención a las imágenes** dado que pueden utilizarse programas de retoque fotográfico y edición para crear fake news.

Por último, las consumidores y usuarios pueden verse muy afectados por el crecimiento de los ciberdelitos.

La situación de miedo pude ser utilizada como arma a favor por parte de los delincuentes. Por ello, las Autoridades Públicas recomiendan extremar las precauciones a la hora de comprar en internet, así como, no confiar en remitentes desconocidos o correo sospechosos.

Resulta especialmente importante saber que mientras dure el Estado de Alarma, los ciberdelincuentes aprovecharán para lanzar ataques de phishing y de todo tipo para sacar provecho y hacerse con información valiosa de losciudadanos.

El modo operandi de los ciberdelincuentes se basa en la suplantación de organizaciones legítimas con información relevante sobre el COVID-19. Lo han hecho a lo largo de estas semanas con el Ministerio de Sanidad, una Consejería de Sanidad de una Comunidad Autónoma, Fuerzas del Orden, Organizaciones Internacionales, simulando prestar ayuda y consejo, o incluso fingiendo ser la empresa para la que se trabaja.

Los canales que pueden utilizar para captar los datos de los ciudadanos, y descargar virus en los dispositivos tecnológicos, es la mensajería instantánea como WhatsApp o Telegram o el correo electrónico. En la gran mayoría de los casos, suelen pedir abrir un archivo con urgencia o seguir un enlace de internet para obtener la información.

Estas son algunas de las recomendaciones realizadas por parte de la Agencia Española de Protección para evitar caer en las trampas de los ciberdelincuentes:

- Acudir a fuentes oficiales y confiables en busca de información, accediendo directamente a las webs de las instituciones o medios de comunicación, nunca mediante un enlace proporcionado en un mensaje o en un email.

- Verificar la dirección de correo electrónico remitente del mensaje y también el enlace web al que te remite. En muchos casos, los ciberdelincuentes son capaces de crear enlaces que se parecen mucho a las direcciones legítimas de las entidades u organizaciones suplantadas.
- No facilitar datos personales a través de webs a las que se ha llegado siguiendo un enlace contenido en un mensaje o correo electrónico.
- Desconfiar de mensajes con faltas de ortografía, errores gramaticales y saludos genéricos sin aportar ningún dato como: "Estimado ciudadano" o "Estimado paciente".
- Desconfiar de correos cuyo contenido establezca como urgente la realización de cualquier tipo de acción.

CONCLUSIÓN.

Tanto el ámbito empresarial como el resto de ciudadanos se han visto durante afectados por esta situación de emergencia sanitaria.

No obstante, es preciso tener en cuenta que, en el exclusivo ámbito de la normativa de protección de datos personales, que la actual normativa sigue vigente y permite adoptar a las organizaciones todo tipo de decisiones que sean necesarias para salvaguardar los intereses vitales de las personas físicas, así como, cumplir con las obligaciones legales o salvaguardar los intereses esenciales en el ámbito de la salud pública, todo ello, siempre de conformidad con la normativa sectorial.

Es importante aprender de esta situación y mejorar la respuesta por parte de todos los estamentos de la sociedad ante estos tipos de incidentes. En especial, los grandes motores de la economía, deben:

- Estar preparados y protegidos para que ante una situación como esta, los trabajadores puedan, por ejemplo, Tele-trabajar.
- Velar para que la venta o producción no se paralice o no se vea afectada en su totalidad contando con una tienda On-line.
- Reforzar el ámbito IT contratando servicios de ciberseguridad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- También resulta especialmente conveniente las empresas y demás instituciones cuenten con la Certificación de la ISO 27001 e implanten de planes de recuperación ante desastres.

Dpto. Jurídico. de