Cómo afecta la ciberseguridad a los derechos laborales de las personas empleadas y sindicatos. Comentario a la Sentencia del Tribunal Supremo 1033/2020, de 25 de noviembre

Ana Belén Muñoz Ruiz

Profesora titular visitante de Derecho del Trabajo y de la Seguridad Social.
Universidad Carlos III de Madrid
abmunoz@der-pr.uc3m.es | https://orcid.org/0000-0002-8863-9938

Extracto

El puesto de trabajo de las personas trabajadoras es clave desde el punto de vista de la seguridad de la información. La ciberseguridad es un problema creciente en las empresas, y de ahí la necesidad de adoptar medidas de seguridad que protejan los datos de carácter personal de las personas clientes y de las empleadas. En ocasiones, estas medidas pueden colisionar con derechos laborales individuales y colectivos. En el presente trabajo, se analiza el conflicto entre la seguridad de la información y protección de datos y el derecho de la representación sindical a utilizar el móvil y entregar información sindical en papel en las mesas de trabajo de las personas trabajadoras. En el análisis se propone una aproximación que va más allá del caso concreto y se plantean problemas emergentes tales como la parquedad del marco regulador de los deberes digitales de las personas empleadas y el papel de la negociación colectiva en esta materia.

Palabras clave: información; ciberseguridad; sindicatos; persona trabajadora; protección de datos de carácter personal; derecho de libertad sindical.

Fecha de entrada: 04-05-2021 / Fecha de aceptación: 05-05-2021

Cómo citar: Muñoz Ruiz, Ana Belén. (2021). Cómo afecta la ciberseguridad a los derechos laborales de las personas empleadas y sindicatos. Comentario a la Sentencia del Tribunal Supremo 1033/2020, de 25 de noviembre. *Revista de Trabajo y Seguridad Social. CEF*, *459*, 207-219.

How the cybersecurity affects the employees' rights and trade union. Commentary on Supreme Court ruling 1033/2020, of November 25

Ana Belén Muñoz Ruiz

Abstract

The workplace of the workers is very relevant from the point of view of information security. Cybersecurity is a growing problem in companies and hence the need to adopt security measures that protect the personal data of customers as well as employees. Sometimes there are conflicts between the security measures and employees rights and unions. The paper analyses the conflict between information security and data protection and the right of union representatives to use their mobile phones and deliver union information on paper to employee worktables. The study proposes to carry out an approach that goes beyond the specific case and raises emerging problems such as the limited regulatory framework of the digital duties of employees and the role of collective agreements in this matter.

Keywords: information; cybersecurity; trade unions; employee; personal data protection; trade union freedom.

Citation: Muñoz Ruiz, Ana Belén. (2021). How the cybersecurity affects the employees' rights and trade union. Commentary on Supreme Court ruling 1033/2020, of November 25. *Revista de Trabajo y Seguridad Social. CEF*, *459*, 207-219.

Sumario

El conocimiento es poder.

Francis Bacon

1. Introducción

El desarrollo tecnológico que estamos experimentando nos anima a recordar la reflexión de Francis Bacon cuando afirmó que, en todas las épocas, los datos y la información son poder, pero también constituyen una amenaza (Capítulo Español de Internet Society, 2021). En este punto, surge la ciberseguridad, que se define como aquellos conjuntos de técnicas y métodos para proteger de ataques a equipos y programas informáticos y a redes de comunicación. El tema de la ciberseguridad se plantea en la Sentencia del Tribunal Supremo (TS) 1033/2020, de 25 de noviembre; de ahí que resulte especialmente interesante su análisis. La cuestión controvertida es la limitación del derecho fundamental de libertad sindical al prohibir a la representación sindical de una de las empresas del sector del *telemarketing* el uso del teléfono móvil y la distribución de información sindical (en papel) en la plataforma o sala de operaciones.

El argumento empresarial para restringir el derecho sindical es la protección de los datos y seguridad de la información. Las personas empleadas de la empresa realizan operaciones de venta telefónica y «atención al cliente» accediendo a datos reservados de las personas clientes y usuarias del servicio (datos personales; datos de tarjetas de crédito o débito; información financiera; datos de campañas; información o documentación sobre procedimientos/procesos, estrategia o campañas; material de formación; información confidencial de negocio; contraseñas de acceso y documentación, procedimientos y política de la compañía), de cuya seguridad es responsable la empresa.

2. La ciberseguridad como un problema creciente en las empresas

El puesto de trabajo es un aspecto clave desde el punto de vista de la seguridad de la información. Como parte de las tareas cotidianas, cualquier persona trabajadora requiere acceder a diversos sistemas y manipular diferentes tipos de información. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), define, de un modo amplio, las «violaciones

de seguridad de los datos personales» (en adelante, brecha de seguridad) como «todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos» (art. 4.12 RGPD)[1]. Como puede observarse, son incidentes de seguridad informativa que repercuten en la confidencialidad, integridad o disponibilidad de la información (Molina Navarrete, 2021).

Las violaciones de seguridad pueden suponer sanciones económicas de elevada cuantía para las empresas. Por ello, es necesario aplicar un conjunto de medidas de seguridad que garanticen que la información, tanto en soporte papel como en formato electrónico, está correctamente protegida. Al respecto, la empresa del sector del *telemarketing* había publicado unos protocolos de seguridad, en los que se contenía una instrucción sobre «escritorios limpios», que comportaba la prohibición de introducir en las plataformas bolsos, mochilas, abrigos, USB, móviles, dispositivos de memoria externa, *software* de intercambio de ficheros, *software* de mensajería instantánea, PDA, cámaras digitales, papel y bolígrafos. El objetivo era prevenir ciberataques que pusieran en riesgo los datos de la clientela.

Según los datos del primer trimestre de 2021 de la Agencia Española de Protección de Datos (AEPD) (*vid.* tabla 1), de los registros de las brechas de seguridad se extrae un dato revelador: el 36,16 % de las personas afectadas por estas violaciones son las personas clientes de las empresas. Lo que confirma la tesis según la cual la información de dichas personas constituye un valor a preservar por parte de las empresas.

Tabla 1. **Personas afectadas por brechas de seguridad durante el primer trimestre de 2021**

Personas afectadas	Total
Clientes/as	36,16 %
Estudiantes	2,56 %

[1] En caso de violación de la seguridad de los datos personales, la persona responsable del tratamiento debe notificar a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, la persona responsable del tratamiento debe comunicarlo a la interesada sin dilación indebida (arts. 33 y 34 RGPD).

Personas afectadas	Total
Usuarios/as	9,44 %
Pacientes	4,16 %
Empleados/as	28,64 %
Suscriptores/as	0,64 %
Menores	2,4 %
Otras	16 %

Fuente: elaboración propia a partir de datos de la AEPD.

El otro colectivo también especialmente afectado son las personas empleadas de la empresa, cuya afectación se cifra en 28,64 %. Este dato no resulta extraño si se tiene en cuenta el volumen de datos de las personas trabajadoras que manejan las empresas para la gestión de las obligaciones laborales (formalización del contrato de trabajo, pago de salario, registro de jornada, etc.). De ahí que sea muy aconsejable que las políticas de seguridad de la información de las empresas tengan como destinatarios a ambos colectivos: las personas clientes y las trabajadoras.

Para comprender el alcance de la problemática, es preciso aproximarse a la tipología y frecuencia de los medios utilizados para llevar a cabo las violaciones de seguridad. Al respecto, sirve de muestra el análisis realizado por la AEPD durante el primer trimestre de 2021, que se describe en la tabla 2.

Tabla 2. **Medios utilizados para la violación de seguridad durante el primer trimestre de 2021**

Medios	Total
Dispositivo perdido/robado	2,72 %
Documentación perdida/robada	4,51 %
Correo perdido	2,72 %
Hacking	17,6 %

Medios	Total
Malware	44 %
Phishing	5,64 %
Eliminación incorrecta de datos	0 %
Datos personales residuales	0 %
Datos personales mostrados	4 %
Publicación no intencionada	2 %
Revelación verbal	0,3 %
Datos personales enviados	5 %
Otros	11,51 %

Fuente: elaboración propia a partir de datos de la AEPD.

Según los datos consultados, las brechas de seguridad causadas por *malware* son reiteradas, ya que representan el 44 %. Bajo este término cabe entender todo tipo de programas con fines maliciosos que persiguen robar información, hacerse con credenciales de acceso, aprovecharse de los recursos informáticos, abrir puertas traseras para la entrada de otro *malware*, controlar remotamente los equipos para diseminar otro *malware* o lanzar otros ciberataques, extorsionar tras el cifrado de información o para difundirla, etc. Sería conveniente conocer las vías de entrada más frecuentes, como la ingeniería social o los equipos no actualizados o con fallos en su instalación (Instituto Nacional de Ciberseguridad –Incibe–, 2021).

El segundo de los problemas identificados es el *hacking*, que también tiene una posición destacada con un porcentaje del 17,6 %[2]. El perfil del/de la *hacker*, también denominado pirata informático según la RAE, ha cambiado, porque no opera por ocio, sino que

[2] Las técnicas de *hacking* son variadas: i) *Spoofing* (suplantación de la identidad); ii) *Sniffing* (capturar el tráfico que circula por una red); iii) *Man in the middle* (interceptar la comunicación entre dos interlocutores/as y monitorizar esa información o alterar los datos); iv) *Malware* (programas con fines maliciosos); v) Denegación de servicio (interrumpir el funcionamiento de una página web); vi) Ingeniería social (obtener información confidencial de personas o empresas con fines perjudiciales); vii) *Phishing* (tipo de ingeniería social que consiste en suplantación de identidades para obtener información confidencial de un usuario/a); viii) Otros ataques (orientados a aplicaciones web).

causa más daño a las empresas y entidades públicas. Una muestra de ello se observa en el procedimiento número E/08399/2020 resuelto por la AEPD, donde una empresa puso de manifiesto que había recibido un correo electrónico de un *hacker* en el que se le informaba que disponía de una relación de 500.000 personas usuarias y contraseñas de las cuentas de la empresa, exigiendo un pago para no publicar este contenido en la *dark web* y proceder a informar a dichas personas usuarias de estos hechos utilizando el *e-mail* que obraba en su poder. La empresa solicitó evidencias y el *hacker* le facilitó un listado con 30.000 *e-mails* de usuarios/as de la compañía[3].

Se debe prestar también atención al *phishing*, que es una amenaza incipiente en la medida en que ha sido el medio empleado en la violación de seguridad en el 5,64 % de los casos identificados. El término *phishing* viene del inglés *fishing*, que significa pescar, pero no se refiere a pescar peces, sino datos personales (nombres de usuario/a, contraseñas o datos de cuentas bancarias). Este incidente tiene dos facetas: la empresa o las personas empleadas pueden recibir un correo electrónico, una llamada telefónica o un mensaje SMS, que en realidad es un timo, con el que se intenta robar los datos personales, es decir, ser los «pescados»; o la web de la empresa puede ser atacada para suplantar a otra y enviar correos de *phishing* con los que robar datos personales de personas clientes de la entidad suplantada, es decir, ser «la caña del pescador» (Incibe, 2017).

3. Cómo la protección de los datos y seguridad de la información podrían limitar el derecho de libertad sindical en la empresa

La empresa del sector del *telemarketing* había sido objeto de sustracción de datos que desencadenó sanciones económicas impuestas por la AEPD. De ahí que adoptara la política de escritorios limpios que, por cierto, es una práctica muy consolidada en el sector del *telemarketing*.

El TS en la Sentencia de 25 de noviembre de 2020 confirma el fallo de la Audiencia Nacional (AN) de 15 de noviembre de 2018 (proc. núm. 187/2018), declarando, en primer lugar, que es conforme a derecho la prohibición del uso del teléfono móvil en la sala de trabajo también para la representación de las personas trabajadoras. En segundo término, ambos tribunales consideran desproporcionada la prohibición de distribuir información con contenido sindical (en papel) en las mesas de trabajo de las personas empleadas.

[3] En el presente caso, la AEPD concluyó que hubo una brecha de seguridad de datos personales, categorizada como brecha de confidencialidad, como consecuencia del acceso indebido por terceras personas ajenas a la base de datos de la empresa. Ahora bien, de las actuaciones de investigación se desprendió que la empresa disponía de razonables medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias y acordes con el nivel de riesgo.

Se explica en las sentencias analizadas (AN y TS) que la utilización del móvil por la representación sindical en las plataformas comporta un riesgo objetivo para la seguridad de los datos, que pueden fotografiarse con graves consecuencias para la empresa, especialmente si se difunden externamente. Al respecto, la AN explica que:

> La sala, como adelantamos más arriba, comparte la preocupación de la empresa sobre la seguridad de sus datos, que no es baladí ni caprichosa, puesto que ya se han producido problemas significativos. Por ello, consideramos razonable que la empresa haya prohibido la utilización de móviles entre sus trabajadores, puesto que es imposible controlar todas las terminales en todo momento, con el consiguiente riesgo de que se utilicen los móviles para fotografiar información sobre datos relevantes, sin que dicha restricción lesione el derecho de comunicación de los trabajadores, siempre que la empresa despliegue los teléfonos suficientes para que los trabajadores puedan comunicarse ante situaciones de necesidad, lo cual se ha demostrado.

Lo que supone reconocer que la empresa tiene prerrogativas para no autorizar a la representación sindical el uso de móviles en el centro de trabajo por motivos de seguridad razonables. Ahora bien, esta prohibición no debe perjudicar la comunicación de la representación de las personas trabajadoras con sus sindicatos o personal asesor.

En cambio, a juicio de las dos sentencias referenciadas, la prohibición de distribuir información sindical en papel en la sala de operaciones se considera desproporcionada. Las razones principales de esta conclusión son el carácter unilateral de la decisión y la prueba realizada que se considera insuficiente en el sentido de que no se ha acreditado que la introducción de los mencionados comunicados constituyera una amenaza exorbitante para la seguridad de los datos, ya que lo desmiente sobradamente la experiencia del centro de Sevilla, y escapa de qué modo ese papel puede utilizarse torcidamente en una empresa con un sistema de seguridad insuperable[4].

El primero de los argumentos –la falta de acuerdo entre la empresa y los sindicatos– podría considerarse débil si se toma en consideración el convenio colectivo de aplicación. En concreto, el artículo 75 del II Convenio colectivo de ámbito estatal del sector de *contact center* (antes *telemarketing*) –BOE de 12 de julio de 2017– regula el derecho de información de la representación de las personas trabajadoras, indicando:

[4] El sistema de seguridad de la empresa se basa en el establecimiento de las siguientes medidas: «"usuarios de la información"; "managers y equipos de supervisión", que aseguran el cumplimiento por los usuarios de las políticas de seguridad, al igual que los "propietarios de la información", asistidos por los "custodios de la información", "responsables de seguridad", "técnicos de formación", "coordinadores de seguridad y prevención del fraude" y "analistas de seguridad", cuyas funciones concretas se definen en los protocolos de seguridad, que tenemos por reproducidos, orientadas, todas ellas, a garantizar la seguridad de los datos personales, gestionados por la compañía».

> Las empresas pondrán a disposición de la representación unitaria de los trabajadores, y de cada una de las secciones sindicales legalmente constituidas, un tablón de anuncios en cada centro de trabajo –plataformas externas o internas–, que les permita exponer en lugar idóneo, de fácil visibilidad y acceso, propaganda y comunicados de tipo sindical y laboral. Fuera de dichos tablones queda prohibida la fijación de los citados comunicados y propaganda.

Tras la lectura de este precepto, se podría debatir si el medio pactado de comunicación de información sindical es el tablón de anuncios y, por tanto, la política de mesas limpias podría estar justificada en la medida en que ha sido acordada con los sindicatos firmantes del convenio colectivo (UGT y CC. OO.). Si bien el conflicto colectivo fue promovido por CGT, parece que hay una norma consensuada al respecto de las herramientas de uso sindical en las empresas del sector.

En cambio, el segundo argumento parece más sólido, ya que no se ha acreditado que haya resultado vulnerado el sistema de seguridad de la empresa ni los datos personales de alguna persona cliente o usuaria por permitir en el centro de la empresa la difusión de información o comunicados sindicales en formato papel, lo que sirve de argumento suplementario a todo lo razonado. Añade el TS que no parece una medida de seguridad el prohibir los comunicados e información sindicales en papel, pues no se vislumbra en qué puede afectar a la seguridad de los datos personales almacenados en la empresa, ya que la simple introducción de dichos informes o comunicados, sin posibilidad de consignar o escribir nada en el papel, dado que están prohibidos los bolígrafos u otro medio de escritura, resulta una acción inocua, por lo que la prohibición no es una medida idónea. Se expresa también la alegación de la sustitución en el sentido de que la empresa no ha facilitado a la representación de las personas trabajadoras un sistema digital fiable, eficaz y seguro para que puedan repartir comunicados e información sindical a dichas personas trabajadoras.

Consiguientemente, se declara el derecho de la representación de las personas empleadas a distribuir en los puestos de trabajo información sindical en papel, siempre que se notifique a la empresa y no se disturbe la actividad normal del trabajo.

4. Sabemos cuáles son los derechos digitales de las personas empleadas: ¿y los deberes?

Si bien el debate en las sentencias analizadas gira en torno al derecho fundamental de libertad sindical, se expresan algunas ideas sobre la afectación de los derechos individuales de las personas trabajadoras que merecen un breve análisis. En concreto, se menciona que la empresa ha publicado un procedimiento sancionador en el que se tipifican como faltas las conductas que comportan incumplimiento de su política de escritorios limpios. Al hilo de esta afirmación, cabe preguntarse si en verdad existe claridad sobre el contenido y

alcance de los deberes digitales de las personas empleadas que manejan un volumen considerable de datos de carácter personal de clientes/as e información sensible de la empresa.

Conviene recordar que los derechos digitales de las personas empleadas (teletrabajo, derecho a la desconexión, intimidad y protección de datos, etc.) aparecen mencionados en la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (Muñoz Ruiz, 2021). La cuestión que surge aquí es dónde están recogidas las obligaciones de las personas trabajadoras. Un repaso al Estatuto de los Trabajadores (ET) nos permite concluir que las referencias son prácticamente inexistentes en la medida en que el artículo 5 del ET (deberes de las personas empleadas) se refiere a las obligaciones concretas del puesto de trabajo, medidas de prevención de riesgos laborales, órdenes e instrucciones de la empresa, no concurrencia desleal y cuantos otros se deriven del contrato de trabajo.

Por el contrario, la regulación del trabajo a distancia sienta las bases de los deberes digitales de las personas empleadas, si bien se refiere solo a las personas en régimen de teletrabajo. En efecto, en el Real Decreto-Ley 28/2020, de 22 de septiembre, de trabajo a distancia, se menciona en varias ocasiones la brecha de seguridad y el riesgo que supone para las empresas en el preámbulo[5] y en su articulado (arts. 7 y 20). En concreto, constituyen contenido mínimo del acuerdo de trabajo a distancia las instrucciones dictadas por la empresa, previa información a la representación legal de las personas trabajadoras, sobre seguridad de la información, específicamente aplicables en el trabajo a distancia (art. 7 k). Dichas instrucciones son obligatorias para las personas trabajadoras, tal y como explica el artículo 20 en los números 1 y 2:

> Artículo 20. Protección de datos y seguridad de la información.
>
> 1. Las personas trabajadoras, en el desarrollo del trabajo a distancia, deberán cumplir las instrucciones que haya establecido la empresa en el marco de la legislación sobre protección de datos, previa participación de la representación legal de las personas trabajadoras.

[5] Las referencias encontradas a la brecha de seguridad en el preámbulo de la normativa de teletrabajo son:

1. «Sin embargo, también presenta posibles inconvenientes: protección de datos, brechas de seguridad […]» (apdo. III);
2. «Asimismo, se entiende necesario establecer en la medida precisa las facultades de control y organización que corresponden a la empresa, para garantizar un uso y conservación adecuados de los equipamientos entregados, las limitaciones de uso personal de los equipos y conexiones, el cumplimiento por la persona trabajadora de sus obligaciones y deberes laborales y las instrucciones necesarias para preservar a la empresa frente a posibles brechas de seguridad» (apdo. IV);
3. «En su capítulo IV, el real decreto-ley se refiere de manera específica a las facultades de organización, dirección y control empresarial en el trabajo a distancia, incluyendo la protección de datos y seguridad de la información, el cumplimiento por la persona trabajadora de sus obligaciones y deberes laborales y las instrucciones necesarias para preservar a la empresa frente a posibles brechas de seguridad» (apdo. VI).

> 2. Las personas trabajadoras deberán cumplir las instrucciones sobre seguridad de la información específicamente fijadas por la empresa, previa información a su representación legal, en el ámbito del trabajo a distancia.

Es aconsejable que las empresas adopten una política de protección de la información para situación de movilidad siguiendo las Recomendaciones de abril de 2020 para proteger los datos personales en situaciones de movilidad y teletrabajo adoptadas por la AEPD. Dicha política debe contemplar las necesidades concretas y los riesgos particulares introducidos por el acceso a los recursos corporativos desde espacios que no están bajo el control de la organización. El informe BP/18, Recomendaciones de seguridad de situaciones de teletrabajo y refuerzo en vigilancia, publicado en abril de 2020 por el Centro Criptológico Nacional (CCN-CERT), adscrito al Centro Nacional de Inteligencia (CNI), incluye controles y medidas de seguridad específicas a tener en cuenta durante una situación de trabajo en remoto, así como una relación de empresas que operan en nuestro país en el sector de la ciberseguridad y que ofrecen servicios y soluciones en el contexto de accesos remotos a los recursos corporativos.

Más allá de la regulación del teletrabajo, sería deseable que hubiera una modificación del artículo 5 del ET en el sentido de incluir los deberes digitales de las personas empleadas, así como sería muy recomendable que la negociación colectiva entre a regular estos deberes y las consecuencias de su incumplimiento. En el caso concreto de la empresa de *telemarketing*, de la lectura del régimen sancionador del convenio colectivo de aplicación a la empresa se podría interpretar como incluido en dicho precepto el incumplimiento del deber de protección de datos y seguridad de la información por parte de las personas empleadas, pero quedan algunas dudas. En este sentido, el II Convenio colectivo de ámbito estatal del sector de *contact center*, en su artículo 67, tipifica como faltas muy graves susceptibles de despido:

> 9. La violación del secreto de correspondencia de cualquier tipo de documentos de la empresa o de las personas en cuyos locales o instalaciones se realice la prestación de los servicios, y no guardar la debida discreción o el natural sigilo de los asuntos y servicios en que, por la misión de su contenido, hayan de estar enterados, así como hacer uso indebido de la información contenida en las bases de datos, incumpliendo lo establecido en la vigente Ley de protección de datos[6].

En esta lógica propositiva se ha identificado alguna experiencia convencional, como la del VIII Convenio colectivo de Iberdrola Grupo –BOE de 2 de marzo de 2021–, que podría servir de guía a futuras iniciativas negociadoras cuando dice que las personas trabajadoras deben cumplir con la política y normativa interna en materia de ciberseguridad, con el

[6] *Vid.* también el artículo 68.3 del convenio colectivo, que señala: «Por faltas muy graves: a) Suspensión de empleo y sueldo de 11 días a 3 meses. b) Pérdida temporal o definitiva del nivel profesional laboral. c) Despido».

objeto de reducir las consecuencias resultantes de la exposición a riesgos directamente asociados al mal uso, divulgación, degradación, interrupción, modificación o destrucción no autorizada de la información, o de los sistemas de información (art. 90). Y en el mismo convenio colectivo (art. 84.3) se tipifican conductas que suponen una brecha de seguridad y, por ello, pueden ser objeto de sanción laboral, como:

> l) Violar el deber de secreto y de confidencialidad, así como el uso indebido, y/o transmisión a terceros no autorizada de información confidencial o propia de la empresa.
>
> […]
>
> r) La cesión de claves o el uso de claves ajenas para el acceso a cualquier equipo informático, red, fichero, archivo o documentación, etc.
>
> s) La manipulación, no autorizada o indebida de datos contenidos en sistemas operativos propios de la empresa, así como la obtención, divulgación y/o uso o cesión en beneficio propio o ajeno, gratuitamente o mediante precio o contraprestación de cualquier tipo, de datos personales, financieros, comerciales o de cualquier otra información confidencial o propia de la empresa, de sus clientes, proveedores o terceros que conozca por cualquier causa o especialmente por razón o con ocasión de las funciones desempeñadas, así como el hacer uso indebido de la información contenida en las bases de datos, incumpliendo lo establecido en la LOPD y demás normativa de aplicación.

Referencias bibliográficas

Capítulo Español de Internet Society. (20 de febrero de 2021). La desinformación en el marco de la seguridad nacional [*Webinar*]. https://www.youtube.com/watch?v=iLLNUC-ZzZE.

Incibe. (30 de enero de 2017). *Phishing*: no muerdas el anzuelo. *incibe.es.* https://www.incibe.es/protege-tu-empresa/blog/phishing-no-muerdas-el-anzuelo.

Incibe. (6 de abril de 2021). TemáTICas: te infectan, mutan y se extienden; hablemos del *malware*. *incibe.es.* https://www.incibe.es/protege-tu-empresa/blog/tematicas-te-infectan-mutan-y-se-extienden-hablemos-del-malware.

Molina Navarrete, Cristóbal. (2021). *Datos y derechos digitales de las personas trabajadoras en tiempos de (pos)covid19: Entre eficiencia de gestión y garantías*. Bomarzo.

Muñoz Ruiz, Ana Belén. (7 de abril de 2021). ¿Sabemos cuáles son nuestros derechos digitales como empleados? *El Foro de Labos*. https://forodelabos.blogspot.com/2021/04/sabemos-cuales-son-nuestros-derechos.html.