CIBERSEGURIDAD EN EL TRABAJO EN MOVILIDAD Y A DISTANCIA (TELETRABAJO)

CYBERSECURITY AT MOBILITY WORKING AND REMOTE WORKING (TELEWORKING)

Miguel Recio Gayo[1]

Profesor Asociado de la Facultad de Derecho de la Universidad CEU San Pablo

Fecha de recepción: 1/11/2020

Fecha de aceptación: 23/11/2020

RESUMEN: El trabajo en movilidad o a distancia (teletrabajo) era ya una realidad en muchas organizaciones, pero la pandemia por COVID–19 ha dado lugar a la necesidad de

1 Abogado del departamento de TMC y Delegado de Protección de Datos de CMS Albiñana & Suárez de Lezo. Doctor en Derecho. Máster Universitario en Protección de Datos, Transparencia y Acceso a la Información por la Universidad CEU San Pablo. Máster en Derecho de la Propiedad Intelectual por The George Washington University Law School. ORCID 0000–0002–2282–9907 / e–mail: miguelrecio@miguelrecio.com.

que muchas personas trabajadoras teletrabajen. El teletrabajo es una oportunidad, pero también supone un reto para las organizaciones ya que, si no se adoptan medidas de seguridad de la información o ciberseguridad adecuadas, sus activos de información pueden quedar expuestos a amenazas que son un riesgo para la confidencialidad, integridad y disponibilidad de la información. Que las personas trabajadoras sepan identificar ataques como los de *phishing* o evitar que los dispositivos que utilizan queden desatendidos, es esencial. Además, la ciberseguridad tiene otras implicaciones que las organizaciones deben conocer para mitigar los riesgos a los que están expuestas.

ABSTRACT: Mobility work and work from distance (teleworking) was already a reality in many organizations, but the COVID–19 pandemic has led to the need for many working people to telework. Teleworking is an opportunity, but also a challenge for organizations because, if adequate information security or cybersecurity measures are not taken, their information assets may be exposed to threats that are a risk to the confidentiality, integrity and availability of information. It is essential that workers know how to identify attacks such as phishing or prevent the devices they use from being left unattended. In addition, cybersecurity has other implications that organizations must be aware of to mitigate the risks to which they are exposed.

PALABRAS CLAVE: Teletrabajo, ciberseguridad, red privada virtual, *phishing*, protección de datos.

KEY WORDS: telework, cybersecurity, virtual private network (VPN), phishing, data protection.

1. INTRODUCCIÓN

Apesar de que el Real Decreto–ley 28/2020[2] regula el trabajo a distancia en el sector privado y el Real Decreto–ley 29/2020[3] regula el teletrabajo, ambos hacen referencia a la seguridad de la información. En el primer caso, ya en la Exposición de Motivos se indica que 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", debiendo entenderse esta última en un sentido amplio de manera que incluye también a la ciberseguridad. Y en el segundo caso, también en la Exposición de Motivos, se indica que se debe prestar "una especial atención a los deberes en materia de confidencialidad y protección de datos".

Las divergencias entre ambos sectores se producen también por lo que se refieren a las previsiones en materia de seguridad de la información. En el sector privado no existe una norma específica, sin perjuicio de algunas medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado al riesgo incluidas en el artículo 32.1 del Reglamento General de Protección de Datos (RGPD)[4]. Pero en el sector público, las Administraciones Públicas, salvo "los sistemas que tratan información clasificada regulada por Ley 9/1968, de 5 de abril, de Secretos Oficiales y normas de desarrollo"[5], tienen que cumplir con el

2 Real Decreto–ley 28/2020, de 22 de septiembre, de trabajo a distancia, publicado en el Boletín Oficial del Estado núm. 253, de 23 de septiembre de 2020. En relación con este Real Decreto–ley deben tenerse en cuenta tanto la Resolución de 15 de octubre de 2020, del Congreso de los Diputados, por la que se ordena la publicación del Acuerdo de Convalidación, publicado en el Boletín Oficial del Estado núm. 279, de 22 de octubre de 2020, como el Proyecto de Ley de trabajo a distancia, presentado el 15 de octubre de 2020 y publicado en el Boletín Oficial de las Cortes Generales, XIV Legislatura, serie A, 23 de octubre de 2020.

3 Real Decreto–ley 29/2020, de 29 de septiembre, de medidas urgentes en materia de teletrabajo en las Administraciones Públicas y de recursos humanos en el Sistema Nacional de Salud para hacer frente a la crisis sanitaria ocasionada por la COVID–19, publicado en el Boletín Oficial del Estado núm. 259, de 30 de septiembre de 2020. En relación con este Real Decreto–ley debe tenerse en cuenta la Resolución de 15 de octubre de 2020, del Congreso de los Diputados, por la que se ordena la publicación del Acuerdo de Convalidación, publicado en el Boletín Oficial del Estado núm. 279, de 22 de octubre de 2020.

4 En concreto, la lista de medidas de seguridad técnicas y organizativas a las que se refiere el citado artículo son: "a) la seudonimización y el cifrado de datos personales; b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento." Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Publicado en el Diario Oficial de la Unión Europea L 119, de 4 de mayo de 2016.

5 Véase el artículo 3 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Segu-

Esquema Nacional de Seguridad (ENS). El ENS es también aplicable en el caso del teletrabajo.

En ambos casos, una nota esencial es que **el trabajo se lleva a cabo fuera de las instalaciones de la organización lo que supone un cambio relevante**. Y esto es importante también porque la organización tendrá que adoptar medidas adecuadas para reducir el riesgo derivado de amenazas a las que se encuentran expuestos sus activos de información como consecuencia de que **los usuarios puedan trabajar en un entorno no controlado** por aquélla.

Identificar el riesgo al que dan lugar las amenazas, tales como el *phishing*, y adoptar medidas adecuadas, en particular en materia de ciberseguridad, son esenciales. Una de estas medidas es la relativa a la posibilidad de que la información viaje cifrada a través de una red privada virtual, de manera que se evite el acceso no autorizado a la información. Además, estas medidas pueden quedar recogidas en una política de seguridad de la información o ciberseguridad, que debe complementarse con procedimientos.

Por otra parte, la adopción y aplicación de medidas de ciberseguridad pueden implicar un tratamiento de datos personales, lo que supone que la organización tenga que adoptar también medidas para cumplir con la normativa aplicable.

2. TRABAJO EN MOVILIDAD Y A DISTANCIA (TELETRABAJO)

La posibilidad de trabajar en movilidad o a distancia no es algo nuevo en España, tal como pone de manifiesto la Exposición de Motivos del Real Decreto–ley 28/2020, de 22 de septiembre, de trabajo a distancia. Entre otras normas, se mencionan la Ley 3/2012, de 6 de julio, de medidas urgentes para la reforma del mercado laboral[6], que modificó el Estatuto de los Trabajadores[7] para introducir el trabajo a distancia basado en el uso intensivo de las nuevas tecnologías.

En concreto, como se indica también en la Exposición de Motivos del Real Decreto–ley 28/2020, el trabajo a distancia "en su concepción clásica de trabajo a domicilio, como

ridad en el ámbito de la Administración Electrónica, publicado en el Boletín Oficial del Estado núm. 25, de 29 de enero de 2010. Este Real Decreto fue modificado por el Real Decreto 951/2015, de 23 de octubre, publicado en el Boletín Oficial del Estado núm. 236, de 2 de octubre de 2015.

6 Publicada en el Boletín Oficial del Estado núm. 162, de 7 de julio de 2012.

7 Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. Esta disposición fue derogada y el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. A su vez, este último fue modificado por lo que se refiere al trabajo a distancia por el Real Decreto–ley 28/2020, de 22 de septiembre, de trabajo a distancia.

aquel que se realiza fuera del centro de trabajo habitual y sin el control directo por parte de la empresa y vinculado a sectores y ámbitos geográficos muy concretos, se ha visto superado por la realidad de un nuevo marco de relaciones y un impacto severo de las nuevas tecnologías".

Ahora bien, tanto en el caso de las empresas como de las Administraciones Públicas, incluso aunque pudiera trabajarse en movilidad o a distancia, **será necesario analizar o evaluar los riesgos en materia de seguridad de la información** o, en particular, ciberseguridad. Aunque hay multitud de actividades que sí se pueden realizar mediante el teletrabajo, tales como en las áreas de artes gráficas y diseño, servicios para Internet, administración y secretaría, o marketing y atención telefónica[8]; otras no lo son, en particular por razones de confidencialidad de la información que requiere que esta solo pueda ser tratada en las instalaciones de la organización.

En este sentido, sería recomendable realizar una evaluación de la viabilidad del teletrabajo, debiendo tener en cuenta como parte de esta las cuestiones relativas a si podría trabajarse en movilidad o a distancia de manera que la información, sean datos personales o no, quede protegida a través de medidas de ciberseguridad.

Es el riesgo de que se materialice una amenaza contra la confidencialidad de la información de la organización o la disponibilidad de un servicio lo que plantea que deba evaluarse si una actividad es susceptible de trabajo en movilidad o a distancia. En este sentido, toda organización, ya sea del sector privado o público, tiene que **analizar el riesgo existente** y si las medidas técnicas y organizativas aplicables son adecuadas para minimizar o reducir dicho riesgo o si, por el contrario, no es posible teletrabajar.

En el caso de las Administraciones Públicas, debe tenerse en consideración que el ENS incluye como uno de los principios básicos el relativo a la **gestión de la seguridad basada en riesgos**. Este principio, en virtud de lo previsto en el artículo 6 del ENS, implica, por una parte, que el riesgo sea analizado y gestionado, debiendo mantenerse permanentemente actualizado este análisis y gestión. Y, por otra parte, la gestión del riesgo implica también que deba permitirse "el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables" (art. 6.2 del ENS).

Además, cuando se traten datos personales y se encomiende dicho tratamiento a tercero, es necesario tener en cuenta que las medidas de seguridad previstas en el ENS son también aplicables a dicho tercero en virtud de lo previsto en la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)[9].

8 Gobierno de Aragón, *Actividades susceptibles a realizar mediante el teletrabajo*. Consultado en http://servicios.aragon.es/redo_docs/guias_ol/docs/actividades_teletrabajo.pdf.

9 En concreto, esta disposición adicional primera indica, en el segundo párrafo del apartado 2, que "En los casos

En cualquier caso, el hecho de que los dispositivos que se utilizan para tratar la información estén fuera de las instalaciones de la organización requiere que se adopten también medidas para evitar que, en caso de robo o pérdida, puedan ser utilizados para acceder de manera ilícita a los servicios electrónicos de la organización, así como al sistema de información y/o a la información tratada en este.

3. ¿QUÉ ES Y POR QUÉ ES FUNDAMENTAL LA CIBERSEGURIDAD?

Ciberseguridad (en inglés *cybersecurity* o *cyber security*) es un término complejo de definir y todavía bastante reciente. Este término surgió a partir del término ciberespacio (en inglés *cyberspace* o *cyber space*) y fue elaborado por profesionales de Tecnologías de la Información (TI), consultores, grupos de presión (*lobbyists*) y políticos para abordar las preocupaciones de seguridad del ciberespacio[10].

Aunque no hay una definición normativa de ciberseguridad, siguiendo referencias internacionales sería posible definirla como la **capacidad de proteger o defender el uso del ciberespacio de los ciberataques**[11]**,** o también como que comprende todas las actividades necesarias para proteger el ciberespacio, sus usuarios y las personas afectadas por las ciberamenazas[12].

No obstante, sí hay definiciones normativas del concepto de seguridad de las redes y de la información. El ENS define este concepto en el Anexo IV, que incluye un glosario, como "la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles". Y en la Directiva europea sobre la seguridad de las redes y sistemas de información, también conocida como Directiva NIS[13], define este concepto como "la capacidad de las redes y sis-

en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad".

10 European Union Agency for Network and Information Security, *Definition of Cybersecurity – Gaps and overlaps in standardization*, December 2015.

11 National Institute of Standards and Technology, *Managing Information Security Risk, Organization, Mission, and Information System View,* NIST Special Publication 800–39.

12 European Union Agency for Network and Information Security, *ENISA overview cybersecurity and related technology, September 2017.*

13 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Diario Oficial de la Unión Europea L 194, de 19 de julio de 2016.

temas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos".

La ciberseguridad es un término genérico que, en la práctica, **es también una obligación de las organizaciones, ya sean públicas o privadas, para proteger tanto sus activos de información**[14] **como los derechos fundamentales de las personas físicas**, lo que ocurre en este último caso cuando se tratan datos personales.

En relación con la ciberseguridad, si se sigue el modelo clásico de la seguridad de la información, los tres objetivos son proteger la confidencialidad, la integridad y la disponibilidad.

Al respecto, siguiendo al Instituto Nacional de Ciberseguridad (INCIBE)[15], cada uno de estos conceptos puede ser definido de la siguiente manera:

A estas tres dimensiones de seguridad pueden añadirse, si se sigue una aproximación actual, los siguientes atributos:

Para sistemas de información y redes tangibles	Para apoyar la dinamicidad del ciberespacio	Para apoyar la seguridad de la información
▪ Fiablidad ▪ Seguridad ▪ Mantenibilidad	▪ Fiablidad ▪ Seguridad ▪ Mantenibilidad	▪ Fiablidad ▪ Seguridad ▪ Mantenibilidad

14 El Instituto Nacional de Ciberseguridad define el activo de información como "cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización." Instituto Nacional de Ciberseguridad, Glosario de términos de ciberseguridad: una guía de aproximación para el empresario, Febrero de 2017 https://www.incibe.es/protege–tu–empresa/guias/glosario–terminos–ciberseguridad–guia–aproximacion–el–empresario.

15 *Cit.*

4. AMENAZAS O CIBERAMENAZAS

Según la definición dada por INCIBE[16] una amenaza es una "[c]ircunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor." Y, siguiendo esta definición de INCIBE, hay que tener en cuenta que "[u]na amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad."

Las amenazas o ciberamenazas, si se presta atención específica en este último caso al entorno cibernético, son constantes y cambiantes, siendo buena muestra el hecho de que durante "el confinamiento en España[17], el Ministerio del Interior informó y/o alertó, entre otros, de un intento viral de fraude a través de phishing[18], del bloqueo por la Policía Nacional de 45.773 dominios web utilizados para actividades criminales utilizando el Covid–19 como gancho[19] o de la detención de un menor de 16 años que llevó a cabo numerosos ciberataques a organismos públicos y entidades privadas[20]."[21]

Y el teletrabajo, que es una oportunidad para las organizaciones ya que, entre otros, facilita la movilidad y permite la conciliación laboral; lo es también para los ciberdelincuentes, que en muchas ocasiones dirigen sus ataques contra el usuario, como "eslabón más débil de la cadena y posiblemente, el más débil"[22].

Algunos ataques relevantes son el phishing y los correos electrónicos fraudulentos con archivos adjuntos que tienen por finalidad la descarga e instalación de *malware*.

4.1. *Phishing*

INCIBE define el *phishing* como "la estafa cometida a través de medios telemáticos me-

16 Instituto Nacional de Ciberseguridad, *Glosario de términos de ciberseguridad …*, *Cit.*

17 Declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID–19 y prorrogado en varias ocasiones.

18 Ministerio del Interior, "La Policía Nacional alerta de una tentativa viral de fraude a través de phishing", Madrid, 31 de marzo de 2020. Consultado en https://bit.ly/2zzpMqx

19 Ministerio del Interior, "La Policía Nacional bloquea 45.773 dominios web utilizados para actividades criminales relacionadas con el COVID–19", Madrid, 16 de abril de 2020. Consultado en https://bit.ly/2VBl9ES

20 Ministerio del Interior, "La Policía Nacional detiene a un hacker de 16 años por realizar numerosos ciberataques a organismos públicos y entidades privadas", Madrid, 17 de abril de 2020. Consultado en https://bit.ly/2KC1Cxy

21 RECIO GAYO, M., *Hacker ético: el profesional frente a quienes aprovechan la Covid–19 para cometer fraudes o estafas online y ciberataques*, Revista de Derecho Digital e Innovación, núm. 5, Abril–Junio 2020.

22 Instituto Nacional de Ciberseguridad, *La formación como elemento imprescindible en ciberseguridad,* 2019 https://www.incibe.es/protege–tu–empresa/blog/formacion–elemento–imprescindible–ciberseguridad.

diante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta.

El *phishing* es una de las formas de ingeniería social[23] en las que el ciberdelincuente trata de manipular a la víctima potencial para lograr llevar a cabo un ciberataque ya sea a partir de la información que pueda obtener de esta o de alguna acción, tal como instalar un virus en el dispositivo del usuario que le permita después obtener acceso al sistema de información de la organización para la que trabaja.

El estafador o *phisher* suplanta la personalidad de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e–mail, fax, SMS o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador"[24].

Aunque los ataques de *phishing* se llevan a cabo principalmente a través del correo electrónico, existen también otras técnicas como *smishing*, *vishing* y *spear phishing*.

En el caso del *smishing*, la víctima potencial recibe un mensaje de texto, ya sea SMS o través de una plataforma de mensajería electrónica, de alguien desconocido que le pide proporcionar alguna información, ya sean credenciales de usuario del sistema de información, datos personales u otra. El *phisher*, no obstante, intenta suplantar la identidad de alguien en quien la víctima confiaría como, por ejemplo, una personal del departamento o área de TI, etc.

De esta manera, intentando aprovechar además una situación de urgencia y confidencialidad como, por ejemplo, que se esté llevando a cabo una auditoría, el *phisher* busca conseguir la información o la realización de una acción que le sirve para conseguir su objetivo o llevar a cabo un ataque o ciberataque posterior.

El *vishing* tiene la misma finalidad, llevándose a cabo a través de Voz sobre IP. Y en el caso del *spear phishing*, como explica INCIBE, "los atacantes intentan mediante un correo electrónico, que aparenta ser de un amigo o de empresa conocida, conseguir que les facilitemos: información financiera, números de tarjeta de crédito, cuentas bancarias o contraseñas"[25].

Con independencia de cuál sea la modalidad de *phishing*, una persona trabajadora que desconozca este tipo de ataques podría ser víctima y, al mismo tiempo, ayudar a un ciberatacante a conseguir su objetivo cuando el objetivo sea el sistema de información o la información de la organización en la que trabaje.

23 Por ingeniera social se entienden las "tácticas utilizadas para obtener información datos de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima". Instituto Nacional de Ciberseguridad, *Glosario de términos de ciberseguridad …*, *Cit.*

24 *Cit.*

25 *Cit.*

Los ataques de phishing son frecuentes y en particular cuando se trabaja en movilidad o a distancia pueden dar lugar a situaciones graves, que requieren que la persona que reciba alguna de estas comunicaciones pueda reaccionar y no responder o no hacer nada de lo que le piden. La posibilidad de comunicarse de inmediato con el área de seguridad de la información o TI pueden ser relevantes al respecto.

4.2. Correos electrónicos fraudulentos

El *malware*, según la definición dada por INCIBE, es "un tipo de *software* que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de *software* malintencionado: *malicious software*."[26]

El envío de correos electrónicos fraudulentos que adjuntan ficheros con *malware* o incluyen un enlace son un riesgo para los sistemas de información ya que el ciberdelincuente trata de engañar al destinario con la finalidad de que lleve a cabo una acción como, por ejemplo, abrir el archivo adjunto o un enlace que permitirá ejecutar el virus e infectar la red o sistema de información de la organización o, incluso, llevar a cabo un ataque de *ransomware*, cifrando la información y pidiendo un rescate a cambio.

Al igual que en el caso de los ataques de *phishing*, la persona trabajadora tiene que conocer, para poder identificar, los riesgos derivados de este tipo de correos electrónicos. Aun estando fuera de la ubicación de la organización y, por tanto, no conectado a la red, este tipo de ataques podrían permitir el acceso no autorizado por el ciberdelincuente.

4.3. *Ransomware*

Dada su importancia debe hacerse una referencia específica al *ransomware* o "secuestro de datos" que puede ser definido como aquella acción en la que un ciberdelincuente "toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos"[27]. Se trata, por tanto, de una extorsión que surgió en los años 80 pero que aumenta de manera exponencial[28].

26 *Cit.*
27 *Cit.*
28 Instituto Nacional de Ciberseguridad, *Ransomware: una guía de aproximación para el empresario*, 2017 https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

Si la persona que recibe el correo electrónico fraudulento o malicioso que incluye un archivo adjunto, que es un virus, o abre el enlace que, por lo general, permite la descarga y ejecución automática del virus, podría producirse el cifrado de la información, o al menos de una parte, que se trata en el sistema de información, pidiendo un rescate a cambio. El pago del rescate se suele pedir a través de monedas virtuales como, por ejemplo, *bitcoins*, evitando así el rastreo del pago.

4.4. Riesgos y amenazas en el caso de videoconferencias y reuniones virtuales

La pandemia ha dado lugar también a un aumento exponencial del uso de aplicaciones o soluciones para videoconferencias y reuniones virtuales. Estas no están exentas de amenazas y, por tanto, requieren también de la adopción y aplicación de medidas de seguridad.

Según explica el Centro Criptológico Nacional (CCN), estas soluciones para videoconferencias "hacen referencia a aquellas tecnologías que permiten la comunicación audiovisual a través de redes LAN o WAN con infraestructuras locales (on–premise), en la nube (Cloud VaaS o SaaS) o soluciones hibridas on–premise y cloud y con terminales (endpoints) físicos dotados de procesador (códec), cámara, micrófono y mando remoto (pantalla táctil o mando convencional); o soluciones software ejecutándose en diferentes plataformas hardware (sobremesa, portátiles, móviles y tabletas), con aplicativos software (MS Windows, iOS, Android o Linux)."[29]

INCIBE señala que los principales riesgos que podrían presentar las aplicaciones de videollamadas[30] son:

"
- **Cifrados inseguros**. En muchos casos, la comunicación puede ser vista, grabada y compartida por la compañía proveedora del servicio. Para que esto no suceda, se debe escoger una herramienta que permita el cifrado de extremo a extremo (E2EE, *end–to–end encryption*).
- ***Bombing***. Un atacante accede a la videoconferencia haciéndose pasar por un participante legítimo, mediante esta técnica pueden espiar las conversaciones y proceder a la extorsión.
- **Ataques de denegación de servicio (DoS)**. Estos ataques sobrecargan las plataformas de videoconferencia haciendo imposible utilizar sus servicios.

29 Centro Criptológico Nacional, *Recomendaciones de Seguridad para situaciones de teletrabajo y refuerzo en vigilancia,* CCN–CERT BP/18, Mayo 2020.

30 Instituto Nacional de Ciberseguridad, Videollamadas: riesgos asociados a su uso y recomendaciones de seguridad, 2020. Consultado en https://www.incibe.es/protege–tu–empresa/blog/videollamadas–riesgos–asociados–su–uso–y–recomendaciones–seguridad

- **Acceso a salas sin control de seguridad**. Hay que establecer el acceso a las salas de videoconferencia de forma segura, empleando contraseñas o enlaces de invitación seguros en las salas de espera de video.
- **Aplicaciones no actualizadas frecuentemente**. No actualizar la plataforma de videoconferencia puede provocar vulnerabilidades graves que podrían permitir a un ciberdelincuente tomar el control de un equipo y la información que gestiona.
- **Descargas de las aplicaciones de videoconferencia desde páginas no seguras**. Es de vital importancia asegurarse de descargar la aplicación de videollamada desde su web oficial, verificando que el sitio es seguro, mediante los certificados *https* y los sellos de confianza que pueda tener.
- **Contraseñas poco seguras**. Es importante tomarse en serio la importancia de una contraseña segura (compuesta por letras, números, símbolos, mayúsculas y minúsculas y que no forme palabras de diccionarios), ya que de esta forma podemos evitar suplantaciones de identidad. Además, aún mejor si la plataforma ofrece más mecanismos de autenticación, como la verificación en 2 pasos."

Y, según INCIBE[31], las principales recomendaciones a adoptar con la finalidad de evitar el riesgo de sufrir un incidente de ciberseguridad son:

- Utilizar un plan empresarial en lugar de uno básico.
- Activar la sala de espera y bloquear la reunión.
- Requerir contraseña para acceder a la reunión.
- Vigilar a quién se envía la convocatoria.
- Vídeo y micrófono apagados por defecto.
- Software actualizado y descargado desde de la web oficial.
- Cifrado de las comunicaciones.

Además, el uso de aplicaciones para videoconferencias y reuniones virtuales pueda dar lugar a un tratamiento de datos personales, en concreto, la necesidad de registrarse mediante nombre de usuario y contraseña para poder unirse a la sesión, así como el tratamiento de su imagen y/o voz en caso de que la sesión sea grabada. Este tratamiento, cuando se produzca, tendrá que cumplir con los requisitos establecidos en la normativa sobre protección de datos, en particular el RGPD y la LOPDGDD.

31 Instituto Nacional de Ciberseguridad, *Aplica estos consejos y protege tus videollamadas*, 2020. Consultado en https://www.incibe.es/protege-tu-empresa/blog/aplica-estos-consejos-y-protege-tus-videollamadas

5. MEDIDAS DE CIBERSEGURIDAD

La regulación actual en España sobre la seguridad de la información, en particular cuando se trata de datos personales, difiere para los sectores público y privado. Mientras que en el primer caso es aplicable el ENS, en el segundo, actualmente, el RGPD prevé que "el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo" (art. 32.1).

Es decir, las medidas de seguridad de la información o ciberseguridad que adopte e implemente la organización dependerán del riesgo existente, debiendo tenerse en cuenta las amenazas y el impacto que estas podrían tener para los activos de información en caso de materializarse.

Algunas medidas de ciberseguridad relevantes son las relativas a la red privada virtual y la adopción de una política específica para situaciones de movilidad.

5.1. Red privada virtual

Si atendemos a la definición dada por INCIBE, una red privada virtual (en inglés *Virtual Private Network*, VPN) es "una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet.

Al establecerlas, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado.

Se trata realmente de una conexión virtual punto a punto entre dos redes LAN usando para la conexión una red pública como es Internet y consiguiendo que esta conexión sea segura gracias al cifrado de la comunicación".

Es decir, la VPN, como medida de ciberseguridad, permite a la persona que está fuera de las instalaciones de la organización poder conectarse desde un dispositivo (portátil, *tablet*, etc.) al servidor de aquella de manera que toda la información que se intercambia viaja cifrada y, por tanto, queda protegida frente a terceros no autorizados que intenten interceptar la comunicación y acceder a su contenido.

Por tanto, una VPN es una herramienta que "además de permitir una comunicación directa entre el lugar de teletrabajo y la empresa, ofrecen una alta seguridad al construir un túnel seguro a través de internet por donde viajan los datos"[32].

32 Junta de Andalucía, *Guía de recomendaciones y buenas prácticas para el impulso del teletrabajo*, Consejería de Economía, Innovación y Ciencia, 2010.

5.2. Necesidad de una política para situaciones de movilidad

Esta política formaría parte, en su caso, de la política de protección de datos y seguridad de la información, que es o son las políticas corporativas aplicables con la finalidad de proteger los activos de información.

En el caso del tratamiento de datos personales, el artículo 24.2 del RGPD indica que el responsable del tratamiento, cuando resulte adecuado para la organización, adoptará una política de protección de datos. Esta política tiene por objeto, entre otros, establecer las directrices o instrucciones que deberán seguir quienes tratan datos personales en la organización, siendo compatible con cualesquiera otras políticas o procedimientos en materia de seguridad de la información, tanto si la información son datos personales o no. Es decir, se trata de proteger de manera adecuada los activos de información de la organización, debiendo entenderse y aplicarse en un sentido amplio de manera que quedarían incluidos en dicho concepto tanto datos personales como cualquier otra información de la organización.

En relación con la política específica para situaciones de movilidad en el caso del tratamiento de datos personales, la Agencia Española de Protección de Datos (AEPD), en sus Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo[33], indica que tendrá que 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". Es decir, es esencial prestar atención a que la persona usuaria podría acceder a través de conexiones no seguras, utilizar dispositivos que no han sido aprobados o acceder a más recursos de los necesarios para el desempeño de sus funciones.

De igual manera, la política de seguridad de la información o política de ciberseguridad, dependiendo del nombre que le dé cada organización y de su alcance, tiene por objeto proporcionar a quienes tratan la información las directrices e instrucciones a seguir para proteger la confidencialidad, integridad y disponibilidad de la información, además de otros factores a tener en cuenta cuando se trate de las Administraciones Públicas, conforme al ENS.

En cualquier caso, las Recomendaciones de la AEPD, aunque están centradas en el tratamiento de datos personales, podrían aplicarse en cualquier otro ámbito, es decir, aunque se trate de cualquier otro activo de información de la organización, ya que se trata de lograr la seguridad de la información. Y ateniendo a estas Recomendaciones, en situaciones de movilidad o trabajo a distancia habría que considerar las siguientes cuestiones:

33 Agencia Española de Protección de Datos, *Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo*, 2020. Consultadas en https://www.aepd.es/sites/default/files/2020–04/nota–tecnica–proteger–datos–teletrabajo.pdf

1. Formas de acceso remoto. De manera que, por ejemplo, el acceso remoto solo esté permitido a través de una red privada virtual (VPN por las siglas en inglés de *Virtual Private Network*).
2. Dispositivos válidos. Lo que podría dar lugar a que solo se puedan utilizar dispositivos corporativos, de manera que estaría prohibido el uso de dispositivos personales o el uso de dispositivos corporativos con fines personales. Además, estos dispositivos corporativos podrían tener instalado un DLP (siglas en inglés de *Data Loss Prevention*), que es una herramienta que permite prevenir pérdidas o fugas de información de manera que, por ejemplo, no es posible el envío fuera de la organización de correos electrónicos que contengan información que haya sido clasificada como confidencial.
3. Nivel de acceso. Debe tenerse en cuenta que un acceso desde espacios o ubicaciones no controladas por la organización, como podrían ser tanto el domicilio de la persona trabajadora como cualquier otro lugar en el que pueda estar trabajando, puede suponer un riesgo cuando se accede y trata o procesa la información ya que puede exponerse a la vista de terceros que no están autorizados. Por ejemplo, en un entorno no controlado sería necesario que bloquear la sesión de usuario cuando la persona se ausenta de su puesto de trabajo, además de no poder dejar desatendido el dispositivo de que se trate con la finalidad de evitar su robo o manipulación por terceras personas.

Junto con lo anterior, es importante también que las personas usuarias estén informadas continuamente sobre las amenazas específicas a las que podrían exponerse al trabajar fuera de las instalaciones de la organización, tales como conexiones inseguras, dejar desatendido el dispositivo, exponer información a la vista de terceros no autorizados para ver la información o la pérdida de información por no hacer copias de seguridad debido a que se guarden en ubicaciones no previstas.

5.3. Recomendaciones de diversas autoridades y entidades

El Centro Criptológico Nacional (CCN) fue creado en 2004 con funciones, entre otras, tales como "elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración"[34]. En mayo de 2020, el CCN actualizó sus recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia[35].

34 Artículo 2.2.a) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional https://www.boe.es/buscar/act.php?id=BOE–A–2004–5051

35 Centro Criptológico Nacional, *Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia, CCN–CERT BP/18,* Mayo 2020 https://www.ccn–cert.cni.es/informes/informes–de–buenas–practicas–bp/4688–ccn–cert–bp–18–recomendaciones–de–seguridad–para–situaciones–de–teletrabajo–y–refuerzo–en–vigi-

En estas recomendaciones se incluye también una tabla resumen de comprobación con acciones relativas a los usuarios, al acceso remoto, al correo electrónico, a la videoconferencia, a la detección y vigilancia, así como otras acciones.

También en materia de ciberseguridad en el teletrabajo, INCIBE publicó una guía dirigida a empresas[36]. Además de ofrecer información y recomendaciones sobre varias medidas de seguridad, tales como los métodos de acceso remoto, la seguridad del software cliente de acceso o las principales amenazas para los terminales de teletrabajo, INCIBE incluye los principales elementos que deberían estar definidos en una política de teletrabajo y que son:

1. Relación de usuarios que disponen de la opción de trabajar en remoto;
2. Procedimientos para solicitud y autorización del teletrabajo;
3. Aplicaciones y recursos a los que tiene acceso cada usuario;
4. Mecanismos de acceso seguro mediante contraseña;
5. Configuración que deberán tener los dispositivos desde los que se establezcan las conexiones remotas;
6. Procedimiento y tecnología para cifrar los soportes de información;
7. Definición de la política de almacenamiento en los equipos de trabajo, así como de almacenamiento en la red corporativa;
8. Procedimiento y planificación de las copias de seguridad periódicas de todos los soportes;
9. Uso de conexiones seguras a través de una red privada virtual;
10. Virtualización de entornos de trabajo;
11. Utilización de aplicaciones de administración remota cuando se utilicen dispositivos móviles, y
12. Formar a los empleados.

Cuando se tratan datos personales, como ya se ha indicado, la Unidad de Evaluación y Estudios Tecnológicos de la AEPD publicó una nota técnica con recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo[37]. Estas recomendaciones se dirigen, respectivamente, a responsables del tratamiento y al personal que participa en operaciones de tratamiento.

En el caso de los responsables del tratamiento, que es quien solo o junto con otros, determine los fines y medios del tratamiento[38], las Recomendaciones de la AEPD se refieren a:

lancia/file.html.

36 Instituto Nacional de Ciberseguridad, *Ciberseguridad en el teletrabajo: una guía de aproximación para el empresario,* Julio de 2020 https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf.

37 *Cit.*

38 El responsable del tratamiento o responsable es definido como "la persona física o jurídica, autoridad pública,

1. Definir una política de protección de la información para situaciones de movilidad;
2. Elegir soluciones y prestadores de servicio confiables y con garantías;
3. Restringir el acceso a la información;
4. Configurar periódicamente los equipos y dispositivos utilizados en las situaciones de movilidad;
5. Monitorizar los accesos realizados a la red corporativa desde el exterior, y
6. Gestionar racionalmente la protección de datos y la seguridad.

Y las recomendaciones para el personal que participa en las operaciones de tratamiento[39] son:

1. Respetar la política de protección de la información en situaciones de movilidad definida por el responsable;
2. Proteger el dispositivo utilizado en movilidad y el acceso al mismo;
3. Garantizar la protección de la información que se está manejando;
4. Guardar la información en los espacios de red habilitados, y
5. Si hay sospecha de que la información ha podido verse comprometida comunicar con carácter inmediato la brecha de seguridad.

6. PROCEDIMIENTOS EN MATERIA DE CIBERSEGURIDAD

La seguridad de la información, especialmente en situaciones de movilidad y trabajo a distancia, requiere también de **procedimientos ágiles y efectivos para evitar riesgos** y, en caso de materializarse una amenaza, poder responder de manera inmediata.

Un ejemplo de lo anterior podría ser el hecho de que, en situaciones de movilidad o trabajo a distancia, se produjera un acceso no autorizado a datos personales como consecuencia de un ataque de *phishing* en el que el ciberdelincuente consiga que la víctima

servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros" (art. 4.7 del RGPD).

39 El tratamiento es definido como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción" (art. 4.2 del RGPD).

descargue software malicioso que le permita dicho acceso. En este caso, que implicaría una violación de la seguridad de los datos personales y "a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas" (art. 33.1 del RGPD), habría que cumplir con la obligación de notificarla a la autoridad competente en materia de protección de datos.

Y lo anterior al margen de que los operadores de servicios esenciales y los proveedores de servicios digitales, en los términos previstos en el Real Decreto–ley 12/2018[40], estén también obligados a notificar los incidentes o ciberincidentes a las autoridades competentes[41]. Por incidentes, según la definición dada en el citado Real Decreto–ley 12/2018, se entiende un "suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información" (art. 3.h).

También sería necesario revisar otros procedimientos ya establecidos en las organizaciones, dado que, por ejemplo, cuando se tratan datos personales, si se almacenasen en la nube o en los dispositivos de las personas que trabajan a distancia, será necesario tenerlo consideración si el interesado ejerce su derecho de acceso u otros derechos en protección de datos, tales como los de rectificación, supresión o portabilidad. Esto implica que el procedimiento de gestión de solicitudes de ejercicio de derechos que hubiera sido adoptado e implementado por la organización tenga que ser revisado para asegurarse de que contempla todos los tratamientos.

Estos procedimientos, sobre los que se basan las políticas, ya sean la de ciberseguridad o la protección de datos, sirven también para asegurar que los controles sean efectivos. De otra manera, las medidas de seguridad técnicas y organizativas podrían ser insuficientes o no efectivas. Y también es necesario que los usuarios, en particular aquellos que trabajen a distancia, sean informados y los conozcan para garantizar así que si fuera necesario saber cómo actuar.

7. FORMACIÓN DE LAS PERSONAS TRABAJADORAS

Los riesgos que pueden existir en el caso del teletrabajo implican que la aplicación de medidas de seguridad técnicas y organizativas por cualquier organización, pública o

40 Real Decreto–ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, publicado en el Boletín Oficial del Estado núm. 218, de 8 de septiembre de 2018.

41 En relación con la obligación de notificación de incidentes, puede verse la Guía Nacional de Notificación y Gestión de Ciberincidentes, aprobada por el Consejo Nacional de Ciberseguridad el 9 de enero de 2019. Consultada en http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf

privada, tenga que complementarse con la formación de las personas trabajadoras. Podría ser considerada también como una medida de seguridad.

Se trataría tanto de formar a las personas trabajadoras sobre las amenazas existentes, con la finalidad de que las conozcan y entiendan, así como que cumplan con las políticas y procedimientos aplicables[42]; como de ofrecer información sobre estas. En este sentido, medidas tales como sesiones específicas de formación, formación para las personas trabajadoras que se incorporan al puesto de trabajo o incluso que van a teletrabajar, así como la inclusión o distribución de contenidos en materia de ciberseguridad que les recuerden o alerten sobre amenazas.

Esta formación es también necesaria para que las personas trabajadoras comprendan las instrucciones que, en materia de ciberseguridad, les dé la organización para la que trabajan. Además, una formación adecuada es esencial como medida de seguridad, ya que sirve para que la persona pueda identificar y actuar ante amenazas ante las que puedan quedar expuestas.

Al respecto, si por ejemplo la persona no sabe identificar un ataque de *phishing* o alguna otra técnica de ingeniería social, tales como el *vishing* y el *smishing*, ya mencionadas, podría estar dando información confidencial o llevando a cabo un acción que ayude al ciberdelincuente a lograr su objetivo.

También los contenidos que, sobre estas cuestiones, puedan proporcionar diferentes entidades, como hace INCIBE[43] entre otras, son importantes para evitar riesgos y saber responder ante amenazas o ciberamenazas. Estos riesgos y amenazas son continuos y, además, cambiantes de manera que la formación e información deben ser también continuas.

Por último, la formación para personas en situación de movilidad o trabajo a distancia es también importante para evitar riesgos de incumplimiento, ya sea de las políticas adoptadas por la organización como de la normativa que, en su caso, le sea aplicable.

8. INSTRUCCIONES DE LA EMPRESA EN MATERIA DE CIBERSEGURIDAD

En materia de ciberseguridad, el Real Decreto–ley 28/2020 indica que "las personas trabajadoras deberán cumplir con las instrucciones de seguridad de la información específicamente fijadas por la empresa".

42 Instituto Nacional de Ciberseguridad, *Políticas de seguridad para la pyme: concienciación y formación*.
43 Instituto Nacional de Ciberseguridad, *Guía de ciberataques. Todo lo que deber saber a nivel usuario*, 2020.

A falta de algún criterio específico al respecto, cabría considerar que el empresario puede dar estas instrucciones a través de diferentes instrumentos que, en su caso, podrían estar también interrelacionados entre sí.

Desde cláusulas contractuales hasta políticas de ciberseguridad podrían ser medidas adecuadas para dar estas instrucciones que las personas que trabajan en situaciones de movilidad o a distancia. En concreto, cabría considerar:

- Cláusulas contractuales: En virtud de las que las personas trabajadoras se obliguen a cumplir con las medidas de seguridad de la información o ciberseguridad aplicables.
- Política de seguridad de la información o ciberseguridad: Que sea aplicable y, además, efectiva, en el sentido de que incluya consecuencias para quien incumple con la misma, que podrían materialJizarse en sanciones.
- Políticas específicas: Que complementen la política de seguridad de la información o ciberseguridad y que podrían incluir también consecuencias para las personas trabajadoras en caso de incumplimiento.
- Procedimientos específicos: Con los que sea necesario cumplir en situaciones de trabajo en movilidad o a distancia y que incluyen controles de seguridad que desarrollan la política de seguridad de la información o ciberseguridad.

Por último, en el sector público, estas instrucciones serán las derivadas de los deberes y responsabilidades que estén incluidos en la correspondiente política de seguridad. Es decir, toda persona usuaria queda sujeta al cumplimiento de las responsabilidades que les sean exigibles en materia de seguridad de la información.

9. TRATAMIENTO DE DATOS PERSONALES

Las medidas que sea adopten en materia de ciberseguridad para proteger los activos de información puede implicar un tratamiento de datos personales, debiendo considerar que puede ser tanto de las personas trabajadoras como de quienes intentan llevar a cabo un ataque contra una organización.

La aplicación de medidas técnicas y organizativas puede dar lugar a que se produzca incluso un tratamiento de datos personales que no ocurriría en otros ámbitos. Debe tenerse en consideración que **el uso de las tecnologías de la información y las comunicaciones**

(TIC) implica, en casi todas las ocasiones, que se produzca un tratamiento de datos personales que, además, puede ser desconocido para la persona o personas de quienes se tratan.

El Grupo de Trabajo del artículo 29 (GT29), actualmente integrado en el Comité Europeo de Protección de Datos (CEPD), manifestó al respecto, y entre otras cuestiones, que "los avances tecnológicos que han permitido formas de control más nuevas, potencialmente más intrusivas y generalizadas. Estos avances incluyen, entre otros:

- herramientas de prevención de pérdida de datos (DLP), que controlan las comunicaciones salientes con el fin de detectar posibles violaciones de la seguridad de los datos;
- cortafuegos de próxima generación (NGFW) y sistemas de gestión unificada de amenazas (UTM), que pueden proporcionar una variedad de tecnologías de control, entre ellas la inspección profunda de paquetes, interceptación TLS, filtrado de sitios web, filtrado de contenido, informes sobre dispositivos, información de identidad de usuario y (como se describió anteriormente) prevención de pérdida de datos. Estas tecnologías también pueden utilizarse individualmente, dependiendo del empresario;
- aplicaciones y medidas de seguridad que impliquen registrar el acceso de los trabajadores a los sistemas del empresario"[44].

Esto implica que puedan tratarse datos personales de las personas trabajadoras, en particular cuando están trabajando en situaciones de movilidad o a distancia, que deberán ser informadas de dicho tratamiento para evitar así una infracción de la normativa aplicable sobre protección de datos.

Como tratamiento de datos personales y dadas sus implicaciones, el GT29 indica que, en el caso de las personas trabajadoras, se "deben aplicar y comunicar políticas de uso aceptables, junto con políticas de privacidad, que indiquen el uso permisible de la red y los equipos de la organización, y que detallen de manera rigurosa el tratamiento que se está llevando a cabo."[45] Y señala también que "[e]n algunos países, la formulación de una política de este tipo requeriría legalmente la aprobación de un comité de empresa o una representación similar de los trabajadores"[46], ya que "su principal interés será sobre todo la seguridad y no la expectativa legítima de privacidad de los trabajadores"[47]. En cualquier

44 Grupo de Trabajo del artículo 29, Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, WP 249, adoptado el 8 de junio de 2017.
45 *Cit.*
46 *Cit.*
47 *Cit.*

caso, tanto si es necesaria o no la participación del comité de empresa o de una representación de similar de los trabajadores, el GT29 recomienda que siempre "una muestra representativa de trabajadores participe en la evaluación de la necesidad del control, así como en la lógica y accesibilidad de la política"[48].

Y el GT29 ilustra esta cuestión con una referencia específica al uso de la herramienta de prevención de pérdida de datos (DLP), que podría ser aplicada también de manera específica a dispositivos que sean utilizados en situaciones de movilidad o trabajo a distancia e incluye el ejemplo el siguiente ejemplo:

> "Un empresario utiliza una herramienta de prevención de pérdida de datos para controlar automáticamente los correos electrónicos salientes, con el fin de prevenir la transmisión no autorizada de datos protegidos (por ejemplo, datos personales del cliente), independientemente de si dicha acción es involuntaria o no. Cuando se considera que un correo electrónico es fuente potencial de una violación de la confidencialidad de los datos, se realiza una investigación adicional.
>
> Una vez más, el empresario se basa en la necesidad para su interés legítimo de proteger los datos personales de los clientes, así como sus activos contra el acceso no autorizado o la fuga de datos. Sin embargo, dicha herramienta DLP puede implicar un tratamiento de datos personales innecesario, por ejemplo, una alerta de «falso positivo» puede dar lugar a un acceso no autorizado a correos electrónicos legítimos enviados por los trabajadores (que pueden ser, por ejemplo, correos electrónicos personales).
>
> Por tanto, la necesidad de la herramienta DLP y su utilización deben estar plenamente justificadas para lograr el equilibrio adecuado entre sus intereses legítimos y el derecho fundamental a la protección de los datos personales de los trabajadores. Para que se puedan invocar los intereses legítimos del empresario, deben adoptarse determinadas medidas para mitigar los riesgos. Por ejemplo, las reglas que el sistema sigue para definir un correo electrónico como posible violación de la confidencialidad de los datos deben ser completamente transparentes para los usuarios y, en el caso de que la herramienta reconozca un correo electrónico que se va a enviar como posible violación de datos, un mensaje de advertencia debe informar al remitente del correo electrónico antes de su transmisión, a fin de ofrecerle la opción de cancelar dicha transmisión".[49]

48 *Cit.*
49 *Cit.*

Este tratamiento de datos personales tiene que ser, por tanto, lícito. Esto implica, en particular, que el tratamiento de los datos personales tenga que ser transparente; contar con una base de legitimación, que en este caso sería el interés legítimo, y cumplir con los principios aplicables.

Por último, habría que tener también en cuenta que algunas medidas de seguridad pueden dar lugar también a que se traten datos personales de quienes, por ejemplo, intentan atacar la página o sitio web de una organización. Es una cuestión sobre la que el Tribunal de Justicia de la Unión Europea concluyó en su sentencia de 19 de octubre de 2016, en el asunto C–582/14, que el tratamiento de direcciones IP dinámicas por el gestor de un sitio de Internet puede llevarse a cabo sobre la base de su interés legítimo para defenderse de ciberataques[50].

10. CONCLUSIONES

Las principales conclusiones que se derivan de lo expuesto anteriormente son las que se exponen a continuación.

La primera es que el trabajo en movilidad y a distancia (teletrabajo) pueden ser una oportunidad para las organizaciones y las personas trabajadoras, como ha puesto de manifiesto la situación generada por la pandemia por COVID–19. Pero trabajar fuera de las instalaciones de la organización, cuando sea posible, requiere tener en cuenta el riesgo para los activos de la información, ya que tanto estos como las personas trabajadoras están expuestos a múltiples amenazas o ciberamenazas. Esto da lugar a la necesidad de adoptar e implementar medidas de seguridad de la información o ciberseguridad con la finalidad de reducir el riesgo hasta niveles controlables.

La segunda es que las organizaciones tienen que adoptar, en particular, medidas tales como el uso de redes privadas virtuales (VPN) o políticas de seguridad de la información o seguridad que contemplen las situaciones de trabajo en movilidad y a distancia, que protejan la confidencialidad, integridad y disponibilidad de los activos de información. Además, las personas trabajadoras tienen que cumplir con las instrucciones dadas por la organización en materia de ciberseguridad, que pueden incluirse, por ejemplo, en cláusulas contractuales, políticas o procedimientos.

Y la tercera es que la aplicación de medidas de seguridad de la información o ciberseguridad puede dar lugar a un tratamiento de datos personales. La organización tendrá

50 Sentencia del Tribunal de Justicia (Sala Segunda), de 19 de octubre de 2016.

que adoptar, por tanto, medidas para cumplir con la normativa aplicable en protección de datos, asegurando así que el tratamiento sea lícito y legítimo.

REFERENCIAS BIBLIOGRÁFICAS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo, Madrid, 2020.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e ISMS Forum, *Guía para la gestión y notificación de brechas de seguridad*, Madrid, 2019.

ALMENAR PINEDA, F., *El delito de hacking*, Aranzadi, Cizur Menor, 2018.

ARANZADI, *Guía práctica de Ciberseguridad*, Aranzadi, Cizur Menor, 2019.

CENTRO CRIPTOLÓGICO NACIONAL, *Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia*, CCN–CERT BP/18, Madrid, 2020.

CONSEJO NACIONAL DE CIBERSEGURIDAD, *Guía nacional de notificación y gestión de ciberincidentes*, Madrid, 2019.

GARCÍA RAMBLA, J. L. y ALONSO CEBRIÁN, J. M., *Esquema Nacional de Seguridad con Microsoft*, Microsoft, 2009.

INSTITUTO NACIONAL DE CIBERSEGURIDAD, *Guía de ciberataques. Todo lo que tienes que saber a nivel usuario*, 2020.

MERCADER UGUINA, J. R., *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, 3ª edic., Madrid, 2019.

– *Lecciones de Derecho del Trabajo,* Tirant lo Blanch, Valencia, 2018.

PIÑAR MAÑAS, J. L., *Memento Protección de Datos*, Lefebvre, 1ª edic., Madrid, 2019.

PIÑAR MAÑAS, J.L. (Director), ÁLVAREZ CARO, M. y RECIO GAYO, M. (Coords.), *Reglamento General de Protección de Datos, Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016.

RECIO GAYO, M., *Kit de herramientas para el delegado de protección de datos*, Lefebvre, 1ª edic., Madrid, 2020.

SAGARDOY DE SIMÓN, I., *Nuevas Tecnologías y Relaciones Laborales*, Lefebvre, 1ª edic., Madrid, 2020.

VELASCO NÚÑEZ, E., *Delitos cometidos a través de Internet, Cuestiones Procesales*, La Ley, Madrid, 2012.