DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Guía de teletrabajo

Diputación de Valencia

Aspectos a considerar desde la perspectiva de la protección de datos y seguridad de la información.

Información del documento:

Título del documento	Guía de teletrabajo
Tipo de documento	Documento guía
Descripción	Guía de aspectos a considerar para la implementación del teletrabajo en la Diputación de Valencia desde la perspectiva de la protección de datos y seguridad de la información.
Propietario del documento	Documento elaborado por el Departamento de Protección de Datos y Seguridad de la Información de la Diputación de Valencia.

PERMISOS DE ACCESO:

Fecha	Tipo[1]	Identificación
25/09/2020	03	Servicios internos Diputación

[1] Tipo de acceso autorizado

01 Acceso total (02 + 04)

02 Lectura + modificación

03 Lectura

04 Reproducción-copia

05 Cancelación permisos

FECHA DE EMISIÓN: Septiembre 2020

Índice

1 MOTIVACIÓN

En el marco de la organización interna, la Diputación de Valencia ha decidido regular la prestación del trabajo mediante la modalidad denominada "teletrabajo". A tal fin, el Servicio de Personal ha asumido la tarea de elaborar el texto normativo que habrá de ser propuesto para su aprobación por los órganos competentes y, en tal sentido, se dio traslado desde el citado Servicio al Departamento de Protección de Datos y Seguridad de la Información (25-06-2020) de un borrador normativo para que dicho departamento hiciese las apreciaciones oportunas.

La implementación del teletrabajo requiere tener en consideración aspectos de diferente naturaleza. Por lo que hace referencia a la protección de datos personales y seguridad de la información, las cuestiones que suscita guardan relación directa con cambios en los métodos y fórmulas del tratamiento de los datos y sustanciales alteraciones en los instrumentos y canales tecnológicos, así como en los entornos físicos en que se llevan a cabo los procesos de tratamiento de la información, utilizados por los empleados que se incorporen a la modalidad de teletrabajo. Todo ello comporta nuevos escenarios de riesgo que deben ser tenidos en cuenta antes de implementar una regulación. Además, el nuevo paradigma debe conciliarse no solo con la legislación aplicable a dichas materias sino también con las regulaciones internas actualmente vigentes en la Corporación. Lo expresado anteriormente significa que, en el orden práctico, sean distintos Servicios o áreas competenciales de la Corporación los que se vean afectados o implicados en la ejecución de los aspectos específicos que ambas materias, la protección de datos personales y la seguridad de la información, exigen a la nueva modalidad de prestación del trabajo que pretende instaurarse.

Por dicha razón, el **Delegado de Protección de Datos de la Diputación** ha considerado que la mejor manera de abordar las implicaciones comentadas no es interactuando exclusivamente con el Servicio de Personal, sino "abriendo" las directrices y consideraciones al conjunto de Servicios, especialmente a los más estrechamente implicados –Informática, Formación, Contratación, Secretaría general…- para que, desde la primera conformación de lo que será futura normativa interna, puedan apreciar el nivel de participación y exigencia que les pueda suponer y formular con mayor criterio sus inquietudes y/o propuestas al Servicio de Personal.

En base a todo lo expuesto, se ha decidido confeccionar la presente **Guía de Teletrabajo**, al amparo de lo dispuesto en los artículos 31, 37.3 y 39.2 del Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal de la Diputación de Valencia.

2 INTRODUCCIÓN

Con la creciente y constante evolución de las tecnologías de la información y las comunicaciones (TIC) han surgido nuevas posibilidades que están permitiendo transformar los procesos y el entorno laboral de las organizaciones, y con ello aumentar su productividad, competitividad y resiliencia, a la vez que mejora la calidad de vida de las personas.

Este cambio de paradigma se ha podido constatar recientemente en la capacidad que han demostrado muchas organizaciones al facilitar formas de trabajo alternativas en situaciones de crisis como la que estamos viviendo. En el momento en que se publica la presente guía, el mundo se encuentra en una crisis sanitaria derivada del COVID-19. En esta situación, el teletrabajo, entendiendo como tal a cualquier forma flexible de organización del trabajo fuera del entorno de la oficina o instalaciones habilitadas por la organización, incluyendo aquellos denominados como *trabajo a distancia*, *lugar de trabajo flexible*, *trabajo en remoto* y *entornos virtuales de trabajo,* ha mostrado ser uno de los mecanismos más eficaces para mantener la continuidad de las actividades de las organizaciones, mientras se mantienen las medidas de distanciamiento como prevención frente a posibles contagios.

Estas circunstancias han acelerado la generalización y normalización del uso del teletrabajo, el cual, aunque mostrando una trayectoria ascendente en su implantación en la última década, había tenido un impacto poco significativo hasta ahora. Esto a causa, generalmente, de la falta de cultura de esta modalidad de trabajo, acostumbrados a llevar a cabo actividades de forma presencial, pese a la alta demanda de este en la sociedad.

Sin embargo, esta necesidad también conlleva la aparición de nuevos riesgos. De hecho, la celeridad para reanudar la operativa y la falta de previsión ante este escenario de crisis, ha abocado a muchas organizaciones a implementar cambios organizativos y tecnológicos drásticos, sobre entornos no preparados y sin la posibilidad de disponer de una planificación de tiempo y recursos adecuado; hecho que puede suponer, en términos generales, el descuido de las medidas de seguridad necesarias para garantizar la protección de la información y el ejercicio de los derechos y libertades de las personas.

Debemos ser conscientes que la seguridad de la información cobra especial relevancia en estos escenarios. Se debe tener en cuenta no sólo aquellos riesgos derivados de su propia naturaleza, sino que además existe una tendencia evidente en el incremento significativo de incidentes de seguridad relacionados con ataques malintencionados, y

es de esperar que los atacantes aprovechen la situación actual, donde se generan potenciales vulnerabilidades a explotar.

La falta de previsión generalizada se ve reflejada de igual forma en el ordenamiento jurídico. Hasta hoy, las únicas referencias regulatorias relacionadas presentes en el ordenamiento español se encontraban en el artículo 13 de la Ley del Estatuto de los trabajadores, donde se hace mención al *trabajo a distancia*. No obstante, en fecha 22 de septiembre se ha aprobado **Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia**, que regula las condiciones de esta modalidad de trabajo en el ámbito de las relaciones laborales comunes (Estatuto de los Trabajadores).

En el contexto del sector público tampoco existe una legislación básica del teletrabajo. El EBEP ni siquiera contemplaba algo similar al referido artículo 13 del ET. Esta actual carencia lo que ha propiciado son regulaciones sectoriales diversas en diferentes niveles territoriales de la Administración, creando marcos regulatorios dispares y condiciones singulares según la naturaleza del instrumento utilizado y el ámbito de aplicación –instrumento legislativo, norma administrativa, acuerdo de condiciones de trabajo o convenio colectivo…- No obstante, también con fecha 29 de septiembre se ha ratificado por el Consejo de Ministros la regulación básica del teletrabajo en las administraciones públicas, acordada en Mesa General de Negociación, que se incorporará en un nuevo **artículo 47 bis en el texto refundido de la Ley del Estatuto Básico del Empleado Público (TREBEP**) y cuyo texto es el siguiente:

"*ARTÍCULO 47 bis. Teletrabajo*
1. Se considera teletrabajo aquella modalidad de prestación de servicios a distancia en la que el contenido competencial del puesto de trabajo puede desarrollarse, siempre que las necesidades del servicio lo permitan, fuera de las dependencias de la Administración, mediante el uso de tecnologías de la información y comunicación.
2. La prestación del servicio mediante teletrabajo habrá de ser expresamente autorizada y será compatible con la modalidad presencial. En todo caso, tendrá carácter voluntario y reversible salvo en supuestos excepcionales debidamente justificados. Se realizará en los términos de las normas que se dicten en desarrollo de este Estatuto, que serán objeto de negociación colectiva en el ámbito correspondiente y contemplarán criterios objetivos en el acceso a esta modalidad de prestación de servicio.
El teletrabajo deberá contribuir a una mejor organización del trabajo a través de la identificación de objetivos y la evaluación de su cumplimiento.
3. El personal que preste sus servicios mediante teletrabajo tendrá los mismos deberes y derechos, individuales y colectivos, recogidos en el presente Estatuto que el resto del prevención de riesgos laborales que resulte aplicable, salvo aquellos que sean inherentes a la realización de la prestación del servicio de manera presencial.

4.- La Administración proporcionará y mantendrá, a las personas que trabajen en esta modalidad, los medios tecnológicos necesarios para su actividad.
5. El personal laboral al servicio de las Administraciones Públicas se regirá, en materia de teletrabajo, por lo previsto en el presente Estatuto y por sus normas de desarrollo."

2.1 Estructura del documento

De aquí en adelante, la estructura del documento está organizada en las siguientes secciones:

- **Sección 3**: Visión del entorno del teletrabajo, describe los conceptos y tipos de teletrabajo que encontramos; su utilidad; beneficios e inconvenientes; y los derechos y libertades de las personas que deben ser cumplidas en la aplicación de este.
- **Sección 4**: Análisis del contexto y toma de decisiones, trata aquellos aspectos que deben ser analizados para abordar el proceso de transformación en la facilitación del teletrabajo con objetividad, incluyendo la identificación de amenazas, la regulación y marco normativo aplicable, o la capacidad técnica y organizativa actual.
- **Sección 5**: Diseño e implantación del teletrabajo, incide en los elementos que deben ser tenidos en cuenta para una correcta planificación y puesta en marcha del teletrabajo, tanto desde la perspectiva de las medidas organizativas como las soluciones tecnológicas y medidas de seguridad.
- **Sección 6**: Supervisión del estado de la seguridad, aborda los tipos mecanismos de monitorización y control existentes para garantizar la protección y eficiencia de las actividades en un entorno de trabajo a distancia.

Asimismo, esta guía contiene un **listado de anexos** con material de soporte adicional. Concretamente:

- **Anexo A**: Listado de herramientas útiles para la aplicación y control de entornos de trabajo a distancia.
- **Anexo B**: Escenarios de riesgo a considerar en el análisis de la exposición de los tratamientos a amenazas en entornos de trabajo a distancia.
- **Anexo C**: Lista de verificación para el diagnóstico de situación respecto al estado de madurez de las herramientas y medidas establecidas por la organización en relación al trabajo a distancia.
- **Anexo D**: Formulario para la realización de un EIPD sobre el tratamiento en modalidad de teletrabajo.

3 VISIÓN DEL ENTORNO DEL TELETRABAJO

3.1 Concepto y tipos de teletrabajo

En primer lugar, cabe destacar la importancia de concretar y distinguir entre los conceptos de *teletrabajo* y *trabajo a distancia*, ya que son términos generalizados y utilizados indistintamente, los cuales pueden adoptar interpretaciones diferentes según el contexto.

El *trabajo a distancia* es toda aquella actividad laboral que se realiza fuera del centro de trabajo o lugar determinado por la organización, es decir, lo que consideramos como actividad no presencial, como pudieran ser los casos en los que se desarrollan en la vivienda particular del empleado o cualquier otro lugar elegido libremente por esta.

Sin embargo, el *teletrabajo*, según el Acuerdo Marco Europeo sobre Teletrabajo, es aquella forma de organización y/o de trabajo, que se presta mediante el uso de medios y sistemas informáticos, telemáticos y de comunicaciones, en el marco de un contrato o de una relación de trabajo, en la cual un trabajo que podría ser realizado igualmente en los locales de la organización se efectúa fuera de estos locales.

Por su parte, el nuevo artículo 47 bis EBEP considera teletrabajo aquella modalidad de prestación de servicios a distancia en la que el contenido competencial del puesto de trabajo puede desarrollarse, siempre que las necesidades del servicio lo permitan, fuera de las dependencias de la Administración, mediante el uso de tecnologías de la información y comunicación.

No obstante lo indicado anteriormente, debido a la naturaleza y el propósito de esta guía, en todo momento nos referiremos y trataremos lo concerniente al *teletrabajo*, pues aunque no sólo trataremos medidas de índole técnica, y se citarán aspectos que por su transversalidad serán aplicables a cualquier modalidad de trabajo a distancia, en todo momento nos referiremos a aquellos trabajos que se presten a través de medios digitales.

El teletrabajo puede llevarse a cabo es diversas modalidades según la jornada, en los términos acordados entre la organización y el empleado, siendo estas:

- de forma ocasional,
- de forma habitual a tiempo completo, o
- de forma habitual en parte de la jornada laboral.

3.2 El teletrabajo como medio para la continuidad en la prestación de los servicios

Garantizar la continuidad de la prestación de los servicios ante situaciones de crisis o desastres, es un factor crítico que considerar que debe ser tenido en cuenta para en cualquier organización.

Los planes de continuidad, tal y como los entendemos, invitan a analizar la criticidad de los procesos y a evaluar los potenciales riesgos que puedan generar un alto impacto que deterioren la prestación de los servicios, pudiendo derivarse en un quebranto de los compromisos adquiridos con las partes interesadas. Mediante este ejercicio nos permite anticiparnos a estos escenarios, estableciendo medidas de prevención que minimicen el impacto.

Al respecto, una de las amenazas a las que siempre estamos expuestos en relación a la continuidad es la imposibilidad de acceder al centro de trabajo dispuesto por la organización, ya sea por la afectación en la integridad de las oficinas que impidan garantizar la seguridad de las personas o, como se ha podido evidenciar recientemente, por el confinamiento del personal con motivo de prevenir la proliferación de contagios.

En este sentido, una de las medidas más habituales a considerar para tratar dicha tipología de riesgos, por su efectividad y versatilidad en lo que se refiere a la flexibilidad de la movilidad, es el *teletrabajo*.

3.3 Posibles beneficios e inconvenientes

Al plantearse la opción de implantar el teletrabajo y poner a disposición los mecanismos necesarios para hacerlo posible, debemos ser conscientes y analizar las posibles ventajas y desventajas que suscita sobre los distintos ámbitos en los que impacta, ya sea directa o indirectamente.

Asimismo, cabe mencionar que el teletrabajo no implica siempre beneficios e inconvenientes de forma unidireccional y global, sino que será variable dependiendo de cada uno de los aspectos analizados, e incluso de la perspectiva de cada una de las partes afectadas, ya sea de la del empleado o de la organización. Es responsabilidad de la entidad hallar una fórmula competente, eficaz y balanceada, que contribuya al bienestar y el agrado de la mayoría en la medida de lo posible.

Según se manifiesta en el citado acuerdo de Mesa General de Negociación de las AAPP, las principales ventajas que aporta esta nueva regulación, tanto para la sociedad como para las administraciones públicas son, según el acuerdo firmado, el

fomento de las nuevas tecnologías y el desarrollo de la Administración digital, la reducción en desplazamientos, la sostenibilidad ambiental, en línea con los ODS 2030, o la mejora de la conciliación del desarrollo profesional con la vida personal y familiar.

A continuación se expresa un resumen de beneficios-inconvenientes comúnmente aceptados:

BENEFICIOS	INCONVENIENTES
Inversiones y reducción de costes	
▪ Potencial reducción de espacio físico en oficina. ▪ Ahorro en el consumo de suministros para la organización. ▪ Ahorro de costes y tiempo en desplazamientos.	▪ Inversión inicial en tecnología y medios. ▪ Potencial incremento de gastos indirectos para los empleados.
Gestión adecuada de la productividad y la dedicación	
▪ Aumento de la productividad. ▪ Flexibilización de horarios.	▪ Posible aumento de distracciones y disminución de la eficiencia. ▪ Trabajo en exceso. ▪ Potencial reducción de tiempo de descanso mental y físico.
Conciliación familiar y laboral	
▪ Conciliación familiar y laboral. ▪ Disminución del absentismo laboral.	▪ Posibles dificultades para separar el rol laboral del espacio familiar.
Entorno de trabajo	
▪ Elección libre del entorno de trabajo. ▪ Facilitación de movilidad geográfica. ▪ Generación de oportunidades laborales a colectivos desfavorecidos geográficamente. ▪ Adaptación personalizada del entorno. ▪ Reducción de accidentes laborales.	▪ Gastos adicionales para la adaptabilidad del entorno de trabajo. ▪ Disminución de la interacción con compañeros de trabajo. ▪ Falta de comunicación, colaboración y aprendizaje entre equipos. ▪ Propensión al aislamiento. ▪ Limitación de la identidad corporativa.
Atracción y conservación del talento	
▪ Reclamo para la atracción y conservación del talento frente a otras organizaciones que no ofrecen flexibilidad organizativa. ▪ Facilita la contratación y la prestación de servicios. ▪ Facilidad de empleo a colectivos desfavorecidos.	

3.4 Derechos y libertades de las personas en relación con el teletrabajo

Existen una serie de derechos y garantías relacionados con las personas trabajadoras a distancia, que deben ser considerados y tenidos en cuenta a la hora de implementar cualquier proyecto de teletrabajo en la organización.

En el estricto marco que nos ocupa, cabe destacar:

3.4.1 Desconexión digital

Las personas que trabajan a distancia, particularmente en teletrabajo, tienen derecho a la desconexión digital fuera de su horario de trabajo, a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respecto de su tiempo de descaso, permisos y vacaciones, **así como su intimidad personal y familiar**, de acuerdo a los términos establecidos en el artículo 88 de la LOPD-GDD.

Por este motivo, es necesario regularizar la flexibilidad horaria, estableciendo límites, para lograr una separación efectiva entre el tiempo laboral y el personal.

3.4.2 Intimidad y protección de datos

En el marco del teletrabajo, la organización debe proveer al empleado de los medios telemáticos necesarios para su desempeño. Asimismo, es cada vez más habitual que se recurra a medidas de control de la prestación laboral. Sin embargo, **estos medios y controles deben garantizar el derecho a la intimidad y a la protección de datos**, en los términos previstos en la LOPD-GDD, debiendo asegurar la idoneidad, necesidad y proporcionalidad de estos.

En los casos en los que el teletrabajo se preste a través de dispositivos propiedad de la persona trabajadora, la organización no puede exigir la instalación de aplicaciones.

En caso contrario, el uso personal de medios dispuestos por parte de la organización para el teletrabajo sólo puede realizarse en aquellos casos específicos establecidos previamente.

NOTA: *A los dispositivos utilizados para la prestación laboral en la modalidad de teletrabajo les resulta también de aplicación la norma N/SEG/USU-002-3 NORMAS ESPECÍFICAS PARA DISPOSITIVOS PORTÁTILES Y MÓVILES*

4 ANÁLISIS DEL CONTEXTO Y TOMA DE DECISIONES

Previo a la implantación del teletrabajo, se recomienda realizar un análisis de contexto que permita determinar el estado y capacidades en los cuales se encuentra la organización, a fin de poder tomar decisiones objetivas sobre su viabilidad, diseño y planificación. Los puntos a tener en cuenta implican:

- Detección de riesgos a los que se expone la entidad.
- Identificación de los marcos regulatorios a los que se debe dar cumplimiento.
- Análisis de capacidad técnica y organizativa.

4.1 Identificación de amenazas y gestión de riesgos

La aplicación de teletrabajo implica una modificación de los medios de tratamiento de datos, que pueden estar expuestos a nuevas amenazas, por lo que se presentan otros escenarios de riesgo que deben ser considerados, entendiendo un riesgo como la combinación de la posibilidad de que se materialice una amenaza y las consecuencias de su impacto en caso de que ocurra.

Para ello, **deberemos llevar a cabo un análisis y gestión de riesgos sobre todas aquellas actividades de trabajo que se vean afectadas por el empleo del teletrabajo**, siempre con proporcionalidad y coherencia, y teniendo presente los requisitos de privacidad para el cumplimiento de las garantías de los derechos de las personas.

De acuerdo a las recomendaciones de la Agencia Española de Protección de Datos (AEPD), es fundamental realizar un análisis previo sobre los tratamientos, de forma que podamos discernir entre **aquellos tratamientos que supongan, por los datos que se tratan, un alto riesgo para los derechos y libertades de las personas**, de aquellos otros que en caso de verse afectados por una amenaza no derive en repercusiones y consecuencias graves.

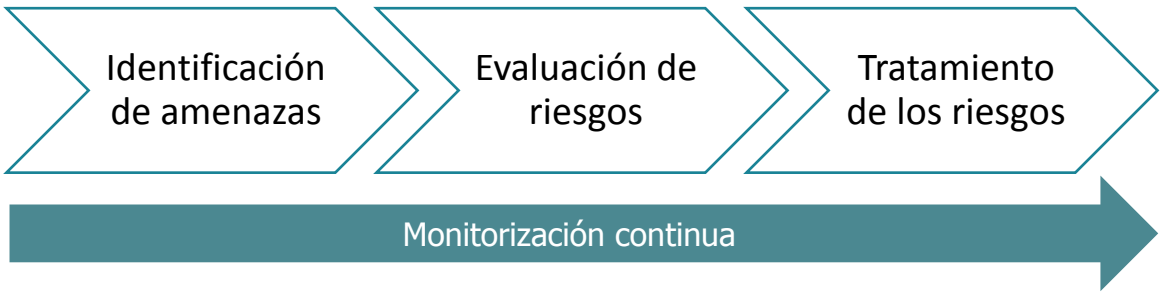
Para hacer esta distinción tendremos en cuenta los siguientes criterios:

- El Reglamento (EU) General de Protección de Datos establece ciertos supuestos en los cuales es obligatorio la realización de una **Evaluación de Impacto sobre la Protección de Datos (EIPD)**, determinados en los puntos 35.3, 35.4 y 35.5.
- Por la naturaleza, alcance, contexto y fines de tratamiento.

Una vez conocida la criticidad de los tratamientos, para aquellos categorizados como de riesgo alto, es recomendable realizar un análisis pormenorizado y en profundidad de las amenazas que pueden afectarle, lo que llamamos una Evaluación de Impacto sobre la Protección de Datos (EIPD). Para el resto de los tratamientos será suficiente con realizar un análisis de riesgos básico y global.

Para aquellos casos en los que ya se hayan analizado los riesgos sobre los tratamientos, en cumplimiento con lo dispuesto por la regulación en materia de protección de datos o, adicionalmente, en cumplimiento de otras regulaciones o estándares de seguridad, se deberá revisar y actualizar dicho análisis teniendo en cuenta los cambios y casuísticas propias de la aplicación del teletrabajo. En caso contrario, si no se han estudiado, deberemos llevar a cabo un análisis de riesgos de acuerdo con lo dispuesto anteriormente.

Independientemente de la complejidad y profundidad del análisis que realicemos, una vez determinados los ámbitos de tratamiento a analizar, aplicaremos una gestión de riesgos comprendida en tres fases:



En primera instancia, bien sobre cada uno de los tratamientos, para datos de riesgo alto, o a nivel general en caso contrario, identificaremos aquellas amenazas a las que se verían expuestas, teniendo en consideración que cuando aplicamos la modalidad de trabajo a distancia, estaremos expuestos a nuevas amenazas.

En este sentido, debemos identificar escenarios de riesgo teniendo en cuenta dos orientaciones:

- Riesgos potenciales orientados a la protección de la información, con foco en la disponibilidad, integridad y confidencialidad de los datos.
- Riesgos asociados al cumplimiento de los requisitos regulatorios relacionados con los derechos y libertades de los interesados; requisitos normativos; y contractuales.

Para facilitar esta tarea, se ha elaborado un listado de escenarios de riesgos recopilada de las guías de la AEPD y otros catálogos de amenazas, que se encuentra disponible en el ANEXO B: Escenarios de riesgo.

El siguiente paso consistirá en evaluar los escenarios de riesgo que se han identificado. Para ello, será necesario establecer unos criterios de valoración determinados y adaptados al contexto de la organización, de forma que todos los escenarios sean evaluados de forma objetiva y homogénea, a fin de poder obtener resultados comparables y repetibles en revisiones posteriores.

El proceso de evaluación tiene como objetivo valorar, teniendo en cuenta la criticidad del tratamiento, el **impacto** de la exposición a la amenaza, junto con la **probabilidad** de que esta se materialice.

Al respecto, existen diversas metodologías de evaluación de riesgos reconocidas, como por ejemplo MAGERIT, ampliamente utilizada en el entorno de las Administraciones Públicas.

La evaluación de estos riesgos en una fase temprana nos permitirá gestionar los riesgos de forma efectiva, al tratarlos mediante la determinación de medidas de control que hagan disminuir su nivel de exposición o impacto hasta alcanzar unos niveles de seguridad adecuados según la criticidad de los datos que tratamos.

Asimismo, estas medidas de seguridad deben ser aplicadas teniendo en cuenta los principios de privacidad desde el diseño y por defecto. El RGPD establece en el artículo 5 los siguientes principios relativos al tratamiento de datos personales que es necesario considerar en la definición de un tratamiento:

- **Licitud, lealtad y transparencia**: Los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado.
- Limitación de la finalidad: Los datos se deben recoger con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
- **Minimización de datos**: Los datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- **Exactitud**: Los datos deben ser exactos, y si fuera necesario, actualizados. Además, se establece que se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación si los datos son inexactos con respecto a los finales para los que se tratan.
- **Limitación del plazo de conservación**: Los datos deben ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.

- **Integridad y confidencialidad**: Los datos deben ser tratados de tal manera que se garantice una seguridad adecuada mediante la aplicación de medidas de control apropiadas.

Finalmente, cabe mencionar que la gestión de riesgos es un proceso continuo en el que debemos aplicar una monitorización activa de los riesgos, que deberá revisarse cada vez que haya un cambio sobre los tratamientos, inclusive la generación de nuevas actividades o la inclusión de nuevas tecnologías.

4.2 Marco normativo y regulatorio aplicable

Siempre que se llevan a cabo nuevas iniciativas, y especialmente en aquellos que tengan impacto sobre el tratamiento de la información y las estructuras organizativas, debemos ser conscientes de los requisitos legales y normativas existentes en el marco regulatorio actual, a fin de implementar las medidas necesarias para darles cumplimiento.

A continuación, se indican los principales marcos normativos y regulatorios que tienen implicaciones en la aplicabilidad del teletrabajo y que deben ser considerados.

4.2.1 Legislación laboral

Cabe señalar que en el ámbito de la Administración Pública, los empleados públicos están sujetos a la Ley del Estatuto Básico del Empleado Público (EBEP). En la actualidad, tal como se citaba en el apartado 2 Introducción, se ha introducido a través del artículo 47 bis EBEP la regulación básica del teletrabajo en el ámbito de la función pública.

4.2.2 Normativa de protección de datos

Tal y como se menciona en el artículo 32 del Reglamento General de Protección de Datos (en adelante RGPD), el Responsable y Encargado de tratamiento han de establecer las medidas técnicas y organizativas de seguridad que se consideren necesarias para minimizar los riesgos de gravedad variable para los derechos y libertades de las personas físicas, en materia de protección de datos.

De esta forma, es imprescindible que la entidad despliegue las herramientas y formación necesarias a los empleados para que actúen con garantías durante el

tratamiento, aplicándose no solo en el lugar de trabajo, sino también fuera de las instalaciones, como podría ser el domicilio.

Es función del Delegado de Protección de Datos de la entidad supervisar que se determinan las medidas necesarias para garantizar la protección de los datos de carácter personal y el cumplimiento de las diferentes normativas complementarias en este ámbito que resulten de aplicación.

4.2.3 Esquema Nacional de Seguridad

La Disposición adicional primera LOPD-GDD establece que, en el ámbito del sector público, los responsables deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica también dispone, en su Anexo II – Medidas de Seguridad, el control **Acceso remoto [op.acc.7]**, el cual define requisitos para todos los Sistemas de Información independientemente de la categorización que haya recibido por la valoración de la información tratada y el servicio prestado. Estos requisitos implican medidas de seguridad a adoptar por la organización para que aquellas labores que se realicen desde fuera de las instalaciones garanticen la protección de los sistemas de información.

Asimismo, para sistemas de mayor criticidad (a partir de una categorización media), el Esquema Nacional de Seguridad requiere medidas adicionales, como el establecimiento de una política que indique las acciones permitidas durante el acceso remoto y su comunicación al empleado.

El CCN propone en la Guía de implantación (CCN-STIC 804), puntos de soporte útiles sobre los que basarse a la hora de implantar teletrabajo en la organización.

4.2.4 Normas internas

En el ámbito de la Diputación de Valencia resultan de obligado cumplimiento las siguientes normativas:

• Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal de la Diputación de Valencia. Acuerdo del Pleno de 18 de junio de 2013.

• Normativa de protección de datos de carácter personal. Decreto nº 5448, de 12 de junio de 2015, del Diputado de Modernización.

• Procedimientos de protección de datos de carácter personal. Decreto nº 6110, de 26 de junio de 2015, del Diputado de Modernización.

• Normas de seguridad para los usuarios de los sistemas de información. Decreto nº 6111, de 26 de junio de 2015, del Diputado de Modernización.

• Normas de seguridad para el personal técnico de los sistemas de información TIC. Decreto nº 6353, de 3 de julio de 2015, del Diputado de Modernización.

4.2.5 Otros marcos de referencia

Adicionalmente, existen otros marcos que, aunque sin tener una obligatoriedad en su cumplimiento, pueden ser referentes y buenas prácticas que faciliten una implantación y transición hacia el teletrabajo segura y con garantías.

La norma ISO/IEC 27001, de Sistemas de Gestión de Seguridad de la Información, dispone del Anexo A de medidas de seguridad, entre los cuales existe una medida (A.6.6.2) específica para el desarrollo del teletrabajo. Esta medida especifica la necesidad de implantar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo. Asimismo, la norma ISO/IEC 27002 especifica una serie de recomendaciones para la implantación de esta medida de control.

Otro marco de control útil es el SP 800-53 rev. 4 "Security and Privacy Controls for Federal Information Systems and Organizations", publicado por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos, que incorpora controles de privacidad y seguridad de la información para hacer frente a las nuevas amenazas, incluidos los relacionados con accesos remotos y teletrabajo.

4.3 Capacidad técnica y organizativa

En último paso para poder analizar la viabilidad, consiste en conocer y analizar los recursos técnicos y organizativos que, de forma aproximada, serán requeridos para una adecuada implantación del teletrabajo en la organización, si disponemos de esos recursos, y si será necesaria la realización de una inversión para alcanzar los objetivos fijados.

Este estudio debería cubrir, al menos:

a) Necesidades de procesamiento.

b) Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
c) Necesidades de comunicación.
d) Necesidades de personal: cantidad y cualificación profesional.
e) Necesidades de instalaciones y medios auxiliares.

Especialmente, en el entorno del teletrabajo, se recomienda focalizar en los siguientes aspectos:

- Identificar el número de usuarios que puedan realizar sus actividades laborales en modalidad de teletrabajo.
- Determinar necesidades del puesto de trabajo. Existe la posibilidad de que la entidad no disponga de recursos suficientes, pudiendo recurrir a la habilitación de una política de BYOD (Bring Your Own Device) que permita a los usuarios utilizar sus propios dispositivos electrónicos para la realización de tareas, siempre cumplimiento con los requisitos legales y de seguridad necesarios.
- Determinar la magnitud de conexiones a través de Redes Privadas Virtuales y a los sistemas, para asegurar la correcta conectividad de los usuarios a los sistemas de información de la entidad.
- Analizar las necesidades que puedan surgir a la hora de transferir archivos, pudiendo requerir la habilitación de un sistema de compartición de archivos o transferencia seguros.

Realizado este análisis previo, la entidad se encontrará en posición de determinar la viabilidad de la implantación del teletrabajo. En caso afirmativo, en el siguiente punto de tratan los aspectos necesarios que permitirán establecer un plan de implantación del teletrabajo.

5 DISEÑO E IMPLANTACIÓN DEL TELETRABAJO

Para que el teletrabajo se implemente de una forma garantistas respecto al cumplimiento de los requisitos técnicos, organizativos y regulatorios, es necesario establecer un plan de implantación a través del cual se establezca una hoja de ruta que nos ayude a alcanzar los objetivos propuestos, **aplicando la seguridad y la privacidad desde el diseño y por defecto.**

En los siguientes puntos se analizan los principales aspectos a tener en cuenta en el diseño e implantación del teletrabajo.

5.1 Política de teletrabajo y normativa de seguridad aplicable

El primer paso lógico es la definición de una política de teletrabajo, a través de la cual la Dirección de la organización transmita una declaración de intenciones respecto al uso y condiciones del teletrabajo, y establezca las directrices que la gobiernen y los objetivos que se pretendan alcanzar.

A su vez, esta política debe ser el referente y dar paso a toda una capa normativa que, en caso de que sea necesario, desarrolle y de cumplimiento a las metas y requisitos definidos.

A continuación se describen algunos de los principales aspectos que deberían considerarse dentro de esta política.

- Aspectos organizativos:
    - Motivación, razón de ser y casuísticas para la aplicación del teletrabajo, así como el apoyo de la Dirección para lograr los objetivos y controlar el cumplimiento de las directrices establecidas.
    - Procedimiento de autorización de los usuarios para el acceso a la modalidad de teletrabajo.
    - Las condiciones de provisión de equipos y mobiliario adecuado para el desarrollo de las actividades de teletrabajo, en caso de no permitir el uso de equipos privados bajo el control de la organización.
    - Las condiciones y mecanismos para prevenir, dado el caso, disputas relativas a derechos de propiedad intelectual de lo desarrollado por el propietario del equipo de manera privada.
    - Referencias a documentación relacionada de soporte al teletrabajo.

- Las condiciones de acceso a la parte privada del propietario del equipo, dado el caso y en cumplimiento de la legislación vigente, para la realización de verificaciones de seguridad o durante un proceso de investigación.
- Determinación de las actividades de trabajo permitidas a desarrollar cuando se encuentra en modalidad de teletrabajo.
- Referencias y procedimientos de participación, dado el caso, en los planes de continuidad de los servicios.
- Procedimiento de notificación y gestión de incidentes de seguridad.
- Indicaciones y pautas sobre la separación entre entornos laborales y de ocio o familiares, evitando simultaneidad de tareas.
- Actuaciones o referencias a actividades de formación y concienciación en el uso de los medios dispuestos para el teletrabajo, así como en materia de seguridad en entornos de teletrabajo.

- Aspectos técnicos y medidas de seguridad:

  - Las medidas de seguridad física requeridas en el entorno del teletrabajo, incluyendo los lugares o características de los lugares donde se permite realizarlo.
  - En caso de permitir el uso de equipos privado, las condiciones de uso y control de estos para garantizar niveles de protección similares a los medios corporativos (como por ejemplo, aplicando políticas de Bring Your Own Device (BYOD)).
  - Los requisitos de seguridad de las comunicaciones, dependiendo de la necesidad de acceso remoto a los sistemas y la sensibilidad de la información que se va a acceder y transmitir; incluyendo, adicionalmente las restricciones de uso de las redes domésticas y los requisitos o restricciones en la configuración de los servicios de la red inalámbrica.
  - La facilitación de acceso a un escritorio virtual que prevenga el tratamiento y almacenamiento de información en equipos de uso personal o privado.
  - Medidas y condiciones proactivas para evitar amenazas de intentos de acceso no autorizados que compartan el espacio de trabajo, como pudiera ser por ejemplo familiares o amigos. En este sentido se recomiendan medidas de bloqueo automático de los equipos por inactividad y cierre de sesiones, además de medidas robustas de identificación y acceso, como el uso de contraseñas de alta fortaleza, biométricos o doble factor de autenticación.
  - Requisitos de protección frente a software malicioso (malware) y de cortafuegos.

- Determinación de la clasificación de confidencialidad de la información que puede tratarse o almacenarse en modalidad de teletrabajo, incluyendo los requisitos de seguridad a considerar y los sistemas a los que se está autorizado acceder.
- Determinación de canales seguros para el intercambio de información.
- Determinación de las condiciones de protección de los equipos, como por ejemplo la obligatoriedad del cifrado de la información.
- La provisión y mantenimiento de hardware y software, incluyendo los acuerdos de licencias de software en los puestos de trabajo de propiedad privada dado el caso.
- Mecanismos y procedimientos para la realización de copias de seguridad y restauración.

NOTA: *Es muy importante conciliar los aspectos citados anteriormente con las normativas internas vigentes en la Diputación. Debe recordarse que dichas normas internas son producto de transponer y/o desarrollar en el ámbito de nuestra organización la legislación en materia de protección de datos personales y seguridad de la información.*

5.2 Seguridad y privacidad desde el diseño y por defecto

El concepto de *privacy by design* o "privacidad desde el diseño", hace referencia a la necesidad de tener presentes las garantías del RGPD desde que se inicia un proceso, previendo adoptar medidas que garanticen que solo se traten los datos necesarios y por el tiempo imprescindible.

El RGPD indica en su considerando 78 que "*al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos*".

En este sentido, la aplicación del teletrabajo no es ajena al cumplimiento de este requisito, ya que implica un cambio potencial en los medios de tratamiento a través de los cuales damos soporte a la prestación de los servicios que la organización ofrece.

Por ello, **la organización debe analizar esas implicaciones y determinar los requisitos a los que se les debe dar cumplimiento, de forma previa a la aplicación del teletrabajo, para garantizar los derechos de las personas y la protección de la información que se trata.**

Adicionalmente, en la determinación de estos requisitos, se debe tener en cuenta la apreciación de riesgos descrita en el punto 4.1 Identificación de amenazas y gestión de riesgos. El motivo de ello es identificar aquellos requisitos que permitan tratar los riesgos reduciendo los niveles de riesgo hasta niveles aceptables.

Estos requisitos se van a traducir en medidas técnicas y organizativas, como pueden ser, por ejemplo, la regulación de algunos procesos mediante el desarrollo de procedimientos y normativa interna, la implantación de soluciones seguras o controles y buenas prácticas de seguridad, tal y como se describen en los siguientes puntos de la presente sección, con el objetivo de aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento.

El principio de *privacy by default* o "privacidad por defecto" está relacionado con el "principio de calidad de los datos", o dicho con otras palabras, con el uso proporcionado de los datos personales a la finalidad por la que se recaban.

Esto es, aplicable tanto a la cantidad de los datos recogidos, como al tipo de datos, los tratamientos que hacemos, el tiempo que los conservamos y el acceso que permitimos a los mismos.

En ambos casos, las estrategias de implementación o requisitos a llevar a cabo se van a traducir en medidas técnicas y medidas organizativas.

Entre otras estrategias básicas que permiten implementar la privacidad por defecto, se proponen:

- **Recogida de datos**: analizar los tipos de datos que se recaban con un criterio de minimización en función de la finalidad;
- **Tratamiento de los datos**: analizar los procesos asociados a dichos tratamientos para que se acceda a los mínimos datos personales necesarios para ejecutarlos;
- **Conservación**: implementar una política de conservación de datos que permita, con un criterio restrictivo, eliminar aquellos datos que no sean estrictamente necesarios;
- **Accesibilidad**: limitar el acceso, tanto interno como externo, de forma que solo los usuarios autorizados tengan acceso a los datos.

5.3 Desarrollo de procedimientos y normativas de seguridad

La aplicación del teletrabajo requiere, normalmente, considerar la adaptación de algunos de los procesos internos de la organización, debido al cambio de entorno, que deben ser reforzados para garantizar una gestión adecuada que tenga en cuenta los nuevos escenarios y casuísticas previstas.

A continuación se describen algunos de los procesos que comúnmente pueden tener especial relevancia en un entorno de teletrabajo.

5.3.1 Gestión de incidentes y brechas de seguridad

Se define un Incidente de seguridad a un evento inesperado que puede comprometer la seguridad de la información perteneciente a la entidad. Para ello, los usuarios deben ser conscientes de la necesidad de comunicar en la mayor brevedad posible, las debilidades o indicios que detecten concernientes a la seguridad, a fin de prevenir o tratar a tiempo estos eventos.

Cabe recalcar la importancia de que los usuarios no realicen actividades de comprobación de que una sospecha sobre una debilidad sea cierta, ya que, en caso de ejecutarse dicha acción, podría entenderse como un uso inapropiado de los elementos y activos de la entidad, pudiendo ocasionar daños en los sistemas de información y en las evidencias de la propia incidencia para investigaciones posteriores.

La entidad debe establecer los procedimientos de comunicación de incidentes de seguridad y brechas adecuados, comunicándose a los empleados, partes interesadas, autoridades de control pertinentes, proveedores y otros actores que puedan requerirlo, atendiendo especialmente la casuística de la aplicación del teletrabajo.

Una vez la comunicación haya sido realizada, se ha de decidir si el evento detectado se clasifica como incidente de seguridad y cómo se prioriza (utilizando protocolos que permitan determinar urgencia, impacto, alcance, etc.).

Se ha de responder ante incidentes de seguridad de la información a través de los procedimientos documentados. Para ello, los incidentes deben atenderse y monitorizarse manteniendo un registro de su estatus. La respuesta ante incidentes debe incluir, al menos:

- Recopilación de las evidencias principales

- Actividades de respuesta inventariadas
- Comunicación a las partes interesadas
- Finalización del incidente y cierre
- Lecciones aprendidas y mejora continua

De esta forma, el departamento resolutor correspondiente se encargará de la toma de medidas oportuna y verificar así, la supuesta debilidad o incidente de seguridad para activar los controles pertinentes de subsanación y otras medidas de prevención que se consideren adecuadas.

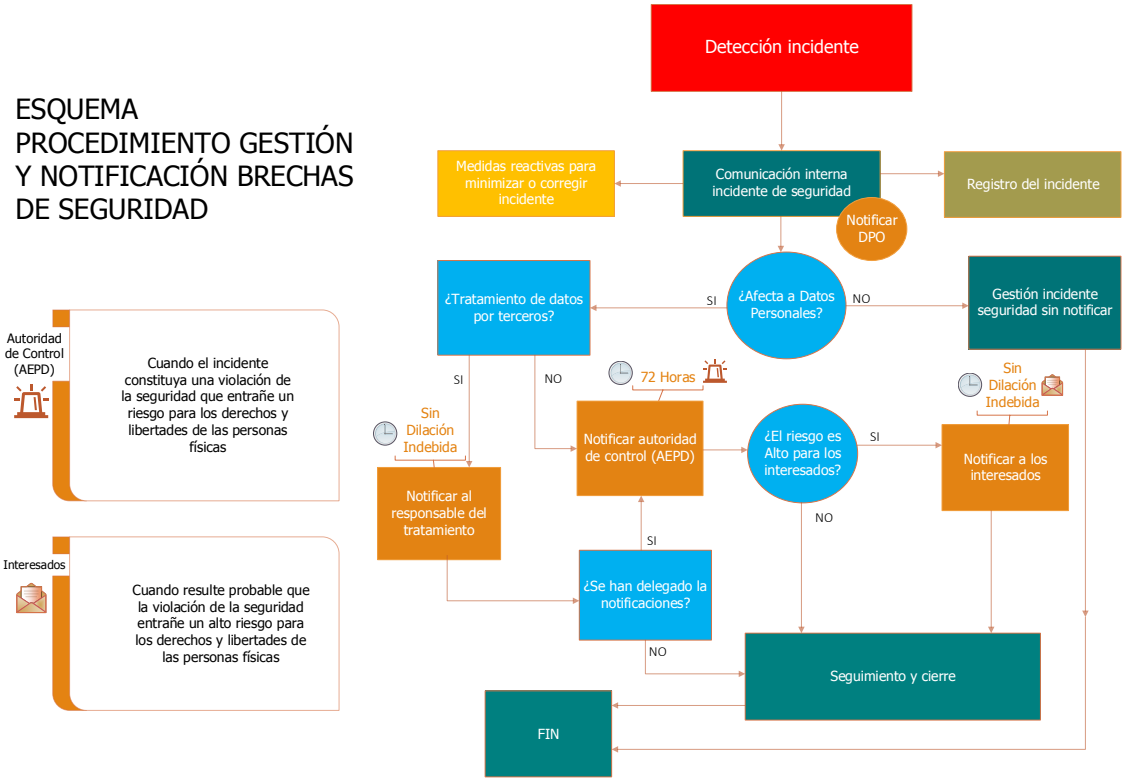
NOTA: *La norma N/SEG/TEC-018 INCIDENTES DE SEGURIDAD describe con detalle cómo debe actuarse en el ámbito de la Diputación ante un incidente de seguridad.*

Adicionalmente a lo anteriormente expuesto, el proceso debe tener en cuenta que, en caso de que el incidente de seguridad suponga una violación de datos de carácter personal, deberemos atenernos a lo establecido por la regulación en materia de protección de datos personales.

Concretamente, entendemos como violación de seguridad de datos personales a todo aquel incidente de seguridad que ocasione 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.

En dicho caso, deberemos:

- Comunicar el incidente de seguridad al Delegado de Protección de Datos y actores internos involucrados.
- Adoptar las medidas de contención necesarias.
- Registrar el incidente de seguridad.
- Evaluar la necesidad de comunicar la brecha de seguridad a la Agencia Española de Protección de Datos (AEPD), antes de 72h desde que tenemos conocimiento de ella, y a los interesados afectados.
- Proceder a la realización de las comunicaciones oportunas.
- Planificar las acciones de resolución que impidan su repetición.
- Realizar seguimiento sobre las acciones planificadas y realizar informe de resolución.



5.3.2 Clasificación de la información

Para una adecuada gestión integral de la seguridad, las entidades deben disponer de una normativa sobre la clasificación y tratamiento de la información.

Durante el teletrabajo, la información puede ser gestionada en diversos formatos y soportes. Cualquiera que sea su forma de presentación, ya sea en formato digital o en papel, es recomendable que sean etiquetados identificando el nivel de confidencialidad de la información o el grado de protección requerido, de forma que los usuarios puedan identificar fácilmente las medidas técnicas y organizativas asociadas a dicho grado para garantizar un tratamiento adecuado y la aplicación de los protocolos de protección necesarios.

NOTA: *La norma N/SEG/USU-001-2 CLASIFICACIÓN DE LA INFORMACIÓN establece los criterios y niveles de clasificación de la información a tratar en el ámbito de la Diputación (Información Pública, Reservada, Restringida o Confidencial) y las obligaciones de actuación conforme al nivel de clasificación.*

5.3.3 Plan de Continuidad

Los planes de continuidad establecen mecanismos que nos ayudan a contener y recuperar las actividades necesarias para la prestación de los servicios en un escenario de desastre.

Para desarrollar un Plan de continuidad, en primer lugar, se deben identificar y valorar aquellos procesos críticos para la organización, evaluando aspectos como los tiempos de recuperación objetivo, los puntos de restauración de la información, o los tiempos máximos tolerables de disrupción del servicio.

En base a este análisis, se determinan protocolos de actuación y coordinación para una gestión eficaz del desastre.

En este sentido, el teletrabajo/trabajo a distancia es un elemento que aporta una gran flexibilidad como mecanismo aplicado dentro de un Plan de Continuidad, ya que permite un acceso rápido y ágil a los sistemas independientemente de la ubicación donde nos encontremos. Asimismo, facilita la movilidad, garantiza el distanciamiento social en el entorno de trabajo en casos de riesgo sanitario o la indisponibilidad de instalaciones, ya sea por la caída duradera de recursos de suministro (luz, red, etc.) inaccesibilidad, o casos de condiciones climatológicas altamente adversas, que puedan ser cubiertas temporalmente con recursos personales evitando desplazamientos.

5.4 Análisis de soluciones y medios tecnológicos

Atendiendo a las necesidades de seguridad demandadas por la práctica del teletrabajo, se han seleccionado algunas soluciones de seguridad y medios tecnológicos, los cuales, a partir de su implantación y puesta en marcha, van a ayudar a mitigar posibles riesgos que puedan comprometer la seguridad de la información en las entidades.

Se ha puesto, por tanto, el foco en los diferentes puntos débiles, en lo que a seguridad se refiere, relativos a la práctica del teletrabajo. En ellos deberá centrar sus esfuerzos la entidad, tanto en el proceso de implantación de las medidas técnicas, como en el proceso de concienciación y formación al usuario, el cual tiene un papel fundamental en el estado de la seguridad en la entidad.

5.4.1 Seguridad de red y de Endpoint

Un Endpoint o dispositivo de punto final, se define como todo aquel dispositivo que se comunica con una red a la cual está conectado. Algunos ejemplos de Endpoint son; ordenadores de mesa, ordenadores portátiles, tabletas, smartphones, servidores, bases de datos, switches o routers.

Debido a la proliferación en la utilización de esta clase de dispositivos fuera de los límites de las instalaciones habituales de trabajo (teletrabajo y movilidad), el nivel de seguridad en el puesto de teletrabajo puede no ser el mismo que en el lugar de teletrabajo habitual. Es por ello que, en la hoja de ruta de los planes de teletrabajo y movilidad, la seguridad tanto del Endpoint como de la red corporativa deben ser una prioridad, la cual debe ser tenida en cuenta desde la fase de planificación.

5.4.1.1 Seguridad de red

Los cortafuegos (del inglés firewall) son mecanismos de seguridad diseñados para restringir los accesos no autorizados a desde una red externa a la entidad hacia la red interna. Es por ello por lo que, su ubicación habitual es el punto de conexión entre la red interna de la entidad y la red externa, la cual normalmente es Internet.

En esencia, los cortafuegos permiten realizar tres acciones principales. Estas son las siguientes:

- Autorizar una conexión (Allow).
- Restringir una conexión (Deny).
- Redireccionan un pedido de conexión sin avisar al emisor (Drop).

Mediante la conjunción de estas tres reglas, se puede establecer un filtrado de información hacia nuestra red el cual puede ir siendo más o menos preciso.

Habitualmente se distinguen dos tipos de políticas de seguridad las cuales permiten:

- Establecer únicamente las comunicaciones autorizadas explícitamente.
- Bloquear las comunicaciones categorizadas como restringidas.

Los principales beneficios que nos brindan los cortafuegos son los siguientes:

- Mitigan amenazas provenientes desde redes externas.
- Permiten configuración personalizada mediante reglas.
- Permiten la generación de alertas.
- Monitorean y registran el uso de servicios.

Los sistemas operativos Windows y Mac cuentan con mecanismos de firewall gratuitos por defecto, los cuales deberemos activar/configurar manualmente.

5.4.1.2 Seguridad de Endpoint

Sin embargo, debemos tener en cuenta que los cortafuegos tienen limitaciones a la hora de proteger los equipos, pues tienen la función única de permitir o no permitir flujos de datos provenientes de redes externas. Es por ello, que para obtener una mayor protección a nivel de Endpoint, se recomienda la utilización de herramientas Endpoint Detection and Response (EDR). Estas son consideradas como la evolución y ampliación, en lo que a funcionalidades y características se refiere, de los antivirus tradicionales.

Por una parte, los antivirus tradicionales son consideradas herramientas de seguridad muy reactivas, las cuales protegen frente a amenazas de seguridad mediante una serie de reglas que actúan de manera estática. Las herramientas EDR, por otra parte, actúan por comportamiento, llegando a detener, responder y remediar posibles riesgos de seguridad antes de que estos lleguen a materializarse en amenazas.

Las herramientas Endpoint Detection and Response (EDR) proporcionan una amplia visibilidad del estado del dispositivo, permitiendo realizar un proceso de monitorización y análisis continuo a nivel de Endpoint y de red.

Estas herramientas se caracterizan por:

- Monitorizar y evaluar las actividades de red, proporcionando una visibilidad completa del estado de las amenazas.
- Detener, responder y remediar ataques informáticos en tiempo real, tratando de reducir el tiempo de exposición a incidentes de seguridad.
- Aplicar machine learning e inteligencia artificial, para optimizar los procesos de identificación, detección y prevención de amenazas.
- Poner en cuarentena posibles amenazas.
- Realizar sandboxing con el objetivo de analizar las amenazas encontradas.
- Configurar alertas generadas por herramientas externas.
- Realizar análisis forense con el objetivo de analizar la amenaza una vez haya ocurrido.
- Contener las amenazas en tiempo real.
- Realizar un perfilado de acciones de usuario y aviso ante usos inesperados o poco habituales.

Mediante este tipo de herramientas, se dota a la infraestructura de seguridad de una capacidad de monitorización y respuesta continua ante cualquier incidente de seguridad, ya sea una amenaza tradicional o una avanzada.

5.4.2 Acceso remoto

El acceso remoto a la red interna corporativa por parte de los diferentes dispositivos de la entidad que se encuentran fuera de su alcance, puede ser un punto de conflicto en lo que a seguridad se refiere, debido a la diferencia en el nivel de seguridad de las medidas o controles de seguridad aplicados entre la infraestructura propia de la entidad y la infraestructura relativa al lugar de teletrabajo. Es por ello, qué deben trazarse unas directrices con el objetivo de hacer seguras las comunicaciones desde el lugar de teletrabajo hasta la red interna corporativa.

Existen diferentes soluciones de comunicación para proporcionar acceso remoto seguro a los usuarios de una entidad en situación de movilidad. Algunas de las más utilizadas son las siguientes:

- Redes privadas virtuales (VPN).
- Servicios de escritorio remotos (RDS).
- Infraestructuras de escritorio virtual (VDI).
- Infraestructura de escritorio móvil (VDM).

Se debe, por tanto, planificar qué solución de acceso remoto es la más adecuada dependiendo de las necesidades de la entidad. Además, deben considerarse las implicaciones y los riesgos de seguridad de cada solución, así como el cumplimiento de los requisitos de seguridad necesarios para llevar a cabo las tareas relativas al desempeño laboral y profesional de los usuarios.

NOTA: *La norma N/SEG/TEC-004-2 ACCESO REMOTO dispone que en los accesos remotos se observarán las mismas condiciones que las señaladas para el acceso local y se protegerá el canal de acceso remoto con las medidas indicadas en el apartado N/SEG/TEC-006 para la protección de las comunicaciones.*

5.4.2.1 Red privada virtual (VPN)

Uno de los medios más utilizados para hacer seguro el acceso remoto a la red interna de la organización y a los recursos corporativos son las conexiones mediante red privada virtual (VPN). Se trata de una tecnología de red la cual permite realizar una

extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet.

Las conexiones establecidas mediante este tipo de tecnología protegen la información que se intercambia, estableciendo un "túnel" o canal cifrado de comunicación entre el dispositivo y el lugar de trabajo, lo cual posibilita una conexión segura y privada entre las partes. Desde nuestro equipo de trabajo conectado a Internet establecemos un "túnel" privado y seguro hasta la red de la entidad, mediante el cual nos comunicamos sin temer que los datos sean vulnerados.

Al establecer una conexión mediante conexión VPN, se preserva la integridad y la confidencialidad (cifrado) de los datos compartidos y se da acceso únicamente a los usuarios autorizados. Y es que, la seguridad de los túneles VPN está por encima del 98%. Son por ello una medida muy recomendable desde el punto de vista de la seguridad.

La utilización de este tipo de conexión ofrece una serie de ventajas tales como:

- Acceso remoto seguro que posibilita la movilidad laboral.
- Comunicaciones totalmente cifradas (se preserva la confidencialidad e integridad de la información).
- Autenticación mutua.
- Protección frente reenvío de información.
- Control de accesos.
- Administración centralizada de aplicaciones.

NOTA: *La norma N/SEG/TEC-006-2 establece que las comunicaciones que discurran por redes fuera del propio dominio de seguridad, en aquellos sistemas de categoría MEDIA y superior, utilizarán redes privadas virtuales (VPN), empleando protocolos estándar como IPSEC, SSL o TLS..*

5.4.2.2 Servicio de escritorio remoto (RDS)

Las aplicaciones de escritorio remoto (del inglés, Remote Desktop Service, RDS) permiten al usuario controlar de manera remota un equipo, ubicado habitualmente el de la oficina de la organización, desde un segundo dispositivo en situación de teletrabajo. El escritorio virtual desplegado es el mismo para todos los usuarios de la entidad.

Esta tecnología permite al usuario acceder a la información almacenada en el dispositivo ubicado en la oficina de manera remota mediante la instalación de un programa cliente en el dispositivo de teletrabajo.

Sin embargo, no es una medida recomendable desde el punto de vista de la seguridad, debido a posible creación de puertas traseras (*backdoors*) mediante las cuales puedan acceder ciberdelincuentes. Para ello, se recomienda utilizar a vez una VPN y un escritorio remoto, con el objetivo de hacer más robusta la comunicación

Las aplicaciones de escritorio remoto presentan una serie de ventajas, tales como:

- Acceso remoto seguro que posibilita la movilidad laboral.
- Comunicaciones están totalmente cifradas (se preserva la confidencialidad e integridad de la información).
- Menor coste de inversión inicial y licencias que otras tecnologías debido al ahorro en hardware.
- Control de accesos.
- Administración centralizada de un escritorio virtual común a todos los usuarios.

5.4.2.3 Infraestructura de escritorio virtual (VDI)

Una infraestructura de escritorio virtual es una tecnología que permite la virtualización de entornos de trabajo de usuario en ubicaciones controladas dentro de la entidad, con el objetivo de permitir la utilización de estos entornos de trabajo de manera remota.

Se trata de una solución que permite al empleado realizar sus funciones de trabajo en un puesto de usuario remoto, el cual replica al de la oficina, desde su lugar de teletrabajo. El usuario dispone del mismo sistema operativo y de las mismas aplicaciones con las que cuenta en su equipo de la oficina, usualmente desde un navegador web, sin la necesidad de tener nada instalado de manera local.

Los escritorios virtuales son tecnologías muy seguras y flexibles, las cuales se adaptan perfectamente a entidades que deseen hacer uso de equipos de manera remota.

A diferencia de las soluciones RDS, las infraestructuras de escritorio virtual permiten personalizar y ofrecer un escritorio virtual configurado a medida para cada usuario. Es por ello, que este tipo de tecnología es entendida como un avance de la vista en el apartado anterior.

Los escritorios virtuales presentan una serie de ventajas, tales como:

- Acceso remoto seguro que posibilita la movilidad laboral.
- Interconexión segura de equipos.
- Comunicación segura.
- Menor coste de inversión inicial y licencias que otras tecnologías debido al ahorro en hardware.
- Escalabilidad.
- Control de accesos.
- Administración centralizada de aplicaciones.
- Flexibilidad en la configuración de cada escritorio.

5.4.2.4 Infraestructura móvil virtual (VMI)

Las infraestructuras móviles virtuales (del inglés, VMI) son una opción segura para proteger las comunicaciones de los dispositivos móviles en una entidad. Al igual que la infraestructura VDI proporciona un escritorio virtual seguro a ordenadores en situación de movilidad, la infraestructura VMI también proporciona un entorno seguro para la utilización de este tipo de dispositivos.

Una infraestructura móvil virtual permite acceder a aplicaciones móviles de manera remota, las cuales se ejecutan en servidores corporativos. Debido a ello, no es posible perder datos o que los roben, incluso tras la pérdida o extravío del dispositivo.

Se trata de una medida muy útil que permite separar el entorno de trabajo del personal en un mismo dispositivo. Si un usuario es dado de baja, la entidad tan solo tendrá que bloquearle el acceso remoto para que toda la información corporativa deje de ser accesible para el mismo.

Las infraestructuras móviles virtuales presentan una serie de ventajas, tales como:

- Entorno de dispositivo móvil virtual seguro.
- Imposibilidad de perder los datos o de que un tercero los robe (las aplicaciones se ejecutan en servidores corporativos).
- Control de accesos.
- Administración centralizada de aplicaciones.

5.4.3 Herramientas de colaboración

Las herramientas de colaboración permiten a los usuarios de una entidad comunicarse y trabajar de manera conjunta sin importar su ubicación física. Se puede producir,

editar y compartir información de manera conjunta por parte de un mismo equipo de trabajo.

La utilización de herramientas colaborativas supone un punto de diferenciación respecto a otras entidades del sector, debido al ahorro de tiempo producido por la sinergia a la hora de trabajar en equipo.

Las dos principales ventajas, las cuales hacen a las herramientas colaborativas ser una opción tan interesante en la actualidad son: el ahorro en costes y la productividad relativa a la posibilidad de colaboración en tiempo real.

Adicionalmente, y como medidas de seguridad frente a este tipo de herramientas, se recomienda:

- Utilizar aplicaciones seguras descargadas de sitios oficiales.
- Utilizar las cuentas profesionales, y no las personales, para acceder a las reuniones.
- Utilizar un plan empresarial en lugar de uno básico.
- Mantener el software actualizado, así como también el navegador si accedemos mediante vía web.

Podemos dividir las herramientas colaborativas en tres tipos, según su funcionalidad:

- Mensajería electrónica.
- Producción, edición y almacenamiento de documentos.
- Videollamadas y reuniones.

5.4.3.1 Servicio de correo electrónico

Los servicios de correo electrónico son de gran ayuda para realizar y clasificar comunicaciones establecidas con otros usuarios o grupos de usuarios de la entidad o externos a ella.

La situación de teletrabajo que muchas entidades han tenido que adoptar como medida a la situación sanitaria excepcional causada por el del COVID-19, ha hecho que la cantidad de correos de suplantación de identidad aumente considerablemente; vacunas contra la enfermedad, nuevas oportunidades laborales o desinformación acerca de medidas adoptadas por parte del Gobierno, han sido la tónica habitual de correos maliciosos orientados a robar información del usuario.

Si el servicio de correo electrónico ya estaba considerado como el principal vector de entrada de amenazas en las organizaciones, la situación descrita anteriormente solo ha hecho que agravar este problema aún más.

Es muy importante, llegados a este punto, la concienciación y la formación del usuario respecto a los posibles emails maliciosos que puedan comprometer la seguridad de la información de nuestra bandeja de correo. Es por ello, que no solo debemos tener en cuenta el factor técnico (firewall, EDR, protección avanzada del servicio de correo, filtro antispam, etc) sino también el factor humano.

5.4.3.1.1 El factor humano en la prevención de ataques de phishing

Mediante una serie de consideraciones teóricas, podemos conseguir que en la práctica el usuario sea capaz de detectar si la situación a la cual se enfrenta puede suponer un riesgo para su seguridad.

Las principales consideraciones de seguridad a la hora de detectar un ataque de phishing son las siguientes:

- Tener un pensamiento crítico frente a los correos que llegan a nuestra bandeja de entrada, pues una parte de ellos pueden llegar a comprometer la seguridad de nuestros equipos. Debemos tener en cuenta los siguientes aspectos con el objetivo de detectar si puede tratarse de un email malicioso:
    - El correo no tiene un destinatario concreto o te trata de una manera genérica.
    - El remitente del correo es poco fiable o no lo tenemos agregado a nuestra agenda de contactos. Para comprobar la veracidad del remitente, deberemos verificar el dominio de su dirección de correo.
    - A lo largo del correo encontramos errores ortográficos, errores de maquetación o símbolos/logos no legítimos o equívocos.
    - El idioma del mensaje de correo, así como el contenido de este, son indicadores para verificar la legitimidad de este. Por ejemplo, es poco probable que nuestro banco, en el caso de vivir en España, nos mande un correo en inglés.
- No descargar ningún tipo de archivo, pues puede contener malware encubierto que comprometa la seguridad de nuestro equipo. Existen algunos tipos de malware que se descargan en segundo plano y son difíciles de detectar.
- Ante la menor sospecha, se recomienda borrar el mensaje de correo electrónico e informar a la autoridad competente dentro de la entidad.

En el caso de que el correo contenga un enlace a un sitio web (no se recomienda acceder si la web no es legítima) y accedamos, debemos comprobar algunos indicadores de seguridad:

- Verificar la legitimidad del enlace, prestando especial atención a las URL.
- Comprobar la validez de la conexión de la página web (certificado SSL) y el candado de la barra de navegación. Debemos tener en cuenta que el protocolo HTTPS es más seguro que otros protocolos como HTTP.
- No descargar ningún tipo de archivo, pues puede contener malware encubierto que comprometa la seguridad de nuestro equipo. Hay algunos tipos de malware que se descargan en segundo plano y son difíciles de detectar.

5.4.3.2 Producción, edición y almacenamiento de documentos

Las herramientas colaborativas destinadas a la producción, edición y almacenamiento de documentos se caracterizan por permitir la realización de documentos en tiempo real de manera conjunta. Los documentos quedan almacenados en la propia herramienta y son editados por los usuarios con derechos para hacerlo, quedando de esta manera actualizados en tiempo real.

La utilización del servicio de correo electrónico es en ocasiones insuficiente para el intercambio y compartición de documentos. Esto se debe principalmente a las restricciones de tamaño impuestas por el servicio de correo electrónico en referencia al envío de documentos. Se debe, por tanto, valorar la opción de utilizar herramientas de compartición y almacenamiento de documentos con el objetivo de tratar documentos más pesados.

Este tipo de herramientas, nos ayudan a tener un acceso ágil a la documentación corporativa en un entorno de teletrabajo y facilitan la compartición y edición de documentos entre usuarios sin necesidad de enviar adjuntos vía correo electrónico o de acceder mediante VPN a los servidores de ficheros de la organización.

Se recomienda revisar los permisos asignados a cada documento que se comparte o se almacena mediante este tipo de herramientas, con el objetivo de asegurar que sólo tendrán permisos las personas indicadas.

NOTA: *En el ámbito de la Diputación, los usuarios disponen de la herramienta TRANXFER para el intercambio seguro de ficheros de todo tipo. Esta herramienta corporativa cumple con las cinco dimensiones de seguridad exigibles para el tratamiento de la información (disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad)*

5.4.3.3 Videollamadas y reuniones

El tercer tipo de herramienta colaborativa que debemos tener en cuenta son las aplicaciones de videollamadas. En situación de teletrabajo está a la orden de día la realización de reuniones de trabajo en línea. Son, por ello, una alternativa muy eficaz a las reuniones presenciales, debido a las diferentes funcionalidades comunicativas.

Sin embargo, un uso poco seguro de este tipo de aplicaciones podría comprometer la seguridad de la información compartida. Se recomienda, por tanto, seguir una serie de recomendaciones y buenos hábitos de seguridad referentes a la utilización de este tipo de herramientas colaborativas:

- Activar la funcionalidad de sala de espera, con el objetivo de que el administrador de la sala compruebe la identidad de los usuarios antes de empezar la reunión.
- Evitar compartir información confidencial (credenciales, números de tarjetas de crédito, etc.) en el chat de la reunión
- Evitar, en la medida de lo posible, enlaces poco seguros compartidos en el chat de la reunión.
- No compartir enlace de la reunión, si lo hay, con terceros.
- Requerir contraseña de acceso a la reunión.
- Contar con el papel de un moderador en las reuniones el cual gestione el transcurso de la reunión.
- El número de participantes debe ser limitado y estar controlado.
- Contar con indicadores visuales/sonoros que nos permitan conocer la entrada/salida de los participantes.
- Tener constancia en todo momento del estado de nuestro micrófono y cámara (ambos apagados por defecto y configurables en todo momento).
- En caso de grabar la reunión, el administrador deberá informar previamente a los participantes.
- Comprobar que la aplicación cuente con cifrado de las comunicaciones.
- Conocer la política de privacidad de la herramienta antes de hacer uso de ella.

A título de ejemplo, Microsoft Office 365 es una suite ofimática de aplicaciones orientada a la productividad, la cual permite englobar estos y más servicios de manera conjunta.

5.4.4 Protección de la información

La información es el activo más valioso en muchas entidades actualmente. Es por ello que debe asegurarse de una manera robusta con el fin de evitar robos, filtraciones o fugas de información. En primer lugar, se debe de concienciar al usuario sobre su importancia en este apartado, así como también de la importancia de la información en la entidad a la cual pertenece. En segundo lugar, se debe tratar de proteger a través de medios técnicos la confidencialidad e integridad de la información tratada.

Para ello, a continuación, analizaremos algunas de las opciones más interesantes para proteger la información de nuestra entidad. Estas son las siguientes:

- Prevención de pérdida de datos (DLP).
- Gestión de los derechos de la información (IRM).
- Gestión de dispositivos móviles (MDM).

5.4.4.1 Prevención de pérdida de datos (DLP)

Las herramientas de prevención de pérdida de datos (del inglés *Data Loss Prevention*, DLP) tienen como objetivo prevenir la fuga de información fuera de la red corporativa, causada por parte de los usuarios, de manera accidental o intencionada.

Estos sistemas se caracterizan por proteger la información de una manera proactiva y sin perder productividad, debido a que actúan en segundo plano mientras los usuarios realizan sus funciones habituales. Adicionalmente, estos sistemas también son utilizados para asegurar el cumplimiento de requisitos legales y regulatorios relacionados con protección de datos.

Las soluciones DLP, permiten realizar una configuración basada en políticas de seguridad y en una adecuada categorización de la información, con el fin de distinguir entre los diferentes tipos de información y los diferentes niveles de confidencialidad determinados. Según la configuración realizada, la solución DLP responderá de una manera o de otra frente a los diferentes casos de uso. Es decir, dependiendo de *"Qué se comparta"* y de *"Cómo se comparta"*, la herramienta responderá de una manera.

Los sistemas de prevención de pérdida de datos protegen principalmente actividades tales como:

- Correo electrónico, chats y mensajería instantánea
- Sistemas de intercambio de ficheros
- Redes locales

- Aplicaciones web
- Dispositivos de almacenamiento externo (USB's, discos duros, etc)

5.4.4.2 Gestión de los derechos de la información (IRM)

Las herramientas de gestión de los derechos de la información, (del inglés, Information Rights Management, IRM) tienen como objetivo proteger la información frente a accesos no autorizados. Las herramientas IRM cuentan con una serie de funcionalidades que permiten el control, la gestión y la protección de la información. Entre ellas, destacan las siguientes:

- Protección frente a accesos no autorizados.
- Protección frente a copias o modificaciones.
- Protección frente a impresión o descarga de los documentos,
- Registro de acceso a los ficheros.
- Gestión de los derechos de los documentos.

La implementación de una herramienta IRM permite tener un mayor control sobre la información de la entidad. Se recomienda su utilización siempre que se trabaje con información sensible para la empresa. Es necesario, al igual que en el caso de las herramientas DLP, que el usuario esté concienciado del motivo de la utilización de este tipo de herramientas, y que, además, se combine con la aplicación de procedimientos y políticas de seguridad con el fin de añadir una capa adicional de protección de la información.

5.4.4.3 Dispositivos móviles (MDM)

Las soluciones de gestión de dispositivos móviles (del inglés Mobile Device Management, MDM) son un tipo de software que permite controlar, monitorizar y garantizar la seguridad de dispositivos móviles corporativos, como smartphones, tabletas o portátiles, mediante las políticas de seguridad que la empresa establezca, lo cual permite asegurar, monitorizar y administrar todos los dispositivos móviles de nuestra organización de una manera centralizada. La intención de las soluciones MDM es optimizar la funcionalidad y la seguridad de los dispositivos móviles dentro de la organización, a la vez que se protege la red corporativa.

Las funcionalidades principales de un MDM son las siguientes:

- Instalación ágil de aplicaciones en remoto desde un único punto de control.
- Administración centralizada de dispositivos.
- Localización vía satélite.
- Sincronización de archivos.

- Bloqueo de funciones.
- Control de gastos.
- Borrado remoto (para casos de extravío, robo o pérdida).
- Gestión de contraseñas.

NOTA: *La norma N/SEG/TEC-011-1 SEGURIDAD POR DEFECTO para dispositivos portátiles y móviles exige la implantación de soluciones de gestión centralizada de los dispositivos, del tipo MDM (Mobile Device Manegement) o similar, que permitan, en cualquier caso, la monitorización, el borrado remoto de datos o la realización de auditorías de seguridad sobre dichos dispositivos.*

5.4.5 Protección de credenciales

Mediante nuestras credenciales de acceso podemos acceder a los diferentes servicios y aplicaciones de la entidad. Se trata de información muy sensible, la cual deberemos proteger de manera adecuada.

Para ello deberemos tener en cuenta dos aspectos fundamentales:

- Creación de credenciales.
- Gestión de credenciales.

5.4.5.1 Creación de credenciales

En primer lugar, deberemos asegurarnos de que las claves que utilicemos sean robustas. Para ello, debemos tratar de que nuestra contraseña:

- Contenga al menos ocho caracteres: "credencial"
  Tiempo estimado de descifrado = 1 hora -> Nivel de seguridad **bajo**

- Contenga tanto letras mayúsculas, como minúsculas: "CredENciaL"
  Tiempo estimado de descifrado = 1 mes -> Nivel de seguridad **medio/bajo**

- Contenga números y caracteres especiales: ""C9e9dEnc!4L"
  Tiempo estimado de descifrado = 400 años -> Nivel de seguridad **alto**

5.4.5.2 Gestión de credenciales

En segundo lugar, debemos asegurar la confidencialidad, integridad y disponibilidad de nuestras credenciales. Para ello, haremos uso de gestores de credenciales, los cuales noes permitirán almacenar y gestionar de una manera segura las contraseñas utilizadas en los servicios y aplicaciones de la entidad.

Mediante una única clave de acceso, se puede acceder a un repositorio con todas nuestras credenciales. Es una muy buena opción desde el punto de vista de la seguridad, reemplazando de esta manera al almacenamiento de credenciales en los navegadores web ("Guardar contraseña para este sitio") o al almacenamiento tradicional en archivos de texto digitales o físicos.

Los gestores de contraseñas nos ofrecen un inicio de sesión unificado a modo de Single Sign-On, mediante el cual no será necesario acceder al repositorio de contraseñas cada vez que necesitemos acceder a un servicio o aplicación.

Los gestores de credenciales nos ofrecen beneficios tales como:

- Almacenamiento seguro y centralizado de contraseñas (tan solo deberemos recordar una contraseña).
- Mejora del nivel de seguridad de las claves almacenadas (periodicidad cambio de claves, comprobación de credenciales, mejora de la robustez de credenciales, etc).
- Algoritmos de cifrado seguro.
- Inicio de sesión automático.
- Gestores multiplataforma.

5.5 Medidas y buenas prácticas de seguridad

Atendiendo a las necesidades de seguridad demandadas por la práctica del teletrabajo, se han seleccionado algunas medidas y buenas prácticas de seguridad, las cuales, a partir de su implantación y realización, van a ayudar a mitigar posibles riesgos que puedan comprometer la seguridad de la información en las entidades.

Estas medidas serán clasificadas en los siguientes apartados:

- Seguridad lógica
- Seguridad física

5.5.1 Seguridad lógica

5.1.1.1 Control de acceso

Con el objetivo de mejorar la seguridad en el acceso lógico a los recursos de la entidad, es necesario que los sistemas cuenten con mecanismos de control de acceso robustos, basados en procesos de identificación y autentificación.

Los controles de acceso deben ser buscar el equilibrio entre permitir un acceso ágil al sistema, y la seguridad y protección de los recursos albergados en este. Según la criticidad de la información que se quiera proteger, la balanza se decantará más hacia un lado o hacia otro.

5.5.1.1.1 Identificación

Mediante el proceso identificación, se identifica de manera exclusiva a un usuario de un sistema entre un conjunto de usuarios. Adicionalmente, este cuenta con un rol determinado (administrador, usuario, etc.).

De esta manera se identifica:

- Quién recibe derechos de acceso.
- Quién ha realizado cada acción en el sistema.

Tendremos, por tanto, una cuenta de usuario con unos derechos de acceso por defecto y configurables por el administrador del sistema.

Conseguiremos, por tanto:

- Establecer una estructura jerarquizada de ID's diferenciando por niveles de acceso.
- Tener una visibilidad completa de toda la actividad de los usuarios.

5.5.1.1.2 Autenticación

El proceso de autenticación permite validar la identidad de un usuario. Es decir, se comprueba si el usuario que se identifica dice quién dice ser.

Los mecanismos de autenticación basan su funcionamiento en la validación de credenciales. Habitualmente se demanda información acerca de:

- Algo que se conoce (por ejemplo, una contraseña o un PIN).
- Algo que se tiene (por ejemplo, tokens)

- Algo que es propio del usuario (por ejemplo, identificación biométrica mediante huella dactilar).

Es una buena práctica de seguridad combinar los diferentes factores de identificación, por ejemplo, demandando contraseña y PIN, o contraseña, PIN y factor biométrico. De esta manera, la seguridad lógica de los controles de acceso a los sistemas de información se ve incrementada.

5.5.2 Seguridad física

Debido a la utilización de dispositivos portátiles en situación de teletrabajo, vamos a estar expuestos a riesgos asociados a la seguridad física del dispositivo, no solo en el entorno de teletrabajo, sino también en el proceso de transporte del dispositivo desde la oficina hasta el lugar de teletrabajo, y viceversa.

Es por ello, que debemos tener en cuenta los riesgos asociados a los dos escenarios descritos anteriormente; seguridad física en el puesto de teletrabajo y seguridad física en el proceso de transporte del dispositivo.

5.5.2.1 Puesto de teletrabajo

En el propio puesto de teletrabajo, debemos contar con medidas de seguridad, tales como:

- Guardar el dispositivo en un lugar seguro. Se recomienda utilizar armarios de seguridad o espacios custodiados bajo llave.
- Utilizar un atril para apoyar el dispositivo, con el fin de mejorar la ergonomía y el equilibrio, y de esta manera evitar caídas o golpes.
- Considerar cambiar el disco duro por uno SSD, con el objetivo de mitigar las posibles consecuencias de cualquier tipo de vibración o caída, lo cual podría llegar a causar una pérdida total de los datos almacenados.
- Implementar una política de puesto de trabajo despejado, o en el caso de existir, seguirla en situación de teletrabajo.

5.5.2.2 Transporte del dispositivo

Por otro lado, mientras estamos transportando el dispositivo desde la oficina hasta el puesto de trabajo, o viceversa, debemos contar también con algunas consideraciones de seguridad, tales como:

- Utilizar una funda, maletín o mochila de seguridad para evitar robos, extravíos, pérdidas o golpes.
- Utilizar candados de seguridad para portátiles para evitar robos, extravíos o pérdidas.
- Implementar soluciones de borrado remoto con el objetivo de proteger información corporativa en caso de robo, extravío o pérdida (explicado en el apartado 5.3).

Adicionalmente, debemos contar unas medidas y buenas prácticas de seguridad, tales como:

- No dejar el dispositivo en el coche.
- No dejar el dispositivo desatendido.

5.5.3 Utilización de dispositivos no corporativos: BYOD

Hoy en día, y debido a factores tales como la proliferación del uso de dispositivos móviles (smartphones, tablets y ordenadores portátiles) en el ámbito laboral, las mejoras en las especificaciones de estos dispositivos en cuanto a software, hardware o conectividad en red, y a la necesidad imperante de teletrabajar en determinadas ocasiones, multitud de entidades siguen políticas de "trae tu propio dispositivo" o también conocidas por sus siglas en inglés BYOD (Bring Your On Device), mediante las cuales se permite al usuario conectarse a la red corporativa y acceder a los recursos de la entidad mediante su dispositivo personal.

Las políticas de BYOD aportan una serie de ventajas respecto a la utilización de dispositivos corporativos, como, por ejemplo:

- Reducción de costes debido al ahorro en hardware que supone la no inversión inicial en dispositivos y la simplificación en la gestión de dispositivos.
- Mejora en la movilidad de los usuarios, posibilitando el teletrabajo (en caso de que la organización no disponga dispositivos portátiles corporativos).
- Mejora en la productividad del usuario y en la colaboración corporativa.

Sin embargo, también encontramos algunos riesgos asociados a este tipo de políticas, los cuales deben ser tenidos en cuenta previamente a la implementación final en la entidad. Los principales riesgos a tener en cuenta asociados a políticas de BYOD son los siguientes:

- Robo, extravío, cesión involuntaria o daño del dispositivo.

- Falta de actualizaciones de seguridad debido a la ausencia de una gestión centralizada de los dispositivos.
- Ausencia de controles de seguridad en el sistema operativo.
- Mecanismos de control de acceso poco seguros.
- Conexiones inalámbricas poco seguras (utilización de redes Wi-Fi inseguras, Bluetooth, NFC).
- Ausencia de cifrado en las comunicaciones.
- Instalación de aplicaciones poco seguras.
- Riesgo en la finalización de relación laboral del usuario debido al almacenamiento de información de la entidad en su dispositivo.

Implantar una política de BYOD en una entidad no es una tarea que deba tomarse a la ligera, pues existen diferentes riesgos que pueden comprometer la seguridad de la de la entidad. Sin embargo, la adecuada adopción de esta, siguiendo una serie de recomendaciones y buenas prácticas de seguridad, puede mejorar notablemente la productividad en la entidad, especialmente cuando no se dispone de dispositivos portátiles corporativos.

Algunos de los puntos que deben tenerse en cuenta en la implementación de políticas de BYOD son los siguientes:

- Crear una política o normativa interna que regule el uso de los dispositivos utilizados y darla a conocer a todos los usuarios de la entidad.
- Definir e implantar un sistema de roles, autorizaciones de acceso, inventario de dispositivos, niveles/privilegios de acceso, etc.
- Mantener actualizados/parcheados de manera continua los sistemas operativos y las aplicaciones del dispositivo.
- Elaborar listas negras y listas blancas de aplicaciones permitidas.
- Prohibir la utilización de dispositivos que hayan sido rooteados o cuenten con un jailbreak.
- Evitar el uso de redes Wi-Fi abiertas o inseguras, así como fomentar el uso de las redes móviles corporativas.
- Utilizar VPN en caso de ser necesario.
- Implementar mecanismos de control de acceso seguros habilitando MFA; contraseñas robustas, acceso biométrico, bloqueo automático por tiempo máximo de inactividad, etc.
- Evitar la cesión voluntaria del dispositivo a terceros.

NOTA: *La opción de incorporar al teletrabajo dispositivos personales de los trabajadores requeriría modificar la normativa interna, pues la norma N/SEG/USU-002-3 solo contempla la posibilidad de utilizarse dispositivos portátiles o móviles no proporcionados por la Diputación con carácter excepcional por tiempo muy limitado, o cuando se trate de información clasificada como PÚBLICA. No obstante, la nueva regulación básica del teletrabajo en el EBEP (art. 47 bis) exige a la administración proporcionar y mantener los medios tecnológicos necesarios para la actividad.*

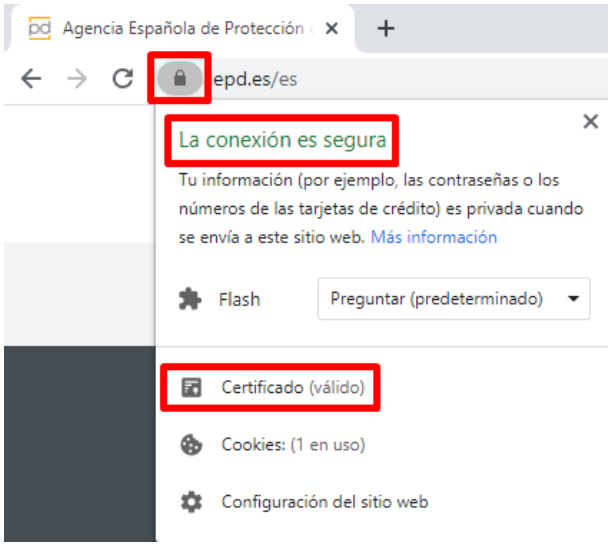
5.5.4 Navegación segura

Se debe evitar la navegación por páginas no seguras y evitar la descarga/instalación de cualquier archivo/software no legítimo. También deberemos evitar acceder a enlaces o hipervínculos de dudosa reputación.

Podemos asegurarnos si la conexión a un sitio web es segura o no, mediante una serie de consideraciones.

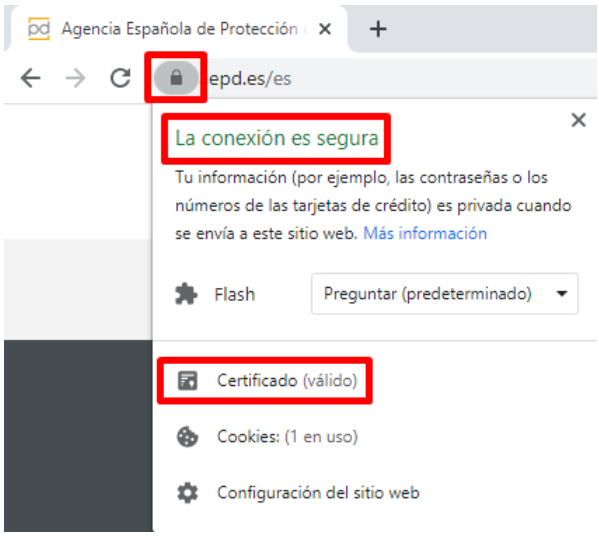
1. Candado de seguridad

   En primer lugar, la inclusión del candado en el encabezamiento de la barra de navegación es un indicador de que la conexión a ese sitio web es segura. El candado va a estar relacionado con el protocolo de transferencia de hipertexto utilizado (3). En caso de ser una página web no segura el candado aparecerá en rojo.



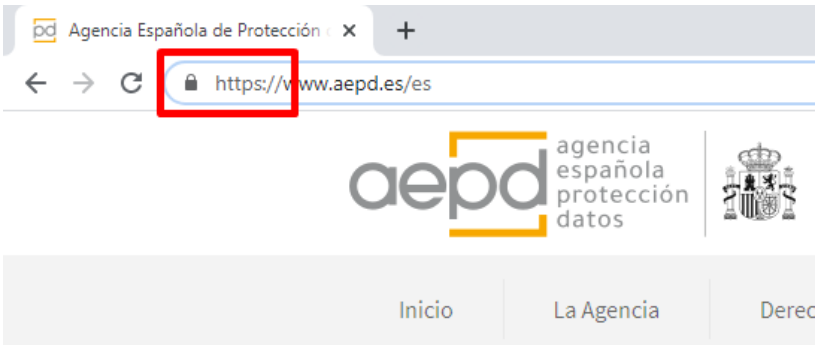
2. Certificado SSL (Secure Sockets Layer)

   Adicionalmente, podremos comprobar la validez y la vigencia del certificado SSL, haciendo click en Certificado. Se trata de un certificado digital que autentica la identidad de un sitio web determinado y asegura el cifrado de información con tecnología SSL.



3. Protocolo HTTPS

   El protocolo seguro de transferencia de hipertexto (HTTPS) valida un cifrado seguro de los datos. Esto repercute en que la información intercambiada entre el navegador y el sitio web no sea accesible a terceros. Se trata de un protocolo más seguro que el HTTP.



Asimismo, se recomienda mantener los navegadores web actualizados y eliminar periódicamente el historial de navegación, las cookies, las contraseñas recordadas por el navegador y otros archivos temporales similares, con el objetivo de reducir el riesgo de sufrir un robo de credenciales por parte de ciberdelincuentes.

5.6 Despliegue progresivo

5.6.1 Diseño de pruebas piloto

El objetivo principal de un **Plan de Despliegue de Teletrabajo** es gestionar una situación en la que los usuarios no puedan realizar sus labores desde las instalaciones convencionales de la organización, asegurando la posibilidad de trabajar desde otros entornos.

La mejor forma de asegurarse de que el Plan de Despliegue del Teletrabajo es claramente eficaz es manteniéndolo actualizado, realizando los cambios sustanciales que se consideren necesarios en la organización y en los Sistemas de la Información y ejecutando las pruebas periódicas que validen que los sistemas están preparados con las funciones establecidas.

Durante las primeras pruebas, consideradas como pruebas piloto, se deben detectar todos aquellos escenarios que puedan amenazar la continuidad de la modalidad de teletrabajo, entre otros:

- Incidentes y problemas a la hora de que los balanceadores de carga funcionen correctamente
- Falta de licencias ante aplicaciones necesarias para una adecuada gestión del teletrabajo.
- Velocidad de adecuada de la línea de internet doméstica, la cual debe proporcionar un caudal y capacidades apropiados para conectarse a los Sistemas de Información de la organización.

5.6.2 Autorización y puesta en marcha

Se recomienda que la organización orqueste el despliegue teniendo en cuenta los puntos tratados en esta guía. Para ello se determinarán las autorizaciones necesarias de forma que, ante la incorporación de elementos en los Sistemas de Información, se atenúe la confianza en el sistema.

Como último punto a trazar, se debe realizar el despliegue asegurando una correcta aplicación de la Mejora Continua.

5.6.3 Concienciación y formación

Se debe concienciar y formar al usuario en materia de seguridad de la información, privacidad y protección de datos. De ello dependerá, en gran medida, y de manera conjunta con las medidas técnicas de seguridad adoptadas en la entidad, el nivel de seguridad global de la entidad y el correcto cumplimiento de la normativa vigente en materia de protección de datos.

Es necesario que los usuarios conozcan y apliquen una serie de hábitos y buenas prácticas de seguridad en referencia al desarrollo de su actividad laboral en un entorno tecnológico como el actual, sin olvidarse de la importancia de proteger los datos de carácter personal bajo su responsabilidad. Será este pues, un punto estratégico en la prevención de incidentes de seguridad, y la comisión de cualquier actividad ilícita en materia de protección de datos.

Con el fin de lograr las metas de seguridad establecidas, será necesario el total compromiso por parte de la dirección y por parte de los usuarios.

Se debe conseguir que los usuarios de la entidad:

- Conozcan la Política de Protección de Datos de la entidad, así como los protocolos internos, fundamentalmente:
  - ejercicio de derechos;
  - notificación de brechas de seguridad.
- Conozcan, entiendan y cumplan las normas y las medidas de seguridad definidas.
- Conozcan y entiendan los riesgos a los que se exponen en el paradigma tecnológico actual, y más concretamente en situación de teletrabajo.
- Sepan cómo prevenir los diferentes riesgos a los que están expuestos y cómo actuar en caso de que el riesgo se materialice en una amenaza.

5.6.3.1 Concienciación

Se debe concienciar de manera regular a los usuarios acerca de su papel y responsabilidad para que la seguridad de la entidad alcance los niveles exigidos en situación de teletrabajo. Es de primera necesidad que el usuario esté concienciado acerca de su función en el devenir de la seguridad de la información en la compañía.

Con el objetivo de concienciar a los usuarios en materia de seguridad de la información, se debe:

- Difundir la Política de Protección de Datos y de Seguridad de la Información.
- Difundir las normas internas de protección de datos y seguridad corporativas.
- Promover una cultura de protección de datos personales y de seguridad de la información.

5.6.3.2 Formación

Se debe formar al usuario de manera continua, con el objetivo de que conozca a qué riesgos se enfrenta en materia de seguridad y qué puede hacer él como usuario para prevenirlos.

En situación de teletrabajo, podemos encontrar una serie de riesgos (de seguridad y en materia de protección de datos) que no suelen darse en el puesto de trabajo. Es por ello, que se debe preparar al usuario, con el objetivo de que su formación, su criterio y su pensamiento crítico, actúen como primera línea de defensa frente a los riesgos y amenazas.

Con el objetivo de formar a los usuarios en materia de protección de datos y seguridad de la información, se recomienda:

- Definir un plan de formación a usuarios.
- Desarrollar programas de formación específicos adecuados a los diferentes puestos de trabajo en la entidad.
- Evaluar el aprendizaje obtenido por parte de los usuarios.
- Promover una cultura de protección de datos y seguridad de la información.
- Promover la difusión y el cumplimiento de los controles y medidas de seguridad referentes al teletrabajo definidos en las normas de seguridad:
    - ISO/IEC 27000:
        - ISO/IEC 27001:2013
        - ISO/IEC 27002:2013
    - NIST SP 800-53 rev. 4
    - NIST SP 800-50
- Promover buenas prácticas de seguridad en el tratamiento de la información.

6 SUPERVISIÓN DEL ESTADO DE LA SEGURIDAD

6.1 Análisis de registros de actividad

Ante un modelo de teletrabajo auditar las acciones procesadas por los Sistemas de Información de la organización es un proceso necesario e importante para poder detectar incumplimientos de las políticas o normativas. En consecuencia, el administrador de sistemas, ante una anomalía, podrá resolver preguntas como, por ejemplo:

- ¿Qué acciones ha realizado un usuario?
- ¿Quién ha eliminado un registro en concreto?
- ¿Quién ha actualizado un valor de un registro? ¿Cuándo lo ha hecho?

Es recomendable disponer de sistemas que generen eventos a partir de reglas establecidas. Ver punto Monitorización y gestión de eventos (SIEM).

6.2 Monitorización y gestión de eventos (SIEM)

Los sistemas de gestión de la seguridad de la información y eventos de seguridad (del inglés Security Information and Event Management, SIEM) representan una solución de seguridad integral, la cual procesa, analiza y correlaciona información proveniente de múltiples fuentes de información, con el objetivo de detectar comportamientos anómalos o sospechosos que puedan transformarse en una amenaza de seguridad. Se recopilan, por tanto, eventos de seguridad de todas las tecnologías que intervienen en una red (antivirus, firewalls, IDS, IPS, etc) con el objetivo de analizar, en tiempo real, tendencias y patrones fuera de lo común que permitan detectar a tiempo potenciales amenazas de seguridad, manteniendo la infraestructura TIC de la entidad segura.

Las herramientas SIEM ofrecen beneficios tales como:

- Integración de diferentes fuentes de información.
- Monitorización del estado global de la seguridad de la infraestructura TIC.
- Detención de amenazas desconocidas mediante la aplicación de machine learning y tecnologías next-gen.
- Gran velocidad de análisis y correlación de eventos de seguridad.
- Posibilidad de buscar amenazas en registros archivados.
- Protección con carácter preventivo.

6.2.1 Sistemas de detección de intrusiones (IDS)

Los sistemas de detección de intrusiones (del inglés Intrusion Detection System, IDS) son herramientas de seguridad que tienen como funcionalidad principal detectar anomalías en los sistemas, que puedan repercutir en amenazas mayores.

Cabe destacar que este tipo de herramientas no frenan amenazas por sí solos, sino que requieren de herramientas adicionales para ello.

Existen dos tipos diferentes de IDS, dependiendo de si actúan a nivel de host o de red:

- HIDS (Host Intrusion Detection System)
- NIDS (Network Intrusion Detection System)

6.2.2 Sistemas de prevención de intrusiones (IPS)

Los sistemas de prevención de intrusiones (del inglés, Intrusion Prevention System, IPS) tienen como funcionalidad principal prevenir amenazas. Los IPS son considerados una extensión, en lo que a prevención de amenazas se refiere, de los IDS, y una tecnología más avanzada en comparativa con los firewalls tradicionales, debido a que las decisiones que se toman en un sistema IDS están basadas en función del comportamiento del tráfico y no de reglas estáticas. Esto es un punto muy a tener en cuenta cuando hablamos de ataques de denegación de servicio distribuido (DDoS), de malware avanzado o de amenazas persistentes avanzadas (ATP).

Al igual que sucede en los IDS, también encontramos diferentes tipos de IPS:

- HIPS (Host Intrusion Prevention System)
- NIPS (Network Intrusion Prevention System)
- WIPS (Wireless Intrusion Prevention System)
- NBA (Network Behavior Analysis)

6.3 Control de la actividad laboral

Las organizaciones pueden adoptar las medidas de vigilancia y control de la actividad laboral que estimen más oportunas, para verificar el cumplimiento de las obligaciones de sus empleados, así como para garantizar la integridad de los activos de la entidad y la seguridad de los propios trabajadores, siempre y cuando se respete la intimidad, la dignidad y el resto de derechos del trabajador que la legislación establece.

La rápida evolución de la tecnología aplicada al entorno laboral ha derivado en la introducción de nuevas herramientas de supervisión capaces de, por ejemplo, monitorizar el tiempo invertido, las operaciones realizadas, los sitios web visitados, las pulsaciones del teclado o incluso lo que se está visualizando en la pantalla. Estas formas de control cada vez se han generalizado más con el paso de los últimos años, especialmente en el momento del incremento del trabajo a distancia, dada la ausencia de supervisión visual en el puesto de trabajo habitual.

No obstante, el control intensivo y permanente de la actividad de las personas puede atentar al derecho de su intimidad, al considerarse una forma desproporcionada de control. Aspecto que se aplica independientemente de la forma de trabajo en la que se desarrolle la actividad.

Los trabajadores tienen derecho así a la protección de su intimidad en el uso de estos dispositivos digitales puestos a su disposición, tal y como se reconoce en la LOPD-GDD.

La entidad debe establecer criterios y protocolos de utilización y control de estos medios respetando en todo caso los estándares mínimos de protección de su intimidad, de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En estos protocolos se deben desarrollar una serie de principios fundamentales para que el control que ejerza la organización se realice siempre de forma legal y justificada, asegurando que los mecanismos de control tecnológico de la actividad laboral cumplan los condicionantes de idoneidad, necesidad y proporcionalidad.

Un adecuado mecanismo para evaluar la conveniencia de estos mecanismos es la realización de un análisis de riesgos, o una Evaluación de Impacto sobre la Protección de Datos para cada tratamiento implicado dado el caso, de acuerdo a los criterios comentados en el punto 4.1 de Identificación de amenazas y gestión de riesgos, a fin de garantizar que estos medios de supervisión no supongan un riesgo sobre los derechos y libertades de las personas.

NOTA: *La norma N/SEG/USU-009 determina que La Diputación de Valencia llevará a cabo esta actividad de monitorización sin utilizar sistemas o programas que pudieran atentar contra los derechos constitucionales de los usuarios, tales como el derecho a la intimidad personal y al secreto de las comunicaciones, manteniéndose en todo momento la privacidad de la información manejada, salvo que, por requerimiento legal e investigación sobre un uso ilegitimo o ilegal, sea necesario el acceso a dicha información, salvaguardando en todo momento los derechos fundamentales de los usuarios.*

6.4 Mejora continua

Aplicar el proceso de mejora continua será una actividad fundamental que pretende mejorar tanto los productos, servicios o procesos de la organización.

Aplicado al entorno del teletrabajo, debemos buscar que todos aquellos cambios que la organización haya implantado logren las metas propuestas, acomodándose a las necesidades y requisitos deseados, y detectando todas aquellas áreas que requieran de mejora hasta alcanzar la plena satisfacción en su conjunto.

Para ello se recomienda definir una serie de indicadores que nos permitan medir la idoneidad, adecuación y eficacia de las soluciones implantadas, de forma que nos permita analizar su capacidad para alcanzar nuestros objetivos, decidiendo sobre su conveniencia o detectando aspectos de mejora.

Por ejemplo, algunos indicadores relacionados con el teletrabajo podrían ser:

- Ratio de usuarios que se han incorporado a la política de teletrabajo.
- Ratio de incidentes de seguridad detectados en entornos de teletrabajo.
- Relación de pruebas de continuidad relacionadas con teletrabajo ejecutadas con resultados satisfactorios.
- Porcentaje del personal que solita modalidad de trabajo a distancia.
- Ratio de carga de la capacidad de la red de datos.
- Nota media obtenida de las pruebas de conocimiento tras la realización de cursos de formación y concienciación en materia de seguridad.
- Porcentaje de equipos y dispositivos con pleno cumplimiento de las directrices de bastionado.

Asimismo, para obtener unas mediciones adecuadas, es recomendable determinar:

- Quién es el responsable de medir.
- Periodos de medición.
- Metas y objetivos a alcanzar.
- Métrica utilizada.

De esta forma, poniendo el foco en los aspectos clave, recabando y analizando los datos adecuados, obtendremos la información necesaria que nos ayude en la toma de decisiones para conseguir una mejora evidente de los procesos, los servicios y el estado de la seguridad del entorno del teletrabajo.

7 RECAPITULACIÓN

La implantación de la modalidad de teletrabajo en la organización supone un impacto fundamentalmente en:

• **La información tratada**. En el específico caso de los datos de carácter personal, se ven afectados básicamente dos colectivos titulares de dichos datos: Los titulares externos –ciudadanos, proveedores de bienes y servicios, usuarios, etc- y los titulares internos –empleados públicos en situación de teletrabajo-

• **Los medios de tratamiento**. Los instrumentos tecnológicos para desarrollar el teletrabajo y, por ende, utilizados en el tratamiento de la información tienen características y singularidades distintas que requieren diferentes actuaciones: dotación, configuración, adaptación y control.

• **El entorno físico de la prestación**. La modalidad de teletrabajo contiene en esencia un traslado del entorno físico del trabajo a ubicaciones ajenas a las de la organización.

• **La organización interna**. Los procesos, dinámicas y controles son diferentes en el caso del teletrabajo.

• **La regulación interna**. La modalidad de teletrabajo exige cambios regulatorios en las normativas internas.

Los citados aspectos impactados **generan nuevos escenarios de riesgo**, tanto en lo relativo a la seguridad como a las garantías de cumplimiento legal, para los datos de carácter personal y los sistemas de información. Este nuevo escenario y los riesgos asociados deben ser tenidos en cuenta en dos momentos: a la hora de abordar una norma interna reguladora del teletrabajo y, posteriormente, cuando deban implementarse todas las actuaciones técnicas, jurídicas y organizativas para facilitar esta nueva modalidad de prestación del trabajo.

En el cuerpo de la presente guía se han abordado directrices para ambos momentos, según los servicios competentes afectados. Como principios generales de aplicación podemos apuntar:

❶ La regulación interna del teletrabajo debe asegurar contener preceptos que contemplen los escenarios que la nueva modalidad supone para los datos de carácter personal y la seguridad de la información. En aquellos aspectos que no difieran de lo ya regulado a nivel interno en la Corporación bastará con hacer referencia a la norma

correspondiente. En cualquier caso, la incorporación del teletrabajo exigirá modificar ciertos aspectos en las normativas internas vigentes, sobre todo las relacionadas con la seguridad de la información.

❷ La regulación interna del teletrabajo no puede suponer, en ningún caso, ir en contra de las garantías de los derechos legales de los titulares de los datos personales; tanto si dichos titulares son externos a la organización como si se trata de los empleados públicos implicados en la modalidad de teletrabajo.

❸ La regulación interna del teletrabajo no puede suponer una merma en la seguridad de la información tratada. Cuando se contemplen situaciones que entren en conflicto con la normativa interna vigente en la materia, deberá modificarse el cuerpo normativo que corresponda. En ningún caso dicha modificación podrá atentar contra disposiciones de carácter superior (ENS, etc).

❹ La regulación interna del teletrabajo deberá contener garantías directas para mantener la **concienciación y formación** en materia de protección de datos y seguridad de la información de los empleados que hagan uso de la modalidad de teletrabajo, incluso con carácter obligatorio para dichos empleados. La formación deberá ser previa y como condición al acceso a la modalidad de teletrabajo, y mantenerse actualizada a lo largo de la permanencia del empleado en dicha situación.

❺ En la puesta en marcha del teletrabajo resulta recomendable la elaboración de un **Plan de implantación**, que atienda a las directrices recogidas en el apartado **4 Análisis del contexto y toma de decisiones y 5 Diseño e implantación del teletrabajo**. Muy especialmente se recomienda poner en práctica un **Plan de Despliegue de Teletrabajo**, donde puedan contrastarse todas las medidas en un grupo piloto.

❻ A nivel organizativo, lo recomendable sería constituir un **grupo de seguimiento corporativo de teletrabajo**, con la presencia de representantes de los servicios más implicados. La mejora continua podría encajar muy bien en el seno de este grupo.

8 GLOSARIO DE TÉRMINOS

Este glosario está basado en la guía de seguridad Glosario y Abreviaturas (CCN-STIC-401)

- **Amenaza**: Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Disponibilidad**: o disposición a ser usado cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.
- **DLP**: medidas de seguridad que tratan de evitar que la información confidencial o valiosa sea copiada o trasladada fuera del entorno de seguridad.
- **Gestión del riesgo**: el proceso, distinto de la evaluación del riesgo, consistente en sopesar las alternativas políticas existentes mediante consultas con las partes interesadas, analizar la evaluación del riesgo y otros factores legítimos y, si fuera necesario, seleccionar las opciones de prevención y control.
- **IDS**: Software o hardware utilizado para identificar o alertar acerca de intentos de intrusión en redes o sistemas. Conformado por sensores que generan eventos de seguridad; una consola que supervisa eventos y alertas y controla los sensores; y un motor central que registra en una base de datos los eventos denotados por los sensores.
- **Riesgo**: una función de la probabilidad de que una vulnerabilidad del sistema afecte a la autenticación o a la disponibilidad, autenticidad, integridad o confidencialidad de los datos procesados o transferidos y la gravedad de esa incidencia, resultante de la utilización intencionada o no intencionada de esa vulnerabilidad.
- **Tratamiento de riesgos**: El proceso de selección e implementación de las medidas encaminadas a modificar los riesgos.
- **Salvaguarda**. Conjunto de acciones, métodos y sistemas destinados evitar que se produzcan actos ilícitos y/o accidentes que puedan afectar al desarrollo natural de las actividades en una organización.
- **VPN**: Acrónimo de "virtual private network" (red privada virtual). Una red informática donde algunas conexiones son circuitos virtuales dentro de redes más extensas, como Internet, en lugar de conexiones directas por medio de cables físicos. Cuando este es caso, los puntos finales de una red virtual se transmiten a través de una red mayor. Al contrario de una aplicación común, formada por comunicaciones seguras en la red pública, una red VPN puede presentar o no funciones de seguridad, como la autenticación y el cifrado de contenidos.

9 BIBLIOGRAFÍA

- **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.**

- **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)**

- **Anteproyecto de ley de trabajo a distancia.**

- **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. Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.**

- **ISO/IEC 27000:2013: Sistemas de Gestión de Seguridad de la Información.**

- **Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.**
  - https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1001

- **Centro Criptológico Nacional (CCN)**

  - Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html
  - Guía de Seguridad de las TIC CCN-STIC 804. ENS. Guía de implantación. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file.html
  - Guía CCN-CERT BP/18. Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia.

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4691-ccn-cert-bp-18-recomendaciones-de-seguridad-para-situaciones-de-teletrabajo-y-refuerzo-en-vigilancia-1/file.html

- Guía de Seguridad de las TIC CCN-STIC 2002. Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE). https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/2000-organismo-de-certificacion/4557-ccn-stic-2002-metodologia-de-evaluacion-para-la-certificacion-nacional-esencial-de-seguridad-lince/file.html
- Guía de Seguridad de las TIC CCN-STIC 836ENS. Seguridad VPN. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2299-ccn-stic-836-seguridad-en-vpn-en-el-marco-del-ens/file.html

- **Instituto Nacional de Ciberseguridad (INCIBE)**
  - Ciberseguridad en el teletrabajo https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf
  - Dispositivos móviles personales para el uso profesional (BYOD) https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf
  - Decálogo ciberseguridad empresas https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf
  - Como gestionar una fuga de información https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_fuga_informacion_0.pdf

- **Common Criteria for Information Technology Security Evaluation (CC)**
  - https://www.commoncriteriaportal.org/

ANEXO A: Listado de herramientas

A.1 Protección de Endpoint y de perímetro de red

A.1.1 Cortafuegos

- Next Generation Firewall (Check Point Software Technologies): https://www.checkpoint.com/es/products/next-generation-firewall/
- FortiGate: Next Generation Firewall (Fortinet): https://www.fortinet.com/products/next-generation-firewall
- Sophos CG Firewall (Sophos): https://www.sophos.com/es-es/products/next-gen-firewall.aspx
- Cisco ASA (Cisco): https://www.cisco.com/c/en/us/products/security/asa-firepower-services/index.html#~models
- Cisco Meraki MX (Cisco): https://meraki.cisco.com/products/security-sd-wan/
- Cisco Firepower (Cisco)
- https://www.cisco.com/c/en/us/products/security/firewalls/index.html
- SonicWall (SonicWall): https://www.sonicwall.com/es-mx/products/firewalls/
- Barracuda CloudGen (Barracuda): https://www.barracuda.com/products/cloudgenfirewall

A.1.2 Endpoint Detection and Response (EDR)

- SentinelOne Endpoint Protection Platform (SentinelOne): https://www.sentinelone.com/services/
- Intercept X Endpoint (Sophos): https://www.sophos.com/es-es/products/endpoint-antivirus.aspx
- Falcon Insight Endpoint Detection and Response (CrowdStrike): https://www.sentinelone.com/services/
- Malwarebytes Endpoint Detection and Response (Malwarebytes): https://es.malwarebytes.com/business/edr/
- Microsoft Defender Advanced Threat Protection (Microsoft): https://www.microsoft.com/en-us/microsoft-365/windows/microsoft-defender-atp
- Kaspersky Endpoint Detection and Response (Kaspersky): https://www.kaspersky.com/enterprise-security/endpoint-detection-response-edr
- Cytomic Endpoint Detection and Response (Cytomic):

https://www.cytomic.ai/es/soporte/edr/

- VMware Carbon Black EDR (VMware): https://www.carbonblack.com/products/endpoint-detection-and-response/
- VMware Carbon Black Cloud Enterprise EDR (VMware): https://www.carbonblack.com/products/enterprise-endpoint-detection-and-response/

A.2 Acceso remoto

A.2.1 Red privada virtual (VPN)

- Check Point Capsule (Check Point Software Technologies): https://www.checkpoint.com/es/products/remote-access-vpn/
- AnyConnect (Cisco): https://www.cisco.com/c/es_es/products/security/anyconnect-secure-mobility-client/index.html
- FortiClient (Fortinet): https://www.fortinet.com/products/vpn
- Citrix Gateway (Citrix): https://www.citrix.com/es-es/products/citrix-gateway/
- GlobalProtect (Palo Alto Networks): https://www.paloaltonetworks.com/products/globalprotect

A.2.2 Infraestructura de escritorio virtual (VDI)

- Red Hat Virtualization (Red Hat): https://www.redhat.com/en/technologies/virtualization/enterprise-virtualization#
- Nuntanix (Nuntanix): https://www.nutanix.com/solutions/vdi
- VirtualBox (Oracle): https://www.virtualbox.org/
- Amazon WorkSpaces (Amazon): https://aws.amazon.com/es/workspaces/

A.2.3 Infraestructura móvil virtual (VMI)

- Nubo VMI (Nubo software): https://nubosoftware.com/what-is-vmi
- Hypori VMI (Hipory virtual mobility): https://hypori.com/
- SierraVMI (Sierraware):

https://www.sierraware.com/vmi-virtual-mobile-infrastructure.html

A.2.4 Escritorio remoto

- TeamViewer (TeamViewer): https://www.teamviewer.com/es/descarga/windows/
- VNC Connect (RealVNC): https://www.realvnc.com/es/connect/
- Chrome Remote Desktop (Google): https://remotedesktop.google.com/?pli=1
- Mikogo (Mikogo): https://www.mikogo.es/
- VMware Workspace ONE (VMware): https://www.vmware.com/es/products/workspace-one.html
- VMware Horizon Cloud (VMware): https://www.vmware.com/es/products/horizon-cloud-virtual-desktops.html
- Citrix Cloud Services (Citrix) https://www.citrix.com/es-es/products/citrix-cloud/
- Prisma Access (Palo Alto Networks): https://www.paloaltonetworks.com/prisma/access
- WebEx Meetings (Cisco): https://www.webex.com/es/index.html

A.3 Herramientas de colaboración

A.3.1 Servicio de correo electrónico

- Gmail (Google): https://mail.google.com/
- Outlook (Microsoft): https://outlook.live.com/owa/
- AOL Mail (AOL): https://www.aol.com/
- Zoho Mail (Zoho): https://www.zoho.com/es-xl/mail/
- Fastmail (Fastmail): https://www.fastmail.com/business/
- Onlyoffice (Onlyoffice): https://www.onlyoffice.com/es/

A.3.2 Producción, edición y almacenamiento de documentos

- Google Drive (Google): https://gsuite.google.com/intl/es-419/products/drive/
- Dropbox (Dropbox): https://www.dropbox.com/business
- Microsoft (Microsoft 365): https://www.microsoft.com/es-es/microsoft-365?rtc=1
- Cisco Webex Teams (Cisco): https://www.webex.com/es/team-collaboration.html
- Zoomrooms (Zoom): https://zoom.us/es-es/zoomrooms.html
- Amazon Web Services (AWS): https://aws.amazon.com/es/
- Box (Box): https://www.box.com/es-419/collaboration
  Onehub (Onehub): https://www.onehub.com/features

A.3.3 Videollamada y reuniones

- Microsoft Teams (Microsoft): https://www.microsoft.com/es-es/microsoft-365/microsoft-teams/group-chat-software
- Skype (Microsoft): https://www.skype.com/es/
- Google Meet (Google): https://gsuite.google.com/intl/es-419/products/meet/
- Cisco Webex (Cisco): https://www.webex.com/es/video-conferencing.html
- Zoom (Zoom): https://zoom.us/es-es/meetings.html
- Slack (Slack): https://slack.com/intl/es-es/solutions/remote-work
- Jitsi (Jitsi): https://meet.jit.si/

A4. Protección de la información

A.4.1 Data Loss Prevention (DLP)

- Symantec DLP (Broadcom):

https://help.symantec.com/home/DLP15.0?locale=ES_MX

- McAfee DLP (McAfee): https://www.mcafee.com/enterprise/en-us/products/data-protection-products.html
- Forcepoint DLP (Forcepoint): https://www.forcepoint.com/es/product/dlp-data-loss-prevention
- Endpoint Protector (CoSoSys): https://www.endpointprotector.es/
- CheckPoint DLP (CheckPoint): https://www.checkpoint.com/products/data-loss-prevention/
- Traxion DLP (Traxion): https://www.traxion.com/en/services/cyber-security-services/preventive-detective-security-services/data-leak-prevention/

A.4.2 Information Rights Management (IRM)

- Sealpath IRM (Sealpath): https://www.sealpath.com/es/sealpath-irm/

A.4.3 Mobile Device Management (MDM)

- Microsoft Intune (Microsoft): https://www.microsoft.com/es-es/microsoft-365/enterprise-mobility-security/microsoft-intune
- IBM Security MaaS360 (IBM): https://www.ibm.com/es-es/security/mobile/maas360
- Airwatch (VMware): https://www.vmware.com/es/products/workspace-one/unified-endpoint-management.html
- Sophos Mobile (Sophos): https://www.sophos.com/es-es/products/free-tools/sophos-mobile-security-free-edition.aspx
- Scalefusion MDM (Scalefusion) https://scalefusion.com/mobile-device-management

A5. Protección de credenciales

A.5.1 Gestión de credenciales

- LastPass Enterprise (LogMeIn): https://www.lastpass.com/es/products/enterprise-password-management-and-sso

- ManageEngine ADSelfService Plus (ManageEngine): https://www.manageengine.com/es/self-service-password/?pos=MEtab&cat=AD&loc=tab&prev=AB2
- 1Password (1Password): https://1password.com/es/business/
- Dashlane (Dashlane): https://www.dashlane.com/es/business/
- Keepass (Keepass): https://keepass.es/
- Keeper (Keeper): https://www.keepersecurity.com/es_ES/business.html

A7. Supervisión del estado de la seguridad

A.7.1 Monitorización y gestión de eventos (SIEM)

- IBM QRadar (IBM): https://www.ibm.com/es-es/marketplace/ibm-qradar-siem
- Splunk (Splunk): https://www.splunk.com/
- ArcSight Enterprise Security Manager (Microfocus): https://www.microfocus.com/es-es/products/siem-security-information-event-management/overview
- AlienVault OSSIM (AT&T Cybersecurity): https://cybersecurity.att.com/products/ossim
- McAfee SIEM (McAfee): https://www.mcafee.com/enterprise/es-es/products/siem-products.html
- FortiSIEM (Fortinet): https://www.fortinet.com/lat/products/siem/fortisiem

A.7.2 Sistemas de detección de intrusiones (IDS)

- Bro (Zeek): https://zeek.org/
- OSSEC (OSSEC): https://www.ossec.net/
- Snort (Snort): https://www.snort.org/
- Suricata (Suricata): https://suricata-ids.org/
- Security Onion (Security Onion): https://securityonion.net/

A.7.3 Sistemas de prevención de intrusiones (IPS)

- McAfee Network Security Platform (McAfee): https://www.mcafee.com/enterprise/es-es/products/network-security-platform.html
- CheckPoint Intrusion Prevention System (IPS): https://www.checkpoint.com/products/intrusion-prevention-system-ips/
- FortiGate: IPS (Fortinet): https://www.fortinet.com/products/ips
- Next-Generation Intrusion Prevention System (NGIPS): https://www.cisco.com/c/es_es/products/security/ngips/index.html
- SolarWinds Security Event Manager (Solarwinds): https://www.solarwinds.com/es/security-event-manager

ANEXO B: Escenarios de riesgo

Se listan a continuación un conjunto de escenarios de riesgo a considerar en el análisis de la exposición de los tratamientos a amenazas.

ID	ESCENARIOS DE RIESGO DE CUMPLIMIENTO
RP	**Escenarios de riesgo que pueden afectar a los principios**
RP.1	La base que legitima el tratamiento no es adecuada, es ilícita o no se ha formalizado adecuadamente (hay que prestar atención a las categorías especiales de datos y la gestión del consentimiento)
RP.2	Si el tratamiento se basa en el interés legítimo: no se ha ponderado adecuadamente este interés legítimo en relación con los intereses, derechos y libertades fundamentales del interesado
RP.3	Las finalidades del tratamiento no son precisas, son ilegítimas, etc.
RP.4	Hay un cambio de finalidad que puede ser incompatible con la finalidad original
RP.5	Hay un cambio de finalidad compatible, pero puede invalidar una evaluación de impacto previa
RP.6	Se recogen datos inadecuadas, no pertinentes, excesivas o innecesarias para la finalidad prevista
RP.7	Se registran datos inexactos o no se mantienen actualizadas
RP.8	Los datos personales se conservan más tiempo del necesario
RP.9	Los datos se tratan de manera desleal o poco transparente (no se cumple la expectativa de la persona interesada respecto al tratamiento de sus datos)
RP.10	Se hacen operaciones de tratamiento desproporcionadas

ID	ESCENARIOS DE RIESGO DE CUMPLIMIENTO
RD	**Escenarios de riesgo que pueden afectar a los derechos**
RD.1	En el momento de la recogida de los datos no se proporciona la información mínima prevista en la persona afectada (cuando los datos se obtienen directamente de la persona) o no se le proporciona ninguna información, cuando se obtienen de terceros
RD.2	La respuesta al ejercicio de los derechos del interesado no se hace en el tiempo y la forma pertinentes
RD.3	Se toman decisiones que afectan a una persona utilizando exclusivamente medios automatizados
RD.4	No hay procedimientos para dar una respuesta adecuada a los derechos
RD.5	La organización desconoce los procedimientos para responder el ejercicio de derechos
RD.6	No se verifica adecuadamente la identidad de la persona que ejerce un derecho
RO	**Escenarios de riesgo que pueden afectar a las obligaciones**
RO.1	Se incumple la regulación general sobre el derecho a la protección de los datos de carácter personal
RO.2	Se incumplen otras regulaciones sectoriales que inciden en la protección de los datos de carácter personal
RO.3	Se incumplen las cláusulas sobre la protección de datos incorporados a los contratos o condiciones de uso
RO.4	Se incumplen estipulaciones recogidas en un código de conducta (si se está adherido)
RO.5	No se puede demostrar el cumplimiento (responsabilidad proactiva)

ID	ESCENARIOS DE RIESGO DE CUMPLIMIENTO
RO.6	Las certificaciones o sellos de protección de datos no se han renovado o han perdido vigencia
RO.7	No se ha tenido cuenta la protección de datos a la hora de diseñar el tratamiento (de manera parcial o total)
RO.8	No se ha incorporado la protección de datos por defecto en las operaciones de tratamiento (de manera parcial o total)
RO.9	No se ha hecho una consulta previa a la autoridad de supervisión, cuando era necesaria
RO.10	Los encargados de tratamiento no se han seleccionado adecuadamente
RO.11	No se ha formalizado adecuadamente la relación con encargados de tratamientos
RO.12	No se ejerce suficiente control sobre la actividad del encargado de tratamiento (en las operaciones de tratamiento que le han sido encargadas)
RO.13	Se desconocen las cadenas de subcontratación de encargados de tratamiento
RO.14	No se dispone del registro de actividades del tratamiento (si es obligatorio)
RO.15	No se mantiene actualizado (no se gestiona) el registro de actividades de tratamiento
RO.16	Las violaciones de datos no se notifican en el tiempo y la forma pertinentes (violación de la seguridad de los datos)
RO.17	Las violaciones de datos no se comunican en el tiempo y la forma pertinentes (violación de la seguridad de los datos)
RO.18	Las limitaciones del tratamiento no se comunican a terceros

ID	ESCENARIOS DE RIESGO DE CUMPLIMIENTO
RO.19	Hay transferencia internacional de datos no autorizada o desconocida
RO.20	Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados
RO.21	No se ha designado delegado de protección de datos (si es obligatorio)
RO.22	No se proporcionan medios suficientes al delegado de protección de datos
RO.23	No se atiende un requerimiento de la autoridad de supervisión competente
RO.24	No se hace la evaluación de impacto (si es obligatoria)
RO.25	No se implantan las medidas derivadas de una evaluación de impacto
RO.26	No se atienden las instrucciones de una autoridad de protección de datos
RO.27	No se verifican las medidas adoptadas (auditoría de cumplimiento)
RDL	**Escenarios de riesgo que pueden afectar a otros derechos y libertades**
RDL.1	Vulneración de la imagen, la intimidad o el honor de las personas
RDL.2	Vulneración del libre desarrollo de la personalidad
RDL.3	Discriminación por razón de sexo, raza, religión, opinión, etc.

ID	ESCENARIOS DE RIESGO DE CUMPLIMIENTO
RDL.4	Violación del secreto de las comunicaciones
RDL.5	Atentado contra la dignidad de las personas
RDP	**Escenarios de riesgo que pueden causar directamente daños y perjuicios**
RDP.1	Discriminar a una persona en un proceso competitivo
RDP.2	Discriminar a un colectivo
RDP.3	Impacto económico negativo
RDP.4	Peligro para la integridad física o salud
RDP.5	Suplantación de la identidad del interesado
RDP.6	Perjudicar a la reputación
RDP.7	Prohibir el acceso físico
RDP.8	Impedir o denegar la obtención de un servicio
RDP.9	Impedir una contratación
RDP.10	Denegar una ayuda o ventaja

ID	ESCENARIOS DE RIESGO DE PROTECCIÓN DE LA INFORMACIÓN
SEG.1	Posible destrucción accidental de datos personales
SEG.2	Posible destrucción malintencionada de datos personales
SEG.3	Posible pérdida de datos personales
SEG.4	Posible alteración no autorizada de datos personales
SEG.5	Posible comunicación no autorizada de datos personales
SEG.6	Falta de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo.
SEG.7	Posible acceso no autorizado a datos personales
SEG.8	Los sistemas de información no están disponibles (incidente que provoca que los datos personales no estén disponibles)
SEG.9	Hay incapacidad para detectar y gestionar incidentes que afectan a la seguridad de los datos
SEG.10	Fuego
SEG.11	Daños por agua
SEG.12	Avería de origen físico o lógico
SEG.13	Corte del suministro eléctrico

ID	ESCENARIOS DE RIESGO DE PROTECCIÓN DE LA INFORMACIÓN
SEG.14	Condiciones inadecuadas de temperatura o humedad
SEG.15	Fallo de servicios de comunicaciones
SEG.16	Degradación de los soportes de almacenamiento de la información
SEG.17	Errores de los usuarios
SEG.18	Errores del administrador del sistema / de la seguridad
SEG.19	Deficiencias en la organización
SEG.20	Difusión de software dañino
SEG.21	Vulnerabilidades de los programas (software)
SEG.22	Errores de mantenimiento / actualización de programas (software)
SEG.23	Errores de mantenimiento / actualización de equipos (hardware)
SEG.24	Caída del sistema por agotamiento de recursos
SEG.25	Pérdida o robo de equipos
SEG.26	Indisponibilidad del personal

ID	ESCENARIOS DE RIESGO DE PROTECCIÓN DE LA INFORMACIÓN
SEG.27	Suplantación de la identidad
SEG.28	Abuso de privilegios de acceso
SEG.29	Uso no previsto
SEG.30	Denegación de servicio
SEG.31	Ingeniería social (picaresca)

ANEXO C: Lista de verificación

A la hora de implantar la modalidad de teletrabajo seguro se recomienda realizar un diagnóstico de situación que permita conocer mejor el estado de madurez de las herramientas y medidas de la organización. De esta forma, la organización podrá conocer cuáles son las prioridades a la hora de abordar un proyecto de esta índole.

Se presentan a continuación una batería de preguntas que, a título orientativo, pueden ser de utilidad:

LISTA DE VERIFICACIÓN	CHECK
Ciberseguridad	
Definir y distribuir entre los empleados la política establecida por la organización sobre seguridad de la información y teletrabajo.	☐
Proteger dispositivos y equipos portátiles mediante cifrado (si es posible, mediante cifrado por hardware).	☐
En los casos en que sea posible, disponer de filtros en la pantalla que dificulten la visualización a personas ajenas.	☐
Establecer obligatoriedad de uso de doble factor de autenticación para el acceso a sistemas de forma remota, incluyendo correo electrónico y cualquier sistema o aplicación crítico.	☐
Fomentar el uso de gestores de contraseñas seguros.	☐
Formar y concienciar a los usuarios en materia de seguridad de la información, como por ejemplo: ▪ evitar el acceso a los equipos por familiares o amigos, ▪ no acceder a páginas web con contenidos sospechosos o inapropiados, ▪ no compartir contraseñas, ▪ conocer los canales de notificación de incidentes establecidos, ▪ bloquear manualmente las sesiones abiertas cuando se abandona el puesto de trabajo, ▪ etc.	☐
Definir y distribuir las normas y directrices establecidas por la organización respecto al uso responsable y protección de la información, particularmente en el entorno de teletrabajo.	☐

LISTA DE VERIFICACIÓN	CHECK
Analizar la posibilidad de filtrar accesos a páginas de contenido inapropiado (Por ejemplo, a través de un Proxy Cloud, Lista Negra, etc.)	☐
Verificar que los equipos y dispositivos se mantienen actualizados y disponen de los elementos de protección establecidos por la organización.	☐
Permisos de los usuarios	
Asegurar que los usuarios no disponen de permisos de administración de los equipos y dispositivos desde los que acceden remotamente a los sistemas de la organización.	☐
Asegurar que los usuarios con permisos de administración disponen de otro identificador sin permisos de administración y lo utiliza para las operaciones diarias que no requieren de privilegios elevados.	☐
Asegurar que los usuarios, y especialmente los que disponen de permisos de administración, cumplen con los requisitos de fortaleza y protección de acceso.	☐
Recordar las obligaciones adquiridas en materia de seguridad.	☐
Correo electrónico	
Prevenir periódicamente de la existencia de correos malintencionados y la necesidad de no abrir bajo ningún concepto adjuntos sospechosos.	☐
Recordar a los empleados la necesidad de reportar cualquier identificación sospechosa de correo electrónico malintencionado.	☐
Videollamadas y reuniones online	
Recordar la necesidad de silenciar los micrófonos cuando no se está hablando activamente en una reunión.	☐
Concienciar sobre la necesidad de bloquear por defecto la webcam.	☐

LISTA DE VERIFICACIÓN	CHECK
Recordar la necesidad de no dejar los dispositivos desbloqueados si abandonamos temporalmente el espacio de trabajo, especialmente durante una videollamada.	☐
Concienciar respecto a no trabajar en espacios públicos si es posible, especialmente cuando se trabaje con documentos o se encuentren en reuniones donde se traten contenidos confidenciales.	☐
Privacidad	
Recordar a todo el personal la responsabilidad de respetar la privacidad y proteger los datos de carácter personal que se están tratando.	☐
Recordar la prohibición de enviar información personal por canales no protegidos, como correo electrónico, almacenar información en ubicaciones distintas a las establecidas por la organización, o mantener los datos más allá de lo estrictamente necesario.	☐
Detección y respuesta a incidentes	
Concienciar periódicamente al personal con objeto de permanecer alerta y saber detectar potenciales ataques o actividades sospechosas.	☐
Formar al personal sobre los canales disponibles para notificar la identificación de cualquier potencial ataque o actividad sospechosa.	☐
Asegurar que los canales establecidos para la gestión de incidentes, tanto propios como de proveedores, están disponibles y funcionan de forma eficaz.	☐
Asegurar que el equipo de seguridad permanezca atento y busque activamente actividades sospechosas, especialmente sobre los canales que existe actividad en remoto.	☐
Definir, distribuir y asegurar que el personal conoce los procedimientos relacionados con la gestión de incidentes de seguridad y las funciones de sus roles.	☐
Copias de seguridad	
Proporcionar el software y los mecanismos necesarios para garantizar que la copia de seguridad de la información tratada.	☐

LISTA DE VERIFICACIÓN	CHECK
Concienciar al personal sobre la necesidad de realizar una copia de seguridad de los datos que están tratando mediante los medios y mecanismos establecidos por la organización.	☐
Concienciar al personal para que no utilice servicios de almacenamiento en la nube externos no aprobados por la organización.	☐

ANEXO D: Formulario para la realización de un EIPD sobre el tratamiento en modalidad de teletrabajo

Rellenando el presente documento estaremos en disposición de elaborar un informe de evaluación de impacto en materia de protección de datos, sobre los nuevos tratamientos de datos que se puedan crear en situación de teletrabajo.

ANÁLISIS DE LA OBLIGACIÓN DE REALIZAR UNA EIPD: EVALUACIÓN DEL RIESGO

INCLUSIÓN DEL TRATAMIENTO EN LA LISTA DE TRATAMIENTOS EXENTOS

☐ Tratamientos que se realizan estrictamente bajo las directrices establecidas o autorizadas con anterioridad mediante circulares o decisiones emitidas por las Autoridades de Control, en particular la AEPD, siempre y cuando el tratamiento no se haya modificado desde que fue autorizado.

☐ Tratamientos que se realizan estrictamente bajo las directrices de códigos de conducta aprobados por la Comisión Europea o las Autoridades de Control, en particular la AEPD, siempre y cuando una EIPD completa haya sido realizada para la validación del código de conducta y el tratamiento se implementa incluyendo las medidas y salvaguardas definidas en la EIPD.

☐ Tratamientos que sean necesarios para el cumplimiento de una obligación legal, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, siempre que en el mismo mandato legal no se obligue a realizar una EIPD, y siempre y cuando ya se haya realizado una EIPD completa.

☐ Tratamientos realizados en el ejercicio de su labor profesional por trabajadores autónomos que ejerzan de forma individual, en particular médicos, profesionales de la salud o abogados, sin perjuicio de que pueda requerirse cuando el tratamiento que lleven a cabo cumpla, de forma significativa, con dos o más criterios establecidos en la lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos publicada por la AEPD.

☐ Tratamientos obligatorios por ley y realizados con relación a la gestión interna del personal de las PYMES con finalidad de contabilidad, gestión de recursos humanos y nóminas, seguridad social y salud laboral, pero nunca relativos a los datos de los clientes.

☐ Tratamientos realizados por comunidades y subcomunidades de propietarios tal como se definen en el artículo 2 (a, b y d) de la Ley 49/1960 de Propiedad Horizontal.

☐ Tratamientos realizados por colegios profesionales y asociaciones sin ánimo de lucro para la gestión de los datos personales de sus propios asociados y donantes, y en el ejercicio de su labor, siempre que no incluyan en el tratamiento de datos sensibles tales como los que se establecen en el artículo 9.1 del RGPD y no sea de aplicación el artículo 9.2(d) de dicho Reglamento.

Si el tratamiento está en la lista de tratamientos exentos establecida en el marco del artículo 35.5 del RGPD, no es obligatorio realizar la EIPD

ANÁLISIS DE LA INCLUSIÓN DEL TRATAMIENTO EN LOS CASOS DE TRATAMIENTOS OBLIGADOS

En este apartado se determinará si hay una obligación de realizar la EIPD. Para ello se tendrá en cuenta, en particular, si el tratamiento:

- Entra en la lista de casos enumerados en el artículo 35.3 del RGPD.
- Cumple con las condiciones que se detallan en la lista, aprobada por el Comité Europeo de Protección de Datos, de tratamientos obligados (artículo 35.4 del RGPD) que puede consultarse aquí y su carácter es meramente orientativo.
- Se dan los supuestos de mayor riesgo de los casos enumerados en el artículo 28.2 de la LOPDGDD.

ELEMENTOS A ANALIZAR	SI/NO
¿La autoridad de supervisión competente ha publicado una lista de tratamientos para los cuales se debe hacer la evaluación de impacto? Responder sólo en caso afirmativo. ¿El tratamiento objeto de evaluación se puede considerar incluido en esta lista?	
¿La autoridad de supervisión competente ha publicado una lista de tratamientos que no se deben evaluar? Responder sólo en caso afirmativo.	
¿Consideramos que el tratamiento no encaja claramente en ninguno de los supuestos de la lista?	
¿Con las operaciones de tratamiento, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables?	

A todos los efectos, ¿podemos considerar que una de las finalidades del tratamiento es elaborar perfiles personales o predecir comportamientos?	
A partir del tratamiento de los datos, ¿se toman decisiones con efectos jurídicos para las personas afectadas?	
A partir del tratamiento de los datos, ¿se toman decisiones que pueden afectar significativamente o perjudicar de alguna manera las personas afectadas?	
¿Se tratan datos a gran escala de alguna categoría especial?	
¿Se tratan datos relativos a condenas o infracciones penales?	
¿El tratamiento implica un control sistemático, monitorización o supervisión a gran escala de áreas de acceso público?	

Si alguna de las respuestas es "SI", muy probablemente estaremos ante un tipo de tratamiento de los previstos en el artículo 35.3 del RGPD y por tanto habrá que hacer la EIPD.

FACTORES DE RIESGO (WP 248)	SI/NO
¿El tratamiento implica la evaluación o puntuación de personas?	
¿El tratamiento implica elaborar perfiles de personas o hacer predicciones sobre su comportamiento?	
¿La finalidad del tratamiento es tomar decisiones de manera automatizada, que puedan tener efectos jurídicos?	
¿La finalidad del tratamiento es tomar decisiones de manera automatizada, que puedan tener efectos similares a los jurídicos, o efectos significativos para las personas?	
¿El tratamiento implica algún tipo de vigilancia sistemática? (observación, supervisión y control de personas)	
¿Se tratan categorías especiales de datos?	
¿Se tratan datos relativos a condenas o infracciones penales?	
¿Se traten datos que es puedan considerarse como muy personales?	
¿Se tratan datos a gran escala?	

¿El tratamiento implica combinar diferentes fuentes de información o datos relacionados con tratamientos diversos?	
¿Se tratan datos relativos a personas en situación de vulneración o de desequilibrio respecto del responsable del tratamiento?	
¿Se tratan datos de niños? (personas menores de 18 años)	
¿Las operaciones de tratamiento utilizan o aplican soluciones tecnológicas u organizativas de forma innovadora?	
¿El tratamiento puede impedir a las personas afectadas utilizar un servicio o ejecutar un contrato?	

ELEMENTOS COMPLEMENTARIOS A ANALIZAR	SI/NO
¿La iniciativa o proyecto supone recoger datos de carácter personal que hasta ahora no se recogían?	
¿La iniciativa implica relacionar diferentes fuentes u orígenes de datos personales (cruzar información), que de alguna manera incrementen la capacidad de análisis de la información?	
¿La información se ha sometido a un proceso de disociación o seudonimización?	
¿Se prevé utilizar información personal de la que se dispone, para finalidades o usos diferentes a los previstos inicialmente?	
¿La iniciativa que se tiene que evaluar implica el uso de tecnologías que se pueden percibir como especialmente intrusivas para la privacidad?	
¿Hay riesgos específicos para la seguridad de la información, especialmente un riesgo relevante de que terceros no autorizados accedan?	
¿Se han previsto transferencias internacionales de datos?	
¿Se tratan datos de personas menores de 18 años?	
¿Se tratan datos de personas menores de [14] años?	

Estas preguntas, y el análisis de las respuestas, nos permiten detectar cuestiones que, si bien de forma aislada tal vez tendrían una incidencia

directa en la decisión de hacer la EIPD, su valoración conjunta quizás sí que nos lleva a considerar que estamos ante un tratamiento que supone un alto riesgo.

ANÁLISIS DE LA NECESIDAD DEL TRATAMIENTO

El Juicio de Idoneidad: si el tratamiento planteado consigue los objetivos propuestos.

El Juicio de Necesidad: determinar si el tratamiento es necesario, en el sentido de que no existe otra alternativa menos invasiva para la privacidad para conseguir este propósito con la misma eficacia o con una eficacia razonable.

ASPECTOS DEL TRATAMIENTO	SI/NO	JUSTIFICACIÓN
Los datos recogidos se van a usar exclusivamente para la finalidad declarada y no para ninguna otra no informada ni incompatible con la legitimidad de su uso (principio de limitación de la finalidad).		
La finalidad que se pretende cubrir requiere de todos los datos a recabar y para todas las personas interesados afectados (principio de minimización de datos).		
Las tecnologías empleadas para el tratamiento son adecuadas para la finalidad establecida desde el punto de vista del cumplimiento de los principios fundamentales de la privacidad.		
Los datos no se mantienen más tiempo del necesario para las finalidades del tratamiento (principio de limitación del plazo de conservación)		

CONCLUSION	

BENEFICIOS PARA LOS INTERESADOS

☐ Beneficios directos y objetivos para los sujetos sobre los que inciden los riesgos.

☐ Beneficios globales para la sociedad

☐ Mejor servicio para todos los ciudadanos y/o los sujetos bajo riesgo

☐ Mayor accesibilidad a la información

☐ Mayor sostenibilidad medioambiental

☐ Mayor transparencia en el tratamiento de los datos

☐ Mejora sustancial de la salud para los ciudadanos y/o los sujetos bajo riesgo

☐ Ayuda y protección a personas en situación de riesgo o desfavorecidas

☐ La protección frente a amenazas para la seguridad del Estado, la defensa o la seguridad pública.

☐ Aumentar la eficacia de los servicios a los ciudadanos y/o los sujetos bajo riesgo

☐ Servicios públicos más accesibles e integradores.

☐ Disminuir la discriminación (por género, por edad, por nacionalidad, por discapacidad, etc)

☐ Empoderamiento del interesado.

☐ Otros

BENEFICIOS PARA LA ENTIDAD O LAS AA.PP. EN GENERAL

☐ Cumplimiento normativo

☐ Mejora de la eficiencia

☐ Reducción de costes

☐ Incremento del control de las actuaciones de las AA.PP.

☐ Mejora del factor de transparencia para el responsable

☐ Mejora de la seguridad de las entidades

☐ Mejora de imagen

☐ Objetivos de responsabilidad social de la organización

☐ Otros

EVALUACIÓN DEL NIVEL DE RIESGO

Es necesario realizar un análisis del riesgo intrínseco, de acuerdo con el artículo 35.7.c del RGPD, para determinar e identificar los elementos de riesgo para los derechos y libertades de las personas, tanto los inherentes al tratamiento como los que se derivan del entorno en los que se desenvolverá el tratamiento.

Ejemplo Amenazas tratamiento teletrabajo:

- Accesos no autorizados a datos personales.
- Violaciones de la confidencialidad de los datos personales por parte de los empleados de la organización.
- Inexistencia de responsable de seguridad o deficiente definición de sus funciones y competencias.
- Inexistencia de política de seguridad en situaciones de teletrabajo.
- Deficiencias organizativas en la gestión del control de accesos.
- Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.
- Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información.
- Uso de identificadores que revelan información del afectado.
- Deficiencias en la protección de la confidencialidad de la información.
- Falta de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo.
- Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados.

MEDIDAS PARA LA REDUCCIÓN DEL RIESGO

El objeto de este apartado es el de establecer medidas de gestión, organización, definición del tratamiento, procedimentales y técnicas que permiten gestionar cada uno de los elementos de riesgo identificados en el apartado anterior.

IDENTIFICACIÓN AMENAZA	MEDIDA DE CONTROL

ALTERNATIVAS AL TRATAMIENTO Y POR QUÉ NO SE HAN ELEGIDO

En los casos de tratamientos de alto riesgo, en este apartado hay que evaluar por qué no se han elegido otras alternativas a la forma de diseñar e implementar el tratamiento que impliquen un menor riesgo.

Para el caso de que sea una mejora, extensión o modificación de un tratamiento, es necesario señalar las ventajas de la nueva aproximación al tratamiento y que la finalidad que se persigue no se pueda conseguir por otros medios.

Guías del Departamento de Protección de Datos y
Seguridad de la Información