DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Guia de teletreball

Diputació de València

Aspectes a considerar des de la perspectiva de la protecció de dades i seguretat de la informació

Informació del document:

Títol del document	Guia de teletreball
Tipus de document	Document guia
Descripció	Guia d'aspectes a considerar per a la implementació del teletreball en la Diputació de València des de la perspectiva de la protecció de dades i seguretat de la informació.
Propietari del document	Document elaborat pel Departament de Protecció de Dades i Seguretat de la Informació de la Diputació de València.

PERMISOS D'ACCÉS:

Data	Tipus[1]	Identificació
25/09/2020	03	Serveis interns Diputació

[1] Tipus d'accés autoritzat

01 Accés total (02 + 04)

02 Lectura + modificació

03 Lectura

04 Reproducció-còpia

05 Cancel·lació de permisos

DATA D'EMISSIÓ: Setembre 2020

Índex

1 MOTIVACIÓ

En el marc de l'organització interna, la Diputació de València ha decidit regular la prestació del treball mitjançant la modalitat denominada teletreball. Amb aquesta finalitat, el Servei de Personal ha assumit la tasca d'elaborar el text normatiu que s'haurà de proposar per a la seua aprovació pels òrgans competents i, en aquest sentit, el Servei citat va traslladar al Departament de Protecció de Dades i Seguretat de la Informació (25-06-2020) un esborrany normatiu perquè aquest departament fera les apreciacions oportunes.

La implementació del teletreball requereix tindre en consideració aspectes de diferent naturalesa. Pel que fa referència a la protecció de dades personals i seguretat de la informació, les qüestions que suscita guarden relació directa amb canvis en els mètodes i les fórmules del tractament de les dades i les alteracions substancials en els instruments i canals tecnològics, com també en els entorns físics on es duen a terme els processos de tractament de la informació utilitzats pels empleats que s'incorporen a la modalitat de teletreball. Tot això comporta uns nous escenaris de risc que han de ser tinguts en compte abans d'implementar una regulació. A més, el nou paradigma ha de conciliar-se no sols amb la legislació aplicable a aquestes matèries sinó també amb les regulacions internes actualment vigents en la corporació. L'expressat anteriorment significa que, en l'ordre pràctic, siguen diferents serveis o àrees competencials de la corporació els que es vegen afectats o implicats en l'execució dels aspectes específics que les dues matèries, la protecció de dades personals i la seguretat de la informació, exigeixen a la nova modalitat de prestació del treball que es pretén instaurar.

Per aquesta raó, el **delegat de Protecció de Dades de la Diputació** ha considerat que la millor manera d'abordar les implicacions comentades no és interactuant exclusivament amb el Servei de Personal, sinó obrint les directrius i consideracions al conjunt dels serveis, especialment als més estretament implicats —Informàtica, Formació, Contractació, Secretaria General…— perquè, des de la primera conformació del que serà futura normativa interna, puguen apreciar el nivell de participació i exigència que els puga suposar i formular amb un major criteri les seues inquietuds i/o propostes al Servei de Personal.

Sobre la base de tot l'exposat s'ha decidit confeccionar la present **Guia de Teletreball**, a l'empara del que es disposa en els articles 31, 37.3 i 39.2 del Reglament de política de seguretat i de la protecció de dades de caràcter personal de la Diputació de València.

2 INTRODUCCIÓ

Amb l'evolució creixent i constant de les tecnologies de la informació i les comunicacions (TIC) han sorgit noves possibilitats que estan permetent transformar els processos i l'entorn laboral de les organitzacions, i amb això augmentar-ne la productivitat, competitivitat i resiliència, alhora que millora la qualitat de vida de les persones.

Aquest canvi de paradigma s'ha pogut constatar recentment en la capacitat que han demostrat moltes organitzacions en facilitar formes de treball alternatives en situacions de crisi com la que estem vivint. En el moment en què es publica la present guia, el món es troba en una crisi sanitària derivada de la Covid-19. En aquesta situació, el teletreball, entenent com a tal qualsevol forma flexible d'organització del treball fora de l'entorn de l'oficina o les instal·lacions habilitades per l'organització, incloses aquelles denominades com treball a distància, lloc de treball flexible, treball en remot i entorns virtuals de treball, ha mostrat que és un dels mecanismes més eficaços per a mantindre la continuïtat de les activitats de les organitzacions, mentre es mantenen les mesures de distanciament com a prevenció de possibles contagis.

Aquestes circumstàncies han accelerat la generalització i normalització de l'ús del teletreball, el qual, encara que mostrava una trajectòria ascendent en la seua implantació en l'última dècada, havia tingut un impacte poc significatiu fins ara. Això, generalment, a causa de la falta de cultura d'aquesta modalitat de treball, acostumats a dur a terme activitats de manera presencial, malgrat l'alta demanda d'aquest en la societat.

No obstant això, aquesta necessitat també comporta l'aparició de riscos nous. De fet, la celeritat per a reprendre l'operatiu i la falta de previsió davant aquest escenari de crisi ha abocat moltes organitzacions a implementar canvis organitzatius i tecnològics dràstics sobre entorns no preparats i sense la possibilitat de disposar d'una planificació de temps i recursos adequats, fet que pot suposar, en termes generals, el descuit de les mesures de seguretat necessàries per a garantir la protecció de la informació i l'exercici dels drets i les llibertats de les persones.

Hem de ser conscients que la seguretat de la informació cobra especial rellevància en aquests escenaris. S'ha de tindre en compte no sols aquells riscos derivats de la seua naturalesa mateixa, sinó que, a més, hi ha una tendència evident en l'increment significatiu d'incidents de seguretat relacionats amb atacs malintencionats, i cal esperar que els atacants aprofiten la situació actual, on es generen potencials vulnerabilitats a explotar.

La falta de previsió generalitzada es veu reflectida igualment en l'ordenament jurídic. Fins hui, les úniques referències reguladores relacionades, presents en l'ordenament espanyol, es trobaven en l'article 13 de la Llei de l'Estatut dels Treballadors, en el qual es fa esment al treball a distància. No obstant això, en data 22 de setembre s'ha aprovat el **Reial decret llei 28/2020, de 22 de setembre, de treball a distància**, que regula les condicions d'aquesta modalitat de treball en l'àmbit de les relacions laborals comunes (Estatut dels Treballadors).

En el context del sector públic tampoc no hi ha una legislació bàsica del teletreball. L'EBEP ni tan sols contemplava cap cosa similar al referit article 13 de l'ET. Aquesta mancança actual ha propiciat regulacions sectorials diverses en diferents nivells territorials de l'Administració i ha creat marcs reguladors dispars i condicions singulars segons la naturalesa de l'instrument utilitzat i l'àmbit d'aplicació —instrument legislatiu, norma administrativa, acord de condicions de treball o conveni col·lectiu…— Amb tot, també amb data 29 de setembre, s'ha ratificat pel Consell de Ministres la regulació bàsica del teletreball en les administracions públiques, acordada en la Mesa General de Negociació, que s'incorporarà en un nou **article 47 bis al text refós de la Llei de l'Estatut Bàsic de l'Empleat Públic (TREBEP),** el text del qual és el següent:

> «ARTICLE 47 bis. Teletreball
>
> 1. Es considera teletreball aquella modalitat de prestació de serveis a distància en la qual el contingut competencial del lloc de treball pot desenvolupar-se, sempre que les necessitats del servei ho permeten, fora de les dependències de l'Administració, mitjançant l'ús de tecnologies de la informació i comunicació.
>
> 2. La prestació del servei mitjançant teletreball haurà de ser expressament autoritzada i serà compatible amb la modalitat presencial. En tot cas, tindrà caràcter voluntari i reversible excepte en supòsits excepcionals degudament justificats. Es farà en els termes de les normes que es dicten en desenvolupament d'aquest Estatut, les quals seran objecte de negociació col·lectiva en l'àmbit corresponent i contemplaran criteris objectius en l'accés a aquesta modalitat de prestació de servei.
>
> El teletreball haurà de contribuir a una organització millor del treball a través de la identificació d'objectius i l'avaluació del seu compliment.
>
> 3. El personal que preste els seus serveis mitjançant teletreball tindrà els mateixos deures i drets, individuals i col·lectius, recollits en el present Estatut, que la resta del personal que preste els seus serveis en modalitat presencial, incloent-hi la normativa de prevenció de riscos laborals que resulte aplicable, excepte aquells que siguen inherents a la realització de la prestació del servei de manera presencial.

4. L'Administració proporcionarà i mantindrà, a les persones que treballen en aquesta modalitat, els mitjans tecnològics necessaris per a la seua activitat.

5. El personal laboral al servei de les administracions públiques es regirà, en matèria de teletreball, pel que es preveu en el present Estatut i per les seues normes de desenvolupament.»

2.1 Estructura del document

D'ara en avant, l'estructura del document està organitzada en les seccions següents:

- **Secció 3**: Visió de l'entorn del teletreball. Descriu els conceptes i tipus de teletreball que trobem; la seua utilitat; beneficis i inconvenients, i els drets i les llibertats de les persones que s'han de complir en l'aplicació d'aquest.
- **Secció 4**: Anàlisi del context i presa de decisions. Tracta aquells aspectes que s'han d'analitzar per a abordar el procés de transformació en la facilitació del teletreball amb objectivitat, incloent-hi la identificació d'amenaces, la regulació i el marc normatiu aplicable, o la capacitat tècnica i organitzativa actual.
- **Secció 5**: Disseny i implantació del teletreball. Incideix en els elements que s'han de tindre en compte per a una correcta planificació i posada en marxa del teletreball, tant des de la perspectiva de les mesures organitzatives com de les solucions tecnològiques i les mesures de seguretat.
- **Secció 6**: Supervisió de l'estat de la seguretat. Aborda els tipus de mecanismes de monitoratge i control existents per a garantir la protecció i eficiència de les activitats en un entorn de treball a distància.

Així mateix, aquesta guia conté un **llista d'annexos** amb material de suport addicional. Concretament:

- **Annex A**: Llista d'eines útils per a l'aplicació i el control d'entorns de treball a distància.
- **Annex B:** Escenaris de risc que cal considerar en l'anàlisi de l'exposició dels tractaments d'amenaces en entorns de treball a distància.
- **Annex C**: Llista de verificació per al diagnòstic de situació respecte a l'estat de maduresa de les eines i mesures establides per l'organització en relació amb el treball a distància.
- **Annex D**: Formulari per a la realització d'una AIPD (Avaluació d'impacte sobre protecció de dades) sobre el tractament en modalitat de teletreball.

3 VISIÓ DE L'ENTORN DEL TELETREBALL

3.1 Concepte i tipus de teletreball

En primer lloc, cal destacar la importància de concretar i distingir entre els conceptes de teletreball i de treball a distància, ja que són termes generalitzats i utilitzats indistintament, els quals poden adoptar interpretacions diferents segons el context.

El treball a distància és tota aquella activitat laboral que es porta a terme fora del centre de treball o el lloc determinat per l'organització, és a dir, allò que considerem com activitat no presencial, com podrien ser els casos en els quals l'activitat es desenvolupa en l'habitatge particular de l'empleat o en qualsevol altre lloc triat lliurement.

Malgrat això, el *teletreball*, segons l'Acord marc europeu sobre teletreball, és aquella forma d'organització i/o de treball que es presta mitjançant l'ús de mitjans i sistemes informàtics, telemàtics i de comunicacions, en el marc d'un contracte o d'una relació de treball, en la qual un treball que podria ser realitzat igualment en els locals de l'organització s'efectua fora d'aquests locals.

D'altra banda, el nou article 47 bis de l'EBEP considera teletreball aquella modalitat de prestació de serveis a distància en la qual el contingut competencial del lloc de treball pot desenvolupar-se, sempre que les necessitats del servei ho permeten, fora de les dependències de l'Administració, mitjançant l'ús de tecnologies de la informació i comunicació.

No obstant això indicat anteriorment, a causa de la naturalesa i el propòsit d'aquesta guia, en tot moment ens referirem i tractarem allò concernent al teletreball, ja que, encara que no sols tractarem mesures d'índole tècnica i se citaran aspectes que per la seua transversalitat seran aplicables a qualsevol modalitat de treball a distància, en tot moment ens referirem a aquells treballs que es presten a través de mitjans digitals.

El teletreball pot dur-se a terme en diverses modalitats segons la jornada, en els termes acordats entre l'organització i l'empleat, i aquestes són:

- de manera ocasional,
- de manera habitual a temps complet, o
- de manera habitual en part de la jornada laboral.

3.2 El teletreball com a mitjà per a la continuïtat en la prestació dels serveis

Garantir la continuïtat de la prestació dels serveis davant situacions de crisis o desastres és un factor crític que cal considerar que s'ha de tindre en compte per a qualsevol organització.

Els plans de continuïtat, tal com els entenem, conviden a analitzar la criticitat dels processos i avaluar els riscos potencials que puguen generar un alt impacte que deteriore la prestació dels serveis i puguen derivar-se en un crebant dels compromisos adquirits amb les parts interessades. Mitjançant aquest exercici ens permet anticipar-nos a aquests escenaris, i establir mesures de prevenció que minimitzen l'impacte.

Sobre això, una de les amenaces a les quals sempre estem exposats en relació amb la continuïtat és la impossibilitat d'accedir al centre de treball disposat per l'organització, ja siga per l'afectació en la integritat de les oficines que impedisquen garantir la seguretat de les persones o, com s'ha pogut evidenciar recentment, pel confinament del personal amb motiu de previndre la proliferació de contagis.

En aquest sentit, una de les mesures més habituals que cal considerar per a tractar aquesta tipologia de riscos, per la seua efectivitat i versatilitat quant a la flexibilitat de la mobilitat, és el teletreball.

3.3 Possibles beneficis i inconvenients

En plantejar-se l'opció d'implantar el teletreball i posar a disposició els mecanismes necessaris per a fer-lo possible, hem de ser conscients i analitzar els possibles avantatges i desavantatges que suscita sobre els diferents àmbits en els quals impacta, ja siga directament o indirectament.

Així mateix, cal esmentar que el teletreball no implica sempre beneficis i inconvenients de manera unidireccional i global, sinó que serà variable depenent de cadascun dels aspectes analitzats i fins i tot de la perspectiva de cadascuna de les parts afectades, ja siga la de l'empleat o la de l'organització. És responsabilitat de l'entitat trobar una fórmula competent, eficaç i balancejada, que contribuïsca al benestar i el grat de la majoria en la mesura que siga possible.

Segons es manifesta en l'acord esmentat de la Mesa General de Negociació de les Administracions Públiques, els principals avantatges que aporta aquesta nova regulació, tant per a la societat com per a les administracions públiques són, segons l'acord signat, el foment de les noves tecnologies i el desenvolupament de l'Administració digital, la reducció en els desplaçaments, la sostenibilitat ambiental, en línia amb els ODS 2030, o la millora de la conciliació del desenvolupament professional amb la vida personal i familiar.

A continuació s'expressa un resum de beneficis-inconvenients comunament acceptats:

BENEFICIS	INCONVENIENTS
Inversiones y reducció de costes	
▪ Potencial reducció d'espai físic en oficina. ▪ Estalvi en el consum de subministraments per a l'organització. ▪ Estalvi de costos i temps en desplaçaments.	▪ Inversió inicial en tecnologia i mitjans. ▪ Potencial increment de despeses indirectes per als empleats.
Gestió adequada de la productivitat i la dedicació	
▪ Augment de la productivitat. ▪ Flexibilització d'horaris.	▪ Possible augment de distraccions i disminució de l'eficiència. ▪ Treball en excés. ▪ Potencial reducció de temps de descans mental i físic.
Conciliació familiar i laboral	
▪ Conciliació familiar i laboral. ▪ Disminució de l'absentisme laboral.	▪ Possibles dificultats per a separar el rol laboral de l'espai familiar.
Entorn de treball	
▪ Elecció lliure de l'entorn de treball. ▪ Facilitació de mobilitat geogràfica. ▪ Generació d'oportunitats laborals a col·lectius desafavorits geogràficament. ▪ Adaptació personalitzada de l'entorn. ▪ Reducció d'accidents laborals.	▪ Despeses addicionals per a l'adaptabilitat de l'entorn de treball. ▪ Disminució de la interacció amb companys de treball. ▪ Falta de comunicació, col·laboració i aprenentatge entre equips. ▪ Propensió a l'aïllament. ▪ Limitació de la identitat corporativa.
Atracció i conservació del talent	
▪ Reclam per a l'atracció i conservació del talent en front d'altres organitzacions que no ofereixen flexibilitat organitzativa. ▪ Facilita la contractació i la prestació de serveis. ▪ Facilitat d'ocupació a col·lectius desafavorits.	

3.4 Drets i llibertats de les persones en relació amb el teletreball

Hi ha una sèrie de drets i garanties relacionats amb les persones que treballen a distància que han de ser considerats i tinguts en compte a l'hora d'implementar qualsevol projecte de teletreball en l'organització.

En l'estricte marc que ens ocupa, cal destacar:

3.4.1 Desconnexió digital

Les persones que treballen a distància, particularment en teletreball, tenen dret a la desconnexió digital fora del seu horari de treball, a fi de garantir, fora del temps de treball legal o establit convencionalment, el respecte del seu temps de descans, permisos i vacances, com també la seua intimitat personal i familiar, d'acord amb els termes establits en l'article 88 de la LOPDGDD.

Per aquest motiu, és necessari regularitzar la flexibilitat horària, establint límits, per a aconseguir una separació efectiva entre el temps laboral i el personal.

3.4.2 Intimitat i protecció de dades

En el marc del teletreball, l'organització ha de proveir l'empleat dels mitjans telemàtics necessaris per al seu acompliment. Així mateix, és cada vegada més habitual que es recórrega a mesures de control de la prestació laboral. Amb tot, **aquests mitjans i controls han de garantir el dret a la intimitat i la protecció de dades**, en els termes previstos en la LOPDGDD, i han d'assegurar la idoneïtat, necessitat i proporcionalitat d'aquests.

En els casos en els quals el teletreball es preste a través de dispositius propietat de la persona treballadora, l'organització no pot exigir la instal·lació d'aplicacions.

En cas contrari, l'ús personal dels mitjans disposats per part de l'organització per al teletreball només pot fer-se en aquells casos específics establits prèviament.

NOTA: Als dispositius utilitzats per a la prestació laboral en la modalitat de teletreball també se'ls aplica la norma N/SEG/USU-002-3 NORMES ESPECÍFIQUES PER A DISPOSITIUS PORTÀTILS I MÒBILS

4 ANÀLISI DEL CONTEXT I PRESA DE DECISIONS

Prèviament a la implantació del teletreball, es recomana fer una anàlisi de context que permeta determinar l'estat i les capacitats en els quals es troba l'organització, a fi de poder prendre decisions objectives sobre la seua viabilitat, disseny i planificació. Els punts que cal tindre en compte impliquen:

- Detecció de riscos als quals s'exposa l'entitat.
- Identificació dels marcs reguladors als quals s'ha de donar compliment.

- Anàlisi de capacitat tècnica i organitzativa.

4.1 Identificació d'amenaces i gestió de riscos

L'aplicació de teletreball implica una modificació dels mitjans de tractament de dades, que poden estar exposats a noves amenaces, per la qual cosa es presenten altres escenaris de risc que han de ser considerats, entenent un risc com la combinació de la possibilitat que es materialitze una amenaça i les conseqüències del seu impacte en cas que ocórrega.

Per això, **haurem de dur a terme una anàlisi i gestió de riscos sobre totes aquelles activitats de treball que es vegen afectades per l'ús del teletreball**, sempre amb proporcionalitat i coherència, i tenint presents els requisits de privacitat per al compliment de les garanties dels drets de les persones.

D'acord amb les recomanacions de l'Agència Espanyola de Protecció de Dades (AEPD), és fonamental fer una anàlisi prèvia sobre els tractaments, de manera que puguem discernir entre **aquells tractaments que suposen, per les dades que es tracten, un risc alt per als drets i les llibertats de les persones**, i aquells altres que, en cas que es vegen afectats per una amenaça, no deriven en repercussions i conseqüències greus.

Per a fer aquesta distinció tindrem en compte els criteris següents:

- El Reglament (EU) general de protecció de dades estableix certs supòsits en els quals és obligatòria la realització d'una **Avaluació d'Impacte sobre la Protecció de Dades (AIPD)**, determinats en els punts 35.3, 35.4 i 35.5.
- Per la naturalesa, abast, context i finalitats de tractament.

Una vegada coneguda la criticitat dels tractaments, per a aquells categoritzats com de risc alt és recomanable efectuar una anàlisi detallada i en profunditat de les amenaces que poden afectar-los, fet que anomenem una Avaluació d'Impacte sobre la Protecció de Dades (AIPD). Per a la resta dels tractaments serà suficient fer una anàlisi de riscos bàsica i global.

Per a aquells casos en els quals ja s'hagen analitzat els riscos sobre els tractaments, en compliment d'allò disposat per la regulació en matèria de protecció de dades o, addicionalment, en compliment d'altres regulacions o estàndards de seguretat, s'haurà de revisar i actualitzar aquesta anàlisi tenint en compte els canvis i les casuístiques pròpies de l'aplicació del teletreball. En cas contrari, si no s'han estudiat, haurem de dur a terme una anàlisi de riscos d'acord amb el que es disposa anteriorment.

Independentment de la complexitat i profunditat de l'anàlisi que efectuem, una vegada determinats els àmbits de tractament que cal analitzar, aplicarem una gestió de riscos compresa en tres fases:

En primera instància, bé sobre cadascun dels tractaments, per a dades de risc alt, o a nivell general, en cas contrari, identificarem aquelles amenaces a les quals es veurien exposades, tenint en consideració que quan apliquem la modalitat de treball a distància, estarem exposats a unes noves amenaces.

En aquest sentit, hem d'identificar escenaris de risc tenint en compte dues orientacions:

- Riscos potencials orientats a la protecció de la informació, amb focus en la disponibilitat, integritat i confidencialitat de les dades.
- Riscos associats al compliment dels requisits reguladors relacionats amb els drets i les llibertats dels interessats; requisits normatius, i contractuals.

Per a facilitar aquesta tasca, s'ha elaborat un llistat d'escenaris de riscos recopilat de les guies de l'AEPD i altres catàlegs d'amenaces, que es troba disponible en l'**annex B: Escenaris de risc**.

El pas següent consistirà a avaluar els escenaris de risc que s'han identificat. Per a fer-ho serà necessari establir uns criteris de valoració determinats i adaptats al context de l'organització, de manera que tots els escenaris siguen avaluats de manera objectiva i homogènia, a fi de poder obtindre resultats comparables i repetibles en revisions posteriors.

El procés d'avaluació té com a objectiu valorar, tenint en compte la criticitat del tractament, l'**impacte** de l'exposició a l'amenaça, juntament amb la **probabilitat** que aquesta es materialitze.

Sobre això hi ha diverses metodologies d'avaluació de riscos reconegudes, com per exemple Magerit, àmpliament utilitzada a l'entorn de les administracions públiques.

L'avaluació d'aquests riscos en una fase primerenca ens permetrà gestionar els riscos de manera efectiva, en tractar-los mitjançant la determinació de mesures de control que facen disminuir el seu nivell d'exposició o impacte fins a aconseguir uns nivells de seguretat adequats segons la criticitat de les dades que tractem.

Així mateix, aquestes mesures de seguretat han de ser aplicades tenint en compte els principis de privacitat des del disseny i per defecte. El RGPD estableix en l'article 5 els principis següents, relatius al tractament de dades personals que cal considerar en la definició d'un tractament:

- **Licitud, lleialtat i transparència**: Les dades personals han de ser tractades de manera lícita, lleial i transparent en relació amb l'interessat.
- **Limitació de la finalitat**: Les dades s'han de recollir amb uns fins determinats, explícits i legítims, i no seran tractades ulteriorment de manera incompatible amb aquests fins.
- **Minimització de dades**: Les dades han de ser adequades, pertinents i limitades al que és necessari en relació amb els fins per als quals són tractades.
- **Exactitud**: Les dades han de ser exactes, i si fora necessari, actualitzades. A més, s'estableix que s'adoptaran totes les mesures raonables perquè se suprimisquen o rectifiquen sense dilació, si les dades són inexactes respecte als fins per als quals es tracten.
- **Limitació del termini de conservació**: Les dades han de ser mantingudes de manera que es permeta la identificació dels interessats durant un temps no superior al necessari per a les finalitats del tractament de les dades personals.
- **Integritat i confidencialitat**: Les dades han de ser tractades de manera que es garantisca una seguretat adequada mitjançant l'aplicació de mesures de control apropiades.

Finalment, cal esmentar que la gestió de riscos és un procés continu en el qual hem d'aplicar un monitoratge actiu dels riscos, que haurà de revisar-se cada vegada que hi haja un canvi sobre els tractaments, inclusivament la generació de noves activitats o la inclusió de noves tecnologies.

4.2 Marc normatiu i regulador aplicable

Sempre que es duen a terme noves iniciatives, i especialment en aquelles que tinguen impacte sobre el tractament de la informació i les estructures organitzatives, hem de ser conscients dels requisits legals i les normatives existents en el marc regulador actual, a fi d'implementar les mesures necessàries per a donar-los compliment.

Tot seguit s'indiquen els principals marcs normatius i reguladors que tenen implicacions en l'aplicabilitat del teletreball i que han de ser considerats.

4.2.1 Legislació laboral

Cal assenyalar que en l'àmbit de l'Administració Pública els empleats públics estan subjectes a la Llei de l'Estatut Bàsic de l'Empleat Públic (EBEP). En l'actualitat, tal com se citava en l'apartat 2 Introducció, s'ha introduït, a través de l'article 47 bis de l'EBEP, la regulació bàsica del teletreball en l'àmbit de la funció pública.

4.2.2 Normativa de protecció de dades

Tal com esmenta l'article 32 del Reglament general de protecció de dades (d'ara en avant RGPD), el responsable i l'encarregat de tractament han d'establir les mesures tècniques i organitzatives de seguretat que es consideren necessàries per a minimitzar els riscos de gravetat variable per als drets i les llibertats de les persones físiques, en matèria de protecció de dades.

D'aquesta manera, és imprescindible que l'entitat desplegue les eines i la formació necessàries als empleats perquè actuen amb garanties durant el tractament, aplicant-les no sols en el lloc de treball, sinó també fora de les instal·lacions, com podria ser el domicili.

És funció del delegat de Protecció de Dades de l'entitat supervisar que es determinen les mesures necessàries per a garantir la protecció de les dades de caràcter personal i el compliment de les diferents normatives complementàries en aquest àmbit que resulten d'aplicació.

4.2.3 Esquema Nacional de Seguretat

La disposició addicional primera de la LOPDGDD estableix que, en l'àmbit del sector públic, els responsables hauran d'aplicar als tractaments de dades personals les mesures de seguretat que corresponguen de les previstes en l'Esquema Nacional de Seguretat.

El Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica també disposa, en el seu annex II – Mesures de Seguretat, el control **Accés remot [op.acc.7]**, el qual defineix requisits per a tots els sistemes d'informació independentment de la categorització que haja rebut per la valoració de la informació tractada i el servei prestat. Aquests requisits impliquen mesures de seguretat que cal adoptar per l'organització perquè aquelles

tasques que es realitzen des de fora de les instal·lacions garantisquen la protecció dels sistemes d'informació.

Així mateix, per a sistemes de major criticitat (a partir d'una categorització mitjana), l'Esquema Nacional de Seguretat requereix mesures addicionals, com l'establiment d'una política que indique les accions permeses durant l'accés remot i la seua comunicació a l'empleat.

El CCN proposa en la Guia d'implantació (CCN-STIC 804), punts de suport útils sobre els quals basar-se a l'hora d'implantar teletreball en l'organització.

4.2.4 Normes internes

En l'àmbit de la Diputació de València resulten d'obligat compliment les normatives següents:

• Reglament de política de seguretat i de la protecció de dades de caràcter personal de la Diputació de València. Acord del Ple de 18 de juny de 2013.

• Normativa de protecció de dades de caràcter personal. Decret núm. 5448, de 12 de juny de 2015, del diputat de Modernització.

• Procediments de protecció de dades de caràcter personal. Decret núm. 6110, de 26 de juny de 2015, del diputat de Modernització.

• Normes de seguretat per als usuaris dels sistemes d'informació. Decret núm. 6111, de 26 de juny de 2015, del diputat de Modernització.

• Normes de seguretat per al personal tècnic dels sistemes d'informació TIC. Decret núm. 6353, de 3 de juliol de 2015, del diputat de Modernització.

4.2.5 Altres marcs de referència

Addicionalment, hi ha uns altres marcs que, tot i no tindre una obligatorietat en el seu compliment, poden ser referents i bones pràctiques que faciliten una implantació i transició cap al teletreball segura i amb garanties.

La norma ISO/IEC 27001, de Sistemes de Gestió de Seguretat de la Informació, disposa de l'annex A de mesures de seguretat, entre les quals hi ha una mesura (A.6.6.2) específica per al desenvolupament del teletreball. Aquesta mesura especifica la necessitat d'implantar una política i unes mesures de seguretat adequades per a protegir la informació accedida, tractada o emmagatzemada en emplaçaments de teletreball. Així mateix, la norma ISO/IEC 27002 especifica una sèrie de recomanacions per a la implantació d'aquesta mesura de control.

Un altre marc de control útil és el SP 800-53 rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations*, publicat per l'Institut Nacional d'Estàndards i Tecnologia (NIST) dels Estats Units, que incorpora controls de privacitat i seguretat de la informació per a fer front a les noves amenaces, incloses les relacionades amb accessos remots i teletreball.

4.3 Capacitat tècnica i organitzativa

L'últim pas per a poder analitzar la viabilitat consisteix a conéixer i analitzar els recursos tècnics i organitzatius que, de manera aproximada, seran requerits per a una implantació adequada del teletreball en l'organització, si disposem d'aquests recursos, i si serà necessària la realització d'una inversió per a aconseguir els objectius fixats.

Aquest estudi hauria de cobrir, almenys:

a) Necessitats de processament.
b) Necessitats d'emmagatzematge d'informació: durant el seu processament i durant el període que s'haja de retindre.
c) Necessitats de comunicació.
d) Necessitats de personal: quantitat i qualificació professional.
e) Necessitats d'instal·lacions i mitjans auxiliars.

Especialment, en l'entorn del teletreball, es recomana focalitzar en els aspectes següents:

- Identificar el nombre d'usuaris que puguen realitzar les seues activitats laborals en modalitat de teletreball.
- Determinar necessitats del lloc de treball. Hi ha la possibilitat que l'entitat no dispose de recursos suficients i puga recórrer a l'habilitació d'una política de BYOD (Bring Your Own Device) que permeta als usuaris utilitzar els seus dispositius electrònics propis per a la realització de tasques, sempre complint amb els requisits legals i de seguretat necessaris.
- Determinar la magnitud de connexions a través de xarxes privades virtuals i als sistemes, per a assegurar la connectivitat correcta dels usuaris als sistemes d'informació de l'entitat.
- Analitzar les necessitats que puguen sorgir a l'hora de transferir arxius, i poder requerir l'habilitació d'un sistema de compartició d'arxius o transferència segurs.

Feta aquesta anàlisi prèvia, l'entitat es trobarà en posició de determinar la viabilitat de la implantació del teletreball. En cas afirmatiu, en el punt següent es tracten els aspectes necessaris que permetran establir un pla d'implantació del teletreball.

5 DISSENY I IMPLANTACIÓ DEL TELETREBALL

Perquè el teletreball s'implemente d'una manera garantista respecte al compliment dels requisits tècnics, organitzatius i reguladors, cal establir un pla d'implantació mitjançant el qual s'establisca un full de ruta que ens ajude a aconseguir els objectius proposats, **tot aplicant la seguretat i la privacitat des del disseny i per defecte.**

En els punts següents s'analitzen els principals aspectes que cal tindre en compte en el disseny i la implantació del teletreball.

5.1 Política de teletreball i normativa de seguretat aplicable

El primer pas lògic és la definició d'una política de teletreball, a través de la qual la Direcció de l'organització transmeta una declaració d'intencions respecte a l'ús i les condicions del teletreball, i establisca les directrius que la governen i els objectius que es pretenen aconseguir.

Al seu torn, aquesta política ha de ser el referent i donar pas a tota una capa normativa que, en cas que siga necessari, desenvolupe i done compliment a les metes i els requisits definits.

Tot seguit es descriuen alguns dels principals aspectes que haurien de considerar-se dins d'aquesta política.

- Aspectes organitzatius:
    - Motivació, raó de ser i casuístiques per a l'aplicació del teletreball, com també el suport de la Direcció per a aconseguir els objectius i controlar el compliment de les directrius establides.
    - Procediment d'autorització dels usuaris per a l'accés a la modalitat de teletreball.
    - Les condicions de provisió d'equips i mobiliari adequat per al desenvolupament de les activitats de teletreball, en cas que no es permeta l'ús d'equips privats sota el control de l'organització.
    - Les condicions i els mecanismes per a previndre, si es dona el cas, disputes relatives a drets de propietat intel·lectual d'allò desenvolupat pel propietari de l'equip de manera privada.
    - Referències a documentació relacionada de suport al teletreball.
    - Les condicions d'accés a la part privada del propietari de l'equip, si es dona el cas i en compliment de la legislació vigent, per a la realització de verificacions de seguretat o durant un procés d'investigació.

- Determinació de les activitats de treball que es permeta desenvolupar quan es troba en modalitat de teletreball.
- Referències i procediments de participació, si escau, en els plans de continuïtat dels serveis.
- Procediment de notificació i gestió d'incidents de seguretat.
- Indicacions i pautes sobre la separació entre entorns laborals i d'oci o familiars, i evitar la simultaneïtat de tasques.
- Actuacions o referències a activitats de formació i conscienciació en l'ús dels mitjans disposats per al teletreball, com també en matèria de seguretat en entorns de teletreball.

- Aspectes tècnics i mesures de seguretat:

  - Les mesures de seguretat física requerides en l'entorn de teletreball, inclosos els llocs o les característiques dels llocs on es permet realitzar-lo.
  - En cas que es permeta l'ús d'equips privats, les condicions d'ús i control d'aquests per a garantir nivells de protecció similars als mitjans corporatius (com per exemple, aplicant polítiques de Bring Your Own Device [BYOD]).
  - Els requisits de seguretat de les comunicacions, depenent de la necessitat d'accés remot als sistemes i la sensibilitat de la informació a la qual s'accedirà i es transmetrà; incloses addicionalment, les restriccions d'ús de les xarxes domèstiques i els requisits o les restriccions en la configuració dels serveis de la xarxa sense fil.
  - La facilitació d'accés a un escriptori virtual que previnga el tractament i l'emmagatzematge d'informació en equips d'ús personal o privat.
  - Mesures i condicions proactives per a evitar amenaces d'intents d'accés no autoritzats que compartisquen l'espai de treball, com poguera ser, per exemple, familiars o amics. En aquest sentit es recomanen mesures de bloqueig automàtic dels equips per inactivitat i tancament de sessions, a més de mesures robustes d'identificació i accés, com l'ús de contrasenyes d'alta fortalesa, biomètriques o el doble factor d'autenticació.
  - Requisits de protecció contra programari maliciós (*malware*) i de tallafocs.
  - Determinació de la classificació de confidencialitat de la informació que pot tractar-se o emmagatzemar-se en modalitat de teletreball, inclosos els requisits de seguretat a considerar i els sistemes als quals s'està autoritzat accedir.

- Determinació de canals segurs per a l'intercanvi d'informació.
- Determinació de les condicions de protecció dels equips, com per exemple l'obligatorietat del xifratge de la informació.
- La provisió i el manteniment del maquinari i el programari, incloent-hi els acords de llicències de programari en els llocs de treball de propietat privada, si es dona el cas.

- Mecanismes i procediments per a la realització de còpies de seguretat i restauració.

NOTA: És molt important conciliar els aspectes citats anteriorment amb les normatives internes vigents en la Diputació. Ha de recordar-se que aquestes normes internes són producte de transposar i/o desenvolupar en l'àmbit de la nostra organització la legislació en matèria de protecció de dades personals i seguretat de la informació.

5.2 Seguretat i privacitat des del disseny i per defecte

El concepte de *privacy by design*, o privacitat des del disseny, fa referència a la necessitat de tindre presents les garanties del RGPD des que s'inicia un procés, i preveu adoptar mesures que garantisquen que només es tracten les dades necessàries i pel temps imprescindible.

El RGPD indica, en el seu considerant 78, que «en desenvolupar, dissenyar, seleccionar i usar aplicacions, serveis i productes que estan basats en el tractament de dades personals o que tracten dades personals per a complir la seua funció, cal encoratjar els productors dels productes, serveis i aplicacions perquè tinguen en compte el dret a la protecció de dades quan desenvolupen i dissenyen aquests productes, serveis i aplicacions, i que s'asseguren, amb l'atenció deguda a l'estat de la tècnica, que els responsables i els encarregats del tractament estan en condicions de complir les seues obligacions en matèria de protecció de dades».

En aquest sentit, l'aplicació del teletreball no és aliena al compliment d'aquest requisit, ja que implica un canvi potencial en els mitjans de tractament a través dels quals donem suport a la prestació dels serveis que l'organització ofereix. Per això, **l'organització ha d'analitzar aquestes implicacions i determinar els requisits als quals s'ha de donar compliment, de manera prèvia a l'aplicació del teletreball, per a garantir els drets de les persones i la protecció de la informació que es tracta.**

Addicionalment, en la determinació d'aquests requisits s'ha de tindre en compte l'apreciació de riscos descrita en el punt 4.1. Identificació d'amenaces i gestió de riscos. El motiu és identificar aquells requisits que permeten tractar els riscos i reduir els nivells de risc fins a nivells acceptables.

Aquests requisits es traduiran en mesures tècniques i organitzatives, com poden ser, per exemple, la regulació d'alguns processos mitjançant el desenvolupament de procediments i la normativa interna, la implantació de solucions segures o controls i bones pràctiques de seguretat, tal com es descriuen en els punts següents de la present secció, amb l'objectiu d'aplicar de manera efectiva els principis de protecció de dades i integrar les garanties necessàries en el tractament.

El principi de *privacy by default,* o privacitat per defecte, està relacionat amb el principi de qualitat de les dades o, dit amb unes altres paraules, amb l'ús proporcionat de les dades personals a la finalitat per la qual es recapten.

És a dir, aplicable tant a la quantitat de les dades recollides com al tipus de dades, els tractaments que fem, el temps que les conservem i l'accés que permetem a aquestes.

En els dos casos, les estratègies d'implementació o els requisits que cal dur a terme es traduiran en mesures tècniques i mesures organitzatives.

Entre altres estratègies bàsiques que permeten implementar la privacitat per defecte es proposen:

- **Recollida de dades:** analitzar els tipus de dades que es recapten amb un criteri de minimització en funció de la finalitat;
- **Tractament de les dades:** analitzar els processos associats a aquests tractaments perquè s'accedisca a les mínimes dades personals necessàries per a executar-los;
- **Conservació:** implementar una política de conservació de dades que permeta, amb un criteri restrictiu, eliminar aquelles dades que no siguen estrictament necessàries;
- **Accessibilitat:** limitar l'accés, tant intern com extern, de manera que només els usuaris autoritzats tinguen accés a les dades.

5.3 Desenvolupament de procediments i normatives de seguretat

L'aplicació del teletreball requereix, normalment, considerar l'adaptació d'alguns dels processos interns de l'organització, a causa del canvi d'entorn, que s'han de reforçar per a garantir una gestió adequada que tinga en compte els nous escenaris i les casuístiques previstes.

Tot seguit es descriuen alguns dels processos que comunament poden tindre especial rellevància en un entorn de teletreball.

5.3.1 Gestió d'incidents i bretxes de seguretat

Es defineix com un incident de seguretat un esdeveniment inesperat que pot comprometre la seguretat de la informació pertanyent a l'entitat. Per això, els usuaris han de ser conscients de la necessitat de comunicar com més prompte millor les febleses o els indicis que detecten concernents a la seguretat, a fi de previndre o tractar a temps aquests esdeveniments.

Cal recalcar la importància del fet que els usuaris no realitzen activitats de comprovació que una sospita sobre una feblesa siga certa, ja que, en cas que s'execute aquesta acció, podria entendre's com un ús inapropiat dels elements i actius de l'entitat, i podria ocasionar danys en els sistemes d'informació i en les evidències de la incidència per a investigacions posteriors.

L'entitat ha d'establir els procediments de comunicació d'incidents de seguretat i bretxes adequats i comunicar-los als empleats, les parts interessades, les autoritats de control pertinents, els proveïdors i els altres actors que puguen requerir-ho, atenent especialment la casuística de l'aplicació del teletreball.

Una vegada la comunicació s'haja produït, s'haurà de decidir si l'esdeveniment detectat es classifica com a incident de seguretat i com es prioritza (utilitzant protocols que permeten determinar la urgència, l'impacte, l'abast, etc.).

S'ha de respondre, davant incidents de seguretat de la informació, mitjançant els procediments documentats. Per això, els incidents han d'atendre's, monitorar-se i mantenir un registre del seu estatus. La resposta davant d'incidents ha d'incloure, almenys:

- Recopilació de les evidències principals.
- Activitats de resposta inventariades.
- Comunicació a les parts interessades.
- Finalització de l'incident i tancament.
- Lliçons apreses i millora contínua.

D'aquesta manera, el departament al qual correspon resoldre s'encarregarà de la presa de mesures oportuna i verificarà així la feblesa o l'incident de seguretat suposats per a activar els controls pertinents d'esmena i les altres mesures de prevenció que es consideren adequades.

NOTA: La norma N/SEG/TEC-018 INCIDENTS DE SEGURETAT descriu amb detall com ha d'actuar-se en l'àmbit de la Diputació davant un incident de seguretat.

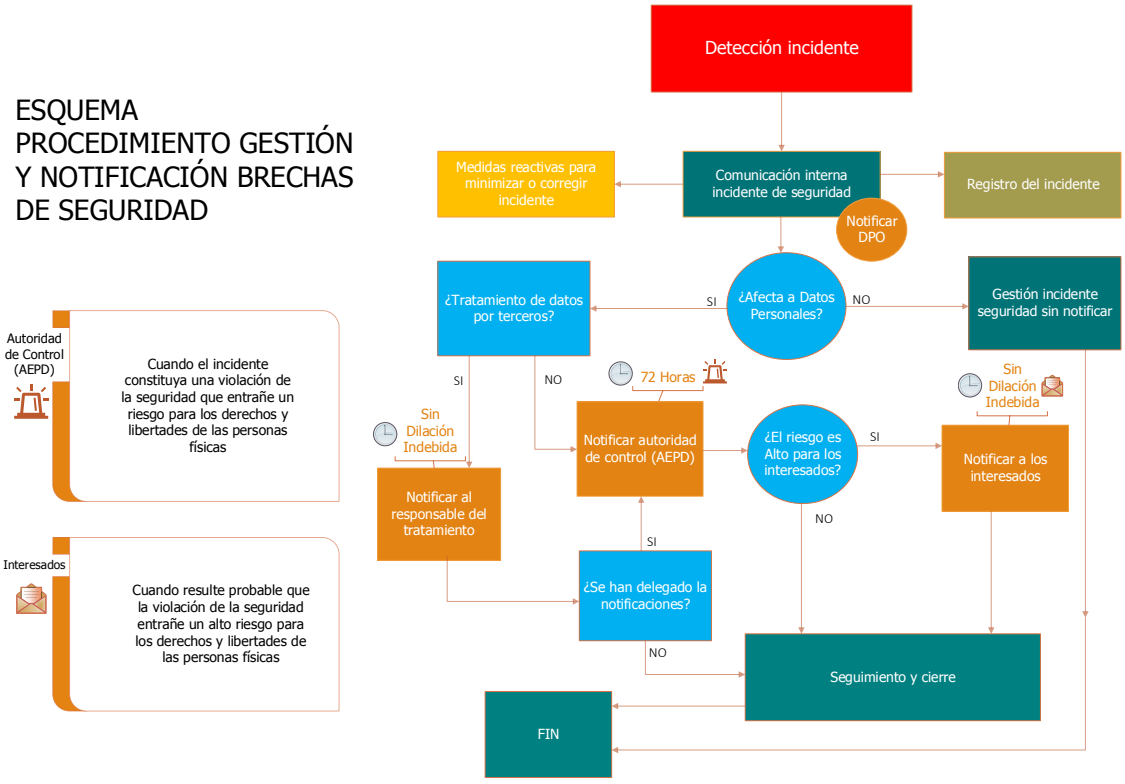
Addicionalment a l'exposat anteriorment, el procés ha de tindre en compte que, en cas que l'incident de seguretat supose una violació de dades de caràcter personal, ens haurem d'atindre a allò establit per la regulació en matèria de protecció de dades personals.

Concretament, entenem com violació de seguretat de dades personals tot aquell incident de seguretat que ocasione la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra forma, o la comunicació o l'accés no autoritzats a aquestes dades.

En aquest cas, haurem de:

- Comunicar l'incident de seguretat al delegat de Protecció de Dades i als actors interns involucrats.
- Adoptar les mesures de contenció necessàries.
- Registrar l'incident de seguretat.
- Avaluar la necessitat de comunicar la bretxa de seguretat a l'Agència Espanyola de Protecció de Dades (AEPD), abans de 72 hores des que en tenim coneixement, i als interessats afectats.
- Procedir a la realització de les comunicacions oportunes.
- Planificar les accions de resolució que impedisquen la seua repetició.
- Fer un seguiment de les accions planificades i un informe de resolució.

ESQUEMA PROCEDIMIENTO GESTIÓN Y NOTIFICACIÓN BRECHAS DE SEGURIDAD



5.3.2 Classificació de la informació

Per a una adequada gestió integral de la seguretat, les entitats han de disposar d'una normativa sobre la classificació i el tractament de la informació.

Durant el teletreball, la informació pot ser gestionada en diversos formats i suports. Qualsevol que siga la seua forma de presentació, ja siga en format digital o en paper, és recomanable que siguen etiquetats identificant el nivell de confidencialitat de la informació o el grau de protecció requerit, de manera que els usuaris puguen identificar fàcilment les mesures tècniques i organitzatives associades a aquest grau per a garantir un tractament adequat i l'aplicació dels protocols de protecció necessaris.

NOTA: La norma N/SEG/USU-001-2 Classificació de la Informació, estableix els criteris i nivells de classificació de la informació a tractar en l'àmbit de la Diputació (informació pública, reservada, restringida o confidencial) i les obligacions d'actuació conforme al nivell de classificació.

5.3.3 Pla de Continuïtat

Els plans de continuïtat estableixen mecanismes que ens ajuden a contindre i recuperar les activitats necessàries per a la prestació dels serveis en un escenari de desastre.

Per a desenvolupar un pla de continuïtat, en primer lloc, s'han d'identificar i valorar aquells processos crítics per a l'organització, avaluant aspectes com els temps de recuperació objectius, els punts de restauració de la informació, o els temps màxims tolerables de disrupció del servei.

Sobre la base d'aquesta anàlisi, es determinen protocols d'actuació i coordinació per a una gestió eficaç del desastre.

En aquest sentit, el teletreball/treball a distància és un element que aporta una gran flexibilitat com a mecanisme aplicat dins d'un Pla de Continuïtat, ja que permet un accés ràpid i àgil als sistemes independentment de la ubicació on ens trobem. Així mateix, facilita la mobilitat, garanteix el distanciament social a l'entorn de treball en casos de risc sanitari o la no disponibilitat d'instal·lacions, ja siga per la caiguda duradora de recursos de subministrament (llum, xarxa, etc.) inaccessibilitat, o casos

de condicions climatològiques altament adverses, que puguen ser cobertes temporalment amb recursos personals evitant desplaçaments.

5.4 Anàlisi de solucions i mitjans tecnològics

Ateses les necessitats de seguretat demandades per la pràctica del teletreball, s'han seleccionat algunes solucions de seguretat i mitjans tecnològics, els quals, a partir de la seua implantació i posada en marxa, ajudaran a mitigar possibles riscos que puguen comprometre la seguretat de la informació en les entitats.

El focus s'ha posat, per tant, en els diferents punts febles, pel que fa a seguretat, relatius a la pràctica del teletreball. En aquests haurà de centrar els seus esforços l'entitat, tant en el procés d'implantació de les mesures tècniques, com en el procés de conscienciació i formació a l'usuari, el qual té un paper fonamental en l'estat de la seguretat en l'entitat.

5.4.1 Seguretat de Xarxa i d'Endpoint

Un Endpoint, o dispositiu de punt final, es defineix com tot aquell dispositiu que es comunica amb una xarxa a la qual està connectat. Alguns exemples d'Endpoint són: ordinadors de taula, ordinadors portàtils, tauletes, telèfons intel·ligents, servidors, bases de dades, *switches* o encaminadors (*routers*).

A causa de la proliferació en la utilització d'aquesta classe de dispositius fora dels límits de les instal·lacions habituals de treball (teletreball i mobilitat), el nivell de seguretat en el lloc de teletreball pot no ser el mateix que en el lloc de teletreball habitual. Per això, en el full de ruta dels plans de teletreball i mobilitat, la seguretat tant de l'Endpoint com de la xarxa corporativa han de ser una prioritat, que s'ha de tindre en compte des de la fase de planificació.

5.4.1.1 Seguretat de xarxa

Els tallafocs (*firewall*) són mecanismes de seguretat dissenyats per a restringir els accessos no autoritzats des d'una xarxa externa a l'entitat cap a la xarxa interna. Per això la seua ubicació habitual és el punt de connexió entre la xarxa interna de l'entitat i la xarxa externa, que normalment és Internet.

En essència, els tallafocs permeten realitzar tres accions principals. Aquestes són les següents:

- Autoritzar una connexió (*allow*).
- Restringir una connexió (*deny*).
- Redirigir una comanda de connexió sense avisar l'emissor (*drop*).

Mitjançant la conjunció d'aquestes tres regles es pot establir un filtratge d'informació cap a la nostra xarxa, que podrà ser més o menys precís.

Habitualment es distingeixen dos tipus de polítiques de seguretat, les quals permeten:

- Establir únicament les comunicacions autoritzades explícitament.
- Bloquejar les comunicacions categoritzades com restringides.

Els principals beneficis que ens brinden els tallafocs són els següents:

- Mitiguen amenaces provinents des de xarxes externes.
- Permeten configuració personalitzada mitjançant regles.
- Permeten la generació d'alertes.
- Monitoren i registren l'ús de serveis.

Els sistemes operatius Windows i Mac disposen de mecanismes de tallafoc gratuïts per defecte, els quals haurem d'activar/configurar manualment.

5.4.1.2 Seguretat d'Endpoint

No obstant això, hem de tindre en compte que els tallafocs tenen limitacions a l'hora de protegir els equips, perquè tenen la funció única de permetre o no permetre fluxos de dades provinents de xarxes externes. Per això, per a obtindre una major protecció a nivell d'Endpoint, es recomana la utilització d'eines Endpoint Detection and Response (EDR). Aquestes són considerades com l'evolució i l'ampliació, pel que fa a funcionalitats i característiques, dels antivirus tradicionals.

D'una banda, els antivirus tradicionals són considerats eines de seguretat molt reactives, les quals protegeixen contra amenaces de seguretat mitjançant una sèrie de regles que actuen de manera estàtica. Les eines EDR, d'altra banda, actuen per comportament, arribant a detindre, respondre i remeiar possibles riscos de seguretat abans que aquests arriben a materialitzar-se en amenaces.

Les eines Endpoint Detection and Response (EDR) proporcionen una àmplia visibilitat de l'estat del dispositiu i permeten realitzar un procés de monitoratge i anàlisi contínua a nivell d'Endpoint i de xarxa.

Aquestes eines es caracteritzen per:

- Monitorar i avaluar les activitats de xarxa, proporcionant una visibilitat completa de l'estat de les amenaces.
- Detindre, respondre i remeiar atacs informàtics en temps real, i tractar de reduir el temps d'exposició a incidents de seguretat.
- Aplicar aprenentatge automàtic (*machine learning*) i intel·ligència artificial, per a optimitzar els processos d'identificació, detecció i prevenció d'amenaces.
- Posar en quarantena possibles amenaces.
- Realitzar *sandboxing* amb l'objectiu d'analitzar les amenaces trobades.
- Configurar alertes generades per eines externes.
- Fer anàlisi forense amb l'objectiu d'analitzar l'amenaça una vegada haja ocorregut.
- Contindre les amenaces en temps real.
- Fer un perfilat d'accions d'usuari i avís davant usos inesperats o poc habituals.

Mitjançant aquesta mena d'eines, es dota la infraestructura de seguretat d'una capacitat de monitoratge i resposta contínua davant qualsevol incident de seguretat, ja siga una amenaça tradicional o una d'avançada.

5.4.2 Accés remot

L'accés remot a la xarxa interna corporativa, per part dels diferents dispositius de l'entitat que es troben fora del seu abast, pot ser un punt de conflicte en allò relatiu a seguretat, a causa de la diferència en el nivell de seguretat de les mesures o controls de seguretat aplicats entre la infraestructura pròpia de l'entitat i la infraestructura relativa al lloc de teletreball. És per això que s'han de traçar unes directrius amb l'objectiu de fer segures les comunicacions des del lloc de teletreball fins a la xarxa interna corporativa.

Hi ha diferents solucions de comunicació per a proporcionar accés remot segur als usuaris d'una entitat en situació de mobilitat. Algunes de les més utilitzades són les següents:

- Xarxes privades virtuals (VPN).
- Serveis d'escriptori remots (RDS).
- Infraestructures d'escriptori virtual (VDI).
- Infraestructura d'escriptori mòbil (VDM).

Per tant, cal planificar quina solució d'accés remot és la més adequada depenent de les necessitats de l'entitat. A més, han de considerar-se les implicacions i els riscos de seguretat de cada solució, com també el compliment dels requisits de seguretat

necessaris per a dur a terme les tasques relatives al compliment laboral i professional dels usuaris.

NOTA: La norma N/SEG/TEC-004-2 ACCÉS REMOT disposa que en els accessos remots s'observaran les mateixes condicions que les assenyalades per a l'accés local i es protegirà el canal d'accés remot amb les mesures indicades en l'apartat N/SEG/TEC-006 per a la protecció de les comunicacions.

5.4.2.1 Xarxa privada virtual (VPN)

Un dels mitjans més utilitzats per a fer segur l'accés remot a la xarxa interna de l'organització i als recursos corporatius són les connexions mitjançant xarxa privada virtual (VPN). Es tracta d'una tecnologia de xarxa que permet realitzar una extensió segura d'una xarxa local (LAN) sobre una xarxa pública o no controlada com Internet.

Les connexions establides mitjançant aquest tipus de tecnologia protegeixen la informació que s'intercanvia, tot establint un «túnel» o canal amb xifratge de comunicació entre el dispositiu i el lloc de treball, la qual cosa possibilita una connexió segura i privada entre les parts. Des del nostre equip de treball connectat a Internet establim un «túnel» privat i segur fins a la xarxa de l'entitat, mitjançant el qual ens comuniquem sense témer que les dades siguen vulnerades.

Quan s'estableix una connexió mitjançant connexió VPN, es preserva la integritat i la confidencialitat (xifratge) de les dades compartides i es dona accés únicament als usuaris autoritzats. I és que la seguretat dels túnels VPN està per damunt del 98 %. Són per això una mesura molt recomanable des del punt de vista de la seguretat.

La utilització d'aquesta mena de connexió ofereix una sèrie d'avantatges, com ara:

- Accés remot segur que possibilita la mobilitat laboral.
- Comunicacions totalment xifrades (es preserva la confidencialitat i la integritat de la informació).
- Autenticació mútua.
- Protecció davant la reexpedició d'informació.
- Control d'accessos.
- Administració centralitzada d'aplicacions.

NOTA: La norma N/SEG/TEC-006-2 estableix que les comunicacions que discórreguen per xarxes fora del propi domini de seguretat, en aquells sistemes de categoria mitjana

i superior, utilitzaran xarxes privades virtuals (VPN), i s'empraran protocols estàndard com IPSEC, SSL o TLS.

5.4.2.2 Servei d'escriptori remot (RDS)

Les aplicacions d'escriptori remot (en anglès Remote Desktop Service, RDS) permeten a l'usuari controlar de manera remota un equip, ubicat habitualment en l'oficina de l'organització, des d'un segon dispositiu en situació de teletreball. L'escriptori virtual desplegat és el mateix per a tots els usuaris de l'entitat.

Aquesta tecnologia permet a l'usuari accedir a la informació emmagatzemada en el dispositiu ubicat en l'oficina de manera remota mitjançant la instal·lació d'un programa client en el dispositiu de teletreball.

No obstant això, no és una mesura recomanable des del punt de vista de la seguretat, a causa de possible creació de portes del darrere (*backdoors*) mitjançant les quals puguen accedir ciberdelinqüents. Per a això, es recomana utilitzar alhora una VPN i un escriptori remot, amb l'objectiu de fer més robusta la comunicació.

Les aplicacions d'escriptori remot presenten una sèrie d'avantatges, como ara:

- Accés remot segur que possibilita la mobilitat laboral.
- Les comunicacions estan totalment xifrades (es preserva la confidencialitat i la integritat de la informació).
- Menor cost d'inversió inicial i llicències que altres tecnologies per l'estalvi en maquinari.
- Control d'accessos.
- Administració centralitzada d'un escriptori virtual comú a tots els usuaris.

5.4.2.3 Infraestructura d'escriptori virtual (VDI)

Una infraestructura d'escriptori virtual és una tecnologia que permet la virtualització d'entorns de treball d'usuari en ubicacions controlades dins de l'entitat, amb l'objectiu de permetre la utilització d'aquests entorns de treball de manera remota.

Es tracta d'una solució que permet a l'empleat realitzar les seues funcions de treball en un lloc d'usuari remot, el qual replica el de l'oficina, des del seu lloc de teletreball. L'usuari disposa del mateix sistema operatiu i de les mateixes aplicacions de les quals disposa en el seu equip de l'oficina, usualment des d'un navegador web, sense la necessitat de tindre res instal·lat de manera local.

Els escriptoris virtuals són tecnologies molt segures i flexibles, les quals s'adapten perfectament a entitats que desitgen fer ús d'equips de manera remota.

A diferència de les solucions RDS, les infraestructures d'escriptori virtual permeten personalitzar i oferir un escriptori virtual configurat a mida per a cada usuari. És per això que aquest tipus de tecnologia s'entén com un avanç de la que s'ha vist en l'apartat anterior.

Els escriptoris virtuals presenten una sèrie d'avantatges, com ara:

- Accés remot segur que possibilita la mobilitat laboral.
- Interconnexió segura d'equips.
- Comunicació segura.
- Menor cost d'inversió inicial i llicències que altres tecnologies per l'estalvi en maquinari.
- Escalabilitat.
- Control d'accessos.
- Administració centralitzada d'aplicacions.
- Flexibilitat en la configuració de cada escriptori.

5.4.2.4 Infraestructura mòbil virtual (VMI)

Les infraestructures mòbils virtuals (en anglès VMI) són una opció segura per a protegir les comunicacions dels dispositius mòbils en una entitat. Igual que la infraestructura VDI proporciona un escriptori virtual segur a ordinadors en situació de mobilitat, la infraestructura VMI també proporciona un entorn segur per a la utilització d'aquesta mena de dispositius.

Una infraestructura mòbil virtual permet accedir a aplicacions mòbils de manera remota, les quals s'executen en servidors corporatius. A causa d'això, no és possible perdre dades o que les roben, fins i tot després de la pèrdua del dispositiu.

Es tracta d'una mesura molt útil que permet separar l'entorn de treball del personal en un mateix dispositiu. Si un usuari és donat de baixa, l'entitat tan sols haurà de bloquejar-li l'accés remot perquè tota la informació corporativa deixe de ser accessible per a aquest.

Les infraestructures mòbils virtuals presenten una sèrie d'avantatges, com ara:

- Entorn de dispositiu mòbil virtual segur.
- Impossibilitat de perdre les dades o que un tercer les robe (les aplicacions s'executen en servidors corporatius).
- Control d'accessos.
- Administració centralitzada d'aplicacions.

5.4.3 Eines de col·laboració

Les eines de col·laboració permeten als usuaris d'una entitat comunicar-se i treballar de manera conjunta sense importar la seua ubicació física. Es pot produir, editar i compartir informació de manera conjunta per part d'un mateix equip de treball.

La utilització d'eines col·laboratives suposa un punt de diferenciació respecte a altres entitats del sector, a causa de l'estalvi de temps produït per la sinergia a l'hora de treballar en equip.

Els dos avantatges principals que fan que les eines col·laboratives siguen una opció tan interessant en l'actualitat són: l'estalvi en costos i la productivitat relativa a la possibilitat de col·laboració en temps real.

Addicionalment, com a mesures de seguretat contra aquest tipus d'eines, es recomana:

- Utilitzar aplicacions segures descarregades de llocs oficials.
- Utilitzar els comptes professionals i no els personals per a accedir a les reunions.
- Utilitzar un pla empresarial en lloc d'un bàsic.
- Mantindre el programari actualitzat, com també el navegador si accedim mitjançant via web.

Podem dividir les eines col·laboratives en tres tipus, segons la seua funcionalitat:

- Missatgeria electrònica.
- Producció, edició i emmagatzematge de documents.
- Videotelefonades i reunions.

5.4.3.1 Servei de correu electrònic

Els serveis de correu electrònic són de gran ajuda per a realitzar i classificar comunicacions establides amb altres usuaris o grups d'usuaris de l'entitat o externs a ella.

La situació de teletreball que moltes entitats han hagut d'adoptar com a mesura a la situació sanitària excepcional causada per la Covid-19, ha fet que la quantitat de correus de suplantació d'identitat augmente considerablement; vacunes contra la malaltia, noves oportunitats laborals o desinformació sobre mesures adoptades per

part del Govern, han sigut la tònica habitual de correus maliciosos orientats a robar informació de l'usuari.

Si el servei de correu electrònic ja era considerat com el vector principal d'entrada d'amenaces en les organitzacions, la situació descrita anteriorment no ha fet més que agreujar més encara aquest problema.

Arribats a aquest punt, és molt important la conscienciació i la formació de l'usuari respecte als possibles correus electrònics maliciosos que puguen comprometre la seguretat de la informació de la nostra safata de correu. És per això que no sols hem de tindre en compte el factor tècnic (tallafoc, EDR, protecció avançada del servei de correu, filtre *antispam*, etc.) sinó també el factor humà.

5.4.3.1.1 El factor humà en la prevenció d'atacs de *phishing*

Mitjançant una sèrie de consideracions teòriques podem aconseguir que en la pràctica l'usuari siga capaç de detectar si la situació a la qual s'enfronta pot suposar un risc per a la seua seguretat.

Les principals consideracions de seguretat a l'hora de detectar un atac de *phishing* són les següents:

- Tindre un pensament crític davant dels correus que arriben a la nostra safata d'entrada, perquè una part d'ells poden arribar a comprometre la seguretat dels nostres equips. Hem de tindre en compte els aspectes següents amb l'objectiu de detectar si pot tractar-se d'un correu electrònic maliciós:
  - El correu no té un destinatari concret o el tracta d'una manera genèrica.
  - El remitent del correu és poc fiable o no el tenim agregat a la nostra agenda de contactes. Per a comprovar la veracitat del remitent, haurem de verificar el domini de la seua adreça de correu-e.
  - Al llarg del correu trobem errors ortogràfics, errors de maquetació o símbols/logos no legítims o equívocs.
  - L'idioma del missatge de correu, com també el contingut d'aquest, són indicadors per a verificar-ne la legitimitat. Per exemple, és poc probable que el nostre banc, en el cas de viure a Espanya, ens envie un correu en anglés.
- No descarregar cap mena d'arxiu, ja que pot contindre programari maliciós encobert que comprometa la seguretat del nostre equip. Hi ha alguns tipus de programari maliciós que es descarreguen en segon pla i són difícils de detectar.
- Davant la menor sospita, es recomana esborrar el missatge de correu electrònic i informar l'autoritat competent dins de l'entitat.

En el cas que el correu continga un enllaç a un lloc web (no es recomana accedir-hi si la web no és legítima) i hi accedim, hem de comprovar alguns indicadors de seguretat:

- Verificar la legitimitat de l'enllaç i prestar especial atenció a les URL.
- Comprovar la validesa de la connexió de la pàgina web (certificat SSL) i el cadenat de la barra de navegació. Hem de tindre en compte que el protocol HTTPS és més segur que altres protocols com a HTTP.
- No descarregar cap mena d'arxiu, perquè pot contindre programari maliciós encobert que comprometa la seguretat del nostre equip. Hi ha alguns tipus de programari maliciós que es descarreguen en segon pla i són difícils de detectar.

5.4.3.2 Producció, edició i emmagatzematge de documents

Les eines col·laboratives destinades a la producció, edició i emmagatzematge de documents es caracteritzen per permetre la realització de documents en temps real de manera conjunta. Els documents queden emmagatzemats en l'eina mateixa i són editats pels usuaris amb drets per a fer-ho, de manera que queden actualitzades en temps real.

La utilització del servei de correu electrònic de vegades és insuficient per a l'intercanvi i la compartició de documents. Això es deu principalment a les restriccions de grandària imposades pel servei de correu electrònic en referència a l'enviament de documents. Per tant, cal valorar l'opció d'utilitzar eines de compartició i emmagatzematge de documents amb l'objectiu de tractar documents més pesats.

Aquest tipus d'eines ens ajuden a tindre un accés àgil a la documentació corporativa en un entorn de teletreball i faciliten la compartició i l'edició de documents entre usuaris sense necessitat d'enviar adjunts via correu electrònic o d'accedir mitjançant VPN als servidors de fitxers de l'organització.

Es recomana revisar els permisos assignats a cada document que es comparteix o s'emmagatzema mitjançant aquest tipus d'eines, amb l'objectiu d'assegurar que només tindran permisos les persones indicades.

NOTA: En l'àmbit de la Diputació, els usuaris disposen de l'eina TRANXFER per a l'intercanvi segur de fitxers de tota classe. Aquesta eina corporativa compleix amb les cinc dimensions de seguretat exigibles per al tractament de la informació (disponibilitat, integritat, confidencialitat, traçabilitat i autenticitat)

5.4.3.3 Videotelefonades i reunions

El tercer tipus d'eina col·laborativa que hem de tindre en compte són les aplicacions de videotelefonades. En situació de teletreball està a l'ordre de dia la realització de reunions de treball en línia. Són, per això, una alternativa molt eficaç a les reunions presencials, a causa de les diferents funcionalitats comunicatives.

No obstant això, un ús poc segur d'aquest tipus d'aplicacions podria comprometre la seguretat de la informació compartida. Es recomana, per tant, seguir una sèrie de recomanacions i bons hàbits de seguretat referents a la utilització d'aquesta mena d'eines col·laboratives:

Activar la funcionalitat de la sala d'espera, amb l'objectiu que l'administrador de la sala comprove la identitat dels usuaris abans de començar la reunió.

- Evitar compartir informació confidencial (credencials, números de targetes de crèdit, etc.) en el xat de la reunió.
- Evitar, en la mesura que siga possible, enllaços poc segurs compartits en el xat de la reunió.
- No compartir enllaç de la reunió, si n'hi ha, amb tercers.
- Requerir contrasenya d'accés a la reunió.
- Comptar amb el paper d'un moderador en les reunions, el qual gestionarà el transcurs de la reunió.
- El nombre de participants ha de ser limitat i ha d'estar controlat.
- Comptar amb indicadors visuals/sonors que ens permeten conéixer l'entrada/eixida dels participants.
- Tindre constància en tot moment de l'estat del nostre micròfon i càmera (tots dos apagats per defecte i configurats en tot moment).
- En cas de gravar la reunió, l'administrador haurà d'informar prèviament els participants.
- Comprovar que l'aplicació tinga xifratge de les comunicacions.
- Conéixer la política de privacitat de l'eina abans de fer-ne ús.

A títol d'exemple, Microsoft Office 365 és un paquet d'aplicacions d'ofimàtica orientat a la productivitat, que permet englobar aquests i més serveis de manera conjunta.

5.4.4 Protecció de la informació

La informació és l'actiu més valuós en moltes entitats actualment. Per això ha d'assegurar-se d'una manera robusta amb la finalitat d'evitar robatoris, filtracions o fuites d'informació. En primer lloc, s'ha de conscienciar l'usuari sobre la seua importància en aquest apartat, com també de la importància de la informació en

l'entitat a la qual pertany. En segon lloc, s'ha de tractar de protegir per mitjans tècnics la confidencialitat i la integritat de la informació tractada.

Per a això, a continuació analitzarem algunes de les opcions més interessants per a protegir la informació de la nostra entitat. Són les següents:

- Prevenció de pèrdua de dades (DLP).
- Gestió dels drets de la informació (IRM).
- Gestió de dispositius mòbils (MDM).

5.4.4.1 Prevenció de pèrdua de dades (DLP)

Les eines de prevenció de pèrdua de dades (en anglès Data Loss Prevention, DLP) tenen com a objectiu previndre la fuita d'informació fora de la xarxa corporativa, causada per part dels usuaris de manera accidental o intencionada.

Aquests sistemes es caracteritzen per protegir la informació d'una manera proactiva i sense perdre productivitat, ja que actuen en segon pla mentre els usuaris realitzen les seues funcions habituals. Addicionalment, aquests sistemes també són utilitzats per a assegurar el compliment de requisits legals i reguladors relacionats amb la protecció de dades.

Les solucions DLP permeten realitzar una configuració basada en polítiques de seguretat i en una categorització adequada de la informació, amb la finalitat de distingir entre els diferents tipus d'informació i els diferents nivells de confidencialitat determinats. Segons la configuració realitzada, la solució DLP respondrà d'una manera o d'una altra davant els diferents casos d'ús. És a dir, l'eina respondrà depenent de «què es compartisca» i de «com es compartisca».

Els sistemes de prevenció de pèrdua de dades protegeixen principalment activitats com ara:

- Correu electrònic, xats i missatgeria instantània.
- Sistemes d'intercanvi de fitxers.
- Xarxes locals.
- Aplicacions web.
- Dispositius d'emmagatzematge extern (USB, discos durs, etc.).

5.4.4.2 Gestió dels drets de la informació (IRM)

Les eines de gestió dels drets de la informació (en anglès Information Rights Management, IRM) tenen com a objectiu protegir la informació davant d'accessos no

autoritzats. Les eines IRM tenen una sèrie de funcionalitats que permeten el control, la gestió i la protecció de la informació. Entre elles, destaquen les següents:

- Protecció davant d'accessos no autoritzats.
- Protecció davant de còpies o modificacions.
- Protecció davant d'impressió o descàrrega dels documents.
- Registre d'accés als fitxers.
- Gestió dels drets dels documents.

La implementació d'una eina IRM permet tindre un major control sobre la informació de l'entitat. Es recomana la seua utilització sempre que es treballe amb informació sensible per a l'empresa. És necessari, igual que en el cas de les eines DLP, que l'usuari estiga conscienciat del motiu de la utilització d'aquesta mena d'eines, i que, a més, es combinen amb l'aplicació de procediments i polítiques de seguretat amb la finalitat d'afegir una capa addicional de protecció de la informació.

5.4.4.3 Dispositius mòbils (MDM)

Les solucions de gestió de dispositius mòbils (en anglés Mobile Device Management, MDM) són un tipus de programari que permet controlar, monitorar i garantir la seguretat de dispositius mòbils corporatius, com telèfons intel·ligents, tauletes o portàtils, mitjançant les polítiques de seguretat que l'empresa establisca, la qual cosa permet assegurar, monitorar i administrar tots els dispositius mòbils de la nostra organització d'una manera centralitzada. La intenció de les solucions MDM és optimitzar la funcionalitat i la seguretat dels dispositius mòbils dins de l'organització, alhora que es protegeix la xarxa corporativa.

Les funcionalitats principals d'un MDM són les següents:

- Instal·lació àgil d'aplicacions en remot des d'un únic punt de control.
- Administració centralitzada de dispositius.
- Localització via satèl·lit.
- Sincronització d'arxius.
- Bloqueig de funcions.
- Control de despeses.
- Esborrament remot (per a casos de robatori o pèrdua).
- Gestió de contrasenyes.

NOTA: La norma N/SEG/TEC-011-1 SEGURETAT PER DEFECTE per a dispositius portàtils i mòbils exigeix la implantació de solucions de gestió centralitzada dels dispositius del tipus MDM (Mobile Device Management) o similar, que permeten en

qualsevol cas, el monitoratge, l'esborrament remot de dades o la realització d'auditories de seguretat sobre aquests dispositius.

5.4.5 Protecció de credencials

Mitjançant les nostres credencials d'accés podem accedir als diferents serveis i aplicacions de l'entitat. Es tracta d'informació molt sensible, la qual haurem de protegir de manera adequada.

Per a això haurem de tindre en compte dos aspectes fonamentals:

- Creació de credencials.
- Gestió de credencials.

5.4.5.1 Creació de credencials

En primer lloc, haurem d'assegurar-nos que les claus que utilitzem siguen robustes. Per a això, hem de tractar que la nostra contrasenya:

- Continga almenys huit caràcters: «credencial»
  Temps estimat de desxifratge = 1 hora -> Nivell de seguretat **baix**

- Continga tant lletres majúscules com minúscules: «credENcial»
  Temps estimat de desxifratge = 1 mes -> Nivell de seguretat **mitjà/baix**

- Continga números i caràcters especials: «C9e9dEnc!4L»
  Temps estimat de desxifratge = 400 anys -> Nivell de seguretat **alt**

5.4.5.2 Gestió de credencials

En segon lloc, hem d'assegurar la confidencialitat, integritat i disponibilitat de les nostres credencials. Per a això, farem ús de gestors de credencials, els quals ens permetran emmagatzemar i gestionar d'una manera segura les contrasenyes utilitzades en els serveis i les aplicacions de l'entitat.

Mitjançant una única clau d'accés es pot accedir a un repositori amb totes les nostres credencials. És una molt bona opció des del punt de vista de la seguretat, i d'aquesta manera es reemplaça l'emmagatzematge de credencials en els navegadors web («guardar contrasenya per a aquest lloc») o l'emmagatzematge tradicional en arxius de text digitals o físics.

Els gestors de contrasenyes ens ofereixen un inici de sessió unificat a manera de Single Sign-On (autenticació única), mitjançant el qual no serà necessari accedir al repositori de contrasenyes cada vegada que necessitem accedir a un servei o aplicació.

Els gestors de credencials ens ofereixen beneficis com ara:

- Emmagatzematge segur i centralitzat de contrasenyes (tan sols haurem de recordar una contrasenya).
- Millora del nivell de seguretat de les claus emmagatzemades (periodicitat, canvi de claus, comprovació de credencials, millora de la robustesa de credencials, etc.).
- Algoritmes de xifratge segur.
- Inici de sessió automàtic.
- Gestors multiplataforma.

5.5 Mesures i bones pràctiques de seguretat

Ateses les necessitats de seguretat requerides per la pràctica del teletreball, s'han seleccionat algunes mesures i bones pràctiques de seguretat, les quals, a partir de la seua implantació i realització, ajudaran a mitigar possibles riscos que puguen comprometre la seguretat de la informació en les entitats.

Aquestes mesures seran classificades en els apartats següents:

- Seguretat lògica
- Seguretat física

5.5.1 Seguretat lògica

5.1.1.1 Control d'accés

Amb l'objectiu de millorar la seguretat en l'accés lògic als recursos de l'entitat, és necessari que els sistemes disposen de mecanismes de control d'accés robustos, basats en processos d'identificació i autenticació.

Els controls d'accés han de buscar l'equilibri entre permetre un accés àgil al sistema i la seguretat i protecció dels recursos allotjats en aquest. Segons la criticitat de la informació que es vulga protegir, la balança es decantarà més cap a un costat o cap a un altre.

5.5.1.1.1 Identificació

Mitjançant el procés d'identificació s'identifica de manera exclusiva un usuari d'un sistema entre un conjunt d'usuaris. Addicionalment, aquest compta amb un rol determinat (administrador, usuari, etc.).

D'aquesta manera s'identifica:

- Qui rep els drets d'accés.
- Qui ha realitzat cada acció en el sistema.

Tindrem, per tant, un compte d'usuari amb uns drets d'accés per defecte i configurat per l'administrador del sistema.

Aconseguirem, per tant:

- Establir una estructura jerarquitzada d'ID diferenciant per nivells d'accés.
- Tindre una visibilitat completa de qualsevol activitat dels usuaris.

5.5.1.1.2 Autenticació

El procés d'autenticació permet validar la identitat d'un usuari. És a dir, es comprova si l'usuari que s'identifica és qui diu ser.

Els mecanismes d'autenticació basen el seu funcionament en la validació de credencials. Habitualment es demana informació sobre:

- Alguna cosa que es coneix, com per exemple: una contrasenya o un PIN.
- Alguna cosa que es té, com per exemple: criptovalors (*tokens*).
- Alguna cosa que és pròpia de l'usuari (per exemple, identificació biomètrica mitjançant empremta dactilar).

Una bona pràctica de seguretat és combinar els diferents factors d'identificació, per exemple, demandar la contrasenya i el PIN, o la contrasenya, el PIN i el factor biomètric. D'aquesta manera es veu incrementada la seguretat lògica dels controls d'accés als sistemes d'informació.

5.5.2 Seguretat física

A causa de la utilització de dispositius portàtils en situació de teletreball, estarem exposats a riscos associats a la seguretat física del dispositiu, no sols en l'entorn de teletreball, sinó també en el procés de transport del dispositiu des de l'oficina fins al lloc de teletreball, i viceversa.

És per això que hem de tindre en compte els riscos associats als dos escenaris descrits anteriorment; seguretat física en el lloc de teletreball i seguretat física en el procés de transport del dispositiu.

5.5.2.1 Lloc de teletreball

En el lloc de teletreball mateix hem de disposar de mesures de seguretat, com ara:

- Guardar el dispositiu en un lloc segur. Es recomana utilitzar armaris de seguretat o espais custodiats sota clau.
- Utilitzar un faristol per a donar suport al dispositiu, amb la finalitat de millorar l'ergonomia i l'equilibri, i d'aquesta manera evitar caigudes o colps.
- Considerar canviar el disc dur per un SSD, amb l'objectiu de mitigar les possibles conseqüències de qualsevol mena de vibració o caiguda, cosa que podria arribar a causar una pèrdua total de les dades emmagatzemades.
- Implementar una política de lloc de treball lliure d'estris, o si ja n'hi ha, seguir-la en situació de teletreball.

5.5.2.2 Transport del dispositiu

D'altra banda, mentre estem transportant el dispositiu des de l'oficina fins al lloc de treball, o viceversa, hem de comptar també amb algunes consideracions de seguretat, com ara:

- Utilitzar una funda, maletí o motxilla de seguretat per a evitar robatoris, pèrdues o colps.
- Utilitzar cadenats de seguretat per a portàtils per a evitar robatoris o pèrdues.
- Implementar solucions d'esborrament remot amb l'objectiu de protegir informació corporativa en cas de robatori o pèrdua (explicat en l'apartat 5.3.).

Addicionalment, hem d'adoptar unes mesures i bones pràctiques de seguretat, com ara:

- No deixar el dispositiu en el cotxe.
- No deixar el dispositiu desatès.

5.5.3 Utilització de dispositius no corporatius: BYOD

Hui en dia, a causa de factors com ara la proliferació de l'ús de dispositius mòbils (telèfons intel·ligents, tauletes i ordinadors portàtils) en l'àmbit laboral, les millores en les especificacions d'aquests dispositius pel que fa a programari, maquinari o connectivitat en xarxa, i a la necessitat imperant de teletreballar en determinades

ocasions, multitud d'entitats segueixen polítiques de «porta el teu propi dispositiu», o també conegudes per les seues sigles en anglès BYOD (Bring Your Own Device), mitjançant les quals es permet a l'usuari connectar-se a la xarxa corporativa i accedir als recursos de l'entitat mitjançant el seu dispositiu personal.

Les polítiques de BYOD aporten una sèrie d'avantatges respecte a la utilització de dispositius corporatius, com per exemple:

- Reducció de costos a causa de l'estalvi en maquinari que comporta la no inversió inicial en dispositius i la simplificació en la gestió de dispositius.
- Millora en la mobilitat dels usuaris, possibilitant el teletreball (en cas que l'organització no dispose de dispositius portàtils corporatius).
- Millora en la productivitat de l'usuari i en la col·laboració corporativa.

No obstant això, també trobem alguns riscos associats a aquesta mena de polítiques, els quals han de ser tinguts en compte prèviament a la implementació final en l'entitat. Els principals riscos a tindre en compte associats a polítiques de BYOD són els següents:

- Robatori, pèrdua, cessió involuntària o dany del dispositiu.
- Falta d'actualitzacions de seguretat a causa de l'absència d'una gestió centralitzada dels dispositius.
- Absència de controls de seguretat en el sistema operatiu.
- Mecanismes de control d'accés poc segurs.
- Connexions sense fils poc segures (utilització de xarxes Wi-Fi insegures, Bluetooth, NFC).
- Absència de xifratge en les comunicacions.
- Instal·lació d'aplicacions poc segures.
- Risc en la finalització de la relació laboral de l'usuari degut a l'emmagatzematge d'informació de l'entitat en el seu dispositiu.

Implantar una política de BYOD en una entitat no és una tasca que s'haja de prendre a la lleugera, perquè hi ha diferents riscos que poden comprometre la seguretat de l'entitat. No obstant això, l'adequada adopció d'aquesta, tot seguint una sèrie de recomanacions i bones pràctiques de seguretat, pot millorar notablement la productivitat en l'entitat, especialment quan no es disposa de dispositius portàtils corporatius.

Alguns dels punts que s'han de tindre en compte en la implementació de polítiques de BYOD són els següents:

- Crear una política o normativa interna que regule l'ús dels dispositius utilitzats i donar-la a conéixer a tots els usuaris de l'entitat.
- Definir i implantar un sistema de rols, autoritzacions d'accés, inventari de dispositius, nivells/privilegis d'accés, etc.

- Mantindre actualitzats/pedaçats de manera contínua els sistemes operatius i les aplicacions del dispositiu.
- Elaborar llistes negres i llistes blanques d'aplicacions permeses.
- Prohibir la utilització de dispositius que hagen sigut desbloquejats rooteados o que disposen d'un *jailbreak*.
- Evitar l'ús de xarxes Wi-Fi obertes o insegures, com també fomentar l'ús de les xarxes mòbils corporatives.
- Utilitzar VPN en cas que siga necessari.
- Implementar mecanismes de control d'accés segurs habilitant MFA; contrasenyes robustes, accés biomètric, bloqueig automàtic per temps màxim d'inactivitat, etc.
- Evitar la cessió voluntària del dispositiu a tercers.

NOTA: L'opció d'incorporar al teletreball dispositius personals dels treballadors requeriria modificar la normativa interna, ja que la norma N/SEG/USU-002-3 només contempla la possibilitat d'utilitzar dispositius portàtils o mòbils no proporcionats per la Diputació amb caràcter excepcional per temps molt limitat, o quan es tracte d'informació classificada com a PÚBLICA. No obstant això, la nova regulació bàsica del teletreball en l'EBEP (article 47 bis) exigeix a l'administració proporcionar i mantindre els mitjans tecnològics necessaris per a l'activitat.

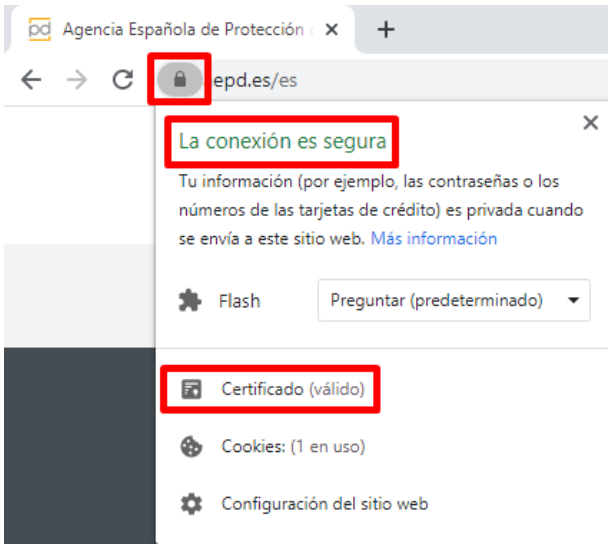
5.5.4 Navegació segura

S'ha d'evitar la navegació per pàgines no segures i evitar la descàrrega/instal·lació de qualsevol arxiu/programari no legítim. També haurem d'evitar accedir a enllaços o hipervincles de reputació dubtosa.

Podem assegurar-nos si la connexió a un lloc web és segura o no mitjançant una sèrie de consideracions.

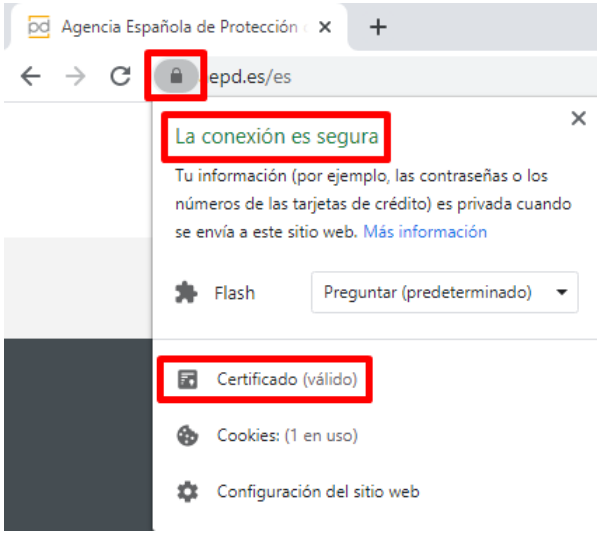
1. Cadenat de seguretat

   En primer lloc, la inclusió del cadenat en l'encapçalament de la barra de navegació és un indicador que la connexió a aquest lloc web és segura. El cadenat estarà relacionat amb el protocol de transferència d'hipertext utilitzat (3). En cas que siga una pàgina web no segura el cadenat apareixerà en roig.



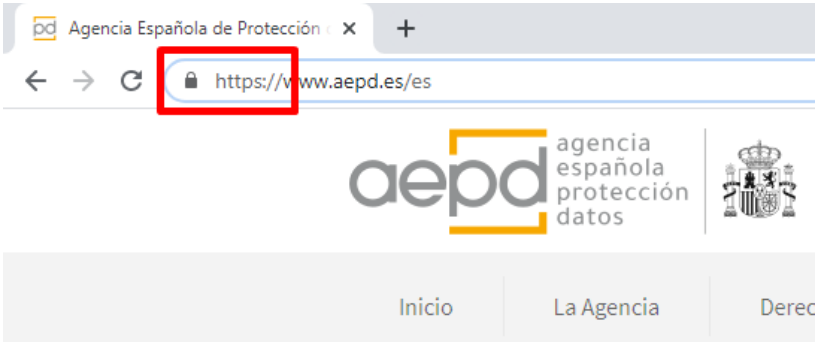
2. Certificat SSL (Secure Sockets Layer)

   Addicionalment, podrem comprovar la validesa i la vigència del certificat SSL fent clic en Certificat. Es tracta d'un certificat digital que autentica la identitat d'un lloc web determinat i assegura el xifratge d'informació amb tecnologia SSL.



3. Protocol HTTPS

   El protocol segur de transferència d'hipertext (HTTPS) valida un xifratge segur de les dades. Això repercuteix en el fet que la informació intercanviada entre el navegador i el lloc web no siga accessible a tercers. Es tracta d'un protocol més segur que l'HTTP.



Així mateix, es recomana mantindre els navegadors web actualitzats i eliminar periòdicament l'historial de navegació, les galetes (*cookies*), les contrasenyes recordades pel navegador i altres arxius temporals similars, amb l'objectiu de reduir el risc de patir un robatori de credencials per part de ciberdelinqüents.

5.6 Desplegament progressiu

5.6.1 Disseny de proves pilot

L'objectiu principal d'un **Pla de desplegament de teletreball** és gestionar una situació en la qual els usuaris no puguen realitzar la seua feina des de les instal·lacions convencionals de l'organització, assegurant la possibilitat de treballar des d'altres entorns.

La millor manera d'assegurar-se que el Pla de desplegament del teletreball és clarament eficaç és mantenir-lo actualitzat, realitzar els canvis substancials que es consideren necessaris en l'organització i en els sistemes de la informació i executar les proves periòdiques que validen que els sistemes estan preparats amb les funcions establides.

Durant les primeres proves, considerades com a proves pilot, s'han de detectar tots aquells escenaris que puguen amenaçar la continuïtat de la modalitat de teletreball, entre altres:

- Incidents i problemes a l'hora que els moduladors de càrrega funcionen correctament
- Falta de llicències davant d'aplicacions necessàries per a una gestió adequada del teletreball.

- Velocitat adequada de la línia d'Internet domèstica, la qual ha de proporcionar un cabal i unes capacitats apropiats per a connectar-se als sistemes d'informació de l'organització.

5.6.2 Autorització i posada en marxa

Es recomana que l'organització orquestre el desplegament tenint en compte els punts tractats en aquesta guia. Per a això, es determinaran les autoritzacions necessàries de manera que, davant la incorporació d'elements en els sistemes d'informació, s'atenue la confiança en el sistema.

Com a últim punt a traçar, s'ha de fer el desplegament i assegurar una aplicació correcta de la millora contínua.

5.6.3 Conscienciació i formació

S'ha de conscienciar i formar l'usuari en matèria de seguretat de la informació, privacitat i protecció de dades. D'això dependrà, en gran manera, i de manera conjunta amb les mesures tècniques de seguretat adoptades en l'entitat, el nivell de seguretat global de l'entitat i el compliment correcte de la normativa vigent en matèria de protecció de dades.

És necessari que els usuaris coneguen i apliquen una sèrie d'hàbits i bones pràctiques de seguretat en referència al desenvolupament de la seua activitat laboral en un entorn tecnològic com l'actual, sense oblidar-se de la importància de protegir les dades de caràcter personal sota la seua responsabilitat. Serà aquest, doncs, un punt estratègic en la prevenció d'incidents de seguretat i la comissió de qualsevol activitat il·lícita en matèria de protecció de dades.

Amb la finalitat d'aconseguir les metes de seguretat establides serà necessari el total compromís per part de la direcció i per part dels usuaris.

S'ha d'aconseguir que els usuaris de l'entitat:

- Coneguen la política de protecció de dades de l'entitat, com també els protocols interns, fonamentalment:
  - L'exercici de drets.
  - La notificació de bretxes de seguretat.
- Coneguen, entenguen i complisquen les normes i les mesures de seguretat definides.
- Coneguen i entenguen els riscos als quals s'exposen en el paradigma tecnològic actual, més concretament en situació de teletreball.
- Sàpiguen com previndre els diferents riscos als quals estan exposats i com actuar en cas que el risc es materialitze en una amenaça.

5.6.3.1 Conscienciació

Els usuaris s'han de conscienciar de manera regular sobre el seu paper i responsabilitat perquè la seguretat de l'entitat aconseguisca els nivells exigits en situació de teletreball. És de primera necessitat que l'usuari estiga conscienciat sobre la seua funció en l'esdevenir de la seguretat de la informació en la companyia.

Amb l'objectiu de conscienciar els usuaris en matèria de seguretat de la informació, caldrà:

- Difondre la Política de Protecció de Dades i de Seguretat de la Informació.
- Difondre les normes internes de protecció de dades i seguretat corporatives.
- Promoure una cultura de protecció de dades personals i de seguretat de la informació.

5.6.3.2 Formació

S'ha de formar l'usuari de manera contínua, amb l'objectiu que conega a quins riscos s'enfronta en matèria de seguretat i què pot fer ell com a usuari per a previndre'ls.

En situació de teletreball, podem trobar una sèrie de riscos (de seguretat i en matèria de protecció de dades) que no solen donar-se en el lloc de treball. És per això que s'ha de preparar l'usuari, amb l'objectiu que la seua formació, el seu criteri i el seu pensament crític, actuen com a primera línia de defensa enfront dels riscos i amenaces.

Amb l'objectiu de formar els usuaris en matèria de protecció de dades i seguretat de la informació es recomana:

- Definir un pla de formació d'usuaris.
- Desenvolupar programes de formació específics adequats als diferents llocs de treball en l'entitat.
- Avaluar l'aprenentatge obtingut per part dels usuaris.
- Promoure una cultura de protecció de dades i seguretat de la informació.
- Promoure la difusió i el compliment dels controls i les mesures de seguretat referents al teletreball definits en les normes de seguretat:
  - ISO/IEC 27000:
    - ISO/IEC 27001:2013
    - ISO/IEC 27002:2013
  - NIST SP 800-53 rev. 4
  - NIST SP 800-50
- Promoure bones pràctiques de seguretat en el tractament de la informació.

6 SUPERVISIÓ DE L'ESTAT DE LA SEGURETAT

6.1 Anàlisi de registres d'activitat

Davant d'un model de teletreball, auditar les accions processades pels sistemes d'informació de l'organització és un procés necessari i important per a poder detectar incompliments de les polítiques o normatives. En conseqüència, l'administrador de sistemes, davant una anomalia, podrà resoldre preguntes com, per exemple:

- Quines accions ha realitzat un usuari?
- Qui ha eliminat un registre en concret?
- Qui ha actualitzat un valor d'un registre? Quan ho ha fet?

És recomanable disposar de sistemes que generen esdeveniments a partir de regles establides. Vegeu el punt Monitoratge i gestió d'esdeveniments (SIEM).

6.2 Monitoratge i gestió d'esdeveniments (SIEM)

Els sistemes de gestió de la seguretat de la informació i esdeveniments de seguretat (en anglès Security Information and Event Management, SIEM) representen una solució de seguretat integral, la qual processa, analitza i correlaciona informació provinent de múltiples fonts d'informació, amb l'objectiu de detectar comportaments anòmals o sospitosos que puguen transformar-se en una amenaça de seguretat. Es recopilen, per tant, esdeveniments de seguretat de totes les tecnologies que intervenen en una xarxa (antivirus, tallafocs, IDS, IPS, etc.), amb l'objectiu d'analitzar en temps real tendències i patrons fora del comú que permeten detectar a temps amenaces potencials de seguretat i mantindre la infraestructura TIC de l'entitat segura.

Les eines SIEM ofereixen beneficis, com ara:

- Integració de diferents fonts d'informació.
- Monitoratge de l'estat global de la seguretat de la infraestructura TIC.
- Detenció d'amenaces desconegudes mitjançant l'aplicació d'aprenentatge automàtic (*machine learning*) i tecnologies *next-gen*.
- Gran velocitat d'anàlisi i correlació d'esdeveniments de seguretat.
- Possibilitat de buscar amenaces en registres arxivats.
- Protecció amb caràcter preventiu.

6.2.1 Sistemes de detecció d'intrusions (IDS)

Els sistemes de detecció d'intrusions (en anglès Intrusion Detection System, IDS) són eines de seguretat que tenen com a funcionalitat principal detectar anomalies en els sistemes, que puguen repercutir en amenaces majors.

Cal destacar que aquest tipus d'eines no frenen amenaces per si sols, sinó que necessiten eines addicionals per a fer-ho.

Hi ha dos tipus diferents d'IDS, depenent de si actuen a nivell d'allotjador (*host*) o de xarxa:

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

6.2.2 Sistemes de prevenció d'intrusions (IPS)

Els sistemes de prevenció d'intrusions (en anglès Intrusion Prevention System, IPS) tenen com a funcionalitat principal previndre amenaces. Els IPS són considerats una extensió, pel que fa a la prevenció d'amenaces, dels IDS, i una tecnologia més avançada en comparació amb els tallafocs tradicionals, pel fet que les decisions que es prenen en un sistema IDS estan basades en funció del comportament del trànsit i no de regles estàtiques. Això és un punt molt a tindre en compte quan parlem d'atacs de denegació de servei distribuït (DDoS), de programari maliciós avançat o d'amenaces persistents avançades (ATP).

Igual que succeeix en els IDS, també trobem diferents tipus d'IPS:

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

6.3 Control de l'activitat laboral

Les organitzacions poden adoptar les mesures de vigilància i control de l'activitat laboral que estimen més oportunes, per a verificar el compliment de les obligacions dels seus empleats, com també per a garantir la integritat dels actius de l'entitat i la seguretat dels mateixos treballadors, sempre que es respecte la intimitat, la dignitat i la resta de drets del treballador que la legislació estableix.

La ràpida evolució de la tecnologia aplicada a l'entorn laboral ha derivat en la introducció de noves eines de supervisió capaces de, per exemple, monitorar el temps invertit, les operacions realitzades, els llocs web visitats, les pulsacions del teclat o fins i tot el que s'està visualitzant en la pantalla. Aquestes formes de control cada vegada s'han generalitzat més amb el pas dels últims anys, especialment en el moment de l'increment del treball a distància, donada l'absència de supervisió visual en el lloc de treball habitual.

No obstant això, el control intensiu i permanent de l'activitat de les persones pot atemptar al dret de la seua intimitat, en considerar-se una forma desproporcionada de control. Aquest aspecte s'aplica independentment de la forma de treball en la qual es desenvolupe l'activitat.

D'aquesta manera, els treballadors tenen dret a la protecció de la seua intimitat en l'ús d'aquests dispositius digitals posats a la seua disposició, tal com es reconeix en la LOPDGDD.

L'entitat ha d'establir criteris i protocols d'utilització i control d'aquests mitjans i respectar en tot cas els estàndards mínims de protecció de la seua intimitat, d'acord amb els usos socials i els drets reconeguts constitucional i legalment. En aquests protocols s'han de desenvolupar una sèrie de principis fonamentals perquè el control que exercisca l'organització es faça sempre de manera legal i justificada, assegurant que els mecanismes de control tecnològic de l'activitat laboral complisquen els condicionants d'idoneïtat, necessitat i proporcionalitat.

Un mecanisme adequat per a avaluar la conveniència d'aquests mecanismes és la realització d'una anàlisi de riscos, o una avaluació d'impacte sobre la protecció de dades per a cada tractament implicat, si s'escau, d'acord amb els criteris comentats en el punt 4.1 Identificació d'amenaces i gestió de riscos, a fi de garantir que aquests mitjans de supervisió no suposen un risc sobre els drets i les llibertats de les persones.

NOTA: La norma N/SEG/SU-009 determina que la Diputació de València durà a terme aquesta activitat de monitoratge sense utilitzar sistemes o programes que pogueren atemptar contra els drets constitucionals dels usuaris, com ara el dret a la intimitat personal i al secret de les comunicacions, i es mantindrà en tot moment la privacitat de la informació manejada, llevat que, per requeriment legal i investigació sobre un ús il·legítim o il·legal, siga necessari l'accés a aquesta informació, salvaguardant en tot moment els drets fonamentals dels usuaris.

6.4 Millora contínua

Aplicar el procés de millora contínua serà una activitat fonamental que pretén millorar tant els productes, serveis o processos de l'organització.

Aplicat a l'entorn del teletreball, hem de buscar que tots aquells canvis que l'organització haja implantat assolisquen les metes proposades, que s'acomoden a les necessitats i els requisits desitjats i que es detecten totes aquelles àrees que requerisquen de millora fins a aconseguir la plena satisfacció en el seu conjunt.

Per a això es recomana definir una sèrie d'indicadors que ens permeten mesurar la idoneïtat, adequació i eficàcia de les solucions implantades, de manera que ens permeta analitzar la seua capacitat per a assolir els nostres objectius, a fi de decidir sobre la seua conveniència o detectar aspectes de millora.

Per exemple, alguns indicadors relacionats amb el teletreball podrien ser:

- Ràtio d'usuaris que s'han incorporat a la política de teletreball.
- Ràtio d'incidents de seguretat detectats en entorns de teletreball.
- Relació de proves de continuïtat relacionades amb teletreball executades amb resultats satisfactoris.
- Percentatge del personal que sol·licita la modalitat de treball a distància.
- Ràtio de càrrega de la capacitat de la xarxa de dades.
- Nota mitjana obtinguda de les proves de coneixement després de la realització de cursos de formació i conscienciació en matèria de seguretat.
- Percentatge d'equips i dispositius amb ple compliment de les directrius de l'allotjador.

Així mateix, per a obtindre uns mesuraments adequats, és recomanable determinar:

- Qui és el responsable del mesurament.
- Períodes de mesurament.
- Metes i objectius a assolir.
- Mètrica utilitzada.

D'aquesta forma, si posem el focus en els aspectes clau, recaptem i analitzem les dades adequades, obtindrem la informació necessària que ens ajudarà en la presa de decisions per a aconseguir una millora evident dels processos, els serveis i l'estat de la seguretat de l'entorn del teletreball.

7 RECAPITULACIÓ

La implantació de la modalitat de teletreball en l'organització suposa un impacte fonamentalment en:

• **La informació tractada**. En el cas específic de les dades de caràcter personal es veuen afectats bàsicament dos col·lectius titulars d'aquestes dades: Els titulars externs —ciutadans, proveïdors de béns i serveis, usuaris, etc.— i els titulars interns (empleats públics en situació de teletreball).

• **Els mitjans de tractament**. Els instruments tecnològics per a desenvolupar el teletreball i, per tant, utilitzats en el tractament de la informació tenen característiques i singularitats diferents que requereixen diferents actuacions: dotació, configuració, adaptació i control.

• **L'entorn físic de la prestació**. La modalitat de teletreball conté en essència un trasllat de l'entorn físic del treball a ubicacions alienes a les de l'organització.

• **L'organització interna**. Els processos, les dinàmiques i els controls són diferents en el cas del teletreball.

• **La regulació interna**. La modalitat de teletreball exigeix canvis reguladors en les normatives internes.

Els aspectes impactats citats generen nous escenaris de risc, tant pel que fa a la seguretat com a les garanties de compliment legal, per a les dades de caràcter personal i els sistemes d'informació. Aquest nou escenari i els riscos associats han de ser tinguts en compte en dos moments: a l'hora d'abordar una norma interna reguladora del teletreball i, posteriorment, quan hagen d'implementar-se totes les actuacions tècniques, jurídiques i organitzatives per a facilitar aquesta nova modalitat de prestació del treball.

En el cos de la present guia s'han abordat directrius per a aquests dos moments, segons els serveis competents afectats. Com a principis generals d'aplicació podem apuntar:

❶ La regulació interna del teletreball ha d'assegurar que contenen preceptes que contemplen els escenaris que la nova modalitat suposa per a les dades de caràcter personal i la seguretat de la informació. En aquells aspectes que no diferisquen d'allò ja regulat a nivell intern en la corporació bastarà amb fer referència a la norma corresponent. En qualsevol cas, la incorporació del teletreball exigirà modificar certs aspectes en les normatives internes vigents, sobretot les relacionades amb la seguretat de la informació.

❷ La regulació interna del teletreball no pot suposar en cap cas anar en contra de les garanties dels drets legals dels titulars de les dades personals; tant si aquests titulars són externs a l'organització com si es tracta dels empleats públics implicats en la modalitat de teletreball.

❸ La regulació interna del teletreball no pot suposar un minvament en la seguretat de la informació tractada. Quan es contemplen situacions que entren en conflicte amb la normativa interna vigent en la matèria, caldrà que es modifique el cos normatiu que hi corresponga. En cap cas aquesta modificació no podrà atemptar contra disposicions de caràcter superior (ENS, etc.).

❹ La regulació interna del teletreball haurà de contindre garanties directes per a mantindre la conscienciació i formació en matèria de protecció de dades i seguretat de la informació dels empleats que facen ús de la modalitat de teletreball, fins i tot amb caràcter obligatori per a aquests empleats. La formació haurà de ser prèvia i com a condició a l'accés a la modalitat de teletreball, i s'haurà de mantindre actualitzada al llarg de la permanència de l'empleat en aquesta situació.

❺ En la posada en marxa del teletreball resulta recomanable l'elaboració d'un Pla d'implantació, que atenga les directrius recollides en l'apartat 4. Anàlisi del context i presa de decisions, i 5. Disseny i implantació del teletreball. Molt especialment es recomana posar en pràctica un Pla de desplegament de teletreball, on puguen contrastar-se totes les mesures en un grup pilot

❻ A nivell organitzatiu, allò recomanable seria constituir un grup de seguiment corporatiu de teletreball, amb la presència de representants dels serveis més implicats. La millora contínua podria encaixar molt bé en el si d'aquest grup.

8 GLOSSARI DE TERMES

Aquest glossari està basat en la guia de seguretat Glossari i Abreviatures (CCN-STIC-401)

- **Amenaça**: Esdeveniment que pot desencadenar un incident en l'organització, produint danys materials o pèrdues immaterials en els seus actius.

- **Disponibilitat**: o disposició a ser usat quan siga necessari. La manca de disponibilitat comporta una interrupció del servei. La disponibilitat afecta directament a la productivitat de les organitzacions.

- **DLP**: mesures de seguretat que tracten d'evitar que la informació confidencial o valuosa siga copiada o traslladada fora de l'entorn de seguretat.

- **Gestió del risc**: el procés, diferent de l'avaluació del risc, consistent a sospesar les alternatives polítiques que hi ha mitjançant consultes amb les parts interessades, analitzar l'avaluació del risc i altres factors legítims i, si fora necessari, seleccionar les opcions de prevenció i control.

- **IDS**: programari o maquinari utilitzat per a identificar o alertar sobre intents d'intrusió en xarxes o sistemes. Conformat per sensors que generen esdeveniments de seguretat; una consola que supervisa esdeveniments i alertes i controla els sensors; i un motor central que registra en una base de dades els esdeveniments denotats pels sensors.

- **Risc**: una funció de la probabilitat que una vulnerabilitat del sistema afecte l'autenticació o la disponibilitat, autenticitat, integritat o confidencialitat de les dades processades o transferides i la gravetat d'aqueixa incidència, resultat de la utilització intencionada o no intencionada d'aqueixa vulnerabilitat.

- **Tractament de riscos**: El procés de selecció i implementació de les mesures encaminades a modificar els riscos.

- **Salvaguarda**. Conjunt d'accions, mètodes i sistemes destinats a evitar que es produïsquen actes il·lícits i/o accidents que puguen afectar el desenvolupament natural de les activitats en una organització.

- **VPN**: Acrònim de *virtual private network* (xarxa privada virtual). Una xarxa informàtica on algunes connexions són circuits virtuals dins de xarxes més extenses, com Internet, en comptes de connexions directes per mitjà de cables físics. En aquest cas, els punts finals d'una xarxa virtual es transmeten a través d'una xarxa major. Al contrari d'una aplicació comuna, formada per comunicacions segures en la xarxa pública, una xarxa VPN pot presentar o no funcions de seguretat, com l'autenticació i el xifratge de continguts.

9 BIBLIOGRAFIA

- **Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.**

- **Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en allò relatiu al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades).**

- **Avantprojecte de llei de treball a distància.**

- **Reial decret legislatiu 1/1995, de 24 de març, pel qual s'aprova el text refós de la Llei de l'Estatut dels Treballadors.**
  Reial decret legislatiu 5/2015, de 30 d'octubre, pel qual s'aprova el text refós de la Llei de l'Estatut Bàsic de l'Empleat Públic.

- **ISO/IEC 27000:2013: Sistemes de Gestió de Seguretat de la Informació.**

- **Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica.**
  - https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1001

- **Centro Criptológico Nacional (CCN)**

  - Guía de Seguridad de las TIC. CCN-STIC 105. 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/

ANNEX A: Llista d'eines

A.1. Protecció d'Endpoint i de perímetre de xarxa

A.1.1. Tallafocs

- 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. Accés remot

A.2.1. Xarxa 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 d'escriptori 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 mòbil 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. Escriptori remot

- 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. Eines de col·laboració

A.3.1. Servei de correu electrònic

- 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. Producció, edició i emmagatzematge de documents

- 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. Videotelefonada i reunions

- 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/

A. 4. Protecció de la informació

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

A.5. Protecció de credencials

A.5.1. Gestió de credencials

- 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

A.6. Supervisió de l'estat de la seguretat

A.6.1. Monitoratge i gestió d'esdeveniments (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.6.2. Sistemes de detecció d'intrusions (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.6.3. Sistemes de prevenció d'intrusions (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

ANNEX B: Escenaris de risc

Es llisten a continuació un conjunt d'escenaris de risc a considerar en l'anàlisi de l'exposició dels tractaments a amenaces.

ID	ESCENARIS DE RISC DE COMPLIMENT
RP	**Escenaris de risc que poden afectar els principis**
RP.1	La base que legitima el tractament no és adequada, és il·lícita o no s'ha formalitzat adequadament (cal prestar atenció a les categories especials de dades i la gestió del consentiment)
RP.2	Si el tractament se basa en l'interés legítim: no s'ha ponderat adequadament aquest interés legítim en relació amb els interessos, drets i llibertats fonamentals de l'interessat
RP.3	Les finalitats del tractament no són precises, son il·legítimes, etc.
RP.4	Hi ha un canvi de finalitat que pot ser incompatible amb la finalitat original
RP.5	Hi ha un canvi de finalitat compatible, però pot invalidar una avaluació d'impacte prèvia
RP.6	Es recullen dades inadequades, no pertinents, excessives o innecessàries per a la finalitat prevista
RP.7	Es registren dades inexactes o no es mantenen actualitzades
RP.8	Les dades personals es conserven més temps del necessari
RP.9	Les dades es tracten de manera deslleial o poc transparent (no es compleix l'expectativa de la persona interessada respecte al tractament de les seues dades)
RP.10	Es fan operacions de tractament desproporcionades

ID	ESCENARIS DE RISC DE COMPLIMENT
RD	**Escenaris de risc que poden afectar els drets**
RD.1	En el moment de la recollida de les dades no es proporciona la informació mínima prevista en la persona afectada (quan les dades s'obtenen directament de la persona) o no se li proporciona cap informació, quan s'obtenen de tercers
RD.2	La resposta a l'exercici dels drets de l'interessat no es fa en el temps i la forma pertinents
RD.3	Es prenen decisions que afecten una persona utilitzant exclusivament mitjans automatitzats
RD.4	No hi ha procediments per a donar una resposta adequada als drets
RD.5	L'organització desconeix els procediments per a respondre l'exercici de drets
RD.6	No es verifica adequadament la identitat de la persona que exerceix un dret
RO	**Escenaris de risc que poden afectar les obligacions**
RO.1	S'incompleix la regulació general sobre el dret a la protecció de les dades de caràcter personal
RO.2	S'incompleixen altres regulacions sectorials que incideixen en la protecció de les dades de caràcter personal
RO.3	S'incompleixen les clàusules sobre la protecció de dades incorporades als contractes o condicions d'ús
RO.4	S'incompleixen estipulacions recollides en un codi de conducta (si s'hi està adherit)
RO.5	No es pot demostrar el compliment (responsabilitat proactiva)

ID	ESCENARIS DE RISC DE COMPLIMENT
RO.6	Les certificacions o segells de protecció de dades no s'han renovat o han perdut vigència
RO.7	No s'ha tingut en compte la protecció de dades a l'hora de dissenyar el tractament (de manera parcial o total)
RO.8	No s'ha incorporat la protecció de dades per defecte en les operacions de tractament (de manera parcial o total)
RO.9	No s'ha fet una consulta prèvia a l'autoritat de supervisió, quan era necessària
RO.10	Els encarregats de tractament no s'han seleccionat adequadament
RO.11	No s'ha formalitzat adequadament la relació amb encarregats de tractaments
RO.12	No s'exerceix suficient control sobre l'activitat de l'encarregat de tractament (en les operacions de tractament que se li han encarregat)
RO.13	Es desconeixen les cadenes de subcontractació d'encarregats de tractament
RO.14	No es disposa del registre d'activitats del tractament (si és obligatori)
RO.15	No es manté actualitzat (no es gestiona) el registre d'activitats de tractament
RO.16	Les violacions de dades no es notifiquen en el temps i la forma pertinents (violació de la seguretat de les dades)
RO.17	Les violacions de dades no es comuniquen en el temps i en la forma pertinents (violació de la seguretat de les dades)
RO.18	Les limitacions del tractament no es comuniquen a tercers

ID	ESCENARIS DE RISC DE COMPLIMENT
RO.19	Hi ha transferència internacional de dades no autoritzada o desconeguda
RO.20	Falta de coneixement expert sobre protecció de dades i de canals de comunicació amb els afectats
RO.21	No s'ha designat delegat de protecció de dades (si és obligatori)
RO.22	No es proporcionen mitjans suficients al delegat de protecció de dades
RO.23	No s'atén un requeriment de l'autoritat de supervisió competent
RO.24	No es fa l'avaluació d'impacte (si és obligatòria)
RO.25	No s'implanten les mesures derivades d'una avaluació d'impacte
RO.26	No s'atenen les instruccions d'una autoritat de protecció de dades
RO.27	No es verifiquen les mesures adoptades (auditoria de compliment)
RDL	**Escenaris de risc que puguen afectar altres drets i llibertats**
RDL.1	Vulneració de la imatge, la intimitat o l'honor de les persones
RDL.2	Vulneració del lliure desenvolupament de la personalitat
RDL.3	Discriminació per raó de sexe, raça, religió, opinió, etc.

ID	ESCENARIS DE RISC DE COMPLIMENT
RDL.4	Violació del secret de les comunicacions
RDL.5	Atemptat contra la dignitat de les persones
RDP	**Escenaris de risc que puguen causar directament danys i perjudicis**
RDP.1	Discriminar una persona en un procés competitiu
RDP.2	Discriminar un col·lectiu
RDP.3	Impacte econòmic negatiu
RDP.4	Perill per a la integritat física o salut
RDP.5	Suplantació de la identitat de l'interessat
RDP.6	Perjudicar la reputació
RDP.7	Prohibir l'accés físic
RDP.8	Impedir o denegar l'obtenció d'un servei
RDP.9	Impedir una contractació
RDP.10	Denegar una ajuda o avantatge

ID	ESCENARIS DE RISC DE PROTECCIÓ DE LA INFORMACIÓ
SEG.1	Possible destrucció accidental de dades personals
SEG.2	Possible destrucció malintencionada de dades personals
SEG.3	Possible pèrdua de dades personals
SEG.4	Possible alteració no autoritzada de dades personals
SEG.5	Possible comunicació no autoritzada de dades personals
SEG.6	Falta de formació del personal sobre les mesures de seguretat que estan obligats a adoptar i sobre les conseqüències que es poden derivar de no fer-ho.
SEG.7	Possible accés no autoritzat a dades personals
SEG.8	Els sistemes d'informació no estan disponibles (incident que provoca que les dades personals no estiguen disponibles)
SEG.9	Hi ha incapacitat per a detectar i gestionar incidents que afecten la seguretat de les dades
SEG.10	Foc
SEG.11	Danys per aigua
SEG.12	Avaria d'origen físic o lògic
SEG.13	Tall del subministrament elèctric

ID	ESCENARIS DE RISC DE PROTECCIÓ DE LA INFORMACIÓ
SEG.14	Condicions inadequades de temperatura o humitat
SEG.15	Fallada de serveis de comunicacions
SEG.16	Degradació dels suports d'emmagatzematge de la informació
SEG.17	Errors dels usuaris
SEG.18	Errors de l'administrador del sistema / de la seguretat
SEG.19	Deficiències en l'organització
SEG.20	Difusió de programari maliciós
SEG.21	Vulnerabilitats dels programes
SEG.22	Errors de manteniment / actualització de programes
SEG.23	Errors de manteniment / actualització d'equips
SEG.24	Caiguda del sistema per esgotament de recursos
SEG.25	Pèrdua o robatori d'equips
SEG.26	No disponibilitat del personal

ID	ESCENARIS DE RISC DE PROTECCIÓ DE LA INFORMACIÓ
SEG.27	Suplantació de la identitat
SEG.28	Abús de privilegis d'accés
SEG.29	Ús no previst
SEG.30	Denegació de servei
SEG.31	Enginyeria social (picaresca)

ANNEX C: Llista de verificació

A l'hora d'implantar la modalitat de teletreball segur es recomana fer un diagnòstic de situació que permeta conéixer millor l'estat de maduresa de les eines i mesures de l'organització. D'aquesta forma, l'organització podrà conéixer quines són les prioritats a l'hora d'abordar un projecte d'aquesta índole.

A continuació es presenten una bateria de preguntes que, a títol orientatiu, poden ser d'utilitat:

LLISTA DE VERIFICACIÓ	CHECK
Ciberseguretat	
Definir i distribuir entre els empleats la política establida per l'organització sobre seguretat de la informació i teletreball.	☐
Protegir dispositius i equips portàtils mitjançant xifratge (si és possible, mitjançant xifratge per maquinari).	☐
En els casos en què siga possible, disposar de filtres en la pantalla que dificulten la visualització a persones alienes.	☐
Establir l'obligatorietat d'ús de doble factor d'autenticació per a l'accés a sistemes de manera remota, incloent-hi correu electrònic i qualsevol sistema o aplicació crític.	☐
Fomentar l'ús de gestors de contrasenyes segures.	☐
Formar i conscienciar els usuaris en matèria de seguretat de la informació, com per exemple: ▪ evitar l'accés als equips per familiars o amics, ▪ no accedir a pàgines web amb continguts sospitosos o inapropiats, ▪ no compartir contrasenyes, ▪ conéixer els canals de notificació d'incidents establits, ▪ bloquejar manualment les sessions obertes quan s'abandona el lloc de treball, ▪ etc.	☐
Definir i distribuir les normes i directrius establides per l'organització respecte a l'ús responsable i protecció de la informació, particularment a l'entorn de teletreball.	☐

LLISTA DE VERIFICACIÓ	CHECK
Analitzar la possibilitat de filtrar accessos a pàgines de contingut inapropiat (Per exemple, a través d'un Proxy Cloud, Llista Negra, etc.)	☐
Verificar que els equips i dispositius es mantenen actualitzats i disposen dels elements de protecció establits per l'organització.	☐
Permisos dels usuaris	
Assegurar que els usuaris no disposen de permisos d'administració dels equips i dispositius des dels quals accedeixen remotament als sistemes de l'organització.	☐
Assegurar que els usuaris amb permisos d'administració disposen d'un altre identificador sense permisos d'administració i l'utilitza per a les operacions diàries que no requereixen privilegis elevats.	☐
Assegurar que els usuaris, i especialment els que disposen de permisos d'administració, compleixen amb els requisits de fortalesa i protecció d'accés.	☐
Recordar les obligacions adquirides en matèria de seguretat.	☐
Correu electrònic	
Previndre periòdicament l'existència de correus malintencionats i la necessitat de no obrir per cap concepte adjunts sospitosos.	☐
Recordar als empleats la necessitat de reportar qualsevol identificació sospitosa de correu electrònic malintencionat.	☐
Videotelefonades i reunions en línia	
Recordar la necessitat de silenciar els micròfons quan no s'està parlant activament en una reunió.	☐
Conscienciar sobre la necessitat de bloquejar per defecte la càmera web.	☐

LLISTA DE VERIFICACIÓ	CHECK
Recordar la necessitat de no deixar els dispositius desbloquejats si abandonem temporalment l'espai de treball, especialment durant una videotelefonada.	☐
Conscienciar per a no treballar en espais públics si és possible, especialment quan es treballe amb documents o es troben en reunions on es tracten continguts confidencials.	☐
Privacitat	
Recordar a tot el personal la responsabilitat de respectar la privacitat i protegir les dades de caràcter personal que s'estan tractant.	☐
Recordar la prohibició d'enviar informació personal per canals no protegits, com correu electrònic, emmagatzemar informació en ubicacions diferents a les establides per l'organització, o mantindre les dades més enllà de l'estrictament necessari.	☐
Detecció i resposta a incidents	
Conscienciar periòdicament el personal a fi de romandre alerta i saber detectar atacs potencials o activitats sospitoses.	☐
Formar el personal sobre els canals disponibles per a notificar la identificació de qualsevol potencial atac o activitat sospitosa.	☐
Assegurar que els canals establits per a la gestió d'incidents, tant propis com de proveïdors, estan disponibles i funcionen de manera eficaç.	☐
Assegurar que l'equip de seguretat romanga atent i cerque activament activitats sospitoses, especialment sobre els canals que hi ha activitat en remot.	☐
Definir, distribuir i assegurar que el personal coneix els procediments relacionats amb la gestió d'incidents de seguretat i les funcions dels seus rols.	☐
Còpies de seguretat	
Proporcionar el programari i els mecanismes necessaris per a garantir que la còpia de seguretat de la informació tractada.	☐

LLISTA DE VERIFICACIÓ	CHECK
Conscienciar el personal sobre la necessitat de fer una còpia de seguretat de les dades que estan tractant mitjançant els mitjans i mecanismes establits per l'organització.	☐
Conscienciar el personal perquè no utilitze serveis d'emmagatzematge en el núvol externs no aprovats per l'organització.	☐

ANNEX D: Formulari per a la realització d'una AIPD sobre el tractament en modalitat de teletreball

Omplint el present document estarem en disposició d'elaborar un informe d'avaluació d'impacte en matèria de protecció de dades, sobre els nous tractaments de dades que es puguen crear en situació de teletreball.

ANÀLISI DE L'OBLIGACIÓ DE REALITZAR UNA AIPD: AVALUACIÓ DEL RISC

INCLUSIÓ DEL TRACTAMENT EN LA LLISTA DE TRACTAMENTS EXEMPTS

☐ Tractaments que es realitzen estrictament sota les directrius establides o autoritzades amb anterioritat mitjançant circulars o decisions emeses per les autoritats de control, en particular l'AEPD, sempre que el tractament no s'haja modificat des que va ser autoritzat.

☐ Tractaments que es realitzen estrictament sota les directrius de codis de conducta aprovats per la Comissió Europea o les autoritats de control, en particular l'AEPD, sempre que una AIPD completa haja sigut realitzada per a la validació del codi de conducta i el tractament s'implementa incloent-hi les mesures i salvaguardes definides en l'AIPD.

☐ Tractaments que siguen necessaris per al compliment d'una obligació legal, compliment d'una missió realitzada en interés públic o en l'exercici de poders públics conferits al responsable, sempre que en el mateix mandat legal no s'obligue a realitzar una AIPD, i sempre que ja s'haja realitzat una AIPD completa.

☐ Tractaments realitzats en l'exercici de la seua labor professional per treballadors autònoms que exercisquen de manera individual, en particular metges, professionals de la salut o advocats, sense perjudici que puga requerir-se quan el tractament que duguen a terme complisca, de manera significativa, amb dos o més criteris establits en la llista de tipus de tractaments de dades que requereixen avaluació d'impacte relativa a protecció de dades publicada per l'AEPD.

☐ Tractaments obligatoris per llei i realitzats en relació amb la gestió interna del personal de les PIMES amb finalitat de comptabilitat, gestió de recursos humans i nòmines, seguretat social i salut laboral, però mai relatius a les dades dels clients.

☐ Tractaments realitzats per comunitats i subcomunitats de propietaris tal com es defineixen en l'article 2 (a, b i d) de la Llei 49/1960 de Propietat Horitzontal.

☐ Tractaments realitzats per col·legis professionals i associacions sense ànim de lucre per a la gestió de les dades personals dels seus propis associats i donants, i en l'exercici de la seua labor, sempre que no incloguen en el tractament de dades sensibles com ara els que s'estableixen en l'article 9.1 del RGPD* i no hi siga aplicable l'article 9.2(d) d'aquest Reglament.

Si el tractament està en la llista de tractaments exempts establida en el marc de l'article 35.5 del RGPD, no és obligatori realitzar l'AIPD.

ANÀLISI DE LA INCLUSIÓ DEL TRACTAMENT EN ELS CASOS DE TRACTAMENTS OBLIGATS

En aquest apartat es determinarà si hi ha una obligació de realitzar l'AIPD. Per a això es tindrà en compte, en particular, si el tractament:

- Entra en la llista de casos enumerats en l'article 35.3 del RGPD.
- Compleix les condicions que es detallen en la llista, aprovada pel Comité Europeu de Protecció de Dades, de tractaments obligats (article 35.4 del RGPD) que pot consultar-se ací i el seu caràcter és merament orientatiu.
- Es donen els supòsits de major risc dels casos enumerats en l'article 28.2 de la LOPDGDD.

ELEMENTS A ANALITZAR	SÍ/NO
¿L'autoritat de supervisió competent ha publicat una llista de tractaments per als quals s'ha de fer l'avaluació d'impacte? S'ha de respondre només en cas afirmatiu. ¿El tractament objecte d'avaluació es pot considerar inclòs en aquesta llista?	
¿L'autoritat de supervisió competent ha publicat una llista de tractaments que no s'han d'avaluar? S'ha de respondre només en cas afirmatiu.	
¿Considerem que el tractament no encaixa clarament en cap dels supòsits de la llista?	
Amb les operacions de tractament, ¿es poden determinar hàbits, comportaments, preferències, gustos, interessos, etc., de persones identificades o identificables?	
Amb caràcter general, ¿podem considerar que una de les finalitats del tractament és elaborar perfils personals o predir comportaments?	

A partir del tractament de les dades, ¿es prenen decisions amb efectes jurídics per a les persones afectades?	
A partir del tractament de les dades, ¿es prenen decisions que poden afectar significativament o perjudicar d'alguna manera les persones afectades?	
¿Es tracten dades a gran escala d'alguna categoria especial?	
¿Es tracten dades relatives a condemnes o infraccions penals?	
¿El tractament implica un control sistemàtic, monitoratge o supervisió a gran escala d'àrees d'accés públic?	

Si alguna de les respostes és «SÍ», molt probablement estarem davant d'una mena de tractament dels previstos en l'article 35.3 del RGPD i per tant caldrà fer l'AIPD.

FACTORS DE RISC (WP 248)	SÍ/NO
¿El tractament implica l'avaluació o puntuació de persones?	
¿El tractament implica elaborar perfils de persones o fer prediccions sobre el seu comportament?	
¿La finalitat del tractament és prendre decisions de manera automatitzada, que puguen tindre efectes jurídics?	
¿La finalitat del tractament és prendre decisions de manera automatitzada, que puguen tindre efectes similars als jurídics, o efectes significatius per a les persones?	
¿El tractament implica algun tipus de vigilància sistemàtica? (observació, supervisió i control de persones)	
¿Es tracten categories especials de dades?	
¿Es tracten dades relatives a condemnes o infraccions penals?	
¿Es tracten dades que es puguen considerar com a molt personals?	
¿Es tracten dades a gran escala?	
¿El tractament implica combinar diferents fonts d'informació o dades relacionades amb tractaments diversos?	
¿Es tracten dades relatives a persones en situació de vulneració o de desequilibri respecte del responsable del tractament?	

¿Es tracten dades de xiquets? (persones menors de 18 anys)	
¿Les operacions de tractament utilitzen o apliquen solucions tecnològiques o organitzatives de manera innovadora?	
¿El tractament pot impedir a les persones afectades utilitzar un servei o executar un contracte?	

ELEMENTS COMPLEMENTARIS A ANALITZAR	SÍ/NO
¿La iniciativa o projecte suposa recollir dades de caràcter personal que fins ara no es recollien?	
¿La iniciativa implica relacionar diferents fonts o orígens de dades personals (creuar informació) que d'alguna manera incrementen la capacitat d'anàlisi de la informació?	
¿La informació s'ha sotmés a un procés de dissociació o pseudonimització?	
¿Es preveu utilitzar informació personal de la qual es disposa, per a finalitats o usos diferents als previstos inicialment?	
¿La iniciativa que s'ha d'avaluar implica l'ús de tecnologies que es poden percebre com especialment intrusives per a la privacitat?	
¿Hi ha riscos específics per a la seguretat de la informació, especialment un risc rellevant que tercers no autoritzats hi accedisquen?	
¿S'han previst transferències internacionals de dades?	
¿Es tracten dades de persones menors de 18 anys?	
¿Es tracten dades de persones menors de 14 anys?	

**** Aquestes preguntes, i l'anàlisi de les respostes, ens permeten detectar qüestions, que si bé de forma aïllada tal vegada tindrien una incidència directa en la decisió de fer l'AIPD, la valoració conjunta de les quals potser sí que ens porta a considerar que estem davant d'un tractament que suposa un risc alt.***

ANÀLISI DE LA NECESSITAT DEL TRACTAMENT

El Judici d'Idoneïtat: si el tractament plantejat assoleix els objectius proposats.

El Judici de Necessitat: determinar si el tractament és necessari, en el sentit que no hi ha cap altra alternativa menys invasiva per a la privacitat per a aconseguir aquest propòsit amb la mateixa eficàcia o amb una eficàcia raonable.

ASPECTES DEL TRACTAMENT	SÍ/NO	JUSTIFICACIÓ
Les dades recollides s'usaran exclusivament per a la finalitat declarada i no per a cap altra no informada ni incompatible amb la legitimitat del seu ús (principi de limitació de la finalitat).		
La finalitat que es pretén cobrir requereix totes les dades a recaptar i per a totes les persones interessades afectades (principi de minimització de dades).		
Les tecnologies emprades per al tractament són adequades per a la finalitat establida des del punt de vista del compliment dels principis fonamentals de la privacitat.		
Les dades no es mantenen més temps del necessari per a les finalitats del tractament (principi de limitació del termini de conservació).		
CONCLUSIÓ		

BENEFICIS PER ALS INTERESSATS

☐ Beneficis directes i objectius per als subjectes sobre els quals incideixen els riscos.

☐ Beneficis globals per a la societat

☐ Millor servei per a tots els ciutadans i/o els subjectes sota risc.

☐ Major accessibilitat a la informació.

☐ Major sostenibilitat mediambiental.

☐ Major transparència en el tractament de les dades.

☐ Millora substancial de la salut per als ciutadans i/o els subjectes sota risc.

☐ Ajuda i protecció a persones en situació de risc o desfavorides.

☐ La protecció enfront d'amenaces per a la seguretat de l'Estat, la defensa o la seguretat pública.

☐ Augmentar l'eficàcia dels serveis als ciutadans i/o els subjectes en risc.

☐ Serveis públics més accessibles i integradors.

☐ Disminuir la discriminació (per gènere, per edat, per nacionalitat, per discapacitat, etc.).

☐ Apoderament de l'interessat.

☐ Altres

BENEFICIS PER A L'ENTITAT O LES ADMINISTRACIONS PÚBLIQUES EN GENERAL

☐ Compliment normatiu

☐ Millora de l'eficiència

☐ Reducció de costos

☐ Increment del control de les actuacions de les AAPP

☐ Millora del factor de transparència per al responsable

☐ Millora de la seguretat de les entitats

☐ Millora d'imatge

☐ Objectius de responsabilitat social de l'organització

☐ Altres

AVALUACIÓ DEL NIVELL DE RISC

És necessari fer una anàlisi del risc intrínsec, d'acord amb l'article 35.7.c del RGPD, per a determinar i identificar els elements de risc per als drets i llibertats de les persones, tant els inherents al tractament com els que es deriven de l'entorn en el qual es desenvoluparà el tractament.

Exemple Amenaces tractament teletreball:

- Accessos no autoritzats a dades personals.
- Violacions de la confidencialitat de les dades personals per part dels empleats de l'organització.
- Inexistència de responsable de seguretat o deficient definició de les seues funcions i competències.
- Inexistència de política de seguretat en situacions de teletreball.
- Deficiències organitzatives en la gestió del control d'accessos.
- Deficiències tècniques en el control d'accessos que permeten que persones no autoritzades accedisquen i sostraguen dades personals.
- Impossibilitat d'atribuir a usuaris identificats totes les accions que es duen a terme en un sistema d'informació.
- Ús d'identificadors que revelen informació de l'afectat.
- Deficiències en la protecció de la confidencialitat de la informació.
- Falta de formació del personal sobre les mesures de seguretat que estan obligats a adoptar i sobre les conseqüències que es poden derivar de no fer-ho.
- Existència d'incentius per a obtindre la informació il·lícitament pel seu valor (econòmic, polític, social, laboral, etc.) per a tercers no autoritzats.

MESURES PER A LA REDUCCIÓ DEL RISC

L'objecte d'aquest apartat és establir mesures de gestió, organització, definició del tractament, procedimentals i tècniques que permeten gestionar cadascun dels elements de risc identificats en l'apartat anterior.

IDENTIFICACIÓ D'AMENAÇA	MESURA DE CONTROL

ALTERNATIVES AL TRACTAMENT I PER QUÈ NO S'HAN TRIAT

En els casos de tractaments de risc alt, en aquest apartat cal avaluar per què no s'han triat altres alternatives a la manera de dissenyar i implementar el tractament que impliquen un risc menor.

Per al cas que siga una millora, extensió o modificació d'un tractament, és necessari assenyalar els avantatges de la nova aproximació al tractament i que la finalitat que es persegueix no es puga aconseguir per altres mitjans.

Guíes del Departament de Protecció de Dades i Seguretat
de la Informació