GUIA SOBRE PROTECCIÓ DE DADES PER A ESTUDIANTS QUE REALITZEN PRÀCTIQUES EXTERNES

VNIVERSITAT DE VALÈNCIA

Càtedra Microsoft
Universitat de València
Privacitat &
Transformació Digital

Guia sobre protecció de dades per a estudiants que realitzen Pràctiques Externes

Autor:

Ricard Martínez, professor de Dret Constitucional de la Universitat de València.
Director de la Càtedra de privacitat i Transformació Digital Microsoft-Universitat de València

Agraïments:

- Helena Villarejo-Galende, professora de Dret Administratiu de la Universitat de Valladolid.
- Mónica Arenas, professora de Dret Constitucional de la Universitat d'Alcalá.
- Cristina Pauner, professora de Dret Constitucional de la Universitat Jaume I.
- Julián Valero, professor de Dret Administratiu de la Universitat de Múrcia.

Índex

Sobre aquesta guia

La universitat duu a terme el servei públic de l'educació superior mitjançant la recerca, la docència i l'estudi. A través dels seus programes de pràctiques prepara per a l'exercici d'activitats professionals amb la inestimable col·laboració de tot tipus d'entitats del sector públic i privat.

La participació en programes de pràctiques constitueix una oportunitat per a molts estudiants d'inserir-se plenament en el context d'una activitat laboral o empresarial. La formació d'excel·lència que proporciona l'ensenyança professional i universitària a Espanya permet que la integració en rutines de treball reals siga pràcticament immediata en la majoria dels casos una integració pràcticament immediata en rutines de treball reals. D'altra banda, la naturalesa d'algunes pràctiques, com les desenvolupades en institucions hospitalàries, escolars, financeres o d'alt valor afegit en R+D+I, trasllada una especial responsabilitat als formadors, als entorns de pràctiques i als estudiants, ja que accedeixen a informació estratègica de les organitzacions que els acullen.

Aquesta guia té per objecte primordial conscienciar entitats educatives, organitzacions i estudiants per a un adequat compliment de la normativa sobre protecció de dades i complementar les guies de pràctiques existents. També aprofita per formar sobre altres normes relacionades amb el desenvolupament de les pràctiques. Pretén, a més, oferir consell per promoure el compliment normatiu amb exemples i indicacions concretes sobre què s'ha de fer en cada cas. Finalment, no podem oblidar que els estudiants d'avui seran els emprenedors de demà, i promoure un futur teixit empresarial i professional conscienciat amb el compliment normatiu en l'àmbit de les tecnologies de la informació i les comunicacions constitueix sens dubte un repte estratègic.

1.-Per què hauries de llegir aquesta Guia?

Vivim en una època de transformació digital. Ens desperta un telèfon intel·ligent que ens ofereix avisos sobre temes pendents, l'agenda del dia, el pronòstic del temps i la ruta més ràpida per arribar a classe. Pugem a l'autobús i validem el bitllet des del telèfon mòbil. Durant el viatge verifiquem —una altra vegada— el WhatsApp i/o el Telegram, mirem el Facebook i l'Instagram —i etiquetem o fem uns m'agrada—, i ja som a classe. Allí ens connectem a Eduroam o la wifi corresponent. A la biblioteca, a la màquina de begudes, a l'hora de fitxar a la classe o a la roba s'usen targetes d'identificació per radiofreqüència (RFID). Fem servir càmeres de vídeo o ens enregistren a tot arreu. Demanar una beca o matricular-se pot ser ja un procés purament electrònic en el qual quatre o cinc entitats diferents intercanvien les nostres dades. Al nostre món es tracten dades contínuament. No hi ha un sol moment del dia en el qual no estiguem fent servir informació personal de tercers o estiguem facilitant la nostra o la d'uns altres. La societat del nostre temps funciona gràcies al processament massiu de dades personals i de tot tipus d'informació complementària.

> Quan un entorn social edita un anunci o suggereix un contacte ha tingut en compte les nostres dades de registre, la nostra xarxa de contactes, els nostres m'agrada, les galetes que ha generat la nostra navegació, la nostra geolocalització; en resum, el nostre perfil de comportament. Per a això tracta desenes de dades nostres i milers de referències contextuals.

Tractar informació imposa obligacions. Ens n'han d'informar mitjançant polítiques de privadesa, consentim en el registre i podem exercir els drets d'accés, rectificació, supressió, portabilitat, limitació del tractament o oposició. El dret fonamental a la protecció de dades està pensat per protegir-nos.

> **Però quan ens inserim en un entorn laboral passem a l'altre costat: tractem dades dels altres, assumim certs compromisos legals i s'espera de nosaltres la capacitat de gestionar adequadament les dades personals i garantir la seguretat de la informació corporativa.**

Per això la lectura d'aquesta guia ens ajudarà a conèixer les nostres obligacions. Seguir-ne les recomanacions no solament és necessari si volem ser bons professionals, sinó que també millora les nostres capacitats. L'objectiu essencial d'aquesta guia és oferir-te informació sobre els aspectes bàsics relatius a la protecció de dades, la seguretat i el compliment normatiu que afecten els estudiants en pràctiques.

2.-Què s'hi juga l'empresa o lloc de pràctiques? I la meua universitat o centre educatiu?

Si no totes, la major part de les activitats professionals estan regulades. Quan ens inserim en un programa de pràctiques, tant si són curriculars com extracurriculars, un conjunt d'organitzacions i persones assumeixen obligacions i drets.

L'organització que ens acull no pot actuar de qualsevol manera. Se li exigeix un lloc de pràctiques segur en termes de prevenció de riscos laborals. Han de formar-nos i informar-nos. Se'ns assigna una persona per fer les funcions de tutoria, que haurà de dirigir i coordinar la nostra activitat i fer un informe final.

El nostre centre educatiu supervisa el programa de pràctiques, assigna als estudiants tutors acadèmics, a més d'assegurar-se que han rebut una formació suficient i tenen les capacitats necessàries per desenvolupar el programa. L'estudiant és responsable dels seus actes. Per això acostuma a signar un conveni o acord de pràctiques, i l'empresa o entitat, a l'inici de l'activitat, pot plantejar-li la signatura d'un document on es recullen els seus deures i les seues obligacions, i en particular les relatives a confidencialitat, seguretat i protecció de dades.

I què passa si per falta de formació o d'informació fem alguna cosa malament? Per exemple, si instal·lem programari no autoritzat o si revelem dades a tercers. Si incomplim una norma, en responem personalment, però també podem causar un dany a l'empresa, a la universitat o al centre educatiu, que també, per la seua banda, haurà de fer front a la responsabilitat jurídica que pot suposar, per exemple, el pagament de multes, sancions i indemnitzacions. A més, podria afectar el prestigi públic de la institució educativa. Així, si la premsa ho publica donarà una mala publicitat al nostre programa de pràctiques, la qual cosa afectarà les nostres oportunitats d'ocupació en el futur.

Per això, la nostra responsabilitat en aquesta matèria consisteix a aprendre correctament les normes deontològiques que regeixen la nostra futura professió. A més, hem de cenyir-nos amb rigor a les instruccions dels nostres formadors i a les que, de manera específica, ens notifiquen en el lloc de pràctiques.

Vegem a continuació en què consisteixen les nostres obligacions en relació amb el tractament de dades de caràcter personal.

3.-Què és una dada personal i què és l'RGPD?

Una dada de caràcter personal és qualsevol informació relativa a una persona física identificada o identificable. Les persones són identificables quan podem establir, sense gaire esforç, una relació entre la informació que obtenim i una persona concreta.

> El nostre nom i cognoms és una dada personal, i també la nostra adreça. Són dades una fotografia, els nostres moviments de la targeta de crèdit, la geolocalització del nostre telèfon, una radiografia o els resultats d'una anàlisi clínica. Quan ens enregistra una càmera, fins i tot si no és per identificar-nos, podríem ser fàcilment identificables.

Avui n'hi ha prou amb posar el nom i cognoms en un cercador, i fins i tot solament una fotografia, per obtenir milers d'informacions.

> Quan sol·licitem una feina és gairebé inevitable el recurs del futur ocupador a les cerques a internet per contrastar el nostre currículum. En l'àmbit de l'Administració les decisions depenen cada vegada més de la informació disponible en mitjans informàtics. No està gaire lluny el dia en què n'hi haurà prou amb connectar-se i demanar una beca, que es concedirà de manera gairebé automàtica encreuant la informació disponible en diferents bases de dades "sense aportar papers".

La societat de la informació té molts avantatges i alguns perills. Si el nostre perfil és incorrecte no ens concediran la beca; si la informació disponible a internet és falsa o no està actualitzada, podrien no contractar-nos, i si algú usa malament les dades podria causar-nos un dany. Per això, la Constitució espanyola i la Carta dels drets fonamentals de la Unió Europea reconeixen el dret fonamental a la protecció de dades personals que regulen el **Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de les seues dades personals i a la lliure circulació d'aquestes dades (RGPD) i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDPGDD)**. Aquestes normes defineixen les garanties que asseguren un control sobre les nostres dades, i que aquestes es tractaran adequadament i amb la deguda seguretat.

Són normes molt exigents que imposen a les organitzacions obligacions d'informació, d'actualització de les dades o de seguretat i secret. I aquestes obligacions han de ser executades i respectades per les persones empleades i els estudiants en pràctiques.

> **Quan complim amb l'RGPD, l'LOPDPGDD i amb altres normes, contribuïm a garantir els drets de les persones i a posar a disposició de l'organització que ens acull una informació de qualitat, confiable i segura.**

4.-Tinc drets en protecció de dades? I obligacions?

Per garantir el control sobre la nostra informació personal les normatives europea i espanyola han definit un conjunt de facultats que afecten tot el cicle de vida de les dades des de la recollida fins a l'esborrament. Aquestes facultats són la transparència o informació en la recollida de la informació, el consentiment i els drets d'accés, rectificació, supressió, portabilitat, limitació del tractament o oposició.

En primer lloc, sempre han d'informar-te sobre qui tractarà les dades, per a què les usarà, si és obligatori facilitar-les, a qui es cediran i on i com pots exercir els teus drets, i, a més, hi haurà d'haver un enllaç a una capa d'informació més detallada sobre aquest tema. Per poder usar aquestes dades, amb caràcter general caldrà obtenir l'acceptació, i el consentiment, segons els casos, haurà de ser específic per a cadascuna de les finalitats diferents del tractament.

> 🔑 Quan et registres en una xarxa social, o quan et descarregues una aplicació mòbil, sempre apareix al final, i abans d'acceptar, una frase que diu que coneixes i acceptes les seues polítiques de privadesa. És aquí on ens informen i, per tant, quan acceptem el tractament de les nostres dades. S'ha demostrat que la immensa majoria de la gent no les llegeix. En un conegut experiment, més del 90% dels qui es van registrar en un web van acceptar la venda de l'ànima al diable.

Pots accedir a les teues dades per conèixer-ne l'estat. Si contenen un error, pots demanar-ne la rectificació, i si hi ha una raó justificada per eliminar-les, pots exercir el dret de cancel·lació. També pots exercir el dret a l'oblit a internet, a oposar-te a l'enviament de publicitat, a reclamar la limitació del tractament de les teues dades i a obtenir-les en un format compatible per usar-les en altres llocs.

> 🔑 Quan volem saber si es van posar bé les notes en l'últim trimestre exercim un dret d'accés, i si hi ha un error en demanem la rectificació o la cancel·lació d'una dada innecessària. Les dades d'un cercador s'obtenen sense el nostre consentiment. Però quan un resultat afecta els nostres drets, per exemple quan les cerques que es fan a partir del nostre nom i cognoms retornen l'enllaç a un contingut que ens perjudica, podem oposar-nos-hi. És el que s'ha anomenat dret a l'oblit.

Però aquests drets suposen costos i un esforç per a les organitzacions, que, a més, han d'assegurar la qualitat de les dades, controlar els proveïdors i invertir en seguretat i assessorament jurídic.

> **Per això s'imposen deures a les persones que treballen i/o presten un servei en l'organització per assegurar un tractament adequat de les dades. Si en el marc de les teues pràctiques no compleixes amb aquestes obligacions poses en perill l'empresa i els drets dels clients. En els següents apartats exposem alguns d'aquests deures que t'afectaran durant les pràctiques.**

Per saber-ne més:

- Agència Espanyola de Protecció de Dades. *Guía para el ciudadano*.

5.-Per què he de guardar secret?

El deure de secret s'exigeix pràcticament en totes les professions. Aquest secret que s'exigeix als funcionaris, als treballadors, als professionals o als estudiants en pràctiques compleix funcions molt diverses.

El secret pot ser fonamental per a la supervivència de l'empresa. Així, quan ens inserim en un entorn laboral en el qual existeix algun tipus d'R+D+I (recerca, desenvolupament i innovació), o quan s'obtenen avantatges competitius per adoptar un cert tipus de processos o localitzar determinats proveïdors o quan es vol llançar un nou producte, el secret pot ser crucial per a la supervivència de l'organització.

> **Si assisteixes a una reunió estratègica de l'empresa, a un curs de formació sobre una nova activitat o producte o et trobes en un lloc restringit i, per exemple, publiques un tuit, una foto a l'Instagram o un comentari en una xarxa social o et geolocalitzes i ofereixes informació a tercers, podries estar filtrant sense voler informació molt valuosa per a la competència.**

En altres ocasions és la pròpia naturalesa de l'activitat la que exigeix aquest deure de secret. En l'exercici de funcions públiques, les persones que presten els seus serveis en l'Administració tenen un deure de secret. Aquest pot ser molt important en llocs en els quals es gestiona informació sensible, com un hospital o consulta clínica, un centre escolar, una entitat amb persones que tenen algun tipus de discapacitat (atenció a la diversitat), o respecte de certes dades econòmiques, fiscals, laborals, judicials... En aquests casos el secret protegeix tant l'organització com els seus clients o usuaris.

> **Si mentre fas pràctiques en una clínica truca algú per telèfon i li facilites informació sobre un pacient o la proporciones a un tercer sense verificar que hi està autoritzat, estàs vulnerant el dret a la intimitat de la persona malalta.**

En protecció de dades també existeix deure de secret. I aquest resulta més exigent fins i tot que els anteriors. Aquest dret afecta qualsevol qui tracta dades personals, és a dir, és qualsevol tipus d'informació referida a una persona identificada o identificable. Per tant, no depèn ni del tipus d'empresa, ni de la seua activitat, ni del tipus de dada, ni del teu perfil professional. N'hi ha prou amb el simple fet d'accedir a dades per haver de complir amb aquest deure.

> **Quan es respecta el secret es garanteix el dret fonamental a la protecció de dades personals i, de retruc, valors jurídics i socials molt valuosos.**

6.-Per a què serveix la seguretat?

Un dels recursos estratègics que maneja tota organització és la informació, tant personal com de qualsevol altra naturalesa. Cada vegada és més comú apreciar que el que és veritablement valuós no es troba tant en un pla físic o material sinó en alguna cosa tan intangible com la informació i el coneixement.

> Comprem en línia, usem una aplicació o ens registrem en un servei pensant que és segur. Si una empresa d'internet té un forat de seguretat perdrà la confiança dels seus clients i s'arriscarà a desaparèixer.

En l'àmbit de la seguretat de la informació es persegueixen quatre objectius bàsics: la confidencialitat, la integritat, la disponibilitat i la resiliència.

a) La confidencialitat és instrumental al secret. La informació no ha de poder ser mai coneguda per tercers no autoritzats.

b) La integritat serveix per assegurar que les dades no han estat alterades indegudament falsejant un perfil.

c) La disponibilitat assegura que els sistemes d'informació podran activar-se i estar disponibles davant qualsevol incident, sia lògic —un virus que col·lapsa un sistema— sia físic —com ara un incendi o una inundació.

d) La resiliència assegura la capacitat dels sistemes d'informació de recuperar-se davant esdeveniments crítics.

Per a la seguretat de la informació és essencial el compromís de cada persona empleada.

> Un hospital no pot permetre's l'accés de tercers no autoritzats a una història clínica, o errors o manipulacions en la història clínica dels pacients, i si hi ha, per exemple, un problema de fluid elèctric, ha de tenir mitjans per mantenir l'alimentació elèctrica dels sistemes d'informació.

La seguretat no solament té una dimensió reactiva; és a dir, no solament serveix per evitar un resultat o arreglar un dany, sinó que també proporciona a l'organització confiança en les seues capacitats, així com en la certesa i en la validesa de la informació que gestiona, i d'aquesta manera permet adoptar decisions basades en informació veraç i confiable.

> **En la seguretat l'element més important, i també la baula més feble, són els usuaris, les persones. En el desenvolupament de les pràctiques has de prestar molta atenció a les polítiques de seguretat de l'entitat i aplicar-les rigorosament. Si no te les han proporcionat abans de començar l'activitat, demana-les.**

7.-Com puc contribuir a complir l'RGPD i l'LOPDPGDD i garantir la seguretat? Quines obligacions tinc?

Quan ens integrem en l'equip de treball d'una organització assumim un conjunt d'obligacions. El nostre lloc de pràctiques pot tenir un protocol de benvinguda o de formació. Si és així, hem de prestar-hi molta atenció i interioritzar els procediments d'actuació i normes establerts. En qualsevol cas, hi ha un conjunt de mesures de seguretat que hauríem de conèixer i aplicar, ja que responen al sentit comú. A continuació, se n'enumeren algunes.

Accés a instal·lacions

Haurem de respectar les possibles prohibicions d'accés, limitar-nos als nostres permisos i, en tot cas, aplicar les condicions corresponents.

> 🔑 No és inusual trobar l'accés restringit a les zones d'arxivament clínic o de l'equipament informàtic. En ocasions, en funció de la naturalesa de la informació, podrien existir regles d'actuació com, per exemple, no apagar determinats equips o no entrar-hi amb un telèfon amb càmera.

Si necessitem accedir a una àrea restringida, haurem de seguir sempre els procediments interns per obtenir l'autorització.

Controls d'accés lògic

El més normal és l'assignació de permisos d'accés als sistemes d'informació, habitualment mitjançant algun tipus de validació de nom d'usuari i contrasenya. Aquestes claus les acostuma a facilitar algun responsable de l'entitat, i haurien de ser individuals. Quan les fem servir hem d'accedir exclusivament als recursos i sistemes autoritzats i únicament des del lloc o terminal assignats.

Serà fonamental bloquejar l'equip si ens n'allunyem, sortir de les aplicacions protegides quan no les fem servir i assegurar-nos que tercers no autoritzats no poden accedir a la pantalla ni llegir-la. S'han d'activar els sistemes de bloqueig de l'ordinador després d'un període d'inactivitat, s'ha d'apagar fora de l'horari de treball i se n'ha d'evitar l'ús per terceres persones.

> 🔑 Una distracció tan comuna com deixar una sessió oberta pot permetre a visitants o a col·legues deslleials robar informació usant el nostre compte d'usuari. I en aquest cas ens n'atribuiran la responsabilitat.

Hem de protegir la nostra contrasenya, no compartir-la mai, canviar-la periòdicament o quan ens ho demanen i activar contrasenyes segures.

🔑 Una de les maneres usuals d'atacar un sistema consisteix a esbrinar la contrasenya d'un usuari. Poses en risc la seguretat del sistema si, per exemple, la dones a un company. També si generes una contrasenya feble, com ara el teu nom o la data de naixement, en comptes d'una combinació de com a mínim vuit caràcters —no ha de ser una paraula—, amb majúscules, algun signe i xifres.

Accés remot i dispositius propis

Si es preveu alguna fórmula de teletreball amb accés remot als sistemes d'informació, o si es permet endur-se a casa dispositius portàtils o usar els propis, hem d'extremar la seguretat. És preferible deixar la informació en el sistema de l'empresa o en el del proveïdor autoritzat. Hem de renunciar a pràctiques de risc amb aquests dispositius, com ara compartir-los amb tercers, instal·lar-hi programari no verificat, emportar-nos informació en una memòria USB per seguir treballant a casa o usar programes de punt a punt.

🔑 Quan descarreguem arxius de tercers, els estem obrint de bat a bat les portes del nostre ordinador. I el mateix passa quan usem una xarxa wifi no segura.

Destrucció de suports

Tenint sempre en compte les instruccions de l'entitat en la qual estiguem, les impressions o còpies de treball d'informació protegida en suport paper, la còpia en DVD o CD o les fotocòpies que no s'han d'utilitzar s'han de destruir. Si la informació s'ha incorporat a una memòria USB, o a qualsevol dispositiu aliè al sistema d'informació, s'ha d'esborrar mitjançant sistemes d'esborrament segur o s'ha de formatar el dispositiu o destruir-lo, si és que es rebutjarà.

🔑 Una de les fugues de dades més freqüent es produeix quan el paper acaba a les escombraries convencionals, o quan es reutilitza un dispositiu. INCIBE recomana, per exemple, la sobreescriptura de dispositius amb eines com Eraser, DBAN o Hardwipe.

Correu electrònic i xarxa corporativa

Un mal ús del correu electrònic posa en risc l'organització. No s'ha d'usar per a tasques privades no corporatives, ni s'han d'executar arxius indeguts. Utilitzar la xarxa per descarregar-se continguts protegits pot generar responsabilitat jurídica a l'ocupador.

🔑 N'hi ha prou amb reproduir una cançó en MP3 per instal·lar un virus o un troià, o per ser indexats pels qui actuen per defensar els drets de propietat intel·lectual. En tots dos casos causem un dany a l'entitat.

Sistemes actualitzats

Les actualitzacions del programari són vitals, perquè serveixen per a la correcció de vulnerabilitats. En moltes ocasions exigeixen una actuació proactiva dels usuaris, que han de verificar una sol·licitud d'actualització, executar-la i reinicialitzar l'equip. Hem de fer les actualitzacions

quan toca, d'acord amb les indicacions rebudes, en particular les que afecten el sistema operatiu, el tallafoc i l'antivirus.

> 🔑 Ens hem d'assegurar que el nostre sistema es connecta per cercar actualitzacions, d'acord amb la política de l'organització i respectant les seues recomanacions. En alguns casos, i amb finalitats promocionals, les actualitzacions inclouen programes que podrien ser no autoritzats, per la qual cosa no hem d'oblidar desmarcar la casella corresponent.

Una taula neta

El lloc de treball ha de ser un lloc ordenat, per poder controlar en tot moment la documentació i, alhora, impedir-hi l'accés indegut de tercers. Sempre hem de custodiar la informació i, si ens ofereixen els mitjans, emmagatzemar-la en lloc segur en finalitzar la jornada.

> 🔑 En moltes organitzacions, serveis com la neteja o la seguretat es presten a la nit o amb l'edifici buit. Si la informació es deixa sobre la taula o en un lloc accessible, l'exposem a un risc de pèrdua o robatori. També podem posar en perill aquesta informació si surt de l'empresa i la usem, per exemple, en una biblioteca.

Incidències

Una incidència és qualsevol esdeveniment que podria afectar la seguretat d'un sistema d'informació. Quan patim una incidència l'hem de comunicar a la persona responsable designada. Tenir una incidència no és una infracció, ni ens n'hem d'avergonyir. Però no comunicar-la comporta un risc per a l'organització i ens en fa responsables.

> 🔑 Trobar l'ordinador engegat quan ens incorporarem a la feina, perdre un document, esborrar informació per accident, un funcionament anormalment lent de l'ordinador, o bloquejar, perdre o oblidar la contrasenya són incidències.

Blogs, xarxes socials

No podem fer comentaris comprometedors per a la nostra empresa en espais socials quan posem en risc el seu prestigi, la intimitat dels seus clients o secrets empresarials o quan la seguretat de la informació es pot veure afectada. Un comentari irresponsable o inadequat pot causar danys dels quals haurem de respondre.

📚 Per saber-ne més:

- INCIBE. *Decálogo ciberseguridad empresas: una guía de aproximación para el empresario*.
- INCIBE. *Glosario de términos de ciberseguridad: una guía de aproximación para el empresario*.

8.-Si treballo amb menors, pacients o en despatxos d'advocats

Alguns entorns de pràctiques resulten particularment delicats. Són sensibles per al dret fonamental a la protecció de dades les pràctiques que impliquen treballar amb persones malaltes, menors, amb expedients judicials o amb diversitat funcional. En alguns d'aquests casos ens poden requerir informació personal addicional com, per exemple, un certificat negatiu d'antecedents penals, i haurem de facilitar-la.

Els pacients o els clients d'un advocat confien plenament en els professionals que els atenen amb l'esperança de trobar solucions. L'atenció d'aquestes persones suposa la revelació de dades íntimes i, en ocasions, socialment vergonyants. Si aquesta informació no es protegeix i es fa pública, o es revela a tercers, posem en risc la intimitat, la dignitat i els drets de les persones.

> **No podem revelar informació clínica per telèfon a una persona no autoritzada, de la mateixa manera que tampoc podem dipositar a les escombraries convencionals una història clínica. Podem comprometre la imatge o l'honor d'una persona, o fins i tot provocar una situació que l'impedirà d'accedir a drets com el treball.**

El mateix succeeix quan desenvolupem la nostra tasca en l'àmbit educatiu. Els menors són persones en formació la informació de les quals resulta particularment sensible. Hem de ser diligents a l'hora de gestionar-la, ja que en moltes ocasions serà fonamental per salvaguardar la seua seguretat. Així mateix, haurem d'assegurar-nos que la informació sobre els menors no es facilita mai a tercers no autoritzats.

> Les situacions familiars desestructurades, en les quals un familiar no autoritzat pretén accedir a informació, o accions aparentment innòcues, com fer-se una foto amb la classe i pujar-la a una xarxa social, comporten seriosos riscos respecte del dret fonamental a la protecció de dades.

Una qüestió a la qual s'ha de prestar particular atenció són els treballs finals de grau (TFG), els treballs finals de màster (TFM) o les memòries de pràctiques desenvolupats amb informació obtinguda en les pràctiques.

> **Hem de ser particularment curosos respecte del maneig de la informació d'aquestes persones quan es redacten memòries de pràctiques o treballs finals de grau o de màster. Cal assegurar la informació i el consentiment i garantir l'anonimat i el respecte de la seua dignitat i els seus drets. Hem de sol·licitar autorització expressa als afectats —o als pares o tutors dels nens o persones incapacitades legalment— per enquestar-los, fer-los fotografies, enregistrar-los en vídeo o usar la seua informació personal. I hem de consultar els procediments habilitats per la nostra universitat o centre educatiu.**

Per saber-ne més:

▪ Ordre SSI/81/2017, de 19 de gener, per la qual es publica l'Acord de la Comissió de Recursos Humans del Sistema Nacional de Salut, pel qual s'aprova el protocol mitjançant el qual es determinen pautes bàsiques destinades a assegurar i protegir el dret a la intimitat del pacient pels alumnes i residents en Ciències de la Salut.

9.-Només l'RGPD? Quines altres obligacions legals hauria de conèixer?

El desenvolupament de pràctiques pot estar subjecte al compliment d'obligacions jurídiques addicionals. En primer lloc, **has de seguir les instruccions del manual d'identitat corporativa**, si n'hi ha, i no comprometre el prestigi de l'entitat.

> Un ús indegut d'un document corporatiu o un logotip o l'enviament d'un missatge de correu inadequat des d'un compte corporatiu pot danyar la reputació de l'organització.

Si gestiones recursos susceptibles de propietat intel·lectual o industrial has de guardar confidencialitat i secret professional sobre les activitats de l'entitat en la qual fas les pràctiques no solament durant l'estada, sinó també una vegada finalitzada.

> Si l'organització desenvolupa un nou producte susceptible de patent, la seua revelació o ús indegut pot posar en perill els drets de l'entitat.

No has de tenir conductes susceptibles de generar responsabilitat. **Has de respectar la política de l'organització i salvaguardar el bon nom de la Universitat**. Si no te l'han proporcionat quan t'hi has incorporat, sol·licita-la.

> **Instal·lar programari sense llicència en un ordinador de l'empresa, traure informació de l'organització, revelar secrets empresarials. Les conductes il·lícites poden suposar multes o indemnitzacions per a l'empresa, i aquesta, al seu torn, pot demandar els responsables dels actes il·lícits. El valor del dany pot ser incalculable. Podríem estar posant en perill la seua supervivència i llocs de treball.**

Recorda que fer fotografies, enregistrar vídeos o entrevistar persones pot afectar el dret a la pròpia imatge, i requereix obtenir els permisos corresponents.

> **Tingues en compte que usar fotografies de menors fent una activitat escolar per il·lustrar la nostra memòria de pràctiques requereix el permís dels seus pares o tutors i seguir els procediments establerts. Compartir-les en xarxes socials o a internet pot afectar greument l'interès superior dels menors o lesionar els seus drets.**

Si fas una memòria o un treball final de grau o de màster amb recursos de l'entitat, aquesta ha de saber-ho i ha de documentar els seus drets i els de l'estudiant.

Finalment, hem d'exercir la nostra activitat amb seguretat respectant les indicacions en matèria de prevenció de riscos laborals. I s'han d'evitar situacions d'alteració de l'ambient laboral, com ara faltes de respecte o situacions de discriminació o assetjament laboral o sexual.

Respectar els protocols d'actuació serà fonamental per salvaguardar la nostra seguretat i la d'altres persones i respectar la seua dignitat.

En el desenvolupament d'una activitat en pràctiques en certs entorns, com ara en la construcció, respectar obligacions tan òbvies com posar-se un casc o un arnès pot ser vital. És també un fet ben conegut que certes pràctiques elementals d'higiene poden ser fonamentals per evitar infeccions hospitalàries.

10.-Com ho puc fer bé amb deu senzilles regles.

I.

La Constitució i les lleis contenen normes l'objectiu de les quals és garantir els nostres drets i els de tercers. Hem d'entendre que tenim l'obligació de respectar les regles. Quan fas una pràctica **has de tenir empatia i posar-te en la pell dels altres**, dels clients de l'empresa, de la mainada al col·legi o dels pacients a l'hospital. **Les teues obligacions en l'entitat no són un capritx; són útils i serveixen per garantir els seus drets**.

II.

Participar en un programa de pràctiques **no és cap joc**. T'integres en un entorn de treball real i **has d'assumir responsabilitats**. Has de comprometre't amb el compliment de les normes. **Si no ho fas, si et comportes inadequadament, poses en un greu risc l'empresa, la institució educativa i el teu futur prestigi professional**.

III.

En les organitzacions públiques i privades **el bé més valuós és la informació** en totes les seues dimensions. Aprèn a gestionar correctament els sistemes i cenyeix-te a les regles que t'han notificat sobre aquest tema.

Els deures de seguretat i secret són fonamentals. Si els infringeixes, **poses en perill l'organització**. Pots arruïnar el seu futur empresarial, perjudicar greument clients o administrats, afectar la reputació de l'organització i ser causa de la imposició de sancions o de l'exigència d'indemnitzacions.

IV.

Has d'assumir un compromís amb la garantia de la seguretat i conèixer les normes de l'organització. Probablement resulta una mica costós, ja que suposa assumir certes obligacions i rutines, però la seguretat és una de les coses que garanteixen el funcionament de les organitzacions i la confiança que hi diposita la societat.

V.

Si coneixes alguna situació que pot posar en risc la seguretat o els béns i valors de l'entitat, comunica-la a la persona responsable. **No advertir d'una bretxa de seguretat és un comportament deslleial i irresponsable** i podria posar en perill l'organització i les persones.

VI.

Els recursos que l'organització posa a la teua disposició **no són per al teu ús i gaudi privat**. No els has d'utilitzar per a finalitats pròpies i no hi has d'instal·lar res de no autoritzat, no hi has d'emmagatzemar la teua informació i no has d'executar ni intercanviar arxius des del teu lloc de treball.

VII.

La propietat intel·lectual i industrial, la identitat i la reputació corporativa de les entitats, i els drets de les persones amb les quals treballes són béns molt valuosos. Aprèn a respectar-los, mira de no comprometre'ls i **evita de fer qualsevol cosa per a la qual no t'han concedit el permís corresponent**.

VIII.

Aplica els protocols de seguretat física i **defuig les imprudències** que poden posar-te en risc a tu o a l'entorn laboral. Cal evitar els riscos a la feina.

IX.

En el desenvolupament i presentació de la memòria de pràctiques o del treballo final de grau o de màster **has de respectar els drets de l'empresa i de les persones a les quals pot afectar el seu contingut**. Assegura't de tenir tots els permisos i autoritzacions necessaris, i, en cas de dubte, consulta-ho sempre amb els tutors a l'empresa i a la institució educativa.

X.

Et prepares per obtenir un títol acadèmic, has après les normes deontològiques de la teua professió i saps com es fan correctament les coses. Aplica la lògica i el sentit comú i **assegura't que la teua acció durant les pràctiques es correspon amb la diligència que s'espera dels bons professionals**.

Recursos

er saber-ne més:

- Agència Espanyola de Protecció de Dades. *Guía para el ciudadano*.
- INCIBE. *Decálogo ciberseguridad empresas: una guía de aproximación para el empresario*.
- INCIBE. *Glosario de términos de ciberseguridad: una guía de aproximación para el empresario*.
- Imatges obtingudes d'https://pixabay.com/

Normes sobre protecció de dades:

- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de les seues dades personals i a la lliure circulació d'aquestes dades (*text en espanyol*).
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

Altres normes:

- Llei orgànica 6/2001, de 21 de desembre, d'universitats.
- Reial decret 1791/2010, de 30 de desembre, pel qual s'aprova l'Estatut de l'estudiant universitari.
- Reial decret 592/2014, d'11 de juliol, pel qual es regulen les pràctiques acadèmiques externes dels estudiants universitaris.
- Ordre SSI/81/2017, de 19 de gener, per la qual es publica l'Acord de la Comissió de Recursos Humans del Sistema Nacional de Salut, pel qual s'aprova el protocol mitjançant el qual es determinen pautes bàsiques destinades a assegurar i protegir el dret a la intimitat del pacient pels alumnes i residents en Ciències de la Salut (*text en espanyol*).

PROMOTORS:

VNIVERSITAT DE VALÈNCIA

Càtedra Microsoft Universitat de València Privacitat & Transformació Digital

COL·LABORADORS:

Universidad de Alcalá

UNIVERSIDAD DE BURGOS

UNIVERSITAT JAUME·I

Universidad de La Laguna

Universitat de Lleida

UNIVERSIDAD DE MURCIA

Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNIVERSIDAD DE LA RIOJA

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

Delegació de Protecció Dades GVA

AMB EL SUPORT DE:

IRTIC lisitt
VNIVERSITAT DE VALÈNCIA