GUÍA SOBRE PROTECCIÓN DE DATOS PARA ESTUDIANTES QUE REALIZAN PRÁCTICAS EXTERNAS

VNIVERSITAT DE VALÈNCIA

Càtedra Microsoft
Universitat de València
Privacitat &
Transformació Digital

Guía sobre protección de datos para estudiantes que realizan Prácticas Externas

Autor:

Ricard Martínez, profesor de Derecho Constitucional de la Universitat de València.
Director de la Cátedra de privacidad y Transformación Digital Microsoft-Universitat de Valencia

Agradecimientos:

- Helena Villarejo-Galende, profesora de Derecho Administrativo de la Universidad de Valladolid.
- Monica Arenas, profesora de Derecho Constitucional de la Universidad de Alcalá.
- Cristina Pauner, profesora de Derecho Constitucional de la Universitat Jaume I.
- Julián Valero, profesor de Derecho Administrativo de la Universidad de Murcia.

Índice

Sobre esta Guía

La Universidad realiza el servicio público de la educación superior mediante la investigación, la docencia y el estudio. A través de sus programas de prácticas prepara para el ejercicio de actividades profesionales con la inestimable colaboración de todo tipo de entidades del sector público y privado.

La participación en programas de prácticas constituye una oportunidad para muchos estudiantes de insertarse plenamente en el contexto de una actividad laboral o empresarial. La formación de excelencia que proporciona la enseñanza profesional y universitaria en España permite que la integración en rutinas de trabajo reales sea prácticamente inmediata en la mayoría de los casos. Por otra parte, la naturaleza de algunas prácticas como las desarrolladas en instituciones hospitalarias, escolares, financieras o de alto valor añadido en I+D+i, traslada una especial responsabilidad a los formadores, a los entornos de prácticas y a los estudiantes, ya que acceden a información estratégica de las organizaciones que los acogen.

Esta Guía tiene por objeto primordial concienciar a entidades educativas, organizaciones y estudiantes para un adecuado cumplimiento de la normativa sobre protección de datos y complementar las guías de prácticas existentes. También aprovecha para formar sobre otras normas relacionadas con el desarrollo de las prácticas. Pretende además ofrecer consejo para promover el cumplimiento normativo con ejemplos e indicaciones concretas sobre qué se debe hacer en cada caso. Por último, no podemos olvidar que el estudiante de hoy será sin duda el emprendedor de mañana y promover un futuro tejido empresarial y profesional concienciado con el cumplimiento normativo en el ámbito de las tecnologías de la información y las comunicaciones constituye sin duda un reto estratégico.

1.-¿Por qué deberías leer esta Guía?

Vivimos en una época de transformación digital. Nos despierta un Smartphone que nos ofrece avisos sobre temas pendientes, agenda del día, el pronóstico del tiempo y la ruta más rápida para llegar a clase. Subimos al autobús y validamos el billete desde el teléfono móvil. Durante el viaje verificamos, -otra vez-, WhatsApp y/o Telegram, ojeamos Facebook e Instagram, -etiquetamos o damos *likes*-, y ya estamos en clase. Allí, nos enganchamos a EDUROAM o la wifi que exista. En la biblioteca, la máquina de bebidas, o al fichar la clase y en la ropa se usan tarjetas de identificación por radiofrecuencia (RFID). Usamos o nos graban videocámaras en todas partes. Pedir una beca o matricularse puede ser ya un proceso puramente electrónico en el que cuatro o cinco entidades diferentes intercambian nuestros datos. En nuestro mundo se tratan datos todo el tiempo. No hay un solo momento del día en el que no estemos manejando información personal de terceros o estemos facilitando la nuestra o la de otros. La sociedad de nuestro tiempo funciona gracias al procesamiento masivo de datos personales y de todo tipo de información complementaria.

> Cuando un entorno social edita un anuncio o sugiere un contacto ha tenido en cuenta nuestros datos de registro, nuestra red de contactos, nuestros *likes*, las *cookies* que ha generado nuestra navegación, nuestra geolocalización, en resumen, nuestro perfil de comportamiento. Para ello trata decenas de datos nuestros y miles de referencias contextuales.

Tratar información impone obligaciones, deben informarnos mediante políticas de privacidad, consentimos en el registro y podemos ejercer los derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición al tratamiento. El derecho fundamental a la protección de datos está pensado para protegernos.

> **Pero cuando nos insertamos en un entorno laboral pasamos al otro lado, tratamos datos de los demás asumimos ciertos compromisos legales y se espera de nosotros la capacidad de manejar adecuadamente los datos personales y garantizar la seguridad de la información corporativa.**

Por ello la lectura de esta Guía nos ayudará a conocer nuestras obligaciones. Seguir sus recomendaciones no solo es necesario si queremos ser buenos profesionales, también mejora nuestras capacidades. El objetivo esencial de esta Guía es ofrecerte información sobre los aspectos básicos relativos a la protección de datos, la seguridad y el cumplimiento normativo que afectan a los estudiantes en prácticas.

2.-¿Qué arriesga la empresa o lugar de prácticas? ¿Y mi universidad o centro educativo?

Todas, si no la mayor parte de las actividades profesionales, están reguladas. Cuando nos insertamos en un programa de prácticas, sean estas curriculares o extracurriculares, un conjunto de organizaciones y personas asumen obligaciones y derechos.

La organización que nos acoge no puede actuar de cualquier manera. Se le va a exigir que el puesto de prácticas sea seguro en términos de prevención de riesgos laborales. Deben formarnos e informarnos. Se nos asigna un tutor que deberá dirigir y coordinar nuestra actividad y realizar un informe final.

Nuestro centro educativo supervisa el programa de prácticas, asigna al estudiante un tutor académico, además de asegurar que ha recibido una formación suficiente y dispone de las capacidades necesarias para desarrollar el programa. El estudiante será responsable de sus actos. Por eso suele firmar un convenio o acuerdo de prácticas, y la empresa o entidad al inicio de la actividad puede plantearle la firma un documento donde se recogen sus deberes y obligaciones, y en particular las relativas a confidencialidad, seguridad y protección de datos.

¿Y qué sucede si por falta de formación o de información hacemos algo mal? Por ejemplo, si instalamos software no autorizado o si revelamos datos a terceros. Si incumplimos una norma respondemos personalmente, pero también podemos causar un daño a la empresa, a la universidad o al centro educativo quienes también, por su parte, deberán hacer frente a su responsabilidad jurídica que puede suponer, por ejemplo, el pago de multas, sanciones e indemnizaciones. Además, podría afectar al prestigio público de la institución educativa. Así, si el hecho se publicase en la prensa daría una mala publicidad a nuestro programa de prácticas lo que afectará a nuestras oportunidades de empleo en el futuro.

Por ello, nuestra responsabilidad en esta materia consiste en haber aprendido correctamente las normas deontológicas que rigen nuestra futura profesión. Además, debemos ceñirnos con rigor a las instrucciones de nuestros formadores y a las que, de modo específico, se nos notifiquen en el lugar de prácticas.

Veamos a continuación en qué consisten nuestras obligaciones en relación con el tratamiento de datos de carácter personal.

3.-¿Qué es un dato personal y qué es el RGPD?

Un dato de carácter personal es cualquier información relativa a una persona física identificada o identificable. Las personas son identificables cuando podemos establecer, sin mucho esfuerzo, una relación entre la información que obtenemos y una persona concreta.

> Nuestro nombre y apellidos son un dato personal, y también nuestra dirección. Son datos una fotografía, nuestros movimientos de la tarjeta de crédito, la geolocalización de nuestro Smartphone, una radiografía o los resultados de un análisis clínico. Cuando nos graba una cámara, aunque no estemos siendo identificados, podríamos ser fácilmente identificables.

Hoy basta con poner el nombre y apellidos en un buscador, e incluso solo una fotografía, para obtener miles de informaciones.

> Cuando solicitamos un trabajo es casi inevitable que el futuro empleador contraste nuestro currículum mediante búsquedas en Internet. En el ámbito de la Administración, las decisiones dependen cada vez más de la información disponible en medios informáticos. Se acerca el día en que solo será necesario conectarse y pedir una beca para que se conceda de modo casi automático cruzando la información disponible en distintas bases de datos "sin aportar papeles".

La sociedad de la información tiene muchas ventajas y algunos peligros. Si nuestro perfil es incorrecto, no nos concederán la beca; si la información disponible en Internet es falsa o desactualizada, podrían no contratarnos; si alguien usa mal los datos, podría causarnos daño. Por ello, la Constitución española y la Carta de los Derechos Fundamentales de la Unión Europea reconocen el derecho fundamental a la protección de datos personales que regulan el **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)** y **la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**. Estas normas definen las garantías que aseguran un control sobre nuestros datos, y que estos se traten adecuadamente y con la debida seguridad.

Son normas muy exigentes, imponen a las organizaciones obligaciones de información, de actualización de los datos, o de seguridad y secreto. Y estas obligaciones deben ser ejecutadas y respetadas por las personas empleadas y los estudiantes en prácticas.

> **Contribuimos a garantizar los derechos de las personas y a que la organización que nos acoge disponga de una información de calidad, confiable y segura, cuando durante nuestras prácticas cumplimos con el RGPD, la LOPDGDD y con otras normas.**

4.-¿Tengo derechos en protección de datos? ¿Y obligaciones?

Para garantizar el control sobre nuestra información personal la normativa de la Unión Europea y la española han definido un conjunto de facultades que afectan a todo el ciclo de vida de los datos desde su recogida hasta su borrado. Estas facultades son la transparencia o información en la recogida de la información , el consentimiento, y los derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición al tratamiento.

En primer lugar, siempre deben informarte sobre quién tratará tus datos, para qué los usará, si es obligatorio facilitarlos, a quién se cederán y dónde y cómo ejercer tus derechos y, además, habrá un enlace a una capa de información más detallada al respecto. Para poder usar esos datos será necesario con carácter general que lo aceptes, y el consentimiento, según los casos, deberá ser específico para cada una de las finalidades diferentes del tratamiento.

> 🔑 Cuando te registras en una red social, o cuando descargas una aplicación móvil, siempre aparece al final y antes de aceptar una frase que dice: "Vd. conoce y acepta nuestras políticas de privacidad". Es allí donde nos están informando y, por tanto, cuando aceptamos el tratamiento de nuestros datos. Se ha demostrado que la inmensa mayoría no las lee. En un conocido experimento más del 90% de los que se registraron en una web aceptaron la venta de su alma al diablo.

Para conocer el estado de tus datos puedes acceder a ellos; si contienen un error, pedir que se rectifiquen; y si hay una razón justificada para eliminarlos, puedes ejercer el derecho de cancelación. También puedes ejercer el derecho al olvido en Internet, oponerte al envío de publicidad, reclamar que se limite el tratamiento de los mismos y obtener tus datos en un formato compatible para usarlos en otros sitios.

> 🔑 Cuando queremos saber si se pusieron bien las notas en el último trimestre ejercemos un derecho de acceso, y si hay un error pedimos su rectificación o que se cancele un dato innecesario. Los datos de un buscador se obtienen sin nuestro consentimiento. Pero cuando un resultado afecta a nuestros derechos podemos oponernos a que las búsquedas que se hagan usando nuestro nombre y apellidos ofrezcan el enlace al contenido que nos perjudica. Es lo que se ha llamado derecho al olvido.

Pero estos derechos suponen costes y un esfuerzo para las organizaciones que, además, han de asegurar la calidad de los datos, controlar a los proveedores, e invertir en seguridad y asesoramiento jurídico.

> 💡 **Por eso se imponen deberes a las personas que trabajan y/o prestan un servicio en la organización para asegurar un tratamiento adecuado de los datos. Si en el marco de tus prácticas no cumples con estas obligaciones pones en peligro a la empresa y a los derechos de los clientes. En los siguientes apartados exponemos algunos de estos deberes que te afectarán durante tus prácticas.**

📚 Para saber más:

- Agencia Española de Protección de Datos. Guía para el ciudadano.

5.-¿Por qué debo guardar secreto?

El deber de secreto se exige prácticamente en todas las profesiones. Este secreto que se exige al funcionario, al trabajador, o al profesional o al estudiante en prácticas cumple funciones muy diversas.

El secreto puede ser fundamental para la supervivencia de la empresa. Así, cuando nos insertamos en un entorno laboral en el que existe algún tipo de I+D+i (investigación, desarrollo e innovación), o cuando se obtienen ventajas competitivas por adoptar cierto tipo de procesos o localizar a determinados proveedores, o cuando se va a lanzar un nuevo producto, el secreto puede ser crucial para la supervivencia de la organización.

Si asistes a una reunión estratégica de la empresa, o a un curso de formación sobre una nueva actividad o producto, o te encuentras en un lugar restringido y por ejemplo publicas un tuit, una foto en Instagram, o un comentario en una red social, o te geolocalizas ofreciendo información a terceros, podrías estar filtrando sin querer información muy valiosa para la competencia.

En otras ocasiones, es la propia naturaleza de la actividad la que exige ese deber de secreto. En el ejercicio de funciones públicas las personas que prestan sus servicios en la Administración tienen un deber de secreto. Éste puede ser muy importante en lugares en los que se maneja información sensible como un hospital o consulta clínica, un centro escolar, una entidad con personas que tienen algún tipo de discapacidad (atención a la diversidad), o respecto de ciertos datos económicos, fiscales, laborales, judiciales... En estos casos el secreto protege tanto a la organización como a sus clientes o usuarios.

Si mientras realizas prácticas en una clínica, alguien llama por teléfono y le facilitas información sobre el paciente o se la proporcionas a un tercero sin verificar que está autorizado, estás vulnerando el derecho a la intimidad de la persona enferma.

En protección de datos también existe deber de secreto. Y este resulta más exigente incluso que los anteriores. Este derecho afecta a cualquiera que trate datos personales, esto es, es cualquier tipo de información referida a una persona identificada o identificable. Por tanto, no depende ni del tipo de empresa, ni de su actividad, ni del tipo de dato, ni de tu perfil profesional. Basta con el simple hecho de que accedas a datos para tener que cumplir con este deber.

Cuando se respeta el secreto se garantiza el derecho fundamental a la protección de datos personales y con ello valores jurídicos y sociales muy valiosos.

6.-¿Para qué sirve la seguridad?

Uno de los recursos estratégicos que maneja toda organización es la información, tanto personal como de cualquier otra naturaleza. Cada vez es más común apreciar que lo verdaderamente valioso no se encuentra tanto en un plano físico o material sino en algo tan intangible como la información y el conocimiento.

> Compramos online, usamos una aplicación o nos registramos en un servicio pensando que es seguro. Si una empresa de Internet tiene un fallo de seguridad perderá la confianza de sus clientes y se arriesgará a desaparecer.

En el ámbito de la seguridad de la información se persiguen cuatro objetivos básicos: la confidencialidad, la integridad, la disponibilidad y la resiliencia.

a) La confidencialidad es instrumental al secreto. La información nunca debe poder ser conocida por terceros no autorizados.

b) La integridad sirve para asegurar que los datos no han sido alterados indebidamente falseando un perfil.

c) La disponibilidad asegura que los sistemas de información podrán activarse y estar disponibles ante cualquier incidente sea lógico -un virus que colapse un sistema-, o físico como un incendio o una inundación.

d) La resiliencia asegura la capacidad de los sistemas de información de recuperarse ante eventos críticos.

Para la seguridad de la información el compromiso de cada persona empleada es esencial.

> Un hospital no puede permitirse que terceros no autorizados accedan a una historia clínica, o que se produzcan errores o manipulaciones en la historia clínica de un paciente, y si hubiera por ejemplo un problema en el fluido eléctrico debe disponer de medios para mantener la alimentación eléctrica de los sistemas de información.

La seguridad no solo posee una dimensión reactiva, esto es, no solo sirve para evitar un resultado o remediar un daño, sino que también, proporciona a la organización confianza en sus capacidades, así como en la certeza y en la validez de la información que maneja, permitiendo de este modo adoptar decisiones basadas en información veraz y confiable.

> **En la seguridad el elemento más importante, y también el eslabón más débil, son los usuarios, las personas. En el desarrollo de tus prácticas debes prestar mucha atención y aplicar rigurosamente las políticas de seguridad de la entidad. Antes de empezar la actividad pregunta por ellas si no te las han proporcionado.**

7.-¿Cómo puedo contribuir a cumplir el RGPD y la LOPDGDD y garantizar la seguridad? ¿Cuáles son mis obligaciones?

Al integrarnos en el equipo de trabajo de una organización asumimos un conjunto de obligaciones. Es posible que nuestro lugar de prácticas cuente con un protocolo de bienvenida o de formación. Si es así, debemos prestar la mayor atención e interiorizar las normas y procedimientos de actuación establecidos. En cualquier caso, existe un conjunto de medidas de seguridad que deberíamos conocer y aplicar, ya que responden al sentido común. A continuación, se enumeran algunas de ellas.

Acceso a instalaciones

Deberemos respetar las prohibiciones de acceso si las hubiera, limitarnos a nuestros permisos y, en todo caso, aplicar las condiciones que existan para ello.

> 🔑 No es inusual que el acceso a las zonas de archivo clínico o el emplazamiento del equipamiento informático resulte restringido. En ocasiones, en función de la naturaleza de la información, podrían existir reglas de actuación como, por ejemplo, no apagar ciertos equipos, o no introducir un Smartphone con cámara.

Cuando necesitemos acceder a un área restringida, seguiremos siempre los procedimientos internos para obtener autorización.

Controles de acceso lógico

En nuestra incorporación lo usual debería ser que nos asignen permisos de acceso a los sistemas de información, habitualmente mediante algún tipo de validación de usuario y contraseña. Estas claves suelen ser facilitadas por algún responsable de la entidad y deberían ser individuales. Al usarlas debemos acceder exclusivamente a los recursos y sistemas autorizados y únicamente desde el puesto o terminal asignados.

Será fundamental bloquear el equipo si nos ausentamos, salir de las aplicaciones protegidas cuando no debamos usarlas, y asegurarnos de que la pantalla no resulte accesible o legible para terceros no autorizados. El ordenador debe apagarse fuera del horario de trabajo, activar sus sistemas de bloqueo tras un periodo de inactividad y evitar su uso por terceras personas.

> 🔑 Un despiste tan obvio como dejar una sesión abierta puede permitir a un visitante o a un colega desleal robar información usando nuestro usuario. Y en tal caso se nos atribuirá la responsabilidad.

Debemos proteger nuestra contraseña, no compartirla nunca, cambiarla periódicamente o cuando se nos requiera, y activar contraseñas seguras.

> 🔑 Uno de los modos usuales de atacar un sistema consiste en averiguar la contraseña de un usuario. Pones en riesgo la seguridad del sistema si, por ejemplo, la cedes a un compañero. También si generas una contraseña débil como tu nombre o fecha de nacimiento, en lugar de una combinación de al menos ocho caracteres que no sean una palabra y que incluyan mayúsculas, algún signo y números.

Acceso remoto y dispositivos propios

Si está prevista alguna fórmula de teletrabajo con acceso remoto a los sistemas de información, o si se permite llevar a casa dispositivos portátiles o usar los propios, debemos extremar la seguridad. Es preferible que la información permanezca en el sistema de la empresa o en el del proveedor autorizado. Debemos renunciar a prácticas de riesgo con estos dispositivos, como compartirlos con terceros, instalar software no verificado, llevarnos información en un pendrive para seguir trabajando en casa, o usar programas *peer to peer*.

> 🔑 Cuando se descargan archivos de terceros, estamos abriendo de par en par las puertas de nuestro ordenador a terceros. Y lo mismo sucede cuando usamos una red Wi-Fi no segura.

Destrucción de soportes

Teniendo siempre en cuenta las instrucciones de la entidad en la que estemos, las impresiones o copias de trabajo de información protegida en soporte papel, la copia en DVD, CD o las fotocopias que no se vayan a utilizar deben ser destruidas. Cuando la información se haya incorporado a un pendrive, o a cualquier dispositivo ajeno al sistema de información deberá borrarse mediante sistemas de borrado seguro, formatearse o destruirse si va ser desechado.

> 🔑 Una de las fugas de datos más frecuente se produce cuando el papel acaba en la basura convencional, o cuando se reutiliza un dispositivo. INCIBE recomienda, por ejemplo, la sobreescritura de dispositivos con herramientas como Eraser, DBAN o Hardwipe.

Correo electrónico y red corporativa

Un mal uso del correo electrónico pone en riesgo a la organización. No debe usarse para tareas privadas no corporativas, o ejecutando archivos indebidos. Utilizar la red para descargarse contenidos protegidos puede generar responsabilidad jurídica al empleador.

> 🔑 Basta con ejecutar una canción en *mp3* para instalar un virus o un troyano, o para ser indexado por quienes actúan para defender los derechos de propiedad intelectual. En ambos casos, causamos un daño a la entidad.

Sistemas actualizados

Las actualizaciones del software son vitales ya que sirven para la corrección de vulnerabilidades. En muchas ocasiones exigen una actuación proactiva del usuario que debe verificar una solicitud de actualización, ejecutarla y reiniciar el equipo. Debemos realizar las actuali-

zaciones siempre que proceda de acuerdo con las indicaciones recibidas y, en particular, las que afecten al sistema operativo, firewall y antivirus.

> Debemos asegurarnos de que nuestro sistema se conecta buscando actualizaciones de acuerdo con la política de la organización respetando sus recomendaciones. En algunos casos y con fines promocionales, las actualizaciones incluyen programas que podrían estar no autorizados, no olvidemos desmarcar la correspondiente casilla.

Una mesa limpia

El puesto de trabajo debe ser un lugar ordenado, que nos permita en todo momento controlar la documentación y a la vez que impida que terceros accedan a la misma indebidamente. Siempre debemos custodiar la información y, si nos ofrecen medios para ello, almacenarla en lugar seguro al finalizar la jornada.

> En muchas organizaciones servicios como la limpieza o la seguridad se prestan por la noche o con el edificio vacío. Si la información se deja sobre la mesa o en un lugar accesible, la exponemos a un riesgo de pérdida o robo. También podemos poner en peligro esta información si sale de la empresa y la usamos, por ejemplo, en una biblioteca.

Incidencias

Una incidencia es cualquier evento que pudiera afectar a la seguridad de un sistema de información. El usuario que padece una incidencia debe comunicarla al responsable designado. Tener una incidencia no es una infracción, ni debe avergonzarnos. Pero no comunicarla comporta un riesgo para la organización y nos hace responsables.

> Encontrar el ordenador encendido al incorporarnos al puesto, perder un documento, borrar por accidente información, un funcionamiento anormalmente lento del ordenador, o bloquear, perder u olvidar la contraseña son incidencias.

Blogs, redes sociales

No podemos comentar nada que comprometa a nuestra empresa en espacios sociales cuando ponemos en riesgo su prestigio, la intimidad de sus clientes, secretos empresariales o podamos afectar a la seguridad de la información. Un comentario irresponsable o inadecuado puede causar daños de los que debamos responder.

Para saber más:

- 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 trabajo con menores, pacientes o en despachos de abogados.

Algunos entornos de prácticas resultan particularmente delicados. Son sensibles para el derecho fundamental a la protección de datos, las prácticas que implican trabajar con personas enfermas, menores, con expedientes judiciales o con diversidad funcional. En algunos de estos casos nos pueden requerir información personal adicional como, por ejemplo, un certificado negativo de antecedentes penales y deberemos facilitarla.

Los pacientes o los clientes de un abogado confían plenamente en los profesionales que les atienden con la esperanza de encontrar soluciones. La atención de estas personas supone la revelación de datos íntimos y en ocasiones socialmente vergonzantes. Si esta información no se protege y se hace pública, o se revela a terceros, ponemos en riesgo la intimidad, la dignidad y los derechos de las personas.

> **No podemos revelar información clínica por teléfono a una persona no autorizada, del mismo modo que tampoco podemos depositar en la basura convencional una historia clínica. Podemos comprometer la imagen o el honor de una persona, o incluso provocar una situación que le impida el acceso a derechos como el trabajo.**

Lo mismo sucede cuando desarrollamos nuestra tarea en el ámbito educativo. Los menores son personas en formación cuya información resulta particularmente sensible. Debemos ser diligentes en su manejo ya que en muchas ocasiones será fundamental para salvaguardar la seguridad del menor. Asimismo, deberemos asegurarnos de que la información sobre el menor no se facilite nunca a terceros no autorizados.

> Las situaciones familiares desestructuradas, en las que un familiar no autorizado pretende acceder a información, o acciones aparentemente inocuas como hacerse una foto con la clase y subirla a una red social entrañan serios riesgos respecto del derecho fundamental a la protección de datos.

Una cuestión a la que debe prestarse particular atención es a las memorias de prácticas, Trabajos finales de Grado (TFGs) o Trabajos finales de Máster (TFMs) desarrollados con información obtenida en las prácticas.

> **Debemos ser particularmente cuidadosos respecto del manejo de la información de estas personas al redactar memorias de prácticas o trabajos finales de Grado o Máster. Hay que asegurar la información y el consentimiento, que se garantiza su anonimato y el respeto de su dignidad y sus derechos. Debemos solicitar autorización expresa al afectado, o a los padres o tutores de los niños o personas incapacitadas legalmente, para encuestarlos, hacer fotografías, grabar vídeos o usar su información personal. Y debemos consultar los procedimientos habilitados por nuestra universidad o centro educativo.**

Para saber más:

- Orden SSI/81/2017, de 19 de enero, por la que se publica el Acuerdo de la Comisión de Recursos Humanos del Sistema Nacional de Salud, por el que se aprueba el protocolo mediante el que se determinan pautas básicas destinadas a asegurar y proteger el derecho a la intimidad del paciente por los alumnos y residentes en Ciencias de la Salud.

9.-¿Solo el RGPD? ¿Qué otras obligaciones legales debería conocer?

El desarrollo de prácticas puede estar sujeto al cumplimiento de obligaciones jurídicas adicionales. En primer lugar, debes **seguir las instrucciones del manual de identidad corporativa** si lo hay, y no comprometer el prestigio de la entidad.

> Un uso indebido de un documento corporativo, de un logotipo, o el envío de un mensaje de mail inadecuado desde una cuenta corporativa puede dañar la reputación de la organización.

Si manejas recursos susceptibles de propiedad intelectual o industrial, debes guardar confidencialidad y secreto profesional sobre las actividades de la entidad en la que realices las prácticas no solo durante tu estancia, sino también una vez finalizada esta.

> Si la organización desarrolla un nuevo producto susceptible de patente, su revelación o uso indebido puede poner en peligro los derechos de la entidad.

No desarrolles conductas que puedan generar responsabilidad. **Debes respetar la política de la organización y salvaguardar el buen nombre de la universidad**. Si no te la han proporcionado al incorporarte solicítala.

> **Instalar software no licenciado en un ordenador de la empresa, sacar información de la organización, revelar secretos empresariales. Las conductas ilícitas pueden suponer multas o indemnizaciones para la empresa, y esta, a su vez, puede demandar al responsable del acto ilícito. El valor del daño puede ser incalculable. Podríamos estar poniendo en peligro su supervivencia y puestos de trabajo.**

Recuerda que, tomar fotografías, grabar vídeos o entrevistar a personas puede afectar al derecho a la propia imagen y requiere obtener los permisos correspondientes.

> **Ten en cuenta que, usar fotografías de menores realizando una actividad escolar para ilustrar nuestra memoria de prácticas requiere el permiso de sus padres o tutores y seguir los procedimientos establecidos. Compartirlas en redes sociales o en internet puede afectar gravemente al interés superior del menor o lesionar sus derechos.**

Si desarrollas una memoria o un Trabajo final de Grado o Máster con recursos de la entidad esta debe saberlo y documentar sus derechos y los del estudiante.

Por último, debemos desempeñar nuestra actividad con seguridad respetando las indicaciones en materia de prevención de riesgos laborales. Y deben evitarse situaciones que alteren

el ambiente laboral como faltas de respeto o situaciones de discriminación o acoso laboral o sexual. Respetar los protocolos de actuación será fundamental para salvaguardar nuestra seguridad y la de otras personas y respetar su dignidad.

> En el desarrollo de una actividad en prácticas en ciertos entornos, como una construcción, respetar obligaciones tan obvias como usar un casco o un arnés puede ser vital. Es también un hecho bien conocido cómo ciertas prácticas elementales de higiene pueden ser fundamentales para evitar infecciones nosocomiales.

10.-Cómo hacerlo bien con diez sencillas reglas.

I.

La Constitución y las leyes contienen normas cuyo objetivo es garantizar nuestros derechos y los de terceros. Debemos entender que tenemos la obligación de respetar las reglas. Cuando realices una práctica **sé empático y ponte en la piel de los demás,** del cliente de la empresa, del niño en el colegio o del paciente en el hospital. **Tus obligaciones en la entidad no son un capricho, son** útiles **y sirven para garantizar sus derechos**.

II.

Participar en un programa de prácticas **no es un juego**. Te integras en un entorno de trabajo real y **debes asumir responsabilidades**. Debes comprometerte con el cumplimiento de las normas. **Si no lo haces, si te comportas inadecuadamente, pones en un grave riesgo a la empresa, a la institución educativa, y a tu futuro prestigio profesional**.

III.

En las organizaciones públicas y privadas **el bien más valioso es la información** en todas sus dimensiones. Aprende a gestionar correctamente los sistemas y cíñete a las reglas que se te hayan notificado al respecto.

Los deberes de seguridad y secreto son fundamentales. Si los infringes, **pones en peligro a la organización**. Puedes arruinar su futuro empresarial, perjudicar gravemente a clientes o administrados, afectar a la reputación de la organización y ser causa de que se le impongan sanciones o se le exijan indemnizaciones.

IV.

Debes **asumir un compromiso con la garantía de la seguridad** y conocer las **normas de la organización**. Probablemente resulte un poco costoso ya que supone el asumir ciertas obligaciones y rutinas, pero la seguridad es una de las cosas que hace que las organizaciones funcionen y que la sociedad confíe en ellas.

V.

Si conoces alguna situación que puede poner en riesgo la seguridad o los bienes y valores de la entidad comunícalo al responsable. **No advertir de una brecha de seguridad es un comportamiento desleal e irresponsable** y podría poner en peligro a la organización y a las personas.

VI.

Los recursos que la organización pone a tu disposición **no son para tu uso y disfrute privado**. No los utilices para fines propios y no instales en ellos nada no autorizado, no almacenes allí tu información, no ejecutes ni intercambies archivos desde tu puesto de trabajo.

VII.

La propiedad intelectual e industrial, la identidad y la reputación corporativa de las entidades, y los derechos de las personas con las que trabajas son bienes muy valiosos. Aprende a respetarlos, no los comprometas y **no hagas nada para lo que no se te haya concedido el oportuno permiso.**

VIII.

Aplica los protocolos de seguridad física y **no cometas imprudencias** que puedan ponerte en riesgo a ti o al entorno laboral. Hay que evitar los riesgos en el trabajo.

IX.

En el desarrollo y presentación de tu Memoria de Prácticas o del Trabajo Fin de Grado o Fin de Máster **debes respetar los derechos de la empresa y de las personas a las que pudiera afectar su contenido**. Asegúrate de contar con todos los permisos y autorizaciones necesarios y, en caso de duda, consulta siempre con tu tutor en la empresa y en la institución educativa.

X.

Eres un futuro titulado, has aprendido las normas deontológicas de tu profesión y sabes cómo se hacen correctamente las cosas. Aplica la lógica y el sentido común y asegúrate de **que tu acción durante las prácticas se corresponda con la diligencia que se espera de un buen profesional**.

Recursos

Para saber más:

- Agencia Española de Protección de Datos. 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
- Imágenes obtenidas de https://pixabay.com/

Normas sobre protección de datos.

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Otras normas.

- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.
- Real Decreto 1791/2010, de 30 de diciembre, por el que se aprueba el Estatuto del Estudiante Universitario.
- Real Decreto 592/2014, de 11 de julio, por el que se regulan las prácticas académicas externas de los estudiantes universitarios.
- Orden SSI/81/2017, de 19 de enero, por la que se publica el Acuerdo de la Comisión de Recursos Humanos del Sistema Nacional de Salud, por el que se aprueba el protocolo mediante el que se determinan pautas básicas destinadas a asegurar y proteger el derecho a la intimidad del paciente por los alumnos y residentes en Ciencias de la Salud.

PROMOTORES:

VNIVERSITAT DE VALÈNCIA

Càtedra Microsoft Universitat de València Privacitat & Transformació Digital

COLABORADORES:

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

CON EL SOPORTE DE:

IRTIC lisitt
VNIVERSITAT DE VALÈNCIA