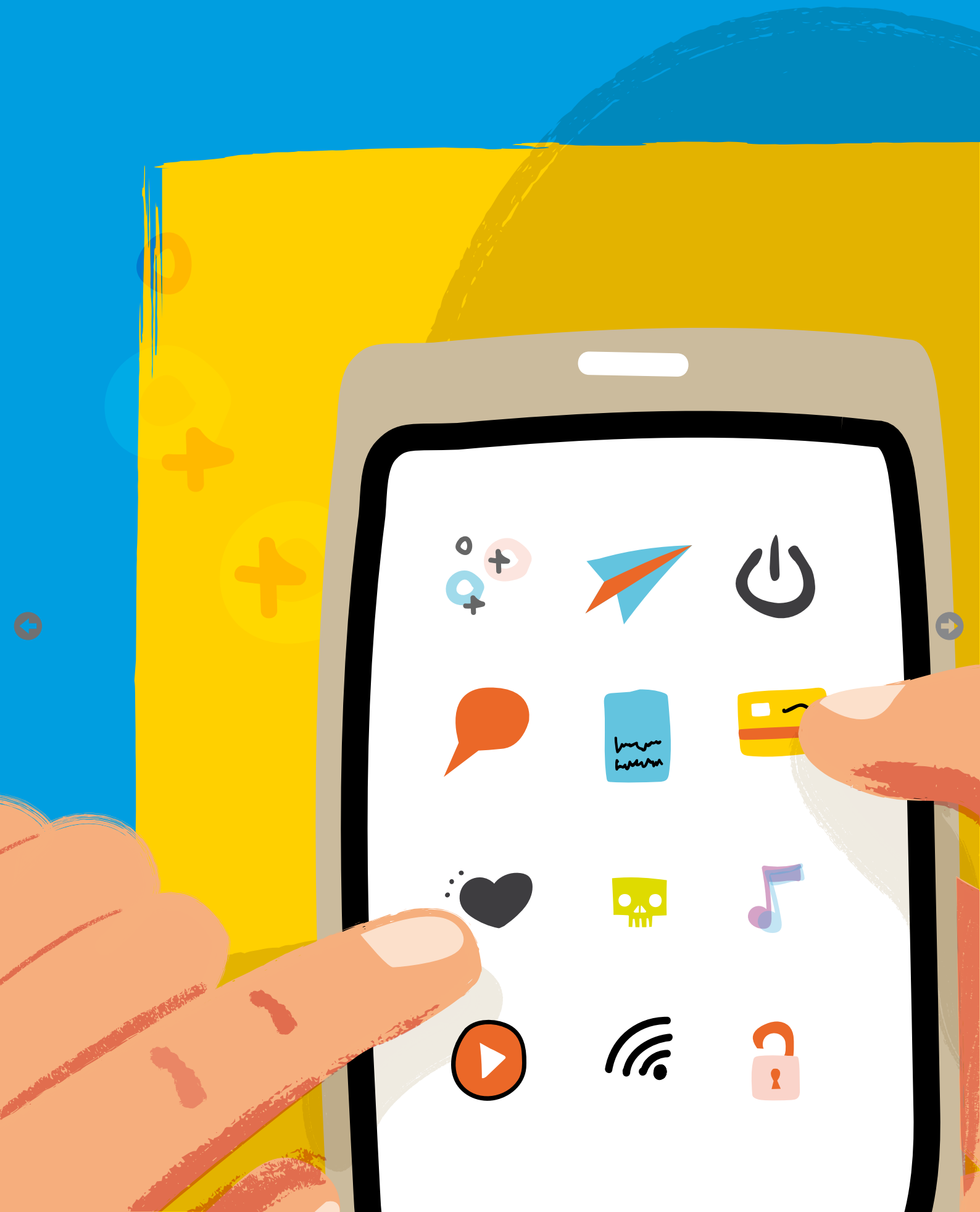
ACCEDER

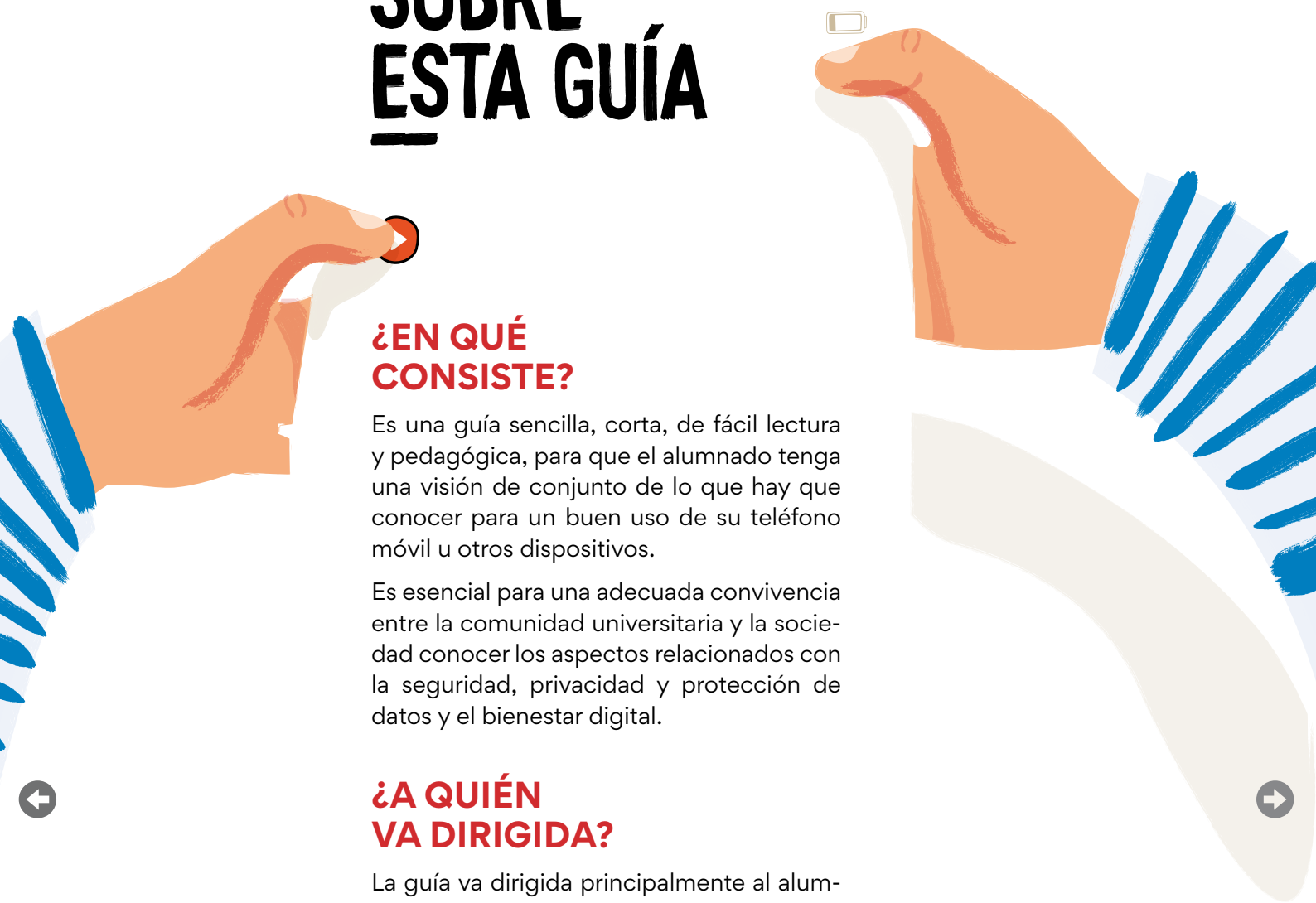
UNIVERSIDAD DE GRANADA

Unidad de calidad, innovación docente y prospectiva



GUÍA DE (BUEN) USO PARA TUS DISPOSITIVOS MÓVILES

SOBRE ESTA GUÍA



¿EN QUÉ CONSISTE?

Es una guía sencilla, corta, de fácil lectura y pedagógica, para que el alumnado tenga una visión de conjunto de lo que hay que conocer para un buen uso de su teléfono móvil u otros dispositivos.

Es esencial para una adecuada convivencia entre la comunidad universitaria y la sociedad conocer los aspectos relacionados con la seguridad, privacidad y protección de datos y el bienestar digital.

¿A QUIÉN VA DIRIGIDA?

La guía va dirigida principalmente al alumnado de la UGR, pero se refiere a aspectos que pueden ser de interés y utilidad para toda la comunidad universitaria y para cualquier comunidad educativa.

OBJETIVOS

Esta guía nace con vocación orientativa y preventiva, para informar sobre un uso adecuado de los dispositivos móviles que utiliza el alumnado de la UGR como instrumento de aprendizaje, pero también para relacionarse con compañeros/as, y con la Universidad.

Para ello es esencial que toda la información esté recogida en un único documento claro y accesible.

CONSEJOS PARA UN USO SEGURO

OJO CON LAS CONEXIONES

Es aconsejable que instales VPN cuando accedas desde fuera de la universidad a los recursos educativos de la UGR. Utiliza **la wifi de la UGR** siempre que sea posible, ahorrarás datos y estarás más seguro/a. No olvides que las **wifi's gratuitas** en cafeterías suelen ser **inseguras**, no tienen clave o todo el mundo la sabe, por lo que se puede visualizar el tráfico de datos de tu teléfono y por tanto averiguar tus claves y/o acceder al mismo.

DESCARGA SIN JUGÁRTELA

Descarga las apps siempre en la tienda oficial (desde la App store para Apple o desde Play store para Android). Y en caso de ordenadores, hay que descargarlas desde el sitio web oficial.

EN VIDEOCONFERENCIAS

Cuando haya una videoconferencia para cursos de formación y reuniones en la UGR, conéctate a través de tu cuenta go.ugr.es.

EN LAS REDES

Recuerda que si utilizas tu teléfono móvil, o cualquier otro dispositivo para acceder a redes sociales, éstos deben contar con soluciones antimalware, (por ej. antivirus y/o firewall) sistema operativo y otro software actualizado. Aquí te dejamos algunas gratuitas.

Antivirus y cleaners

BLINDA TU CONTENIDO

Utiliza contraseñas de acceso que sean robustas para evitar poner en riesgo el perfil de la universidad. No utilices para las contraseñas fechas de nacimiento o el "123456" clásico. Deben llevar números, letras y caracteres especiales.

No uses nunca en los dispositivos móviles la función de "recordar contraseña", pues si cae en manos inapropiadas pueden tener acceso a las apps donde esté activado el recuerdo de contraseña.

No guardes contraseñas a la vista, ni física ni digitalmente. Utiliza lo que se llama un segundo factor de autentificación siempre que se pueda. No compartas contraseñas.

Si tienes muchas, existen gestores de contraseñas que nos ayudan a recordarlas. Aquí van algunos gratuitos.

Gestores de contraseñas

¡NO CLIQUES, NO PIQUES!

Ante la menor duda con el enlace, evita acceder al sitio web, pues pueden redirigir a sitios fraudulentos de tipo phishing o a otros sitios Web.

¿Y ANTE UN ROBO?

Para poner una denuncia en caso de robo, es conveniente guardar la información de IMEI del teléfono. Este número identifica al teléfono de forma unívoca y es conveniente guardarlo en lugar seguro, por si acaso.

También se pueden descargar utilidades antirrobo y siempre hacer copias de seguridad para no perder todas las fotos y resto de nuestros documentos. Echa un vistazo a estas que te proponemos.

Antirrobo **Backup**

REDES SOCIALES Y MENSAJERÍA INSTANTÁNEA

ANTE TODO, "RESPETO DIGITAL".

Recuerda que la DIGNIDAD Y RESPETO conforman los valores y compromisos éticos de nuestra Universidad. Actúa siempre con cortesía y prudencia y de forma cuidadosa con los demás y con nosotros mismos, para respetar la privacidad e intimidad, las opiniones, la propiedad intelectual e industrial, la información y también proteger nuestros datos personales sensibles.
Para ello, veamos algunas recomendaciones a tener en cuenta:

A ADMINISTRACIÓN

Recuerda que en los grupos de whatsapp, el/la administrador del grupo puede incurrir en responsabilidades por los comentarios lesivos vertidos por terceros, si no los elimina o les pone freno con diligencia.

B BUENAS PRÁCTICAS

No olvides que detrás de las pantallas hay personas.

- No filtres conversaciones.
- Si a través de redes sociales te llegan contenidos violentos o lesivos a la intimidad de terceros (ej. *revenge porn* o sexting), "pára-lo", no seas cómplice del daño.
- No generes bulos o noticias falsas, información descontextualizada o sesgada, y con escasa calidad informativa.
- No contribuyas con tus mensajes al discurso de odio y la discriminación. Y evita actuaciones que puedan dar lugar a un caso de *ciberbullyng*.

C CONTROL

No difundas por redes sociales (incluidos grupos de whatsapp) el listado de calificaciones que el profesor/a sube a Prado.

D DIFUSIÓN RESPETUOSA

Evita dar información confidencial o sujeta a propiedad intelectual. No difundas apuntes y material colgado en Prado por el profesor/a. Respeta la propiedad intelectual.

No grabes imágenes ni conversaciones con el dispositivo móvil en clase. No tienes el consentimiento ni del docente ni del alumnado.

E ENVÍOS ADECUADOS

En la actividad académica y en las relaciones entre profesorado y alumnado y entre el alumnado de un mismo grupo o titulación, se recomienda utilizar las herramientas institucionales de comunicación: el correo electrónico institucional y Prado.

Y por el contrario, se recomienda evitar el correo institucional para fines privados no académicos.

BIENESTAR DIGITAL

La desconexión

TENEMOS QUE FOMENTAR LAS RELACIONES SALUDABLES CON LA TECNOLOGÍA

Por ti mismo, en aras a tu salud emocional, que repercutirá entre otros aspectos en un mejor rendimiento académico.

Por el resto de personal de la Universidad. Evita enviar mensajes fuera del horario de trabajo respetando así el derecho a la desconexión digital.

¿QUIÉN ME PROTEGE?

EN CASO DE BRECHAS O FUGAS DE DATOS PERSONALES

En la UGR tenemos un protocolo para la comunicación de brechas o fuga de datos personales. Ante cualquier duda con tu dispositivo puedes preguntar al **Centro de Atención al Usuario de la Universidad** (958241000 ext.3), desde ahí te redirigirán donde corresponda. También puedes enviar un mensaje a **csirc@ugr.es**

Y, ante cualquier robo o pérdida de los dispositivos móviles debes poner denuncia ante la Policía Nacional.

Brigada Investigacion Tecnológica

SI SE PRODUCE UN CONFLICTO DE CONVIVENCIA POR UN USO INADECUADO DE LOS DISPOSITIVOS

Y este conflicto te afecta, puedes acudir a la Comisión de Convivencia creada por la Universidad de Granada, donde canalizarán tales conflictos.

Normativa de convivencia PDF

Si estamos ante un conflicto de convivencia derivado de infracciones al derecho a la protección de datos, lo resolverá el Delegado/a de Protección de Datos.

Si son trámites, quejas y denuncias sobre situaciones de acoso sexual, se canalizarán a través de la Unidad de Igualdad y Conciliación de la UGR.

SI QUIERES EJERCITAR TUS DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Puedes consultar este enlace.

Oficina de proteción de datos UGR

CRÉDITOS

CREACIÓN DE CONTENIDOS

Esta guía es el resultado del proyecto de innovación y buenas prácticas docentes de la Universidad de Granada "Buenas prácticas para un uso adecuado de los dispositivos móviles del alumnado en la UGR" (Código 22-61) formado por:

Carolina Serrano Falcón
Coordinadora del Proyecto. Departamento de Derecho del Trabajo y de la Seguridad Social. UGR.

Rosa Moya Amador
Departamento de Derecho del Trabajo y de la Seguridad Social.

María del Carmen García Garnica
Delegada de Protección de Datos de la UGR.
Departamento de Derecho Civil.

Antonio Muñoz Aropa
Jefe de servicio de Seguridad Informática del CSIRC.

Contenidos revisados y actualizados a 17/05/2023, fecha de finalización de esta guía.

DOCUMENTACIÓN

Esta guía ha sido elaborada siempre teniendo en cuenta la normativa existente, así como las recomendaciones que proporciona la OSI, la AEPD o el CCN.

Esta guía es una colaboración con la campaña de la UGR de concienciación sobre Protección de Datos Personales "Ojo al Dato". La **Universidad de Granada** está adherida al **Pacto Digital para la Protección de las Personas**, promovido por la Agencia Española de Protección de Datos (AEPD).

Esta guía ha sido financiada exclusivamente por el Programa de Innovación y Buenas Prácticas Docentes (PIBPD) de la Universidad de Granada en la Convocatoria 2022-2023.

UNIVERSIDAD DE GRANADA

ENTIDAD ADSCRITA
Pacto Digital para la Protección de las Personas

DISEÑO
Estudio Dixi Grafismo