

¿A QUIÉNES VA DIRIGIDO?

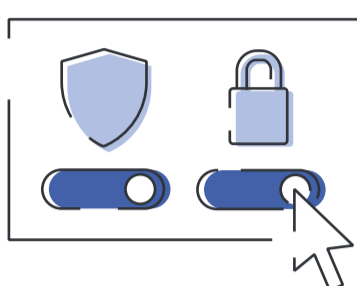
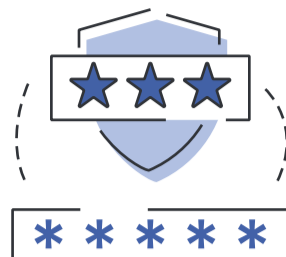
Va dirigido a profesionales de organizaciones, tanto públicas como privadas, que quieran mejorar su ciberseguridad en redes sociales a través de buenas prácticas.

BUENAS PRÁCTICAS DE CIBERSEGURIDAD EN LA ORGANIZACIÓN

Debido al incremento constante de los ataques informáticos que emplean las redes sociales como vehículo para su desarrollo o propagación, resulta fundamental estar protegido y contar con un entorno seguro al momento de utilizarlas:

Primer escudo protector, una contraseña fuerte

Se debe crear una contraseña única, robusta y difícil de adivinar para fortalecer la cuenta de redes sociales (se recomienda el uso de una combinación de letras mayúsculas y minúsculas, números y símbolos, etc.).

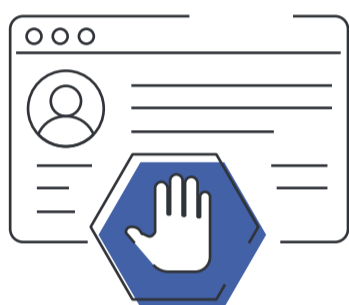


Utilizar las opciones de privacidad y seguridad para asegurar la protección

Verificar que el contenido en las redes sociales sea visible solo para amigos y familiares. No se deben compartir datos personales con desconocidos.

Mantener en la privacidad, la información privada

Es necesario configurar adecuadamente las opciones de privacidad de nuestros perfiles. De esta manera permitiremos el acceso a nuestros datos exclusivamente a las personas que definamos. En consecuencia, se reducirá el riesgo de que pudiera ser utilizada con fines malintencionados.



Cuanta menos información se exponga, mejor

El cronograma (panel, muro, etc.) puede ser un espejo / representación de la persona propietaria de esa cuenta. Por ello es importante controlar qué información se publica en él. Limitar lo que se comparte y a quién se le da acceso.

Acceso seguro

Comprobar que se está accediendo al sitio correcto y que la comunicación está protegida con HTTPS para garantizar que la comunicación está cifrada. No se debe acceder a las redes sociales desde equipos compartidos o públicos y redes Wifi no confiables. Si se accede a través de estos medios, se debe cerrar siempre la sesión al terminar y no permitir al navegador recordar la contraseña.

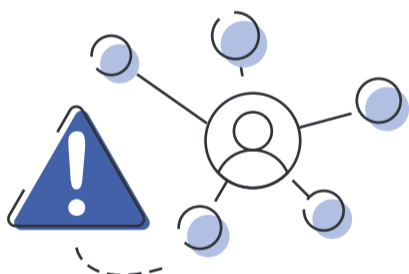


No guardar contraseñas

Si no respetamos esta recomendación, cualquier persona que acceda físicamente a nuestro dispositivo, podría entrar sin problemas a nuestras cuentas.

Cuidado con los enlaces

Se debe tener cuidado con los links que llegan incluso si éstos proceden de algún amigo o conocido. Es necesario fijarse bien en el enlace y si resulta desconocido y/o sospechoso, no se debe pinchar en él.



Cuidado con lo que se comparte

Una vez que se publica algo en redes sociales, se pierde el control sobre aquello que se ha publicado. Aunque después lo elimines, quedará, en la memoria del ciberespacio para siempre.

Sistema de seguridad

Se debe contar con programas y herramientas de seguridad instaladas en el equipo, como programas antimalware.

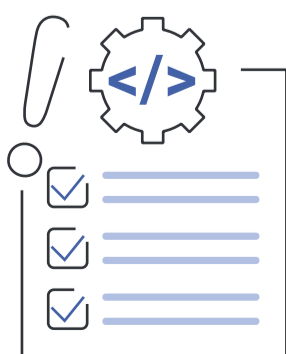


Cuidado con el GPS y la localización

Con la funcionalidad de GPS que ofrecen muchos dispositivos, cualquier contenido multimedia que se transmita puede contener información de ubicación. Los ciberdelincuentes pueden deducir a través de esta información nuestras rutinas diarias, lugares que frecuentamos y en general nuestros hábitos de vida.

Difusión

No hay que creer todo lo que se ve en las redes sociales y es necesario comprobar cualquier noticia antes de difundirla. Los ciberdelincuentes, empleando tácticas de ingeniería social, tratarán de engañar a los usuarios empleando escenarios falsos o simulados: anuncios en redes sociales que al pinchar en ellos conducen a la descarga de malware, avisos fraudulentos simulando ser de entidades bancarias que conducen a formularios diseñados para robar credenciales de tarjetas de crédito, trucos publicitarios para lograr suscribir fraudulentamente al usuario a servicios SMS de tarificación, etc.



Cuidado con los permisos de las aplicaciones

En las redes sociales existen multitud de juegos y aplicaciones. Para poder descargarlas, en ocasiones se nos requiere que aceptemos ciertas condiciones y permisos de acceso a nuestro perfil. En este punto, es necesario revisar cuidadosamente estos permisos que concedemos antes de aceptarlos.