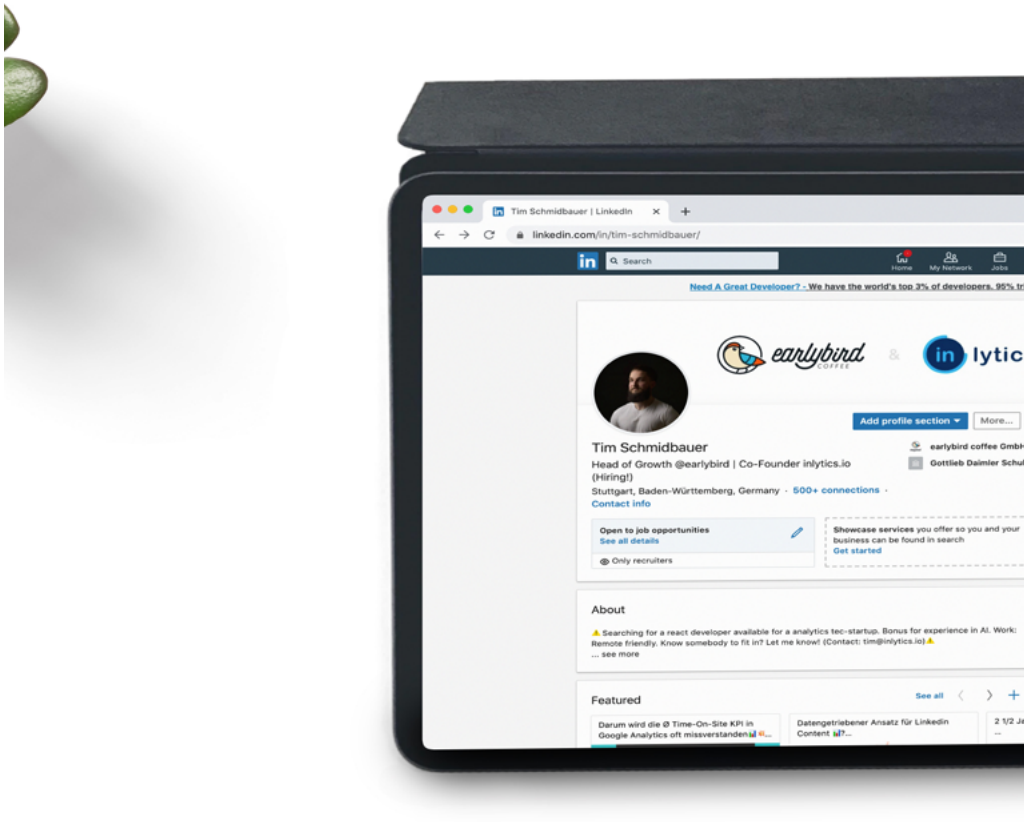
NOVIEMBRE 2020

# Buenas prácticas de seguridad en redes sociales

*Información proporcionada por el Servicio de Seguridad de la Información, D. G. de Telecomunicaciones y Transformación Digital (C. Fomento y Medio Ambiente)*

Seguridad de la Información de Castilla y León




**PRIVACIDAD: Cuida el ámbito del contenido compartido,** diferenciando compartición pública, privada o mensaje directo.

**CONTENIDOS SENSIBLES: Evita difundir información de la propia vida personal o del ámbito laboral, sin una necesidad real.** Esta información puede ser utilizada para la suplantación de tu identidad, no solo digital, o conductas ilícitas.

**SEPARACIÓN: Divide la información publicitada** y que pueda vincular el **puesto de la organización** con la **persona**. No compartas los datos de cuenta de trabajo, identificadores o accesos profesionales en entornos no laborales ni con tu cuenta personal.

**TERCEROS: No proporciones información privada sobre otros.** Esto incluye no etiquetar con su nombre a otras personas, y mencionarlas con precaución sobre todo si no tienen perfil en redes sociales.

**GEOLOCALIZACIÓN: Debes tenerla desactivada por defecto en los perfiles y publicaciones** y hacer un uso inteligente, sobre todo si es información en tiempo real.

**PREVENCIÓN: Ante elementos sospechosos.** Evita abrir contenidos con indicios sospechosos aunque vengan del perfil o mensaje de un conocido. Ten cuidado con aquellos enlaces acortados o de vídeos casualmente llamativos.

**RELACIONES VIRTUALES ACOTADAS:** Mantén en privado tu lista de contactos, y no aceptes cualquier solicitud de amistad, en especial si viene de desconocidos. No entres en discusiones, sobre todo siendo el administrador o moderador de una página o perfil laboral.

**ACTIVIDAD Y CONFIGURACIÓN REVISADA:** Comprueba regularmente ambas para verificar que no hay ninguna actuación sospechosa o modificación automática de valores.

Activa las alertas de inicio de sesión si están disponibles.

**CUENTAS: Diferenciadas**, con contraseñas robustas y doble factor de autenticación. No utilices el mismo identificador de cuentas, ni para diferentes ámbitos personal y laboral. Notifica las intrusiones.

**REPUTACIÓN:** Sé consciente, **la imagen digital es parte de la identidad de uno mismo o de tu organización,** hay que cuidar aquel contenido y perfil que se comparte, siempre mediante sentido común.

Si eres empleado público de la Junta de Castilla y León el uso de medios digitales deberá realizarse conforme a la **política de seguridad** de la ACCyL, así como la política de uso de los **servicios de comunicaciones e informática** para todo usuario de los mismos.

**Descubre más conceptos sobre buenas prácticas de seguridad en redes sociales**