DICIEMBRE 2020

# Buenas prácticas en prevención de suplantación de identidad

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

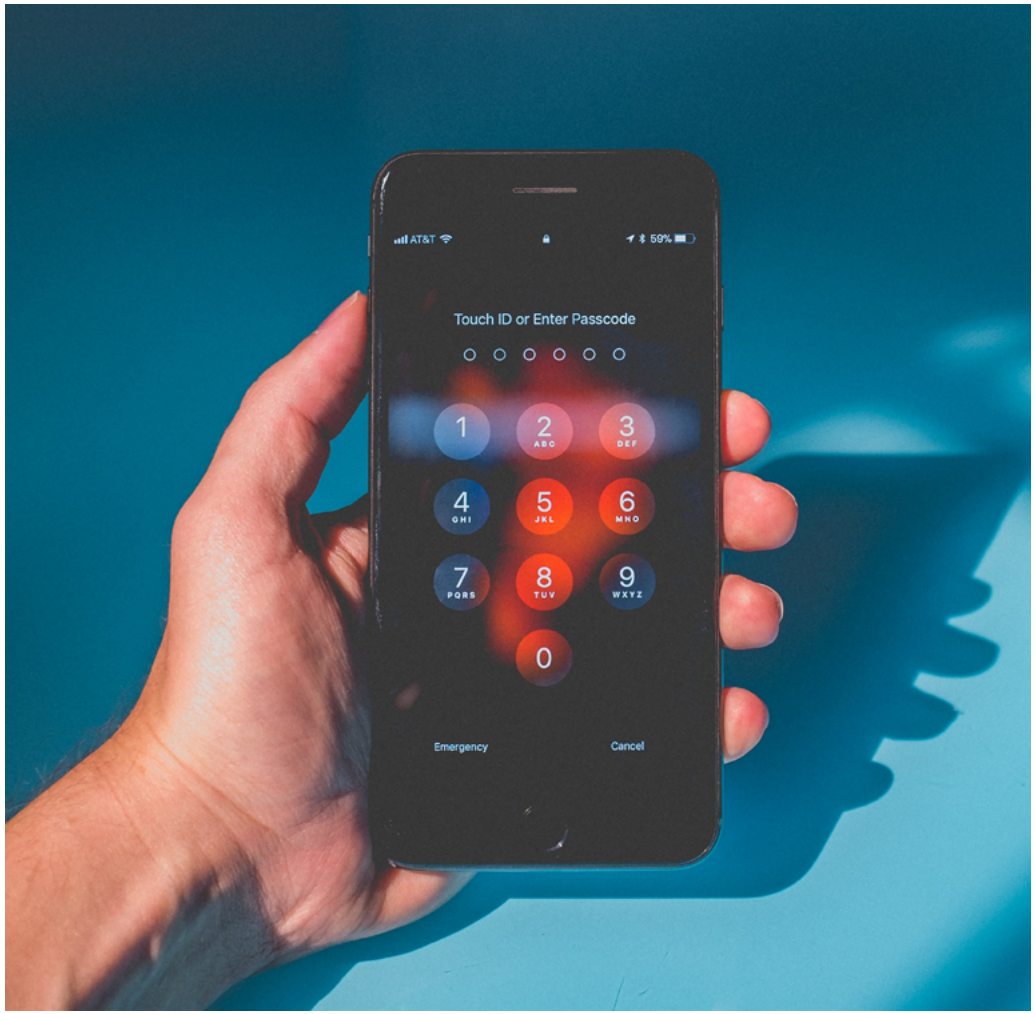
Seguridad de la Información de Castilla y León

**PREVENCIÓN:** utiliza la seguridad y la prevención por defecto, usando adecuadamente tus credenciales y contraseñas según la política de seguridad, y con varias capas de protección en aquellos sitios que lo habiliten.

**CUENTAS:** no intercambies ni prestes tu cuenta de acceso de la Administración de la Comunidad de Castilla y León (ACCyL). No compartas las claves de acceso a tu ordenador ni a las aplicaciones para tu trabajo. Cada usuario es responsable de las acciones que se realicen con la cuenta que se le haya proporcionado o sus aplicaciones.

**POLÍTICAS:** la ACCyL, al igual que las organizaciones con considerable tamaño y responsabilidad, tiene una política de seguridad de la información y otra de uso de servicios. Comprueba las políticas de la ACCyL así como las políticas de las empresas con las que te relaciones.

**REPUTACIÓN:** intercambia información solo con compañías y socios de reputación probada. Antes de proveer cualquier información, como el correo o la cuenta ACCyL, el teléfono, etc. asegúrate de estar comunicándote con la persona con la que debes hacerlo, sobre todo en comunicaciones digitales.



**DIFUSIÓN:** ten cuidado con la información que publicitas. No compartas tus datos de cuenta de trabajo en entornos públicos no laborales.

**REPETICIÓN:** no utilices el mismo usuario y clave en tus cuentas personales, como pueden ser redes sociales y otros sitios web. Esta información, la personal y la laboral, no debería ser la misma y será utilizada para distintos fines.

**ACTUALIZACIÓN:** mantén actualizado y comprueba la vigencia de tu antivirus corporativo y los productos de seguridad análogos que tengas en tu equipo.

**ACTIVIDAD:** comprueba tu actividad regularmente. Revisa regularmente tu correo electrónico así como tus unidades de red para asegurar que no hay ninguna actividad sospechosa.

**IDENTIFICACIÓN:** ante cualquier duda, verifica que el emisor que te envía una información, llamada o correo, es quien dice ser, contactando por otro medio de comunicación. Utiliza firma digital con certificado para asegurar tu identidad frente a otros destinatarios.

**INCIDENTES:** si detectas algún comportamiento sospechoso notifícalo a través de petición a tu CAU. Para aquellos incidentes que también conlleven una brecha de información y datos personales avisa al Responsable de Seguridad y al Delegado de Protección de Datos en tu organismo.

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 en prevención de suplantación de identidad**