AGOSTO 2020

Buenas prácticas en prevención de brechas o fugas de datos

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

Una brecha o fuga de datos se produce en un sistema, por la cual un atacante obtiene parte de la información que almacena el mismo. Los datos obtenidos pueden no estar disponibles públicamente en Internet de forma inmediata, pero se utilizarán en algún momento posterior, habitualmente para *spam*, *phishing* o suplantación de identidad.

Credencial corporativa: Como siempre, no utilices tu identificador ni tu usuario ACCyL en otro servicio o web no laboral.

Protección mejorada: Habilita la verificación en dos pasos o la doble autentificación (2FA), si utilizas una aplicación o servicio web que lo permita, como el correo web. Actualiza regularmente las preguntas de seguridad, en el caso de que las hubiera, con información difícilmente adivinable.

Contraseñas: No utilices las mismas contraseñas para distintos servicios, incluida la utilizada en ACCyL. En el caso haberlas reutilizado, es importante que no olvides modificarlas de forma única.

Información obsoleta: Como medida preventiva, elimina regularmente la información obsoleta, en particular ficheros o mensajes que no sea necesario conservar, incluyendo los que están en la papelera, la carpeta de eliminados, así como contactos obsoletos. No olvides la información impresa.

Almacenamiento: Comprueba tus unidades locales y de red en la ACCyL para asegurar igualmente que no guardas información obsoleta. Si es información clasificada, almacénala y transpórtala cifrada.

Compromiso de cuenta: Si detectas que tu cuenta puede estar comprometida, cambia inmediatamente tu contraseña y pon incidencia en tu Centro de Atención a Usuarios. Siempre sal de tus cuentas al acabar en trabajo no presencial.

Correo alternativo: Si has usado la dirección de correo ACCyL como dirección

alternativa de contacto o de recuperación de contraseña en otros servicios no laborales, deberás modificarla. Evita que sepan dónde trabajas.

Cuenta de correo: Si la cuenta comprometida es tu correo electrónico, verifica las bandejas de entrada, salida, no deseado, elementos eliminados y lista de contactos, para localizar qué información podría haber sido alterada y si ha habido una *exfiltración* no deseada. Notifica a tus contactos habituales.

Información clasificada: En el caso de haber detectado fuga de información clasificada a través de una cuenta comprometida, pon incidencia en tu CAU y no dudes en comunicarlo a tu responsable de seguridad, responsable de tratamiento/funcional de la aplicación, junto con el Delegado de Protección de Datos si contiene datos personales.

Monitorización: La ACCyL monitoriza listas públicas en Internet con direcciones de correo corporativas, para conocer aquellas publicadas y que por ello pueden tener más afectación posterior, mediante *spam* o *phishing*. Cambia la contraseña de tu cuenta si te llega una notificación corporativa indicando la aparición de tu dirección de correo en una de estas listas.

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 brechas o fugas de datos.