Conselleria de Famílies, Benestar
Social i Atenció a la Dependència
Direcció General d'Atenció a la Dependència
i Persones amb Discapacitat

COMUNICACIÓN A LAS PERSONAS AFECTADAS POR LA VIOLACIÓN DE LA SEGURIDAD DE DATOS PERSONALES DEL SERVICIO RESIDENCIAL PARA PERSONAS EN SITUACIÓN DE DEPENDENCIA GESTIONADO A TRAVÉS DE LA ENTIDAD DOMUS Vi

A través de esta comunicación le informamos que, como consecuencia del acceso no autorizado de un tercero a los servidores de DOMUSVi que presta el servicio residencial y estancias diurnas dirigido a personas en situación de dependencia algunos de sus datos personales pueden formar parte de un listado de datos obtenido de forma ilícita.

1. Datos de contacto del Delegado de Protección de Datos de la Administración de la CAIB:

protecciodades@dpd.caib.es

2. Punto de contacto en el que se puede obtener más información:

a) Responsable del tratamiento, directora general de Atención a la Dependencia y Personas con Discapacidad

Datos de contacto: responsabledades@dgad.caib.es

b) Encargado del tratamiento: Servisar Servicios Sociales SLU (DOMUS VI):

Teléfon de contacto: **900 45 65 85.**
Delegado de Protección de Datos (DPD): dpo@domusvi.es

3. Descripción general del incidente y momento en que se ha producido:

Com a consecuencia del acceso no autorizado a datos personales de usuarios del servicio residencial dirigido a personas en situación de dependencia por parte de terceras personas, el pasado 11 de noviembre de 2026 se produjo un incidente de segureidad en los servidores DOMUSVi que comprometió la confidencialidad de los datos personales de los afectados.

4. Posibles consecuencias de la brecha de datos personales:

Las posibles consecuencias de esta brecha de seguridad pueden ser, entre otras:

a) Suplantación de la identidad
b) Fraude

c) Pérdida de privacidad y confidencialidad
d) Daños en la reputación de los afectados
e) Limitación de sus derechos

5. Descripción de los datos e información personal afectada:

Los datos personales a los que se ha tenido acceso no autorizado o ilícito son los siguientes:

a) Nombre y apellidos
b) Sexo
c) Documento nacional de identidad
d) Fecha de nacimiento
e) País y municipio de nacimiento y nacionalidad
f) Teléfono
g) Dirección domicilio
h) Dirección de correo electrónico

6. Resumen de las medidas implantadas hasta ahora para controlar los posibles daños:

a) Bloquear automáticamente el ordenador al que se accedido a la base de datos exfiltrada
b) Cambio y refuerzo de todas las contraseñas de acceso a los datos.
c) bloqueo de todos los usuarios relacionados con el actor sospechoso.

7. Otras informaciones útiles a los afectados para que pueda proteger sus datos o prevenir posibles daños:

a) Prestar especial atención a posibles correos electrónicos, mensajes SMS, comunicaciones a través de aplicaciones de mensajería instantánea o llamadas telefónicas inesperadas (Vishing) en las que alguien se haga pasar por DOMUSVi, entidad que gestiona un servicio residencial , o por la Dirección General de Atención a la Dependencia y Personas con Discapacidad, a fin de obtener información.a) Prestar especial atención a posibles correos electrónicos, mensajes SMS, comunicaciones a través de aplicaciones de mensajería instantánea o llamadas telefónicas inesperadas (Vishing) en las que alguien se haga pasar por DOMUSVi, entidad que gestiona un servicio residencial , o por la Dirección General de Atención a la Dependencia y Personas con Discapacidad, a fin de obtener información.

b) Desconfíe de cualquier comunicación en la que se soliciten contraseñas, códigos de acceso, datos bancarios, documentación personal, información sanitaria o la realización de pagos. No facilite este tipo de información mediante canales no verificados.

c) No abra enlaces ni archivos adjuntos sospechosos y compruebe la autenticidad de cualquier comunicación contactando directamente con DOMUSVi o con la Dirección General de Atención a la dependencia y Personas con Discapacidad a través de sus canales oficiales, sin utilizar los datos de contacto incluidos en el mensaje recibido.

d) No facilite información personal, bancaria o sanitaria a personas cuya identidad y legitimidad no haya podido verificar, especialmente si solicitan información adicional sobre los servicios residenciales que recibe o sobre sus circunstancias personales.

e) Revise periódicamente los movimientos de sus cuentas bancarias y tarjetas de crédito o débito para detectar posibles operaciones no autorizadas. Si observa algún movimiento sospechoso, contacte inmediatamente con su entidad bancaria para comunicarlo y solicitar las medidas de protección oportunas.

f) Extreme las precauciones ante posibles intentos de suplantación de identidad y ante cualquier comunicación que utilice información personal o sanitaria para aparentar legitimidad o generar confianza.

g) Si tiene conocimiento de que sus contraseñas o credenciales de acceso pudieran haberse visto comprometidas, cámbialas inmediatamente y, si utiliza las mismas credenciales en otros servicios, proceda también a modificarlas.

h) Conserve cualquier comunicación sospechosa que pueda recibir y, en caso de detectar un posible uso fraudulento de sus datos personales o bancarios, comuníqueselo a las autoridades competentes ya la Dirección General de Atención a la Dependencia y Personas con Discapacidad a través de sus canales oficiales.

Atentamente,
Palma, en la fecha de la firma electrónica
La directora general de Atención a la Dependencia y Personas con Discapacidad
Maria Castro Amor