MEXICAN WEBSITE NOTICE

17 de noviembre de 2026

AVISO DE VULNERACIÓN DE SEGURIDAD

¿QUÉ SUCEDIO?

El 25 de julio de 2026, WireCo World Group Inc. y sus subsidiarias («WireCo», «nosotros» o «nos») detectaron actividad no autorizada en sus sistemas internos de TI, que posteriormente descubrieron que se trataba de un ciberataque perpetrado por un actor de amenazas conocido y sofisticado. Al descubrir el incidente, aislamos los sistemas afectados y contratamos a expertos en ciberseguridad, por instrucciones de nuestros asesores legales, para realizar una revisión integral de nuestra red interna y ayudar con la investigación, contención y remediación. Es posible que la actividad no autorizada haya ocurrido entre el 9 de julio de 2026 y el 25 de julio de 2026. Después de asegurar nuestros sistemas internos de TI, determinamos que el actor de amenazas había accedido a determinada información que contenía datos personales de empleados de WireCo y los había exfiltrado. Desde que descubrimos el ataque, hemos estado trabajando de forma continua para revisar la información afectada e identificar los datos personales. Este proceso ha llevado tiempo.

¿QUÉ DATOS PERSONALES PUDIERAN ESTAR INVOLUCRADOS?

El incidente afectó datos personales en poder de WireCo, que pueden incluir:

- Nombres completos y datos de contacto (domicilios particulares, números telefónicos y direcciones de correo electrónico)
- Números de identificación nacional y números de Seguridad Social
- Copias de pasaportes o de documentos de identificación emitidos por autoridades
- Fecha de nacimiento
- Información sobre cuentas bancarias y tarjetas de crédito

Además, si era usted empleado o trabajaba para WireCo, los datos personales también pueden incluir:

- Expedientes laborales, incluyendo evaluaciones de desempeño, expedientes disciplinarios e información relativa a la afiliación sindical y antecedentes penales
- Datos de ausencias y relacionados con la salud (como registros de enfermedad e información de salud ocupacional)
- Datos de familiares cercanos y de contactos de emergencia

¿CUÁLES SON LAS POSIBLES CONSECUENCIAS?

Dada la naturaleza de los datos involucrados, existe el riesgo de que usted pueda ser objeto de:

- Fraude o Robo de identidad
- Intentos de phishing (correos electrónicos o mensajes fraudulentos diseñados para obtener datos personales adicionales)

- Fraude financiero, particularmente cuando se haga un uso indebido de datos bancarios o de números de Seguridad Social
- Contactos no deseados o intentos de ingeniería social

Queremos ser transparentes con usted respecto de estos riesgos para que pueda tomar las medidas adecuadas para protegerse.

MEDIDAS QUÉ ESTAMOS TOMANDO

Antes del incidente, manteníamos un programa de ciberseguridad de múltiples capas que incluía medidas de seguridad administrativas, técnicas y organizativas diseñadas para reducir la probabilidad y el impacto de las amenazas cibernéticas, así como para proteger la confidencialidad, integridad y disponibilidad de nuestros sistemas de información y datos.

Desde el 25 de julio de 2026, hemos tomado las siguientes medidas para fortalecer aún más nuestro programa de ciberseguridad y responder al incidente:

- Aislamos y aseguramos los sistemas afectados para evitar nuevos accesos no autorizados
- Contratamos especialistas líderes en ciberseguridad para realizar una investigación forense
- Notificamos a las autoridades nacionales y locales de protección de datos
- Restauramos los sistemas cifrados a partir de copias de seguridad
- Implementamos controles de seguridad reforzados, incluidos el monitoreo adicional y las restricciones de acceso a nuestros sistemas de TI
- Iniciamos una revisión exhaustiva de nuestras medidas de seguridad de la información para evitar que vuelva a ocurrir un incidente similar

Asimismo, contratamos a un tercero para realizar un monitoreo de la dark web a fin de determinar si se ha puesto a disposición en la dark web información proveniente de nuestros sistemas. A pesar de que el actor de amenazas publicó un enlace, hasta la fecha, no hay indicios de que los datos se hayan vendido u ofrecido para su venta, ni pruebas de que se haya hecho un uso indebido de dichos datos.

WireCo ha notificado el incidente a sus empleados actuales. Sin embargo, no disponemos de los datos de contacto de un pequeño número de antiguos empleados, clientes, proveedores y visitantes externos. Por lo tanto, WireCo publica este aviso con el fin de informar a aquellas personas con las que no puede ponerse en contacto directamente.

LO QUÉ USTED PUEDE HACER

Aunque no tenemos conocimiento de algún fraude consumado o intento de fraude derivado del uso indebido de datos personales, ni de algún perjuicio económico sufrido por las personas involucradas como resultado de este incidente, le recomendamos que adopte las siguientes medidas de precaución:

- **Monitore sus cuentas bancarias y reportes de crédito** - esté atento a cualquier transacción inusual o no autorizada y repórtela de inmediato a su banco.

- **Manténgase alerta ante el phishing** - tenga cuidado con correos electrónicos, mensajes de texto o llamadas telefónicas no solicitados en los que se le soliciten datos personales, incluso si parecen provenir de una fuente confiable.
- **Cambie sus contraseñas** - actualice las contraseñas de sus cuentas personales, particularmente si ha reutilizado contraseñas similares a las utilizadas para los sistemas de trabajo.

Como siempre, le recomendamos que se mantenga alerta ante incidentes de fraude y robo de identidad, revise sus estados de cuenta y supervise sus reportes de crédito gratuitos para detectar actividades sospechosas y errores.

SUS DERECHOS

Las leyes de protección de datos otorgan ciertos derechos respecto del uso de datos personales. Los derechos potencialmente aplicables varían según la jurisdicción y pueden incluir el derecho de acceso a sus datos, el derecho de rectificación y, en ciertas circunstancias, el derecho de cancelación (supresión). Si desea ejercer cualquiera de estos derechos, presente una solicitud por escrito utilizando la información de contacto que se proporciona al final del documento.

PARA OBTENER MÁS INFORMACIÓN

Sabemos que usted confía en nosotros para proteger información importante y queremos que sepa que tomamos muy en serio este incidente, y la seguridad y protección de sus datos personales. Lamentamos sinceramente que se haya producido este incidente. Si tiene alguna pregunta o duda, póngase en contacto con Daniel Burch en el correo DanBurch@WireCo.com.

Información del responsable

PAIS	RESPONSABLE
Dinamarca	**Euronete Scandinavia A/S** **Domicilio:** Gothersgade 48, 7000 Fredericia, Dinamarca
Francia	**Le Drezen SAS** **Domicilio:** 12 rue de Kelareun, 29730 Guilvinec-Treffiagat, Francia
Alemania	**WireCo Germany GmbH** **Domicilio:** Casarstraße 1, 66459 Kirkel-Limbach, Alemania
Países Bajos	**Lankhorst Engineered Products B.V** **Domicilio:** Prinsengracht 2, 8607AD, Sneek, Países Bajos **Ekon B.V.** **Domicilio:** Holtum-Noordweg 8, 6121 RE Born, Países Bajos **Lankhorst Touwfabrieken B.V.** **Adress:** Marconiweg 24, 3316 AM Dordrecht, Países Bajos **Royal Lankhorst-Euronete group B.V.** **Domicilio:** Prinsengracht 2, 8607AD, Sneek, Países Bajos
Polonia	**WireCo Poland sp. z o.o** **Domicilio:** Polna 26/74, 87-806 Włocławek, Polonia
Portugal	**Oliveira Sá, S.A.** **Domicilio:** Rua Do Outeiro, 906, 4475-150, Maia, Portugal **Lankhorst Euronete Portugal, S.A.** **Domicilio:** Rua da Cerfil , (Cap.Gramaxo) nº45, 4475-468, Maia, Portugal
Reino Unido	**Euronete (UK) Limited** **Domicilio:** Enerfield Business Park, Foveran, Ellon, Newburgh Aberdeenshire, AB41 6AL, UK
Brasil	**WireCo do Brasil Ltda** **Domicilio:** Rua Minas Gerais 1920, Distrito Industrial Queimados, Rio de Janeiro, Brasil

	Lankhorst-Euronete (Brasil) –Indústria e Comércio Ltda **Domicilio:** Rua Minas Gerais 1920, Distrito Industrial Queimados, Rio de Janeiro, Brasil
México	**Aceros Camesa S.A. de C.V.** **Addres:** Margarita Maza de Juarez 159, Nueva Industrial Vallejo, Gustavo A. Madero, Ciudad de México 07700
Australia	**WireCo Australia Pty Ltd** **Domicilio:** 7 Demand Avenue, Arundel QLD 4214, Australia