BRAZILIAN WEBSITE NOTICE

17 de novembro de 2026

COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

O QUE ACONTECEU?

Em 25 de julho de 2026, a WireCo World Group Inc. e suas subsidiárias ("WireCo", "nós" ou "nosso(a)(s)") identificou atividade não autorizada em seus sistemas internos de TI, que posteriormente identificamos como um ataque cibernético realizado por um autor de incidente conhecido e sofisticado. Ao identificar o incidente, nós isolamos os sistemas afetados e contratamos especialistas externos em cibersegurança, sob orientação de assessoria jurídica, para realizar uma análise abrangente de nossa rede interna e auxiliar na investigação, contenção e remediação. A atividade não autorizada parece ter ocorrido entre 9 de julho de 2026 e 25 de julho de 2026.

Após protegermos nossos sistemas internos de TI, determinamos posteriormente que o autor do incidente acessou e exfiltrou determinados dados contendo dados pessoais. Desde que identificamos o ataque, temos trabalhado continuamente na análise dos dados afetados para identificar os dados pessoais envolvidos, processo que demandou tempo para ser concluído.

QUAIS DADOS PESSOAIS FORAM ENVOLVIDOS?

O incidente envolveu dados pessoais tratados pela WireCo, que podem incluir:

- Nomes completos e informações de contato (endereços residenciais, números de telefone e endereços de e-mail)
- Números de identificação nacional, de seguro nacional ou de seguridade social
- Cópias de passaportes ou de documentos de identificação emitidos por órgãos governamentais
- Data de nascimento
- Informações bancárias e de cartão de crédito

Caso você seja ou tenha sido empregado ou tenha trabalhado para a WireCo, os dados pessoais também podem incluir:

- Registros relacionados ao vínculo de trabalho, incluindo avaliações de desempenho, registros disciplinares e informações relacionadas à filiação sindical e ao histórico de infrações penais
- Dados relacionados a ausências e à saúde (como atestados e registros de afastamentos por motivo de saúde e informações de saúde ocupacional)
- Dados de contato de familiares próximos e de contatos de emergência

QUAIS SÃO AS POSSÍVEIS CONSEQUÊNCIAS?

Considerando a natureza dos dados envolvidos, existe o risco de você estar sujeito(a) a:

- Furto de identidade ou fraude de identidade
- Tentativas de phishing (e-mails ou mensagens fraudulentas destinados a obter dados pessoais adicionais)

- Fraude financeira, especialmente em caso de uso indevido de dados bancários ou números de identificação previdenciária ou de seguridade social
- Contato indesejado ou tentativas de engenharia social

Queremos ser transparentes com você sobre esses riscos para que possa adotar as medidas adequadas para se proteger.

O QUE ESTAMOS FAZENDO

Antes do incidente, mantínhamos um programa de cibersegurança em múltiplas camadas, composto por medidas administrativas, técnicas e organizacionais de segurança destinadas a reduzir a probabilidade e o impacto de ameaças cibernéticas e a proteger a confidencialidade, a integridade e a disponibilidade de nossos sistemas de informação e dados.

Desde 25 de julho de 2026, adotamos diversas medidas para reforçar ainda mais nosso programa de cibersegurança e responder ao incidente:

- Isolamos e protegemos os sistemas afetados para impedir novos acessos não autorizados
- Contratamos especialistas de referência em cibersegurança para conduzir uma investigação forense
- Notificamos as autoridades nacionais e locais de proteção de dados
- Restauramos os sistemas criptografados a partir de backups seguros
- Implementamos controles de segurança reforçados, incluindo monitoramento adicional e restrições de acesso aos nossos sistemas de TI
- Iniciamos uma revisão abrangente de nossas medidas de segurança da informação para evitar a recorrência

Também contratamos um terceiro para realizar o monitoramento da dark web, a fim de determinar se dados de nossos sistemas foram disponibilizados na dark web. Embora um link para os arquivos afetados tenha sido publicado pelo autor do incidente, até o momento, não temos conhecimento de qualquer indício de que dados pessoais tenham sido vendidos ou oferecidos para venda, tampouco de evidências de qualquer uso indevido adicional desses dados.

O QUE VOCÊ PODE FAZER

Embora não tenhamos conhecimento de qualquer fraude efetiva ou tentativa de fraude decorrente do uso indevido de dados pessoais, nem de qualquer prejuízo financeiro sofrido pelos indivíduos envolvidos em decorrência deste incidente, recomendamos que você adote as seguintes medidas de precaução:

- **Monitore suas contas bancárias e seus relatórios de crédito** — fique atento(a) a quaisquer transações incomuns ou não autorizadas e comunique-as imediatamente ao seu banco.
- **Esteja atento(a) a tentativas de phishing** — tenha cuidado com e-mails, mensagens de texto ou chamadas telefônicas inesperados que solicitem dados pessoais, mesmo que pareçam vir de uma fonte confiável.
- **Altere suas senhas** — atualize as senhas de suas contas pessoais, especialmente caso tenha reutilizado senhas semelhantes às utilizadas nos sistemas de trabalho.

Como sempre, recomendamos que você permaneça atento(a) a ocorrências de furto de identidade e fraude, revise seus extratos e monitore seus relatórios de crédito gratuitos em busca de atividades suspeitas e para identificar erros.

SEUS DIREITOS

As leis de proteção de dados conferem determinados direitos em relação ao uso de dados pessoais. Os direitos potencialmente aplicáveis variam conforme a jurisdição e podem incluir o direito de acesso aos seus dados, o direito de retificação e, em determinadas circunstâncias, o direito de eliminação. Caso queira exercer qualquer desses direitos, envie uma solicitação por escrito utilizando as informações de contato abaixo.

PARA MAIS INFORMAÇÕES

Sabemos que você confia à WireCo informações importantes e queremos que saiba que levamos este incidente a sério, bem como a segurança e a proteção de seus dados pessoais. Lamentamos sinceramente que este incidente tenha ocorrido. Caso tenha qualquer dúvida ou preocupação, entre em contato com Daniel Burch pelo e-mail DanBurch@WireCo.com.

Informações sobre os Controladores

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

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