La importancia de un canal de comunicación empresarial seguro en el contexto de las directivas NIS2, DORA y CER

VERSION: 8/2023

Hoy, la interconexión a través de las redes digitales forma parte íntegra de nuestra vida privada y laboral. Desafortunadamente, esto también implica estar expuesto a las amenazas cibernéticas. En 2023, el riesgo de ciberataques que pueden interrumpir el negocio e infligir graves daños a las empresas sigue creciendo: el 86% de las compañías ya sufrieron algún ataque y, por término medio, se estima que se produce un ataque de *ransomware*[1] cada once segundos. Para muchas organizaciones, públicas o privadas, defenderse contra intrusiones digitales no deseadas se ha convertido en rutina diaria; la denegación de servicio distribuida (DDoS), el *phishing,* los ataques de contraseñas o el *ransomware* forman parte de las amenazas habituales más graves[2].

Tres directivas para fomentar la resiliencia

Las nuevas directivas europeas DORA, NIS2 y CER tienen por objeto reducir las vulnerabilidades frente a ciberataques en las instituciones y organizaciones y reforzar la resiliencia física de infraestructuras críticas en la Unión Europea. Puestas en marcha el 27 de diciembre de 2022, responden a una necesidad urgente: para el buen funcionamiento de la economía de la Unión Europea, es imprescindible disponer de mecanismos y protocolos implantados en los sectores esenciales; estas normativas obligan a fomentar la resiliencia de las empresas y organismos ante amenazas externas y la Agencia de la Unión Europea para la Ciberseguridad (ENISA) se erige como órgano responsable de su difusión en la UE.

El alcance de las directivas es amplio e impone cambios profundos en las organizaciones públicas y privadas: por un lado, las nuevas normativas obligan a que la ciberseguridad deje de ser competencia exclusiva de los departamentos de TI de las empresas y la convierte en un asunto estratégico. En este sentido, los órganos de dirección tienen ahora la obligación de adoptar medidas técnicas y operativas para gestionar los riesgos de ciberseguridad de forma proactiva. Por otro lado, las empresas tienen que hacer un seguimiento periódico de los sistemas implantados e identificar áreas vulnerables; además deben reportar posibles incidentes (ciberataques) a las autoridades pertinentes.

NIS2: la directiva sobre ciberseguridad y la seguridad de la información

La directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, conocida como NIS2, regula la ciberseguridad y la seguridad de la información de empresas y gobiernos en la Unión Europea. Pretende armonizar los requisitos de la seguridad cibernética entre los distintos Estados miembros de la UE, planteando obligaciones a todas las entidades medianas y grandes con más de 250 empleados y/o más de 50 millones de facturación. Aunque la normativa distingue entre «sectores esenciales[3]» y «sectores importantes[4]», se podría decir que es **aplicable a toda organización que cumpla con los criterios mencionados;** esto

1 Una forma de malware diseñado para cifrar archivos en un dispositivo.
2 Fuente: https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2023-press.html
3 Sectores esenciales: transporte, finanzas, salud, alimentación, logística, infraestructura digital, administración pública y astronáutica.
4 Sectores importantes: química, tratamiento de desechos, servicios correos, comida, empresas manufactureras y proveedores digitales.

incluye las Administraciones Públicas y las empresas no establecidas en la UE, pero que ofrecen sus servicios en su territorio. Las empresas que incumplan con NIS2 se arriesgan a sanciones económicas basadas en su facturación global.

De aquí al 17 de octubre del 2024, todas estas instituciones necesitan analizar los riesgos de seguridad de sus sistemas informáticos, establecer medidas de gobernanza y mecanismos de notificación a las autoridades pertinentes en los tiempos prescritos (24 horas desde la detección de un ciberataque). Las empresas tienen que asegurarse de la formación, tanto de los trabajadores como de los ejecutivos. Cabe destacar que son los directivos de las empresas *(C-suite)* los que firman como responsables de la implementación y del cumplimiento de la directiva NIS2.

Para cumplir con los principales requisitos NIS2, las empresas tienen que garantizar:

- La continuidad de las actividades en caso de incidentes, catástrofe o crisis
- La seguridad de la cadena de suministro
- La seguridad en la adquisición, el desarrollo y el mantenimiento de redes y sistemas de información
- Políticas y procedimientos para evaluar la eficacia de las medidas de gestión de riesgos en materia de ciberseguridad
- Prácticas básicas de «ciber-higiene» y formación en ciberseguridad
- Políticas y procedimientos relativos al uso del cifrado en comunicación
- La seguridad de los recursos humanos y las políticas de control de acceso
- El uso de soluciones seguras de autenticación, comunicaciones de voz, vídeo y texto
- Sistemas de comunicación de emergencia seguros

DORA: la directiva sobre la resiliencia operativa digital

El propósito del reglamento 2022/2554 del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero, popularmente conocido como DORA *(Digital Operational Resilience Act),* es mejorar la resiliencia y capacidad de respuesta de las **entidades financieras**[5] frente a los ciberataques. La normativa busca fomentar el desarrollo tecnológico, garantizar la estabilidad financiera y la protección de los consumidores.

Como uno de los pilares imprescindibles para el ahorro y la inversión que facilita el desarrollo económico de toda la Unión Europea, el sistema financiero está cada vez más interconectado y es muy dependiente de las tecnologías de la información. En este sentido, es crucial que se arme contra posibles ciberataques, no sólo desde una perspectiva tecnológica y/o informática, pero también en materia de gobernanza. Además de imponer medidas y protocolos de prevención contra posibles incidentes,

5 Entidades financieras: seguros y reaseguros, entidades de crédito (bancos), entidades de pago, entidades de dinero electrónico, proveedores de servicios de información sobre cuentas, agencias de calificación crediticia, empresas de inversión, depositarios centrales de valores, proveedores de servicios de criptomonedas, centros de negociación y servicios de suministro de datos, proveedores de servicios de TIC a terceros.

la normativa busca preparar el sector financiero para que sea capaz de mantener la continuidad de sus operaciones y servicios digitales durante fallos técnicos y ataques informáticos.

DORA establece la necesidad de disponer de un sistema de notificación, tanto para las entidades financieras —que deberán informar de incidentes graves—, como para los usuarios y clientes, para que puedan proteger sus intereses financieros de cara a posibles brechas y/o interrupciones de servicios. En este sentido, se establecerá una plataforma europea para la notificación a las autoridades pertinentes. La normativa, de una importancia estratégica vital para la ciberseguridad de las entidades financieras de la UE, entrará en vigor en enero del 2025. El sector financiero estará bajo la supervisión de las Autoridades Europeas de Supervisión (AES), un comité compuesto por la Autoridad Bancaria Europea (ABE), la Autoridad Europea de Valores y Mercados (AEVM) y la Autoridad Europea de Seguros y Pensiones de Jubilación (AESPJ). Las instituciones que forman el AES tendrán potestad para enviar recomendaciones, realizar inspecciones, (tanto presenciales como virtuales) e imponer sanciones.

Cabe destacar que, aparte de los sectores clásicos que forman la industria financiera (bancos, seguros, etc.), DORA también afectará a los proveedores de servicios digitales que ofrecen servicios relevantes para la prestación de servicios financieros. Aquí se incluyen empresas de tecnología de la información (TIC), proveedores de servicios en la nube, proveedores de servicios de pagos electrónicos y otras empresas que proporcionen servicios digitales con aplicaciones financieras. Para cumplir con DORA, las empresas han de implementar una serie de medidas en función de su tamaño, facturación y actividad.

Principales requisitos para cumplir con DORA:

- Crear un marco de gestión de riesgos (procedimientos internos, evaluación de riesgos, protocolos de actuación y monitorización de colaboradores y proveedores) y hacer un seguimiento periódico para asegurar garantizar el cumplimiento normativo.
- Crear canales seguros de comunicación para la notificación de incidentes. Implementar medidas de seguridad y continuidad de la actividad de la empresa.
- Fomentar una «cultura de ciberseguridad» integral dirigida a todos los empleados con el fin de transformar la empresa para que sea resiliente frente a ciberataques a largo plazo.
- Realizar pruebas periódicas de la resiliencia de los sistemas y realizar tests de los protocolos para comprobar que son suficientemente robustos *(Business Impact Analysis)*. Periódicamente, la empresa ha de publicar un informe que demuestre la implementación de las medidas técnicas pertinentes y/o que exponga posibles deficiencias y áreas de mejora.

CER: la directiva sobre la resiliencia de las entidades críticas

La Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo sobre la resiliencia de las entidades críticas, conocida como directiva CER *(Critical Entities Resilience),* tiene por objeto reducir las vulnerabilidades frente a ciberataques y reforzar la resiliencia física de las entidades críticas, es decir, aquellas que prestan servicios vitales para los ciudadanos de la UE y que son imprescindibles para el buen funcionamiento del mercado interior.

Los Estados miembros disponen hasta el 17 de octubre de 2024 para transponer la directiva a su legislación nacional. Asimismo, tendrán que adoptar una estrategia nacional y llevar a cabo evaluaciones de riesgo periódicas para identificar las entidades consideradas críticas para la sociedad y la economía (antes del 17 de enero de 2026). Más concretamente, la directiva identifica como «entidades críticas[6] de especial importancia europea» aquellas que presten algún tipo de servicio esencial a seis o más estados miembros.

En el caso de que alguna de esas entidades críticas sufriera cualquier tipo de problema que paralice su funcionamiento, tendrá que notificar este hecho: el enfoque de la directiva CER se centra en el apoyo concertado de los Estados miembros a estas entidades. Habrá una mayor cooperación transfronteriza con el objetivo de mejorar su resiliencia. Se trata de establecer una defensa frente a ataques y catástrofes naturales y de mantener intactos los servicios de esas entidades críticas para los ciudadanos de la Unión Europea.

Las entidades críticas deben reforzar su capacidad de prevenir, proteger, responder, resistir, mitigar, absorber, acomodar y recuperarse de incidentes que puedan interrumpir la prestación de servicios esenciales. El abanico de posibles causas incluye ciberataques, pero también pone el foco en las posibles amenazas climáticas, debido al aumento del riesgo de catástrofes naturales que puedan hacer tambalear a dichas entidades críticas.

Requisitos para cumplir con CER:

- Evaluaciones periódicas de riesgos. La primera evaluación deberá ser a los 9 meses de ser determinada como entidad crítica, y de ahí en adelante, cada cuatro años.
- El establecimiento de medidas técnicas, de seguridad y organizativas adecuadas y proporcionadas para garantizar la resiliencia de la entidad, así como el mantenimiento de los servicios esenciales en momentos críticos.
- Notificación inmediata de los incidentes que perturben o puedan perturbar de forma significativa la prestación de los servicios esenciales con la mayor brevedad posible.

6 La directiva se dirige principalmente a los sectores siguientes: energía, transportes, infraestructuras de los mercados financieros, salud, agua potable, aguas residuales, infraestructuras digitales, administración pública, espacio y la alimentación. No incluye a las entidades financieras que ya están reguladas por DORA.

Directivas de largo alcance bien acogidas

El nuevo marco legislativo ayudará a las organizaciones a equilibrar las ventajas de la nueva tecnología con los riesgos cibernéticos que conllevan; y parece que las empresas lo reciben de buen grado: el World Economic Forum (WEF) señala que, a nivel global, el 76% de los dirigentes (y el 70% de los líderes del sector TI) opinan que un marco legislativo más exigente contribuirá positivamente a reforzar la ciber-resiliencia de sus empresas[7].

El alcance de las nuevas directivas es amplio e incluye organizaciones no reguladas anteriormente; por ello, el primer paso lógico para las empresas es comprobar si forman parte de esas entidades sujetas a control. A continuación, deben determinar y aplicar las medidas necesarias para cumplir con las obligaciones correspondientes. Aparte de una planificación detallada, el proceso exige invertir en formación y tecnología: incorporar soluciones anti-*ransomware,* fomentar la «ciber-sensibilización» de los empleados, implantar canales de comunicación seguros y establecer un estricto control de los privilegios de acceso. Estas serían algunas de las medidas indispensables para mantener a raya a los agresores potenciales.

Por otra parte, las empresas tienen que examinar los sistemas y prácticas existentes: ¿qué medidas de seguridad se aplican para el trabajo remoto? o ¿son realmente seguros los canales de comunicación existentes? Lo cierto es que algunos sistemas son más vulnerables que otros: hay que tener en cuenta que las herramientas de uso generalizado tienden a atraer la atención de ciberdelincuentes debido a su popularidad; contrastan con soluciones para grupos cerrados de usuarios que suelen proporcionar mayor protección por diseño.

7 Fuente: https://www.weforum.org/agenda/2023/01/cybersecurity-storm-2023-experts-davos23/

Flancos digitales vulnerables en las empresas: dos ejemplos

Con más de 270 millones de usuarios en todo el mundo, Microsoft Teams es una de las herramientas de colaboración más populares; las comunicaciones por este canal no están encriptadas y lamentablemente, su popularidad la convierte también en uno de los objetivos preferidos de los *hackers,* que consiguen «colar» archivos maliciosos como adjuntos en chats y grupos. Una vez que el archivo malicioso esté abierto, los ciberdelincuentes pueden tener acceso a información sensible y/o secretos profesionales.

Otro ejemplo sería el uso de las aplicaciones de mensajerías personales para la comunicación corporativa. Se realiza a menudo sin las medidas de seguridad pertinentes y escapa a la supervisión del departamento de TI de la empresa (TI en la sombra). Por un lado, es una práctica que no cumple ni con la directiva NIS 2 ni con el marco legislativo europeo sobre la protección de datos (RGPD). Por otra parte, la suplantación de identidad a través de aplicaciones de mensajerías populares como WhatsApp ha ido creciendo, lo que conlleva un mayor riesgo de fraude del CEO y otros ataques. En este contexto, cabe señalar que la encriptación de extremo a extremo (hoy propuesta por la mayoría de las apps) no es necesariamente una garantía contra una «pérdida de datos»: algunas aplicaciones recopilan y procesan sistemáticamente datos sensibles de los usuarios con fines publicitarios y de marketing. Los metadatos rastreados pueden incluir información sobre ubicación, hora y duración de la comunicación, número de teléfono, etc., es decir, datos que, potencialmente, podrían ser utilizados por ciberdelincuentes.

La comunicación interna, vital durante una crisis

En su «Emergency & Crisis Communications Report 2022» el Business Continuity Institute señala que los teléfonos móviles son las herramientas más importantes en una crisis empresarial. Es cuando una aplicación de mensajería instantánea diseñada específicamente para uso corporativo permite a las organizaciones mantener líneas de comunicación vitales con la dirección, expertos en TI, consultores, empleados, responsables de seguridad, equipos jurídicos, etc.

Todo gestor experimentado sabe que la comunicación es clave para superar una crisis en el menor tiempo posible: las operaciones empresariales interrumpidas deben reorganizarse, mientras que los especialistas necesitan identificar y eliminar la causa del incidente. En estos casos, la mayor parte de la infraestructura informática puede estar dañada y/o completamente fuera de servicio. Lo más probable es que los canales de comunicación habituales (por ejemplo, el correo electrónico y MS Teams) no estén disponibles y/o se hayan infectado por el *malware.* ¿Sabe su compañía como mantener la comunicación en un caso así?

A escala global, el coste medio por ciberataque rondó los 4 millones de euros en 2022[8] y el daño económico anual causado por los ciberataques se calcula en miles de millones de euros, en tendencia ascendente.

«Se avecina una tormenta cibernética y es muy difícil anticipar lo malo que pueda ser».
Sadie Creese, profesora de Ciberseguridad en la Universidad de Oxford

Garantizar la continuidad del negocio *(Business Continuity)*

La comunicación interna es esencial para las organizaciones en todo momento. Sin embargo, durante una crisis, la propia existencia de una compañía puede depender de una app de mensajería instantánea segura: permite la gestión de la continuidad del negocio (BCM en sus siglas en inglés) y contribuye a un rápido restablecimiento de las operaciones. Un servicio de mensajería profesional permite evitar cuentas de correo electrónico potencialmente comprometidas y transmitir mensajes a través de un canal seguro a personas clave. También facilita la comunicación con departamentos enteros a través de listas de distribución de emergencia predefinidas y establecer chats de grupo cifrados de extremo a extremo. A diferencia de las aplicaciones más populares para uso personal, un servicio de mensajería profesional cumple plenamente el Reglamento General de Protección de Datos de la UE (GDPR).

Conclusión

DORA, NIS2 y CER son normativas diseñadas para hacer frente a amenazas digitales potencialmente devastadoras contra la Unión Europea y sus Estados miembros. Las evaluaciones periódicas de riesgos y la notificación inmediata de los ataques proporcionan transparencia transfronteriza, sensibilizando a las organizaciones sobre posibles ataques y la importancia de tomar las medidas adecuadas. Una resiliencia cibernética sólida requiere una planificación cuidadosa y la aplicación de procesos organizativos y tecnológicos. La nueva normativa ayuda a reforzar la resiliencia cibernética, prevenir los ciberataques y, en caso necesario, gestionarlos.

Los CISO deben asegurar la seguridad de los sistemas TIC de la empresa en todo momento. En «tiempos normales, una aplicación intuitiva y segura para la comunicación corporativa puede complementar las herramientas de colaboración existentes. En caso de emergencia, garantiza una comunicación segura y ayuda a reaccionar rápidamente ante la situación. Configurarla de antemano permite estar preparado para escenarios de crisis y/o gestionar las interrupciones de los procesos operativos.

El tiempo dirá cómo se aplica la nueva normativa y si las empresas y organizaciones ponen de su parte y toman plena conciencia de los riesgos que conllevan las tecnologías cibernéticas. El incumplimiento de la normativa no sólo puede exponerlas a sanciones, sino que las consecuencias del cese temporal de la actividad de las entidades críticas podrían tener graves repercusiones: siendo los ciudadanos las primeras víctimas, los daños causados podrían llevar incluso al cierre de las propias organizaciones.

Autor
Rodrigo López Crespo
Abogado en el área de Penal y Ciberseguridad
Monereo Meyer Abogados

Co-Autor
Miguel Rodríguez
Chief Revenue Officer
Threema GmbH

8 Fuente: https://www.ibm.com/reports/data-breach

Threema.Work

Resumen ejecutivo

Cómo Threema Work ayuda a cumplir las normativas NIS2, DORA y CER

Con la continua transformación digital de las organizaciones y de la sociedad en general, crece la necesidad de implementar medidas contra las amenazas cibernéticas. La seguridad digital está en el centro de la nueva normativa; se refiere a los aspectos económicos y sociales de la seguridad cibernética, incluidos los que protegen contra las actividades delictivas. El objetivo de las nuevas directivas es concienciar y establecer políticas más seguras en toda la UE.

El nuevo marco jurídico introduce el concepto de responsabilidad de cumplimiento de la gestión e incluye elementos normativos que se aplican a casi todos los sectores. A pesar de que el uso de soluciones de comunicación seguras, como, por ejemplo, de una app de mensajería diseñada para el uso empresarial, es sólo uno de los aspectos que la nueva normativa aborda para reforzar la resiliencia cibernética, los CISO no pueden permitirse pasarlo por alto.

Como app de mensajería empresarial, Threema Work no solo ayuda a cumplir la normativa mencionada, sino que también combina la seguridad con la eficacia y la comodidad de la mensajería instantánea.

Resiliencia cibernética sólida con Threema Work

- **Prevención:** la aplicación Threema Work es muy flexible y puede adaptarse fácilmente a las necesidades de su organización. Como app de mensajería empresarial dedicada con la opción de trabajar con grupos de usuarios cerrados, Threema Work proporciona una protección óptima a su empresa contra los ciberdelincuentes y los ataques de malware.
- **Protección de datos:** el cifrado constante de extremo a extremo impide que terceros accedan a información confidencial. Threema Work permite a su personal intercambiar textos, medios y mensajes de voz de forma segura, protegiendo al mismo tiempo los archivos confidenciales, los secretos comerciales y los datos de los empleados.
- **Comunicación corporativa resistente:** en caso de un ciberataque, los sistemas informáticos pueden verse comprometidos y/o simplemente no funcionar. En este escenario, Threema Work es una herramienta de comunicación esencial que permite a la empresa mantenerse en contacto con clientes, proveedores y partes interesadas; además ayuda a los ejecutivos a gestionar una situación crítica. El tiempo es clave durante cualquier crisis: en la cabina de gestión de Threema Work, la aplicación puede configurarse de antemano (por ejemplo, creando listas de distribución predefinidas), lo que ayuda a reducir el tiempo de reacción y contribuye a la continuidad de la empresa.

Threema Work ayuda a cumplir con las exigencias de las normativas NIS2, DORA y CER, ya que permite establecer un canal de comunicación seguro y contribuye a mejorar la resiliencia cibernética de la empresa.

Threema Work, que ofrece todas las funciones que cabe esperar de una aplicación de mensajería instantánea moderna, puede utilizarse como canal de comunicación principal o como complemento de las herramientas existentes. ¿Quiere comprobar por sí mismo cómo la mensajería empresarial segura mejora su comunicación corporativa? Active ahora su versión de prueba gratuita para 30 días.

Probar Threema Work ahora →