



“Protegiendo las empresas y los datos con soluciones de resiliencia y transferencia de riesgos”

Servicios de Resiliencia de Ciberseguridad

Servicios de Prevención y Soluciones de Transferencia de Riesgos

El creciente ritmo de la transformación digital y la aparición de nuevas tecnologías ha hecho que las empresas sean vulnerables a la explotación por parte de los ciberdelincuentes.

Desde la resiliencia hasta los seguros, ofrecemos una gama de soluciones de ciberseguridad corporativa para ayudar a las empresas a protegerse contra los riesgos.

Desafíos



Aumento de los ciberataques

El panorama de las amenazas cibernéticas se vuelve más complejo y los ataques cada vez más avanzados. Las empresas deben mantenerse a la vanguardia.



Necesidad de proteger los datos críticos y evitar pérdidas financieras

A medida que las empresas recopilan más datos, es importante identificar aquellos que son críticos para sus operaciones y la integridad del cliente.



Los requisitos reglamentarios son cada vez mayores y cada vez más complejos

Desde la Ley de Protección de Datos Personales hasta la Ley de Ciberseguridad, desde IFETEL hasta la CNSF, las empresas se enfrentan a una demanda cada vez mayor para demostrar e informar sobre acciones efectivas.



Solución



Aporta claridad y simplificación

Le ayudamos a navegar a través de la complejidad cibernética y a cumplir con los últimos requisitos normativos.



Combine servicios de prevención y soluciones de transferencia de riesgos

Nuestras soluciones de resiliencia se basan en investigaciones científicas, para ayudarlo a concentrarse en los controles cibernéticos más impactantes y generar asegurabilidad.



Aumente la madurez cibernética y la resistencia a las ciberamenazas

Con Zurich Cyber Resilience Solutions, ofrecemos un enfoque pragmático y rentable de la ciberseguridad



Consultoría y Formación



Consultoría especializada en ciberseguridad, cumplimiento normativo, gobierno del riesgo, auditorías de ciberseguridad y madurez. Acompañamiento de estrategias de ciberseguridad y concientización de usuarios



Consultoría de Gobierno y Riesgo

Gestión del Riesgo alineado con los objetivos del negocio e implementación de un GRC (Gobierno, Riesgo y Cumplimiento).

Cumplimiento y Regulación

Cumplimiento de estándares internacionales y normativos de acuerdo con la vertical de negocio y el mercado donde se desenvuelve la Organización.

Consultoría y Assessments en Ciberresiliencia

Se establece una estrategia de recuperación rápida ante impactos de un incidente de ciberseguridad en sus activos críticos.



Campañas de concientización de usuarios de phishing programado

Capacitación y promoción de una cultura de ciberseguridad en la Organización, mediante: e-learning, elementos lúdicos, entre otros.

Auditoría y Consultoría de Estrategia Integral de Ciberseguridad

Evaluación del estado de madurez de la Organización y establecimiento de una estrategia integral de ciberseguridad.

Auditoría de Arquitectura de Ciberseguridad y Sanidad de la misma

Verificación de efectividad de la arquitectura de ciberseguridad y de las configuraciones de los equipos de seguridad de la Organización.



CISO Virtual

Acompañamiento de especialistas en la operación estratégica, táctica y técnica de ciberseguridad, para la consultoría de temas de decisión a nivel CISO.

Asesoría Ciber-Legal

Consultoría para la asistencia en temas jurídicos en ciberseguridad, relacionados con sucesos o requerimientos de cumplimiento legal.



Servicios Técnicos y Administrados



Análisis de vulnerabilidades externas e internas

Verificación de vulnerabilidades a través de un monitoreo continuo o eventual, con la integración de sugerencias de remediación



Pruebas de penetración

Evaluación del grado de tolerancia a ciberataques reales, para identificar aquellos que pudiesen evadir los controles de seguridad implementados en una aplicación y/o infraestructura de una Organización.



Security Operation Center (SOC 3.0) / Cybersecurity Center (CCS)

Monitoreo y administración de tecnologías de ciberseguridad, así como protección de aplicaciones y bases de datos. Protección total y cobertura 24x7.



Análisis Forense

Revisión de las actividades asociadas a incidentes de seguridad confirmados para detectar y prevenir las debilidades en materia de ciberseguridad que han ocasionado el ataque.



Gestión de crisis "Ejercicio table-top"

Ejercicio basado en escenarios para evaluar y mejorar sus estrategias de preparación y respuesta en caso de ciberataque.



Arquitecturas de Interoperabilidad y Tecnologías Emergentes

Basado en estándares (NIST, CIS e ISO), se asegura la interoperabilidad de la tecnología actual de una Organización con la integración de una nueva infraestructura o con tecnologías emergentes para brindar soluciones puntuales.



Servicios Técnicos Especializados

Diagnóstico de alineación a una estrategia integral de ciberseguridad, verificación de sanidad de arquitecturas, pruebas de desempeño y cumplimiento.



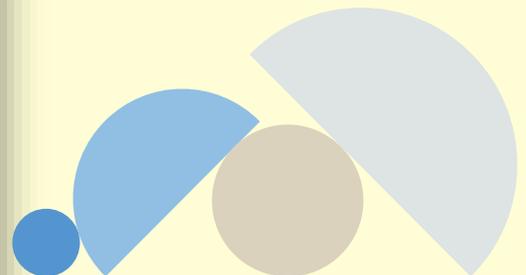
Plataforma de Protección y Administración de Ciberseguridad, SDWAN, SASE y ZTNA

Venta de más de 60 plataformas de ciberseguridad (conformadas por SW, HW, Servicios en la Nube, entre otros) con tecnologías y marcas reconocidas en el mercado y respaldados por profesionales certificados para la implementación, la programación, las pruebas, la operación y el soporte.



Plataformas de Data Loss Prevention (DLP) | Gobierno, Riesgo y Cumplimiento (GRC) | Protección de Bases de Datos (DBP) | Simulación de Ataque y Administración de Vulnerabilidades (VM)

Integración y comercialización de soluciones líderes en el mercado para complementar los Servicios de Consultoría de Ciberseguridad, así como de Gobierno y Riesgo.



Soluciones de Ciberseguridad



Cyber Healthcheck: Evaluación de madurez de ciberseguridad

Evaluación basada en los cuestionarios estándar de Zurich y NIST que incluye un informe detallado y recomendaciones.



Threat Hunting

Integración de herramientas especializadas e investigadores expertos para trazar actividad maliciosa, monitorear ataques cibernéticos y detenerlos oportunamente.



Ciberpatrullaje

Detección de delincuentes dedicados al fraude cibernético que incidan sobre información sensible o confidencial de una Organización, para protegerla de posibles extorsiones.



Protección de Reputación y Marca

Monitoreo del ciberespacio en búsqueda de uso de marca o sitios apócrifos que intenten suplantar a una Organización en Internet o Redes Sociales.



Protección de la Cadena de Suministro

Monitoreo del cumplimiento normativo, riesgo y reputación de terceros con los que se relaciona una Organización, a fin de reducir el riesgo de un ciberataque por cadena de suministro.



Correlación de fuentes externas de inteligencia de Amenazas

Herramientas de análisis y correlación de BIGDATA Security para integrar fuentes de ciberinteligencia y recibir información contextual de una Organización.

Soporte Estratégico



Gobernanza de Ciberseguridad

Apoyo en la redacción de su documentación de gobernanza de seguridad cibernética (control de acceso, contraseña, clasificación de datos, cifrado y otros)



Plan de Incidentes

Procedimiento documentado que describe la respuesta y la gestión de incidentes de ciberseguridad.



Exposición Financiera (Cuantificación Cibernética)

Evaluación continua del impacto financiero para guiar la priorización y justificación de las inversiones y estrategias cibernéticas.



Cadena de suministro cibernética

Marco agregado que monitorea la madurez cibernética de toda la cadena de suministro, basado en diferentes niveles de evaluación.



Servicios de Continuidad de Negocio (BCP)

Definición de la Estrategia de Continuidad del Negocio, incluyendo la Evaluación de Impacto en el Negocio (BIA), desarrollo de políticas y otros.



Servicios de Recuperación ante Desastres (DRP)

Definición de la Estrategia de Recuperación ante Desastres, incluyendo pruebas, las comunicaciones del plan de recuperación y de la protección de la reputación de la Organización



Marco López

Cyber Risk Engineer Manager
Zurich Resilience Solutions

marco.lopez1@mx.zurich.com
+52 56 2567 1781



Oscar Pérez

Head of Zurich Resilience
Solutions México

oscar.perez@zurich.com
+52 33 1862 5105



Alberto Ambe

Business Development Manager
Zurich Resilience Solutions

alberto.ambe@mx.zurich.com
+52 56 2567 1650

¿Por qué Zurich Cyber Resilience Solutions?



Apoyo para mejorar la asegurabilidad



Combinación de datos de siniestros y evaluación comparativa del sector



Paquetes de servicios adaptados a cada tamaño de empresa y sus necesidades.



Métodos y soluciones respaldados por estudios científicos y nuestro equipo interno de investigación y desarrollo



Presencia global para soluciones remotas e in situ



This is a general description of (insurance) services such as risk engineering or risk management services by Zurich Resilience Solutions which is part of the Commercial Insurance business of Zurich Insurance Group, and does not represent or alter any insurance policy or service agreement. Such (insurance) services are provided to qualified customers by affiliated companies of Zurich Insurance Company Ltd (Zurich Insurance Group). The prices stated are exclusive of VAT and are subject to change at any time.

The opinions expressed herein are those of Zurich Resilience Solutions as of the date of the release and are subject to change without notice. This document has been produced solely for informational purposes. All information contained in this document has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Company Ltd or any members of Zurich Insurance Group as to their accuracy or completeness. This document is not intended to be legal, underwriting, financial, investment or any other type of professional advice. Zurich Insurance Group disclaims any and all liability whatsoever resulting from the use of or reliance upon this document. Nothing express or implied in this document is intended to create legal relations between the reader and any member of Zurich Insurance Group.

Certain statements in this document are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by numerous unforeseeable factors. The subject matter of this document is also not tied to any specific service offering or an insurance product nor will it ensure coverage under any insurance policy.

This document may not be distributed or reproduced either in whole, or in part, without prior written permission of Zurich Insurance Company Ltd, Mythenquai 2, 8002 Zurich, Switzerland. No member of Zurich Insurance Group accepts any liability for any loss arising from the use or distribution of this document. This document does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction.