



Ciberseguridad en el Sector Financiero

Décimo Cyberdrill para Américas - Honduras 2022

Oscar Reyes

Coordinador de Seguridad y Aseguramiento de TI

**Banco Centroamericano de Integración Económica
(BCIE)**

Tegucigalpa, Honduras - 21 de Noviembre de 2022



Allianz Risk Barometer 2022

The most important business risks for the next 12 months and beyond, based on the insight of 2,650 risk management experts from 89 countries and territories.



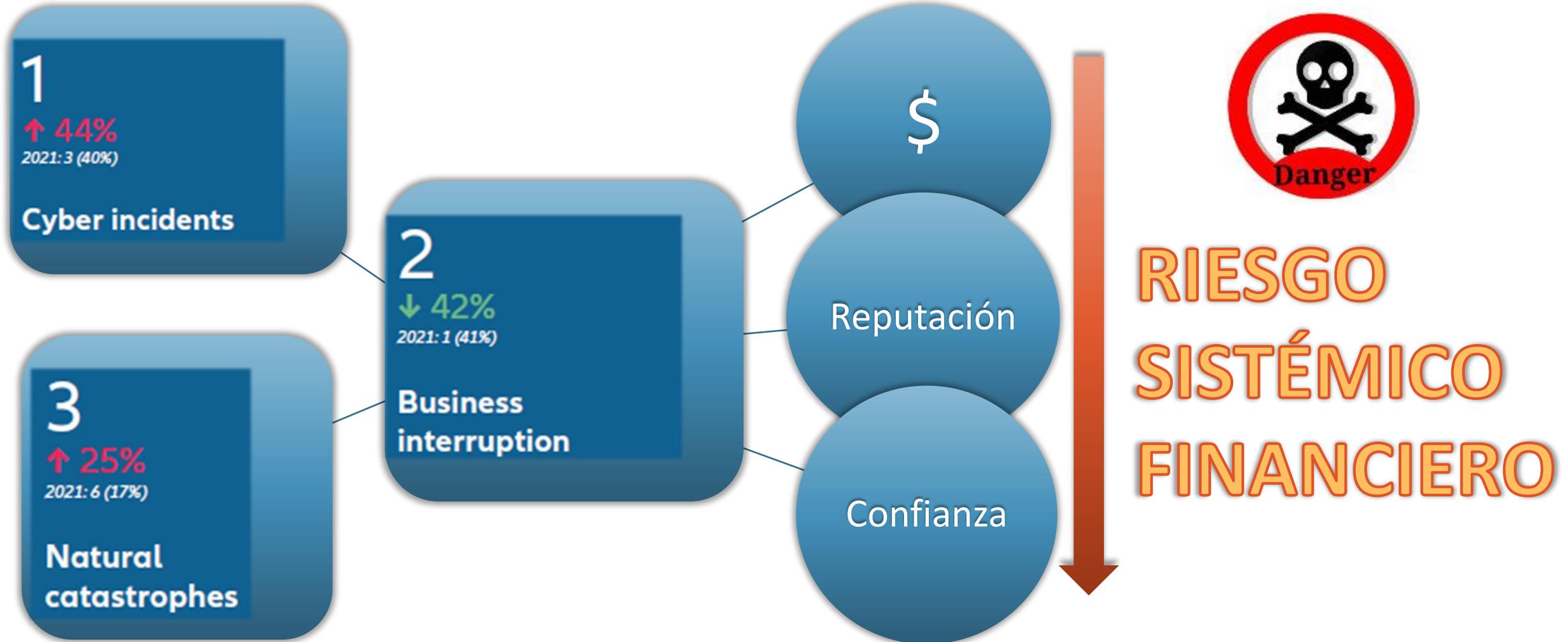
1
↑ 44%
2021: 3 (40%)
Cyber incidents
(e.g. cyber crime, IT failure/ outage, data breaches, fines and penalties)



2
↓ 42%
2021: 1 (41%)
Business interruption
(incl. supply chain disruption)



3
↑ 25%
2021: 6 (17%)
Natural catastrophes
(e.g. storm, flood, earthquake, wildfire, weather events)



PILARES CIBERSEGURIDAD	MEDIDAS PREVENTIVAS	MEDIDAS DETECTIVAS	MEDIDAS CORRECTIVAS	COMUNIDAD
<ul style="list-style-type: none"> • Confidencialidad • Integridad • Disponibilidad 	<ul style="list-style-type: none"> • Arquitectura de seguridad en capas • Campañas Concientización • BCP • DRP • OWASP • EH • Simulacros Phishing, Smishing, Ing. Social, etc • Red Team/Blue Team • Clasificación, etiquetado, retención y destrucción de la información • Configuration Management 	<ul style="list-style-type: none"> • SOC • NOC • SIEM • IDS/IPS • Anti-Malware • Firewalls • DLP • Antispam • Branding 	<ul style="list-style-type: none"> • CIRT • CERT 	<ul style="list-style-type: none"> • Fondo o Seguro Sector Financiero • Knowledge Base • Experiencias • Red Confianza • Benchmarks • Simulacros en conjunto



Preguntas a Panelistas



Panelista	Pregunta
<ul style="list-style-type: none"> Fredis Medina <i>Banco Central de Honduras</i> 	<ol style="list-style-type: none"> Un incidente de ciberseguridad puede generar una interrupción parcial o total del negocio en una institución financiera con su consecuente impacto económico y reputacional. Desde la perspectiva del Banco Central, <ul style="list-style-type: none"> ¿Qué acciones se están adelantando y se deberían adelantar para reducir el impacto en el sector financiero y en la economía del país? ¿Cuál es el efecto sistémico que pudiera generar la interrupción parcial o total de una institución financiera por temas de ciberseguridad? ¿Qué rol deben jugar en el sector financiero los equipos CIRT /CERT como mecanismos de respuesta ante incidentes de seguridad?
<ul style="list-style-type: none"> Luis Cruz <i>Asesor de TI de la Secretaría de Finanzas de Honduras</i> 	<ol style="list-style-type: none"> Cómo es el esquema de seguridad que plantea la SEFIN y Qué actividades han adelantado y pretenden adelantar para fomentar el desarrollo mancomunado de esfuerzos del sector financiero para hacer frente al riesgo de ciberataques? ¿En que etapa de madurez en ciberseguridad se ubica el Gobierno de Honduras??
<ul style="list-style-type: none"> Freddy Videz <i>Investigador en Jefe de Análisis de Datos de la Comisión Nacional de Bancas y Seguros de Honduras</i> 	<ol style="list-style-type: none"> ¿Cuál es el direccionamiento normativo y de supervisión que está generando la CNBS para asegurar que las instituciones financieras realmente cuentan con prácticas y controles apropiados para hacer frente al riesgo de ciberseguridad? ¿Existe algún estándar, metodología o línea base que recomiendas adoptar para asegurar el debido alineamiento de la seguridad de Información?
<ul style="list-style-type: none"> José Cardona <i>Subgerente de Gobierno Tecnológico y Ciberseguridad de Bac Credomatic</i> 	<ol style="list-style-type: none"> ¿Cómo en nuestras instituciones financieras podemos saber si estamos preparados para hacer frente a un incidente de ciberseguridad? ¿Qué hacer si ya sucedió? Los ciberdelincuentes atacan tanto a las instituciones financieras como a sus clientes, ¿Qué estrategia debería seguir el sector financiero para fortalecer la postura de sus clientes ante estas amenazas?



THANK YOU

