Cuantificación riesgo cibernético. Stress test y ciberresiliencia

Federico Muller

Country Manager
Microsoft
femuller@microsoft.com


8 Agosto 2016...
2,000 Vuelos Cancelados
US$900,000 Por vuelo
DELTA
JFK JITNEY
JFK JITNEY
DELTA
900588
3141

Passengers at Terminal 3 of Delhi's Indira Gandhi International Airport look at a blue screen displaying an error message on Friday when a technology outage affected computers worldwide. PHOTO: PTI

When all systems in the world go down

The tech outage marks the risk of depending on a single firm's software, report **SHIVANI SHINDE** & **ASHUTOSH MISHRA**

The technology outage on Friday proved the peril of an increasingly interconnected digital world. A software update by cybersecurity firm CrowdStrike affected 8.5 million Microsoft Windows devices, causing one of the largest tech outages. Less than 1 per cent of Windows machines were affected, according to Microsoft, but it had a cascading effect on centralised software systems.

CrowdStrike's Falcon update led to the 'blue screens of death' in Windows systems, disrupting emergency services, airlines, financial transactions and individuals.

The outage raised questions about the rising trend of single point of failure in technology infrastructure and centralised software dependency, where the control of critical systems sits with a single vendor.

Centralised dependency

"This has nothing to do with the Cloud. This was a failure of massive centralised software dependency. When you have one centralised software dependency across so many industries and countries, and when it goes down centrally then this is what happens. Add to this is the fact that it is a proprietary piece of software, which means only its maker knows what is happening. Everyone has to wait for that one company to explain what broke," said Kailash Nadh, chief technology officer of Zerodha, a leading stockbroker.

A centralised approach means that critical software worldwide relies on one opaque service. "Irrespective of whether there is more than one such product, if they're all controlled online by an external entity which is highly centralised then such issues can happen."

Zerodha runs in-house computer security systems and uses open source technologies. "It (security modules) doesn't leave our premises. It doesn't connect to the internet and it's not controlled by an external entity. It's managed and controlled by us fully internally. So even if something went wrong, it would only impact Zerodha, and not the entire world," said Nadh.

The Falcon glitch is not the first time that failure in a single piece of software has pulled down systems. In 2023, employees of the Federal Aviation Administration in the United States (US) accidently deleted computer files when they updated a database. It disrupted a system used to communicate with pilots, leading to the cancellation of thousands of flights. Last year, when AT&T updated a software in the US it caused thousands of customers to lose telecom connectivity.

The Falcon outage was wider and raises the question of whether enterprises should trust a single vendor like CrowdStrike.

Neil MacDonald, vice-president and distinguished analyst at Gartner, said the issue will force companies to review their vendor portfolio and contracts. "First, where there is concentration risk in an IT (information technology) vendor, does the vendor have documented and third-party evaluated development processes to prevent this type of issue? Second, what penalties does the vendor have for releasing faulty software that results in downtime?

"Third, outside of cyber insurance (it covers downtime and losses from attacks), does the company have any business outage/downtime coverage? And fourth, in the event IT systems are down, what are the business continuity and resiliency plans for reaching employees in these types of occasions where their computer may be unavailable," said MacDonald. The

THE OUTA
WILL LIKE
FORCE FIR
TO REVIEW
THEIR VEN
PORTFOLI
AND SOFT
CONTRACT

Un ciberataque interrumpe el oleoducto Colonial, que transporta 100 millones de galones de combustible al día

2014 CIBERSEGURIDAD = PROBLEMA TÉCNICO

2020 CIBERSEGURIDAD = PRIORIDAD DE NEGOCIO

2022 CIBERSEGURIDAD = EXISTENCIA ORGANIZACIONAL

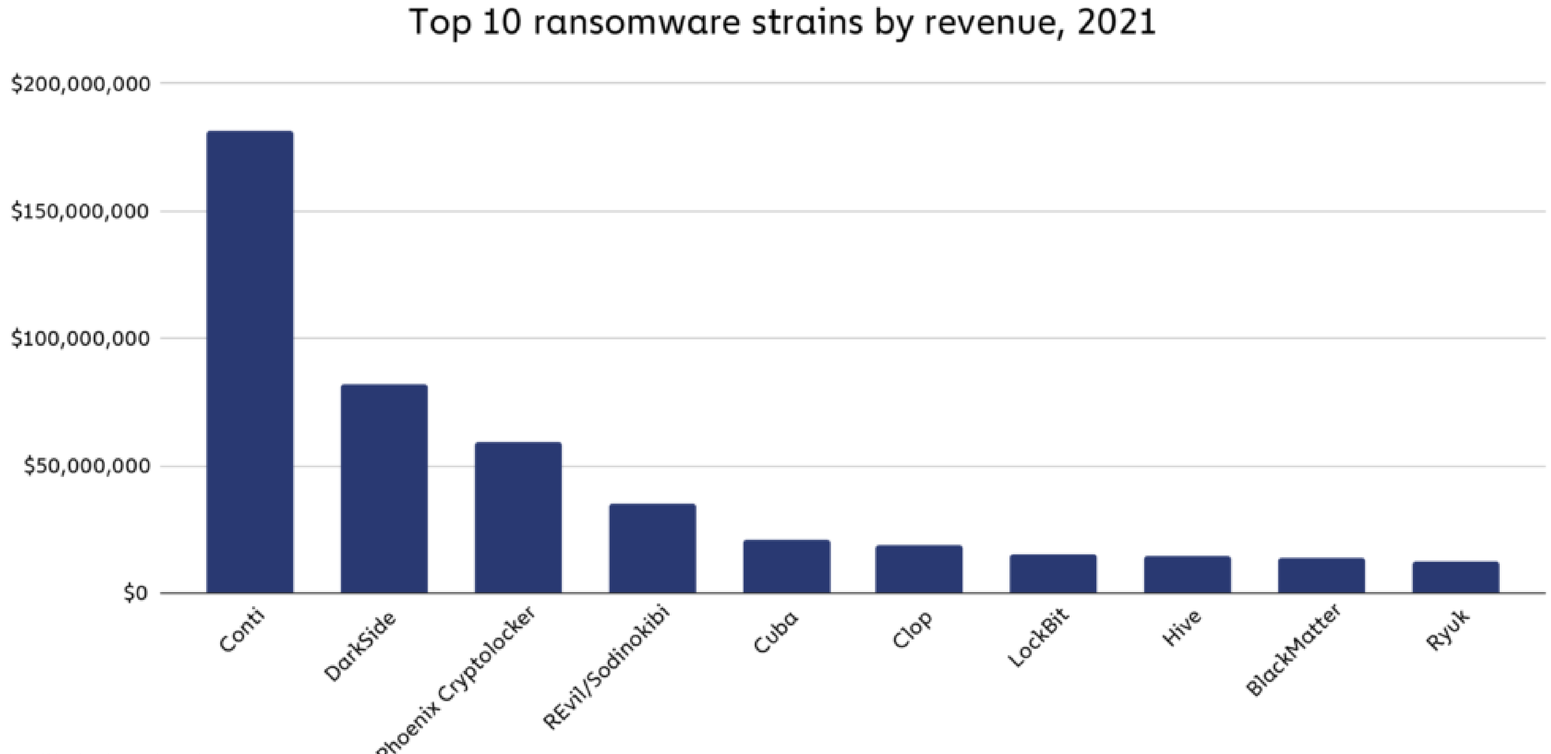
2024 CIBERSEGURIDAD = PROBLEMA DE ESTADO - MACROECONOMICO

PARAÍSO HACKEADO

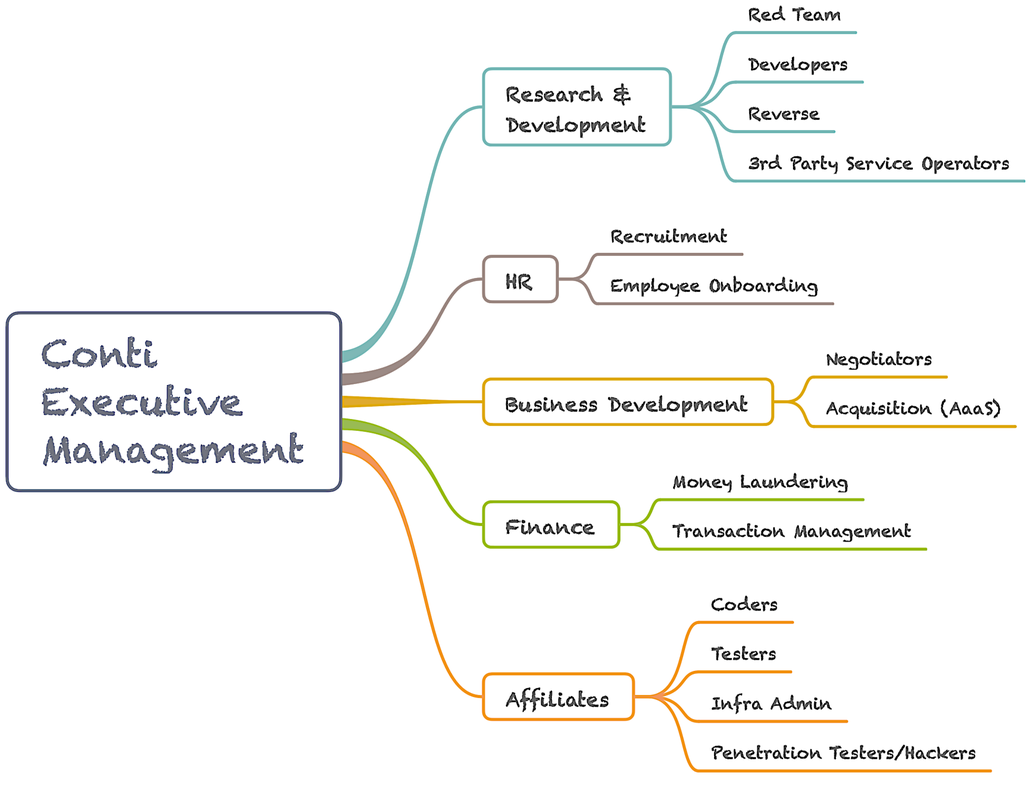
UN INFORME ESPECIAL

En opinión de los analistas de Moodys, dicho evento afecta negativamente el riesgo de crédito del país.

Moody's prevé que la ejecución presupuestaria se deteriorará mientras el gobierno logra reanudar las operaciones digitales. Ello pone en riesgo la meta de un déficit fiscal de 4,8 % del PIB previsto para este año.



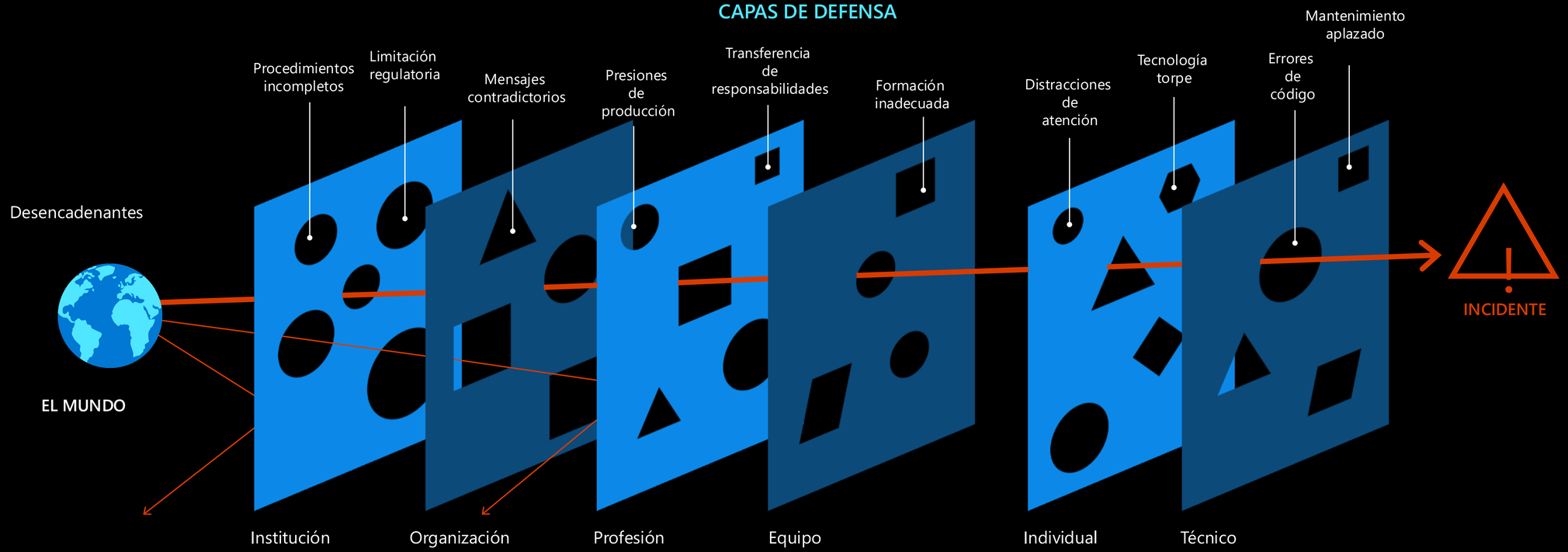
Fuente: https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/



The Missing Piece in the RaaS Business Model

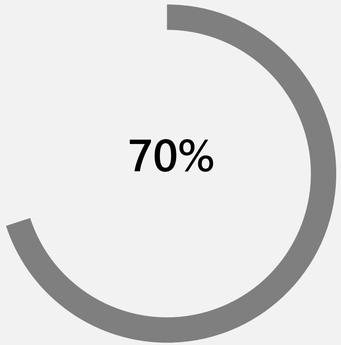
¿Por qué suceden las cosas malas?

Modificado de
Reason, 1991



Seguridad: desafíos de la transformación digital

La mayoría de las **iniciativas no alcanzan** sus objetivos

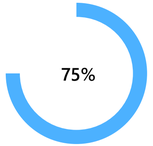


de todas **las iniciativas de transformación digital no** alcanzan sus objetivos

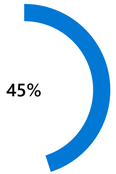
Source: Harvard Business Review

El reto es lograr resultados a tiempo y dentro del presupuesto

de las migraciones están **atrasadas con respecto al calendario** previsto



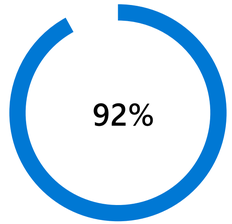
de las migraciones a la nube **están gastando por encima** del presupuesto



del presupuesto gastado en **exceso se dedica a la gestión del cambio**, debido a que **no se aborda la gestión del cambio por adelantado**

Source: McKinsey & Company

El mayor desafío no es tecnológico: Cultura



de las empresas informan que **continúan luchando con desafíos culturales** relacionados con la **alineación organizacional, los procesos comerciales, la gestión del cambio, la comunicación, las habilidades de las personas** y la **resistencia o falta de comprensión** para permitir el cambio

Source: Harvard Business Review


ANALYSIS
STRATEGY
PROCESS
RISK
REVIEW
EVALUATE
CONTROL
ASSESSMENT

NIST RMF
RISK MANAGEMENT FRAMEWORK
nist.gov/rmf

FAIR INSTITUTE

VALUE AT RISK (VaR)

OCTAVE SM

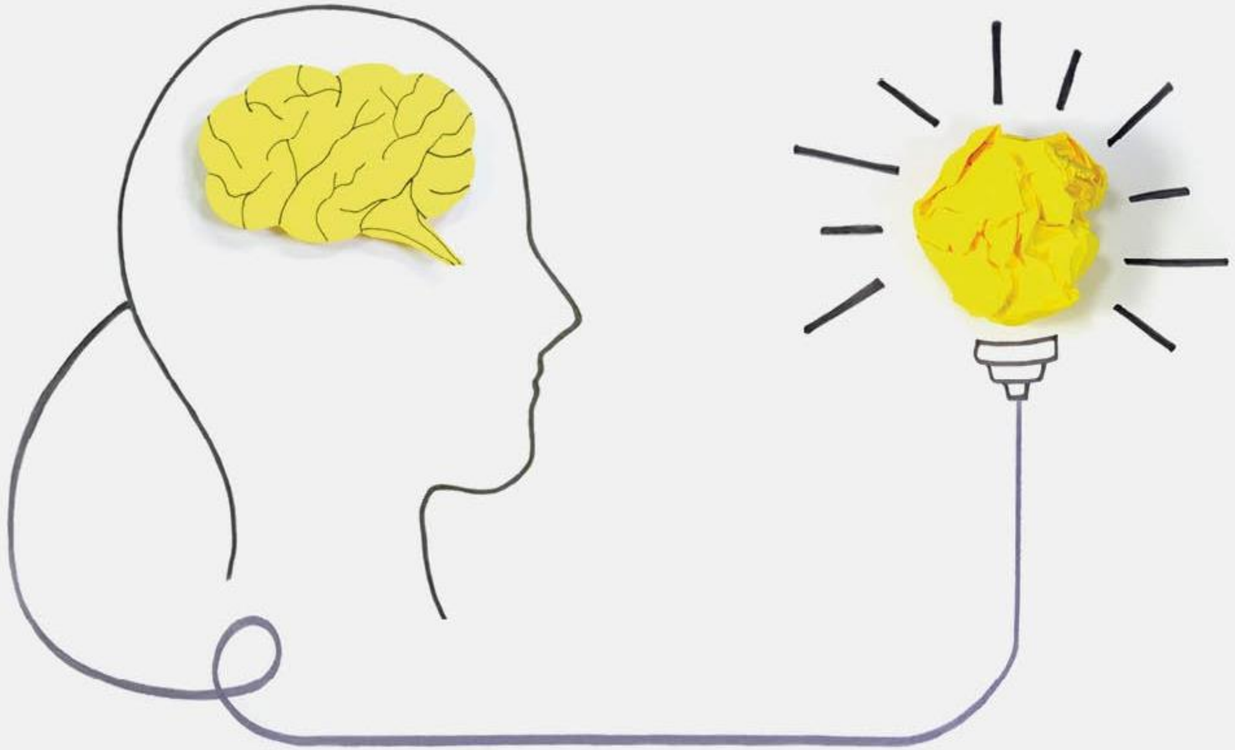
ISO 27005

RISK

Punto de Inflexión

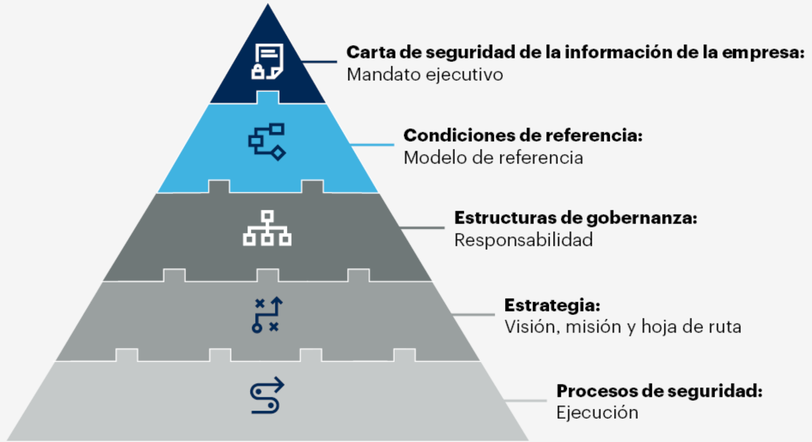
quantum computing

Data Center



Ciberseguridad

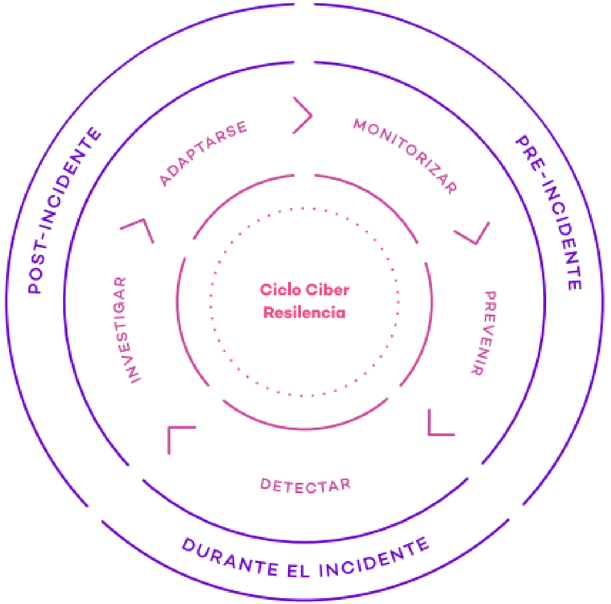
Elementos de un programa de ciberseguridad



Fuente: Gartner

Gartner

Ciberresiliencia



Diseñando para el éxito y el fracaso

Entonces

FIABILIDAD
Diseñado para no fallar

PREVENIR
Todos los ataques posibles

Ahora

RESILIENCIA
Diseñado para recuperarse rápidamente

ASUMIR COMPROMISO
Proteja, detecte y responda a lo largo de las fases de ataque

Seguridad → Resiliencia

¿Qué es la "Resiliencia"?

La resiliencia es la capacidad de Recuperarse de errores y seguir funcionando. No se trata de evitar fallas, sino de responder a ellas de una manera que evite el tiempo de inactividad o la pérdida.

Antifragilidad	La capacidad de crecer en el fracaso
Resiliencia	La capacidad de recuperarse de un error
Robustez	La capacidad de resistir un fracaso

Principales riesgos de resiliencia

Riesgo de resiliencia	Descripción
Resiliencia geográfica	La falta de resiliencia geográfica en el personal, las funciones, la autoridad y la capacitación podría resultar en la incapacidad de manejar las interrupciones en las operaciones comerciales y tomar decisiones críticas para una recuperación oportuna
Cadena de suministro	Limitaciones de capacidad en la nube a corto plazo (aumento) y a largo plazo que requieren la necesidad de ampliar la cadena de suministro a múltiples proveedores y países de origen y garantizar que los servicios estén diseñados para aprovechar tecnologías alternativas.
Capacidad de la nube (E/S, red, TPS)	Restricciones de capacidad y limitaciones a contingencias de conmutación por error

Lo que queremos lograr - Resiliencia cibernética integral - Largo plazo

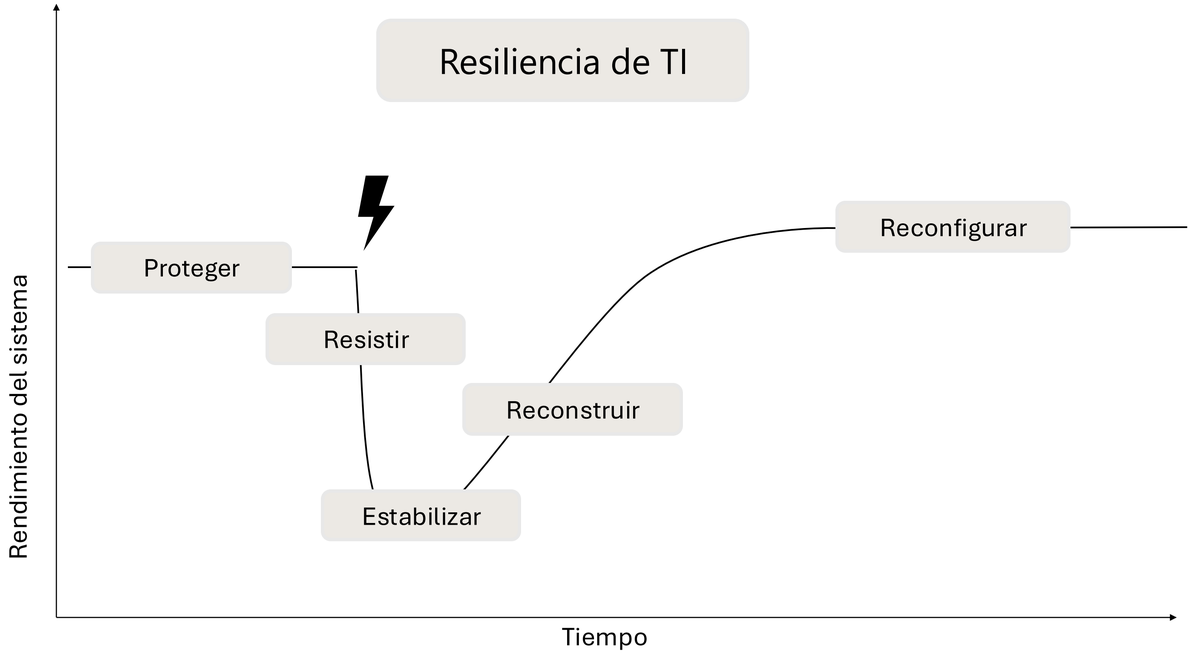
DESARROLLO DE LA RESILIENCIA

Establezca resiliencia sostenible

Resiliencia cibernética

Análisis, Estrategia y Planificación

Operaciones de seguridad, protección contra amenazas y supervisión de la resiliencia



¿Resiliencia a las crisis? Trillizos digitales

Cambiar los modelos habituales de continuidad del negocio a la infraestructura externa (externalizada)

Beneficios de una prueba de estrés de resiliencia cibernética

Identificación de vulnerabilidades

Una prueba de estrés de resiliencia cibernética ayuda a identificar vulnerabilidades en el sistema que podrían ser explotadas por los atacantes cibernéticos. Este conocimiento ayuda a las organizaciones a tomar medidas proactivas para fortalecer sus defensas y reducir los riesgos.

Beneficios de una prueba de estrés de resiliencia cibernética

Identificación de vulnerabilidades

Una prueba de estrés de resiliencia cibernética ayuda a identificar vulnerabilidades en el sistema que podrían ser explotadas por los atacantes cibernéticos. Este conocimiento ayuda a las organizaciones a tomar medidas proactivas para fortalecer sus defensas y reducir los riesgos.

Mejorar la respuesta a los ciberataques

Una prueba de estrés de resiliencia cibernética ayuda a las organizaciones a mejorar su respuesta a los ciberataques al identificar las áreas que necesitan mejoras. Al realizar pruebas de estrés periódicas, las organizaciones pueden afinar su proceso de respuesta y estar mejor preparadas para un ataque real.

Beneficios de una prueba de estrés de resiliencia cibernética

Identificación de vulnerabilidades

Una prueba de estrés de resiliencia cibernética ayuda a identificar vulnerabilidades en el sistema que podrían ser explotadas por los atacantes cibernéticos. Este conocimiento ayuda a las organizaciones a tomar medidas proactivas para fortalecer sus defensas y reducir los riesgos.

Mejorar la respuesta a los ciberataques

Una prueba de estrés de resiliencia cibernética ayuda a las organizaciones a mejorar su respuesta a los ciberataques al identificar las áreas que necesitan mejoras. Al realizar pruebas de estrés periódicas, las organizaciones pueden afinar su proceso de respuesta y estar mejor preparadas para un ataque real.

Reducir el riesgo de ciberataques exitosos

Una prueba de estrés de resiliencia cibernética ayuda a las organizaciones a reducir el riesgo de un ataque cibernético exitoso al identificar vulnerabilidades y mejorar los tiempos de respuesta. Cuando una organización está mejor preparada, es menos probable que sea víctima de ciberataques.

Beneficios de una prueba de estrés de resiliencia cibernética

Identificación de vulnerabilidades

Una prueba de estrés de resiliencia cibernética ayuda a identificar vulnerabilidades en el sistema que podrían ser explotadas por los atacantes cibernéticos. Este conocimiento ayuda a las organizaciones a tomar medidas proactivas para fortalecer sus defensas y reducir los riesgos.

Mejorar la respuesta a los ciberataques

Una prueba de estrés de resiliencia cibernética ayuda a las organizaciones a mejorar su respuesta a los ciberataques al identificar las áreas que necesitan mejoras. Al realizar pruebas de estrés periódicas, las organizaciones pueden afinar su proceso de respuesta y estar mejor preparadas para un ataque real.

Reducir el riesgo de ciberataques exitosos

Una prueba de estrés de resiliencia cibernética ayuda a las organizaciones a reducir el riesgo de un ataque cibernético exitoso al identificar vulnerabilidades y mejorar los tiempos de respuesta. Cuando una organización está mejor preparada, es menos probable que sea víctima de ciberataques.

Aumentar la confianza de las partes interesadas

La realización periódica de pruebas de estrés de resiliencia cibernética ayuda a aumentar la confianza de las partes interesadas. Cuando las partes interesadas saben que una organización está probando regularmente sus defensas y mejorando sus procesos de respuesta, es más probable que inviertan en la organización y apoyen sus iniciativas.

Lecciones aprendidas

Empieza con: Estás comprometido.> **Ciberseguridad**

- La integridad de sus datos se ve comprometida.
- Tu tapadera de las identidades del adversario.
- Sus dispositivos no están protegidos.
- Reinicie con Zero Trust Security.

Lidera con: Te recuperarás.> **Resiliencia cibernética**

- Todos los componentes del sistema necesitarán recuperación.
- Se recuperará a diferentes infraestructuras.
- Reconstruirás todo desde cero.
- Reinicie con la resiliencia a gran escala.

Lecciones aprendidas de la prueba de resistencia cibernética del BCE de 2024 y las perspectivas para DORA

- Escenario de ataque complejo
  - Un atacante desconocido accedió y cifró la base de datos principal del sistema bancario central
  - No fue posible ninguna preparación específica ni trabajo previo
- Cuantificación del impacto económico
  - Determinación de pérdidas directas e indirectas
  - Evaluar el impacto en funciones económicas clave como préstamos, captación de depósitos y procesamiento de pagos
- Exigente horario de CRST
  - Responder a 395 preguntas y recopilar pruebas requirió cientos de horas
  - Coordinación interdepartamental intensivo
  - Amplia colaboración con proveedores externos

A menudo se incumplían los plazos de recuperación

Falta de procesos para cuantificar los daños

- Falta de procesos establecidos
  - No hay métodos estandarizados para cuantificar los daños
- Necesidad de un enfoque multidisciplinario
  - Determinación holística del impacto económico
- Confianza en los juicios de los expertos
  - Valores a menudo basados en suposiciones
  - Enfoques incoherentes y poco fiables

Conclusión

Riesgo ahora asunto economía

Punto de inflexión de los nuevos riesgos

Ciber resiliencia como northstar

Stress Test como barra de medición.