Ciberresiliencia: Navegando el caos en las organizaciones

Construyendo resiliencia en un entorno digital turbulento

Israel Gutiérrez

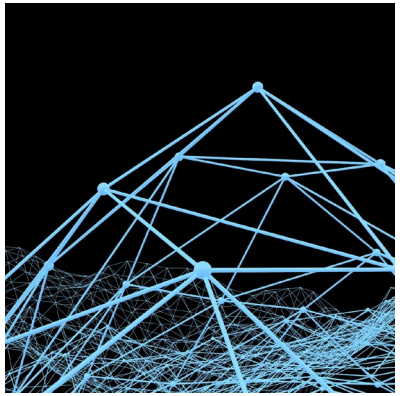
@gutzba

Agenda

- Definiciónes – Caos – Resiliencia - Antifragil
- A que nos enfrentamos
- Estrategias frente al caos
- Cierre

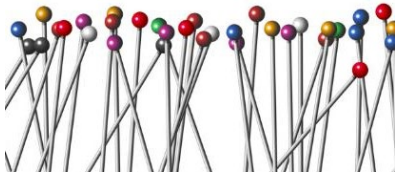
Teoría del caos
Resiliencia
Antifragil

Caos



Teoría del Caos

La teoría del caos establece que incluso pequeños cambios en un sistema pueden llevar a resultados impredecibles y drásticos.



Complejidad de los Sistemas

La complejidad en los sistemas es fundamental para entender cómo las interacciones pueden resultar en comportamientos inesperados.

Amenazas Cibernéticas

Las pequeñas vulnerabilidades en sistemas pueden resultar en grandes brechas de seguridad, resaltando la importancia de la teoría del caos.

Resiliencia en las organizaciones

Definición de Resiliencia Organizacional

La resiliencia organizacional es la capacidad de una empresa para adaptarse a cambios y superar desafíos inesperados.

Importancia de la Continuidad del Negocio

Mantener la continuidad del negocio es vital para la supervivencia organizacional, especialmente durante situaciones adversas.

Cultura de Adaptación y Aprendizaje

Fomentar una cultura que valore la adaptación y el aprendizaje es esencial para el crecimiento y la resiliencia organizacional.

ANTIFRAGILIDAD

- Nassim Taleb- Albanes

Se trata de la propiedad de un sistema para progresar al ser expuesto a shocks, fallas y la aleatoriedad que caracteriza a nuestro mundo

CIBER-RESILIENCIA

- Arturo García - Mexicano

Capacidad de una organización o nación para anticiparse, soportar y recuperarse parcial o totalmente de un ciberataque, permitiendo la continuidad de sus operaciones y adaptarse a nuevas condiciones

A que nos enfrentamos en términos de ciberseguridad del 2025-2035

2025-2035

Incidentes Cibernéticos Notables

Se estima que el costo del cibercrimen a nivel mundial alcanzara los 10.5 billones de dólares para el cierre de 2025

Impacto en la Percepción

La inteligencia artificial generativa y sus evoluciones presentan un reto desde la gestión y gobierno de la misma hasta la creación de ciberarmas asociadas al uso de esta tecnología para la innovación en protocolos de ataque

América Latina

América Latina es una de las regiones mas afectadas, específicamente el sector financiero, salud y gubernamental

Foro económico mundial

Este foro mantiene el ciberataque dentro de los principales riesgos a nivel mundial

Lo único constante es el cambio

Como podemos navegar ante el caos

Visibilidad

Identificar

Creemos y apliquemos procesos que nos ayuden a identificar la informacion, activos digitales y sus responsables.

Conocer

Ver, Conocer, Asegurar, Sepamos que estamos protegiendo.

Medir

Tenemos claros los estados y sus cambios cuando existen los identificamos

Ingeniería del caos

Premisa de los Fallos

El principio fundamental de la ingeniería del caos es que los fallos son inevitables en cualquier sistema, y deben ser esperados.

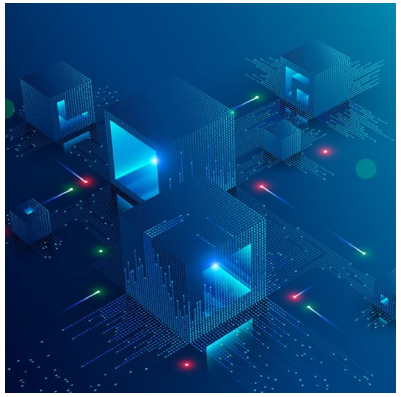
Diseño de Experimentos

Se crean experimentos controlados para observar cómo los sistemas reaccionan ante fallos, con el fin de aprender y adaptarse.

Aprender de las brechas de seguridad

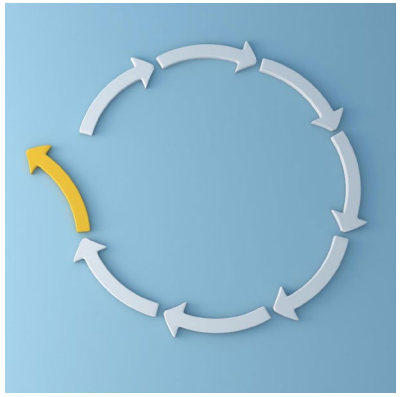
Las brechas de seguridad deben ser vistas como oportunidades para aprender.

Analizar los incidentes e identificar brechas y áreas de mejora



Fortalecimiento de sistemas

Implementar cambios tras incidentes y ejercicios de fallo fortalece los sistemas y los procesos de la organización.



Cultura de mejora continua

Fomentar una cultura de mejora continua permite a las organizaciones adaptarse y evolucionar ante nuevas amenazas cibernéticas.

Aplicación en la ciberseguridad

Seguridad del Caos

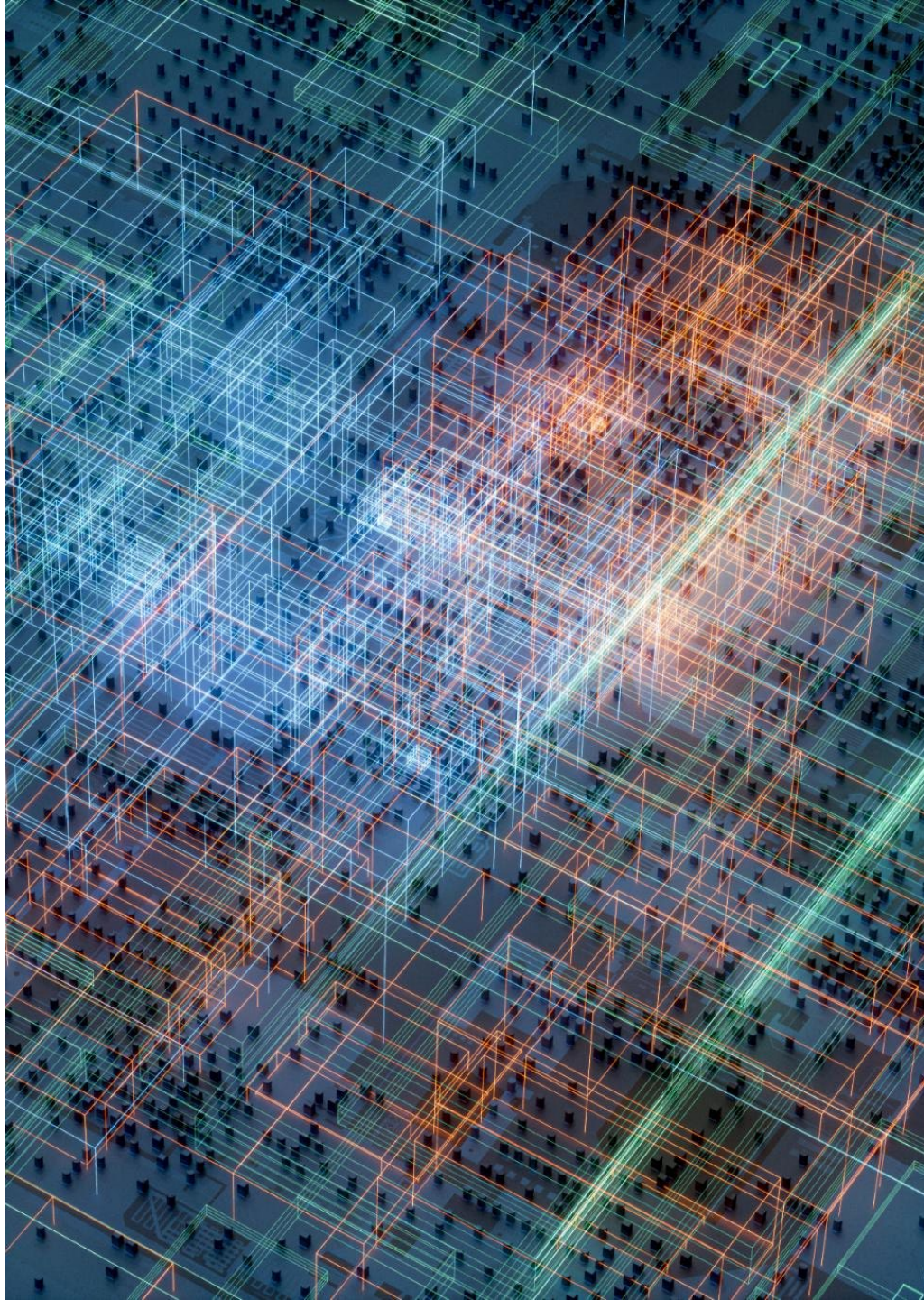
La seguridad del caos permite a las organizaciones simular fallas y ataques para evaluar su preparación ante incidentes cibernéticos.

Identificación de Vulnerabilidades

Simulando situaciones adversas, las organizaciones pueden descubrir y abordar vulnerabilidades en sus sistemas de seguridad.

Fortalecimiento de Defensas

Las prácticas de seguridad del caos ayudan a fortalecer las defensas cibernéticas, preparándolas para amenazas reales y evitando brechas de seguridad.



Ciber-Resiliencia Adaptativa

Importancia de la Ciber-Resiliencia

La ciber-Resiliencia es crucial para enfrentar y recuperarse de incidentes cibernéticos, garantizando la continuidad del negocio.

Adaptación

Todos los entornos y organizaciones son diferentes, cada una debe observar su estado actual para reconocer y adaptar el proceso de Ciber-Resiliencia posible.

Conocer, Identificar y Reconocer nuestro estado actual es el mejor punto para establecer el camino a seguir, Adaptar es posible siempre que reconozcamos nuestro estado actual.

Estrategias de ciberresiliencia implementadas con éxito

Planeación

Crea escenarios posibles y menos posibles, involucra múltiples personas que aporten múltiples puntos de viste

Iteraciones

Genera múltiples iteraciones para identificar eventos fortuitos dentro de los procesos de evaluación

Aprendizaje Continuo

Sistematiza el proceso de documentación y aprendizaje para que sea lo mas fácil posible y lleve el menor tiempo, de esa forma podemos asegurar un modelo continuo de mejora.

Conclusión

¿Como podemos saber si estamos listos?

Enfoque Proactivo

La ciber-Resiliencia debe ser un enfoque proactivo, anticipando y navegando por el caos en lugar de solo reaccionar a incidentes.

Kintsugi

La filosofía del Kintsugi enseña que las imperfecciones pueden ser una fuente de fortaleza, no solo es resistir es Evolucionar ser mejores y mas valiosos en cada proceso

Seguridad del Caos

La ingeniería del caos permite a las organizaciones simular fallos y prepararse para desafíos cibernéticos inesperados, mejorando su Ciber-Resiliencia.

Probar, Ejercitar, Simular