VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Que temer, qué pelear y que sacrificar

- Navegando entre los desafíos actuales de la seguridad de la información

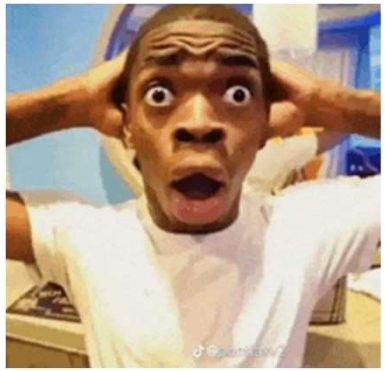
Harom Ramos Rivera

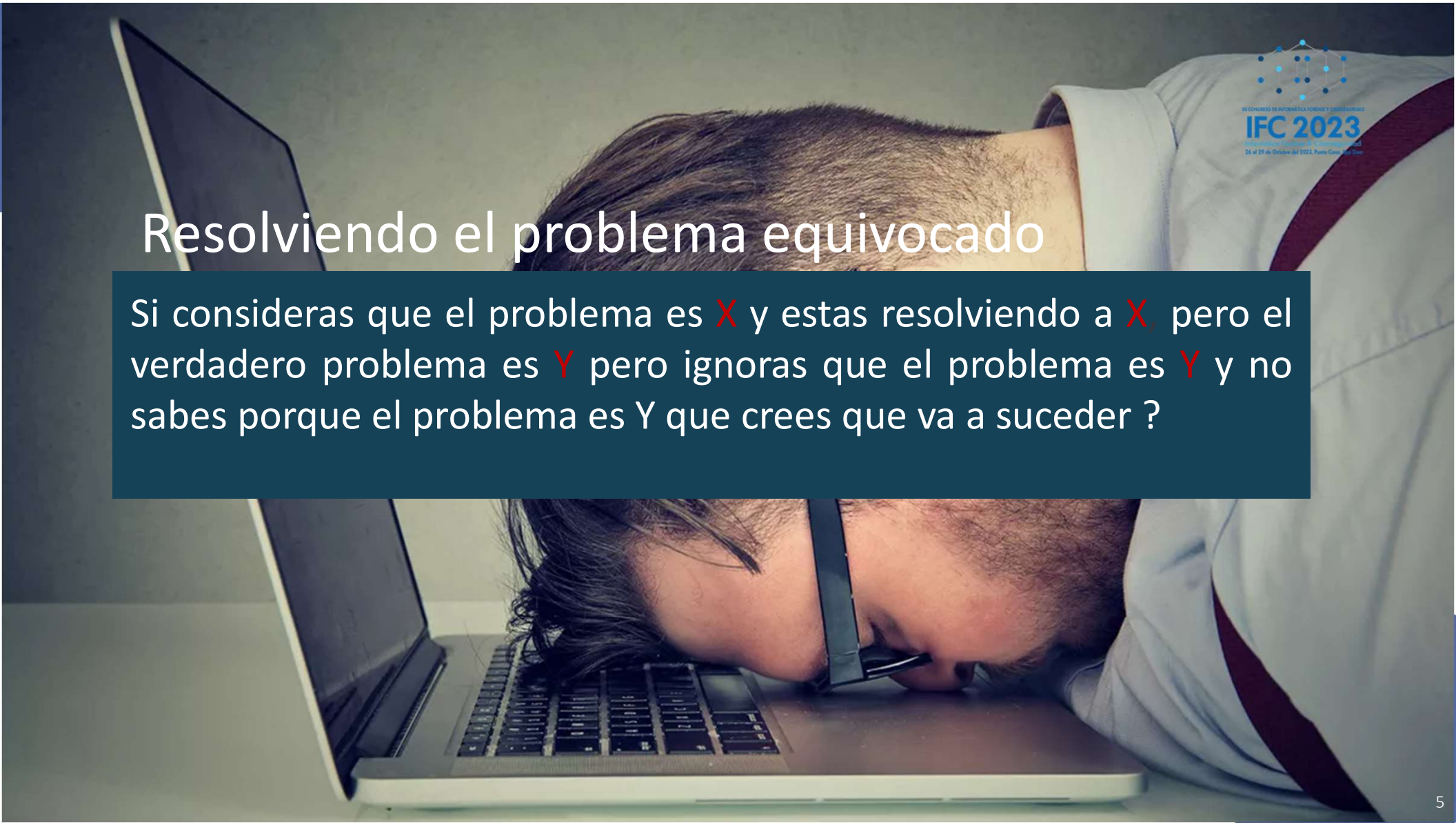
"Si la *seguridad fuera lo único importante*, los **computadores nunca se encenderían**, y *mucho menos se conectarían a una red con, literalmente, millones de intrusos potenciales*".

Dan Farmer
Distinguished Engineer @Mercedes-Benz R&D

Existe un problema fundamental en las organizaciones, NO SABEMOS QUE ES CIBERSEGURIDAD.

Estas son sus caras en este momento





Resolviendo el problema equivocado

Si consideras que el problema es X y estas resolviendo a X, pero el verdadero problema es Y pero ignoras que el problema es Y y no sabes porque el problema es Y que crees que va a suceder ?

Hay una solución pero …

LA CIBERSEGURIDAD ES UN PROBLEMA DEL NEGOCIO

Cybersecurity is not a technical problem, it is a bussines problem, cybersecurity doesn't get fixed by buying firewalls IDS's and IPS's.

If that was true, every organization would be secure.

DR. ERICK COLE

LA CIBERSEGURIDAD ES UN PROBLEMA DEL NEGOCIO

Hasta que no tratemos la Ciberseguridad como un problema del negocio vamos a fallar terriblemente.

Que es Ciber Seguridad?

Se define como la “protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

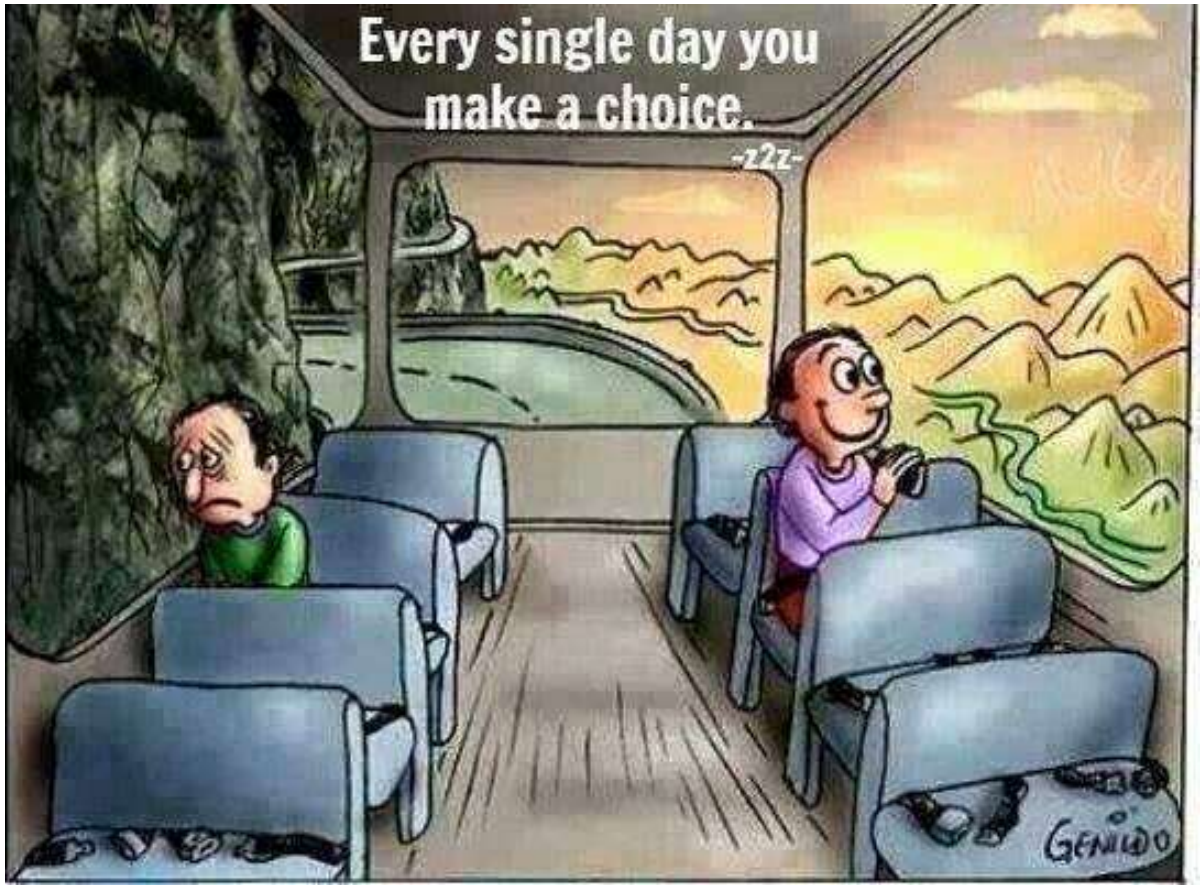
Que es Ciber Seguridad?

La Ciberseguridad es el ejercicio de comprender, gestionar y mitigar los riesgos asociados a tus activos críticos, evitando que la información sea divulgada, alterada o se niegue su acceso.

En que consiste la Ciber seguridad?

Consiste en disminuir el atractivo para el atacante reduciendo las vulnerabilidades, aprendiendo de sus metodos y resolviendo los incidentes dentro de los limites de la capacidad de la organización.

Cual es el secreto de la felicidad ~~En Ciber~~?



Vas a tener que entender el riesgo

"... los métodos "convencionales" de análisis de riesgos (es decir, los que se basan en un análisis de amenazas y vulnerabilidades) *no funcionan en el ciberespacio*, principalmente *porque los conjuntos de amenazas y vulnerabilidades son abrumadoramente grandes* y el sistema a proteger, es decir, una infraestructura informática, *es excesivamente compleja*".

Rolf Oppliger & Andreas Gruner, 2023

Tomado de: Oppliger, R. & Grunert, A. (2023). How to Manage Cyber Risks: Lessons Learned From Medical Science. *IEEE Computer*. 56(1). pp. 117-119. doi: 10.1109/MC.2022.3218387

Vas a tener que entender el riesgo

> No es lo mismo una organización que cumple con lo que las buenas prácticas y estándares predican para asegurar la "tranquilidad de la empresa y sus procesos" (así como la necesidad de certezas de sus ejecutivos", a una que comprende que *el reto no está en la protección y aseguramiento de aquello que se conoce, sino en la capacidad de minimizar los impactos de los riesgos latentes y emergentes, y cómo se encuentra preparada para recuperarse rápidamente con el mínimo daño, costo e impacto en la reputación en caso de que se produzca esa situación* (Milică & Pearlson, 2023).

Cumplimiento (CUMPLO y MIENTO)

When you hear "best practices," run for your lives. The Titanic was built with best practices. It was faithfully operated in accordance with best practices.

- Retired US Army Colonel Gregory Fontenot, Director of the University of Foreign Military and Cultural Studies (Red Team University), 2011

Vas a tener que entender el riesgo

Riesgo TI Vs Riesgo Cibernético

	Riesgo TI	*Riesgo Cibernético*
Fundamento:	Reducción de costos	*Apetito de riesgo*
Foco:	Operación/Procesos	*Negocio/promesa de valor*
Tipo:	Conocido	*Sistémico*
Gestión:	Estándares y prácticas	*Capacidades y patrones*
Basado en:	Continuidad del negocio	*Resiliencia del negocio*
Estrategia:	Mitigación	*Umbrales de operación*
Objetivo:	Proteger y asegurar	*Defender y anticipar*

Hacer las preguntas claves

Junta Directiva

- ¿Qué tipo de ataques se están produciendo y si se ha establecido un marco adecuado de atención de riesgos cibernéticos?
- ¿Cómo se alinea el programa y capacidades de ciberseguridad con los estándares de la industria y las organizaciones del sector?
- ¿Qué ha hecho la dirección para proteger a la organización contra los riesgos cibernéticos de terceros?
- ¿Es posible contener rápidamente los daños y movilizar diversos recursos de respuesta en caso de que se produzca un ciberincidente?
- ¿Cómo se evalúa la eficacia del programa de ciberseguridad de la organización?

Equipo Ejecutivo

- ¿Cuál es el nivel de madurez de la organización en la gestión del riesgo cibernético?
- ¿La inversiones que hemos hecho aumentan la resiliencia del negocio frente a eventos cibernéticos?
- ¿La priorización de amenazas corresponde a la nivel de madurez en la gestión del riesgo cibernético?
- ¿Sabemos el tiempo de inactividad de los sistemas críticos y el tiempo de recuperación ante eventos adversos?
- ¿Conocemos el nivel de higiene cibernética que tiene la organización (empleados y terceros de confianza)?

Partes interesadas

- ¿Cómo podemos evitar convertirnos en el próximo titular?
- ¿Estamos abordando las vulnerabilidades y amenazas clave?
- ¿Cuál es el impacto potencial para la empresa si no se abordan estos riesgos?
- ¿Cómo construyo un caso de negocio sobre los riesgos potenciales?
- ¿Qué capacidades requerimos para hacernos más resistentes a los ataques?

Vas a tener que aceptar el riesgo

"*Sin riesgo no hay negocio*, y quien *no se atreve a asumir la incertidumbre* o su *cuota razonable de riesgo* nunca triunfará en la actividad profesional".

Soto, E. & Cárdenas, J. (2007). *Ética en las organizaciones*. México, D.F., México: McGraw Hill Interamericana Editores. P. 21.

Vas a tener que gestionar el riesgo

"*Sin riesgo no hay negocio*, y quien *no se atreve a asumir la incertidumbre* o su *cuota razonable de riesgo* nunca triunfará en la actividad profesional".

Soto, E. & Cárdenas, J. (2007). *Ética en las organizaciones*. México, D.F., México: McGraw Hill Interamericana Editores. P. 21.

Vas a tener que aprender tu rol

1. Estamos resolviendo el problema equivocado
2. No comprendemos el riesgo
3. Abordamos la ciberseguridad como un tema técnico

La Ciberseguridad consiste en asegurarnos que las organizaciones entiendan y acepten riesgos.

“Si crees que la tecnología puede solventar tus problemas de seguridad, entonces no entiendes los problemas y no entiendes de tecnología”

- Bruce Schneier


Bye