Above Compliance

Cómo aprovechar las regulaciones de ciberseguridad como herramientas de gobierno y gestión de riesgos.

Jorge Litvin

NUESTRO CONTRATO

Esta charla será exitosa si al finalizar pueden identificar qué tenemos que cambiar para pasar de gestionar ~~controles~~ a gestionar *riesgos*.

¿Qué tienen en común estas marcas?

Microsoft

Google

OpenAI

solarwinds

CROWDSTRIKE

Meta

El piso ya existe.
La pregunta es qué *hacemos con él.*

01 **Ley Marco de Ciberseguridad**

02 **Ley de Protección de Datos Personales**

03 **NCG 514 · Sistema de Finanzas Abiertas**

ISO NIST PCI

AICPA SOC 2 aicpa.org/soc4so SOC for Service Organizations

HIPAA Health Insurance Portability and Accountability Act

>safe/. u/*]]

Cumplir no es lo mismo que *gestionar*.

CUMPLIR

Pasar la auditoría.

Seguir los requisitos, evitar la sanción, demostrar en el papel que los controles existen.

GESTIONAR

Decidir sobre el riesgo.

Identificar los riesgos propios, decidir cómo tratarlos, construir criterio. Protegerse en la realidad.

GRC: Un sistema malinterpretado.

Riesgo

Datos para tomar decisiones

Gobierno

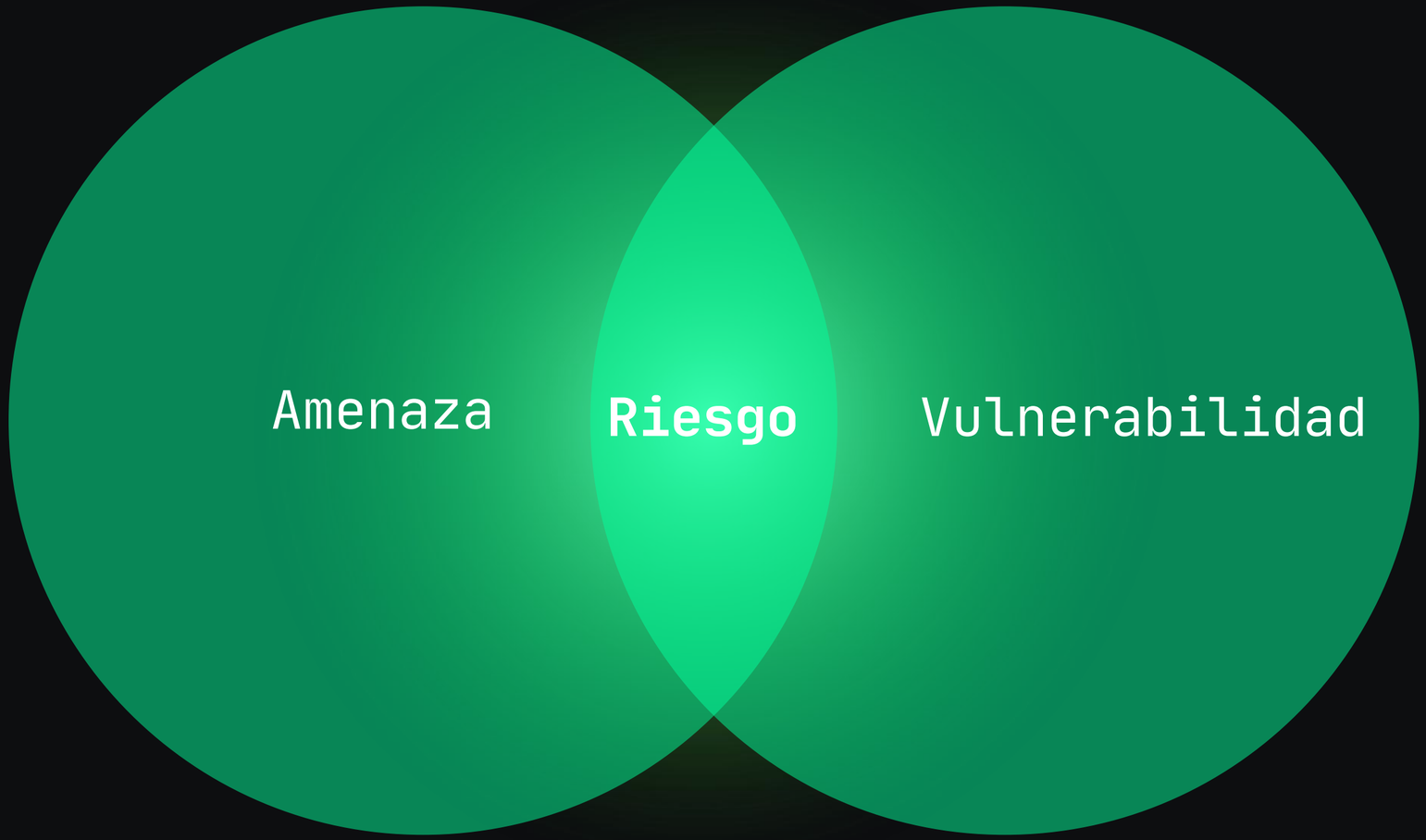
Proceso para tomar decisiones

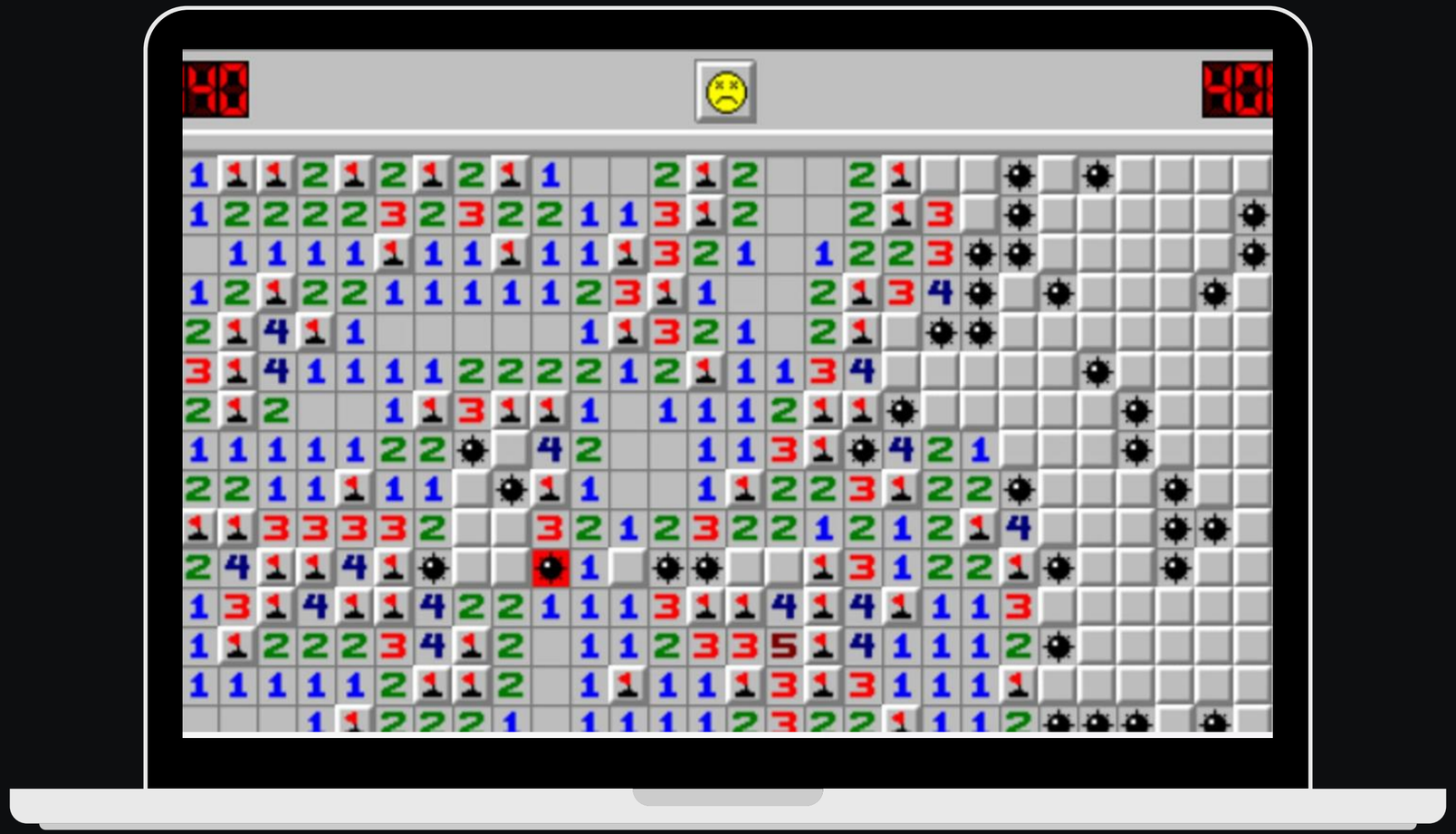
Cumplimiento

Evidencia de decisiones

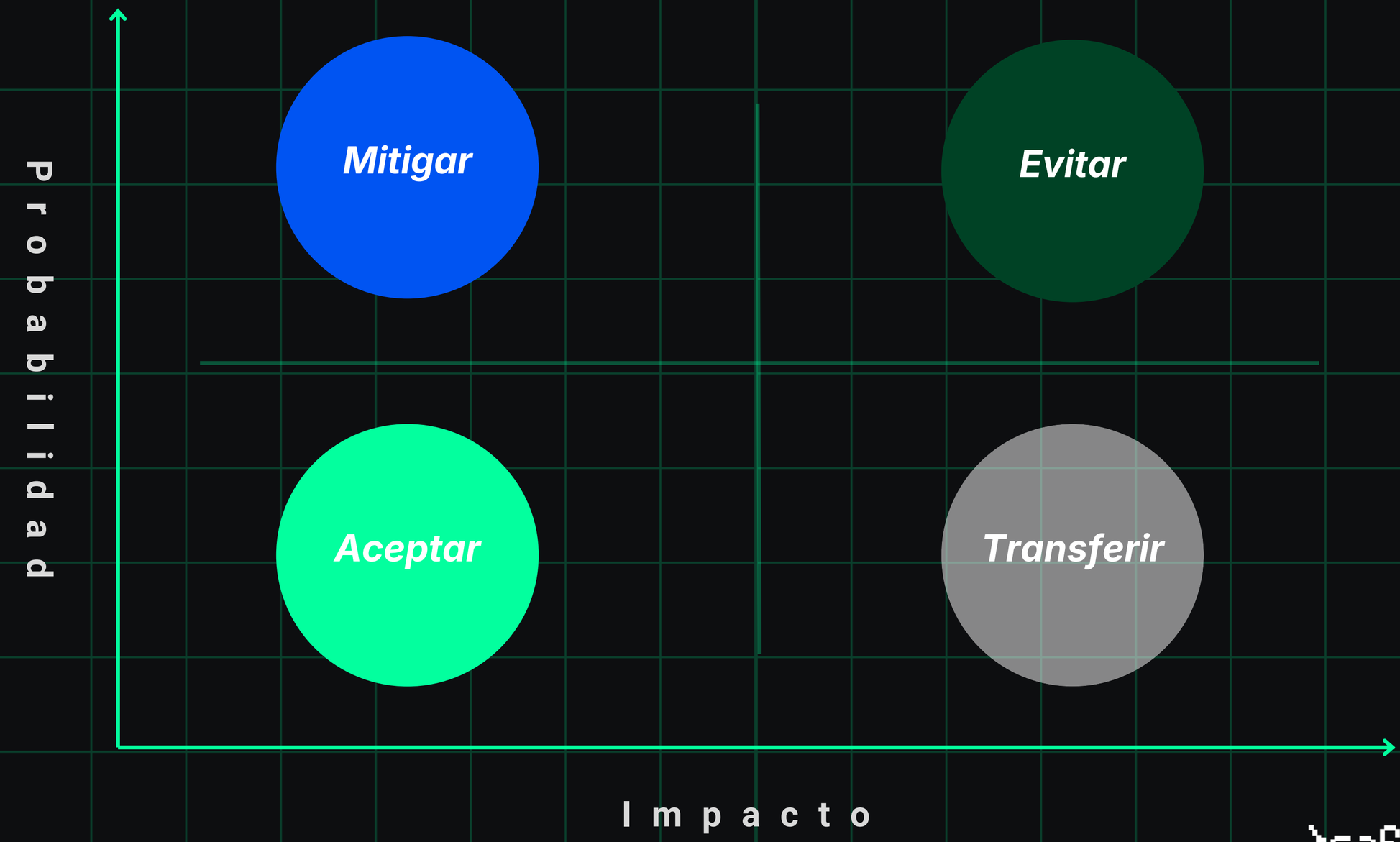
El **riesgo** no se evita.
Se ***gestiona***.

</Qué es un Riesgo>


Amenaza
Riesgo
Vulnerabilidad



>safe/. u/*]]


Mitigar
Evitar
Aceptar
Transferir
Probabilidad
Impacto

El gobierno del riesgo cibernético le pertenece a la *dirección*.

DIRECTORIO	**Responsable del riesgo cibernético**
C-SUITE	**Operacionaliza la decisión**
CISO & IT	**Ejecuta y reporta**
Y el resto?	

NCG 514 · CMF

Establece **explícitamente** la responsabilidad del Directorio sobre la gestión de riesgos y la ciberseguridad.

Gobernar requiere tres cosas. Solo una es *tecnología* — y no es la principal.

Políticas

Las reglas del juego, documentadas y conocidas por todos.

Cultura

De riesgos y de ciberseguridad

Decisiones

El criterio de gestion de riesgos

85%

menos incidentes cuando el CEO toma decisiones basadas en datos de riesgo correctamente informados.

FUENTE — MIT ESTUDIO CAMS

Compliance

El piso que habilita confianza.

>safe/. u/*]]

</cumplimiento>

Las regulaciones no son la mala de la película.
Son el *punto de partida* más ordenado que alguien nos ofreció.

>safe/. u/*]]

El cumplimiento ya no le rinde cuentas *solo al regulador.*

CLIENTES	Miden tu postura de seguridad antes de firmar.
PARTNERS	Revisan tu perfil de riesgo antes de integrarse.
INVERSORES	Leen tu gobierno de riesgos antes de invertir o definir el monto.

Cumplir abre puertas. No cumplir las cierra.

>safe/. u/*]]

TAKEAWAYS

No podemos decidir sobre lo que no conocemos

El rol de riesgos es proveer la información suficiente para tomar decisiones con criterio

El gobierno se ve reflejado en la cultura, el involucramiento trasversal y las decisiones

El cumplimiento es el piso, no el techo. Es además un habilitador del crecimiento.

Lo que tenemos que demostrar no es seguridad, es *criterio*.

safe-u.com

JORGE LITVIN

>safe/. u/*]]