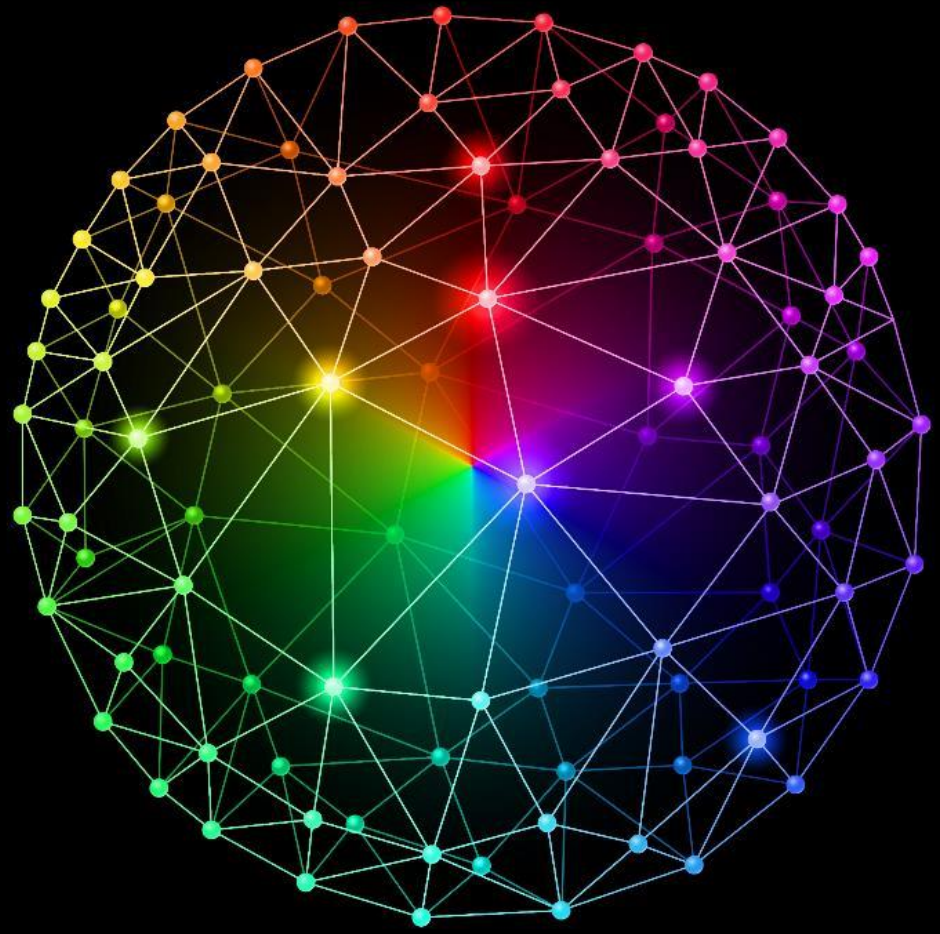
Deloitte.



# Comprometidos con su seguridad

## Presentación: Prácticas de Seguridad y Compartiendo Información

Julio 23, 2018

# Antecedentes – Nos encontramos en desventaja.

## El cibercrimen se ha vuelto una industria muy lucrativa.

**Sin límites físicos y Sin Fronteras:** El Ciberespacio no tiene fronteras. El enemigo no tiene que pertenecer a un país, solo ser parte de un grupo con igualdad de pensamiento.

**7*24*365:** El ataque puede ser ejecutado en cualquier momento del día, lo que lo vuelve difícil de predecir.

**Fácil y económico de organizar:** Se requiere un par de computadoras con acceso a internet para iniciar una guerra cibernética, se utilizan herramientas públicas y fácil de operar.

**Sin presencia física:** No se requiere entrar a las instalaciones de una empresa o un país, solo se requiere entrar a los sistemas.

**Difícil de detectar y Rastrear**: Si el ataque es bien planeado será difícil detectar el origen y quien es el responsable. Se puede lanzar una ataque haciendo creer que es de alguien más

# Antecedentes

## ¿Por qué necesito una práctica CiberSeguridad?

1. **"La seguridad de la información es un tema del negocio" CEO**
2. **…"Me preocupa no saber lo que tengo que saber"… CIO**
3. **.."Hoy no es cuestión de si me van a comprometer la seguridad, la pregunta es ¿cuándo va a suceder?"…CISO**

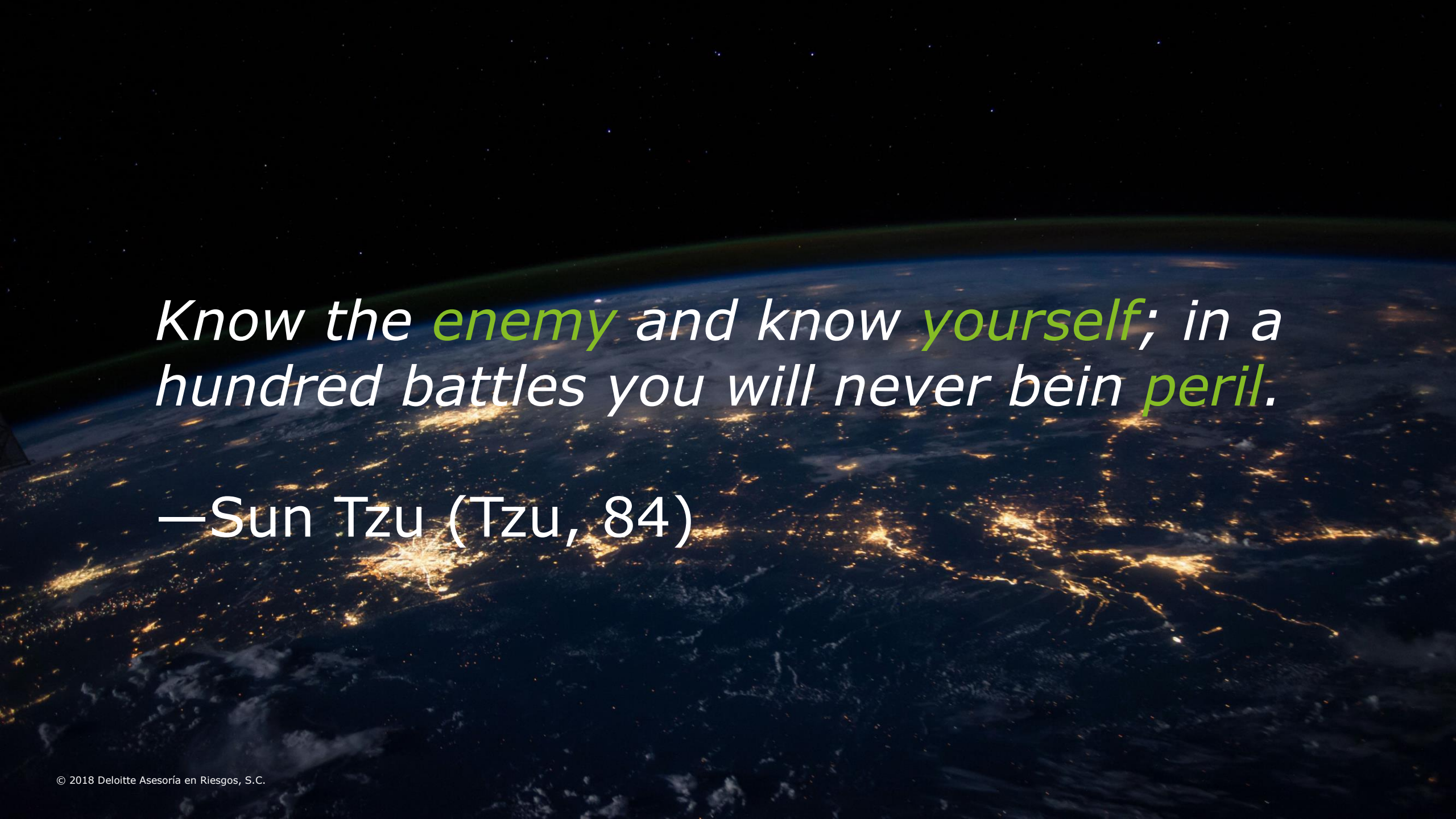
*** Joyas de la corona: Activos críticos (información sensible)**

En el contexto de negocios actual, las organizaciones están siendo cada vez más blanco de distintos tipos de amenazas que atentan contra sus "**joyas de la corona**". Entre algunas de estas ciberamenazas que están causando daños se encuentran:

1) ***Robo de Información.***
2) ***Daño Reputacional.***
3) ***Fraudes.***
4) ***Caída de servicios***.

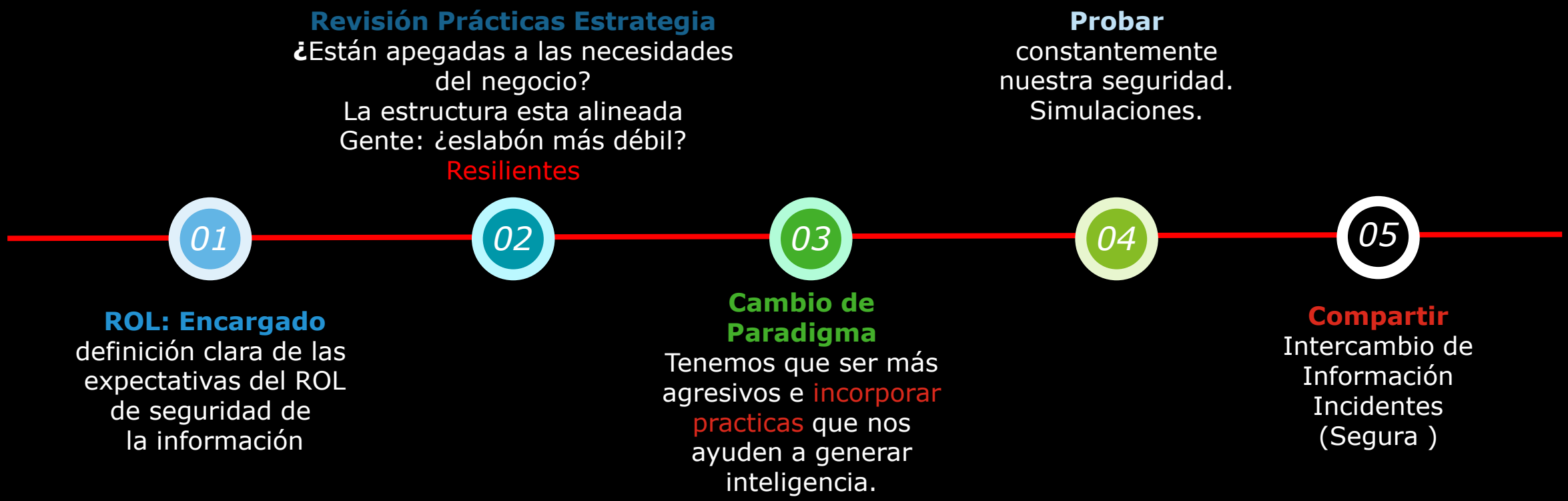
Los directivos de las organizaciones requieren contestar preguntas como: *¿Estoy expuesto a estas ciber amenazas?, ¿Tengo capacidad de anticiparme ante estos eventos?, ¿Tengo los controles alineados y requeridos por mi negocio?, ¿Estoy detectando oportunamente los incidentes?.*

Es a través de la implementación de un programa de CiberSeguridad, alineado al apetito de riesgo de la organización y las ciber amenazas de la industria, que los directivos podrán dar respuesta a las preguntas mencionadas.

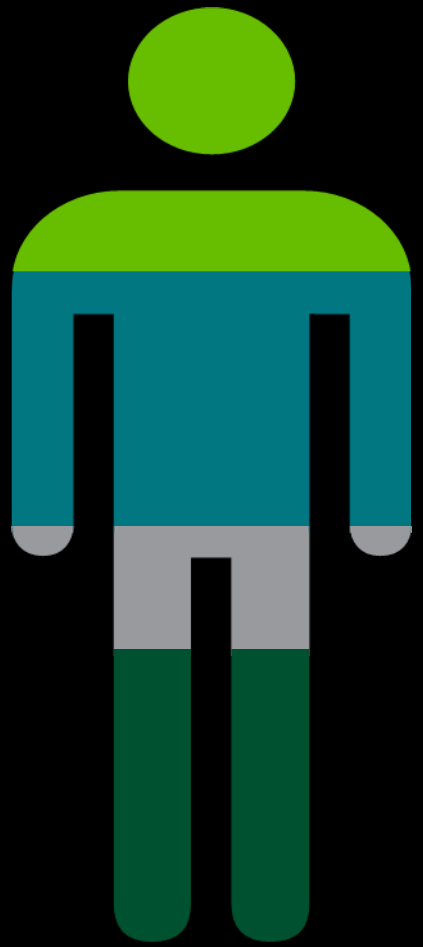


# Prácticas

## 5- Recomendaciones para mejorar la postura en ciberseguridad



# Perfil del Responsable de Seguridad



## 32% - Estratégico

Liderar la alineación de las necesidades de ciber seguridad con el negocio.
**Priorización.**

## 35% - Asesor

Estar integrado con el negocio para poder asesorar, educar e influenciar en las actividades que tienen que ver con ciberriesgos.
**Concientización.**

## 12% - Tecnológico

Evaluar e implementar arquitecturas de seguridad (Gente-Proceso-Tecnología) que contengan los controles adecuados orientados a mitigar los riesgos identificados.
**Arquitecturas de Seguridad Resilientes.**

## 22% - Guardián

Llevar a cabo el correcto monitoreo de la efectividad del programa de ciber seguridad, controles y procesos con la finalidad de proteger la confidencialidad, integridad y disponibilidad (resiliencia) de la información.
**Contar con Indicadores.**

# Alineación
## Construir organizaciones cyber resilentes (I)

El Common Store Front (CSF) de Deloitte incorpora una metodología probada que se encarga de evaluar la capacidad de recuperación de una organización, focalizándose en:

- Paquetes de contenidos que nos permitan llevar a cabo evaluaciones con respecto a normas específicas.
- Plataformas online que incorporan de forma automática una gama de cuadros de mando que se pueden personalizar alcanzando un público tanto ejecutivo, gerencial como operacional.

**Tres factores fundamentales que impulsan el crecimiento y generan cyber riesgos:**

**INNOVACIÓN**

**INTERCAMBIO DE INFORMACIÓN**

**CONFIANZA ENTRE COMPAÑEROS**

**CEO**
"He leído sobre suplantación de identidad en la prensa. ¿Supone un riesgo para nosotros?"

**CIO**
"¿Dónde y cuánto tengo que invertir para optimizar mis cyber habilidades?"

**Junta Directiva**
"¿Cuál es nuestro nivel de resiliencia contra los cyber ataques?"

**Las organizaciones necesitan un enfoque holístico, basado en las amenazas e impulsados por las empresas para poder gestionar los cyber riesgos. Así como la seguridad de los activos es fundamental, vigilar y ser resiliente a la hora de enfrentarse a los cyber ataques es imperativo.**

**RIESGOS DE NEGOCIO**

- ¿Cuál es mi **estrategia de negocio?**
- ¿Cuál es mi **interés en los riesgos?**
- ¿Cuáles son mi ***Crown Jewels?***

**EL CONTEXTO DE LA AMENAZA**

- ¿Qué tácticas utilizarán?
- ¿En qué están interesados?
- ¿Quiénes son mis adversarios?

**CYBER HABILIDADES**

**Strategy**

Identificar los riesgos más importantes y desarrollar un programa de cyber riesgo dirigido por ejecutivos.

**Secure**

Adoptar un enfoque mediante el que se prioricen los riesgos con el objetivo de establecer una sólida defensa contra las amenazas tanto conocidas como emergentes.

**Vigilant**

Desarrollar una conciencia e inteligencia vinculada a amenazas para identificar acciones potencialmente peligrosas para la organización.

**Resilient**

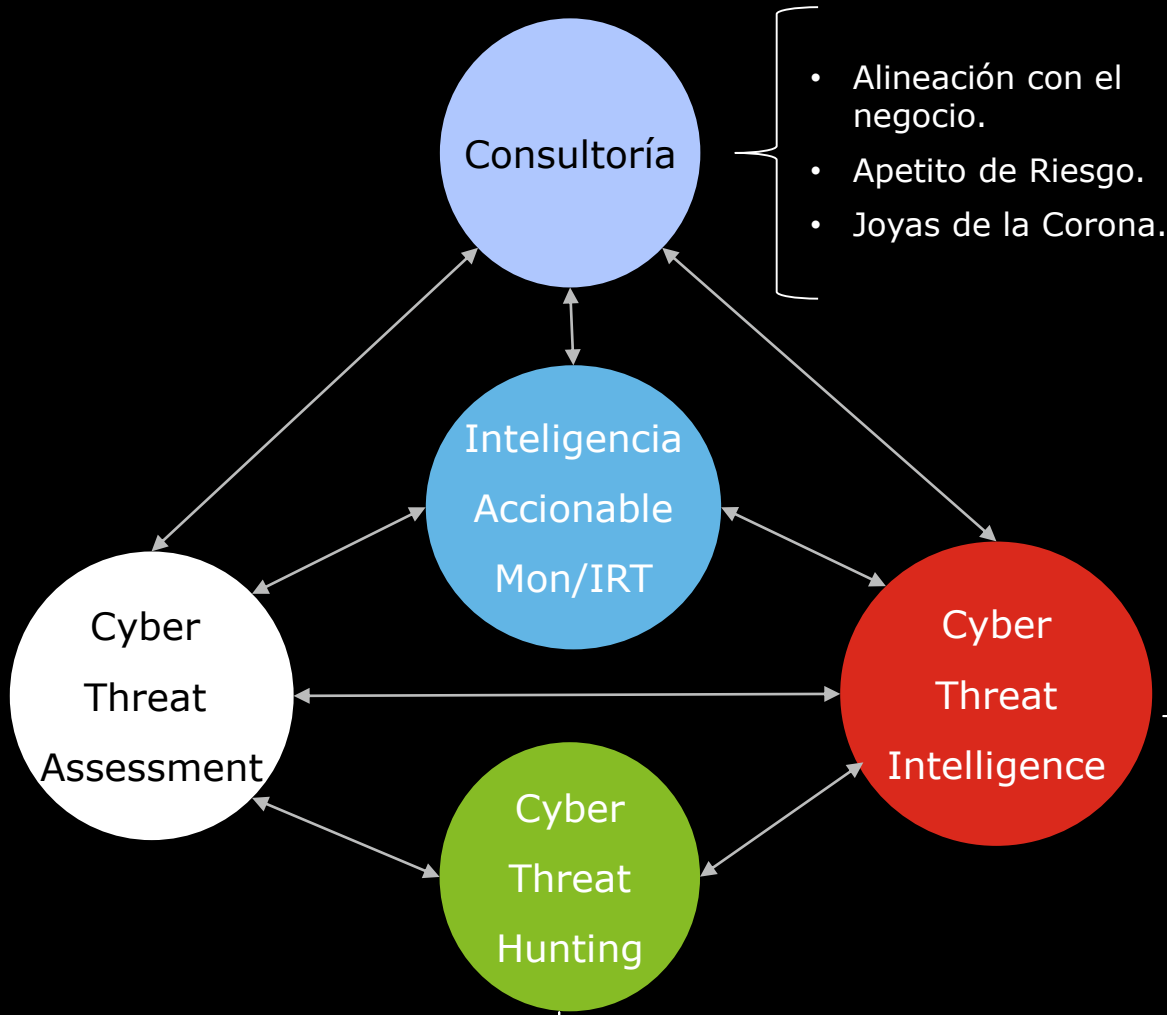
Desarrollar la habilidad de reponerse ante los cyber incidentes, así como de minimizar el impacto de los mismos.

Un programa de cyber riesgo sólido impulsa el crecimiento y ayuda a los ejecutivos a estar en el top de las cyber amenazas

1. Entender el contexto de negocio y los objetivos
2. Comprender el contexto de las amenazas
3. Adquirir un profundo nivel de madurez relacionado con las cyber habilidades
4. Centrarse en las prioridades correctas
5. Definir el nivel de madurez de las cyber habilidades
6. Desarrollar la hoja de ruta de la cyber estrategia
7. Potenciar el valor de las inversiones en ciberseguridad
8. Comunicarse con *stakeholders* internos y externos

# Enfoque Actual

Se requiere de la integración de nuevas prácticas que ayuden en la generación de inteligencia y búsqueda constante de intrusiones.




- Alineación con el negocio.
- Apetito de Riesgo.
- Joyas de la Corona.

- Aplicación de técnicas de intrusión para la Identificación de amenazas y generación de Inteligencias.
  * Aprender del enemigo.
  * Simulaciones

- Creación de inteligencia de amenazas
  - IoC
  - Información focalizada a la industria

- Búsqueda de Indicadores de compromiso

# Proceso de inteligencia
## Generación, compartición y consumo

MISP tiene la finalidad de generar desarrollo y habilitación de procesos de consumo para la creación de inteligencia.

### Generación

- Determinar los **requerimientos de inteligencia** de la organización
- **Analizar** la información interna
- **Enriquecer** la información
- **Validar** la información
- **Almacenar** la información
- **Compartir** la información

### Compartición


**Intercambio de Información**

### Consumo

- **Consumo a nivel estratégico**

Entendimiento a la dirección del ambiente de amenazas que permitan identificar riesgos y cambios en términos de inversión para mitigar dichos riesgos.

- **Consumo a nivel Operacional**

Traducir los objetivos estratégicos en tácticos y viceversa mediante el entendimiento de campañas y tendencias.

- **Consumo a nivel táctico**

Consumo de inteligencia a nivel de IOCs (indicadores de compromiso) y TTPS (Tactics, Techniques and Procedures) que permitan la identificación y respuesta ante amenazas.

# Malware information sharing platform
## Características principales

### Almacenamiento estructurado

MISP nos provee de la capacidad de almacenar IOCs de una manera estructurada, que nos permita realizar correlación y exportaciones automatizadas para el IDS, SIEM y otros sistemas mediante el uso de formatos como STIX u Open IOC. Podemos apalancar el valor de información de valor con un menor esfuerzo y de manera automatizada

### Simplicidad

El principal objetivo del MISP es ser amigable para el usuario. Esta es la razón por la cual simplicidad es la fuerza impulsora del proyecto. Almacenar y usar la información sobre amenazas y malware no debe ser difícil. MISP está para que nosotros y nuestros cliente puedan obtener el máximo provecho de los datos sin que sea complejo

### Compartición

Compartir es clave para garantizar la detección rápida y efectiva de ataques. Frecuentemente organizaciones similares son atacadas por el mismo agente amenaza independientemente de si forman parte o no de la misma campaña. MISP está diseñado para facilitar este proceso. Compartir también permite el análisis colaborativo y evita que se repita el trabajo realizado por alguien más.

### Estándar de industrias

Cada vez más organizaciones utilizan MISP para almacenar y compartir IOCs y ha ganado la confianza entre las organizaciones de inteligencia de amenazas, incluyendo Deloitte.

Deloitte.