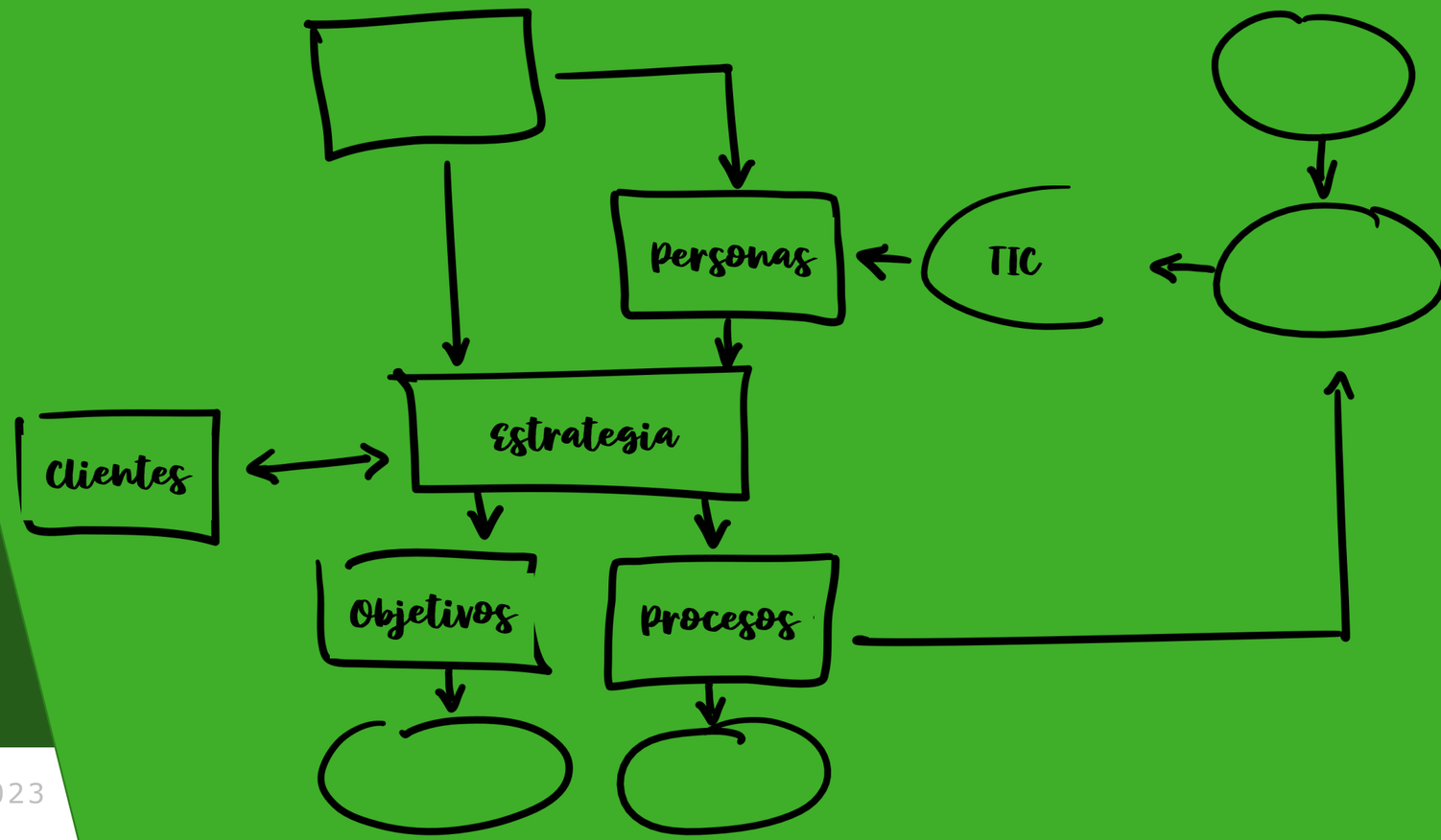
La gestión por procesos clave para la gestión del riesgo operacional y de ciberseguridad



Noviembre de 2023

corus
CONSULTING

PROCESOS Y RIESGO OPERACIONAL

Riesgo operacional

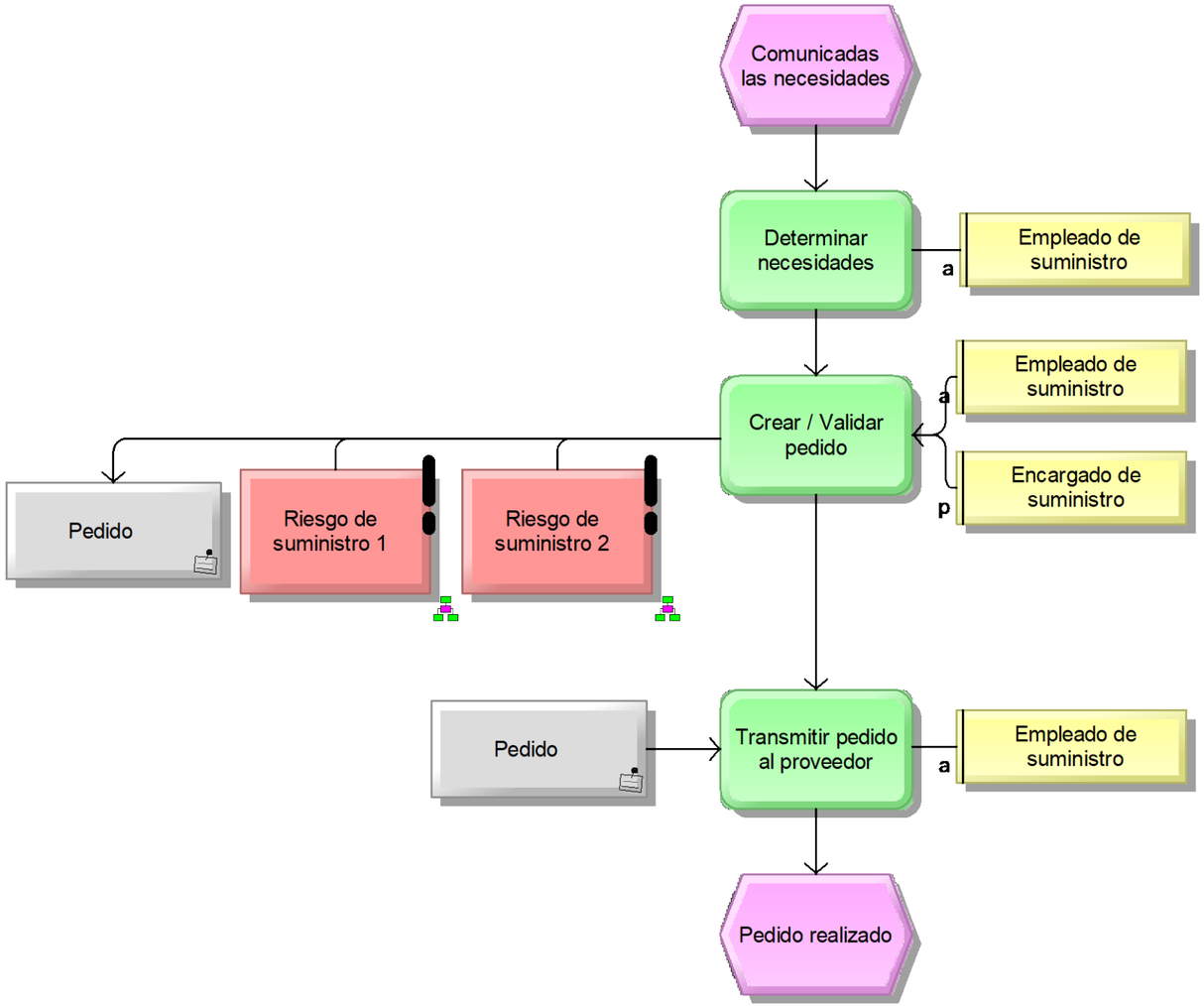
“Su tarjeta de crédito es correcta.

Solo me queda validar que su banco no haya expirado”

La Gestión de los Procesos de Negocio es la disciplina que consigue que el rendimiento excepcional de las organizaciones sea una cuestión de diseño y no de suerte.

Michael Hammer - “The Agenda”

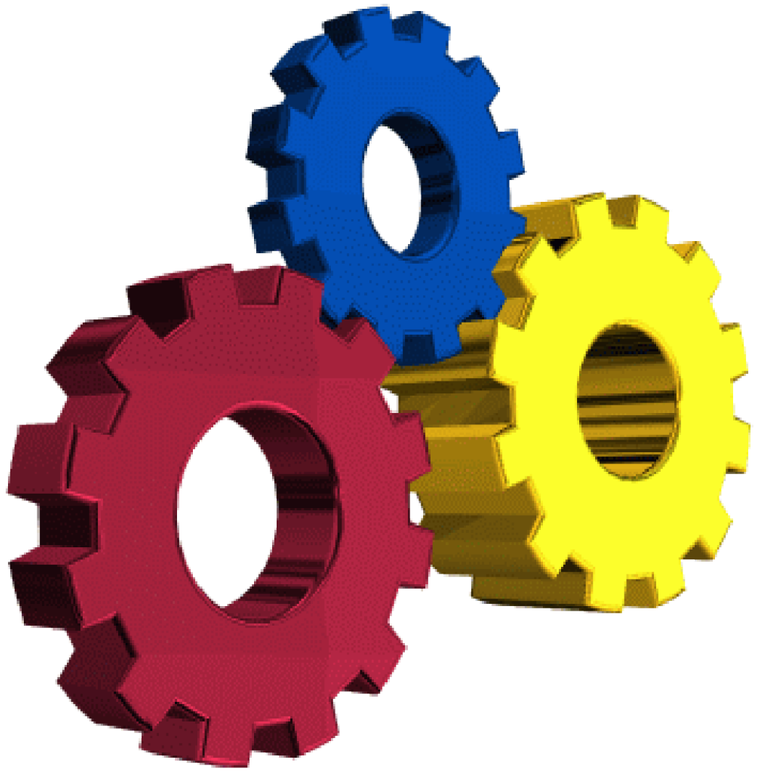
Riesgo operacional



Riesgo operacional es aquel que puede provocar pérdidas como consecuencia de procesos internos, recursos humanos o sistemas inadecuados o defectuosos, o por causas externas

Riesgo operacional

Económico



Social

Misión

Causas del riesgo operacional

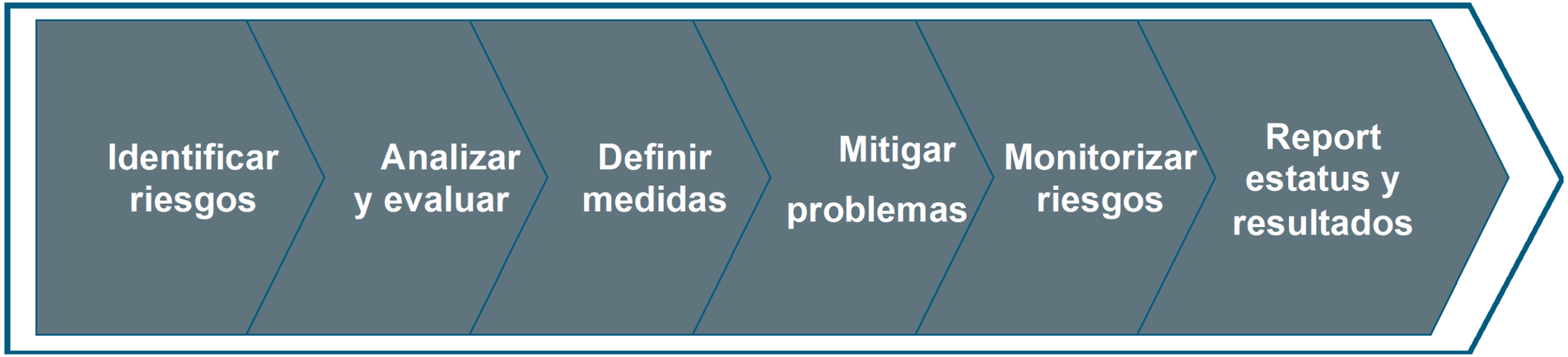
Tipologías:

- Riesgo operacional intrínseco
  - Recursos Humanos, volumen de transacciones, procesos manuales, tecnología, desastres, etc.

- Riesgo residual
  - Seguridad física, seguridad lógica, segregación funcional, adecuación de aplicativos, contratos, cumplimiento normativo, etc.

Mitigación del riesgo operacional

Nuestras capacidades



Principales objetivos:

1. **Rendimiento**: El negocio funciona con eficiencia y eficacia.
2. **Información**: Confiabilidad, integridad y oportunidad de la información financiera y de gestión.
3. **Cumplimiento**: Leyes, regulaciones y políticas.

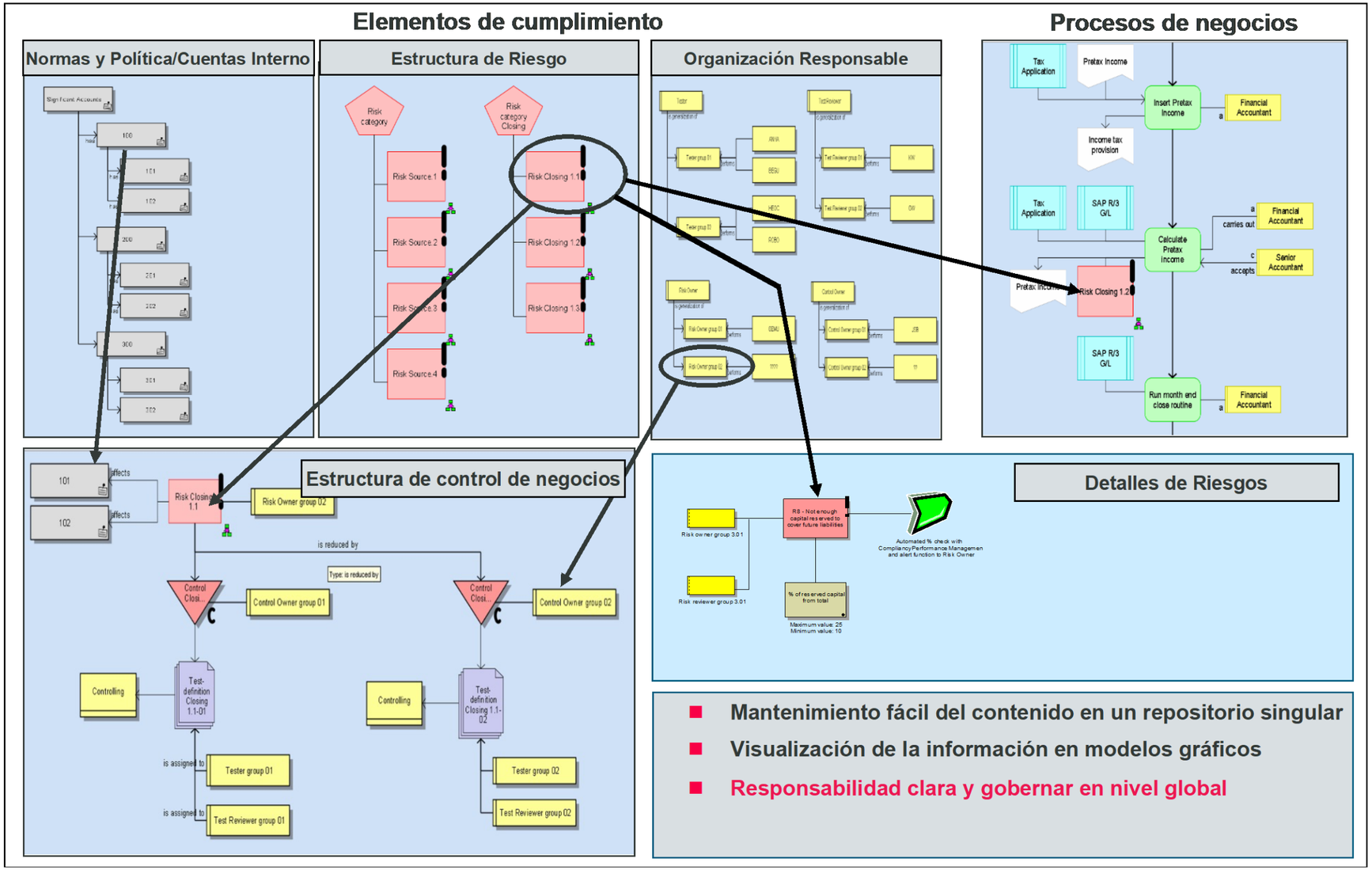
Control interno

Es un proceso que involucra a todos los integrantes de la organización sin excepción, diseñado para dar un grado razonable de apoyo en cuanto a la obtención de los objetivos en las siguientes categorías:

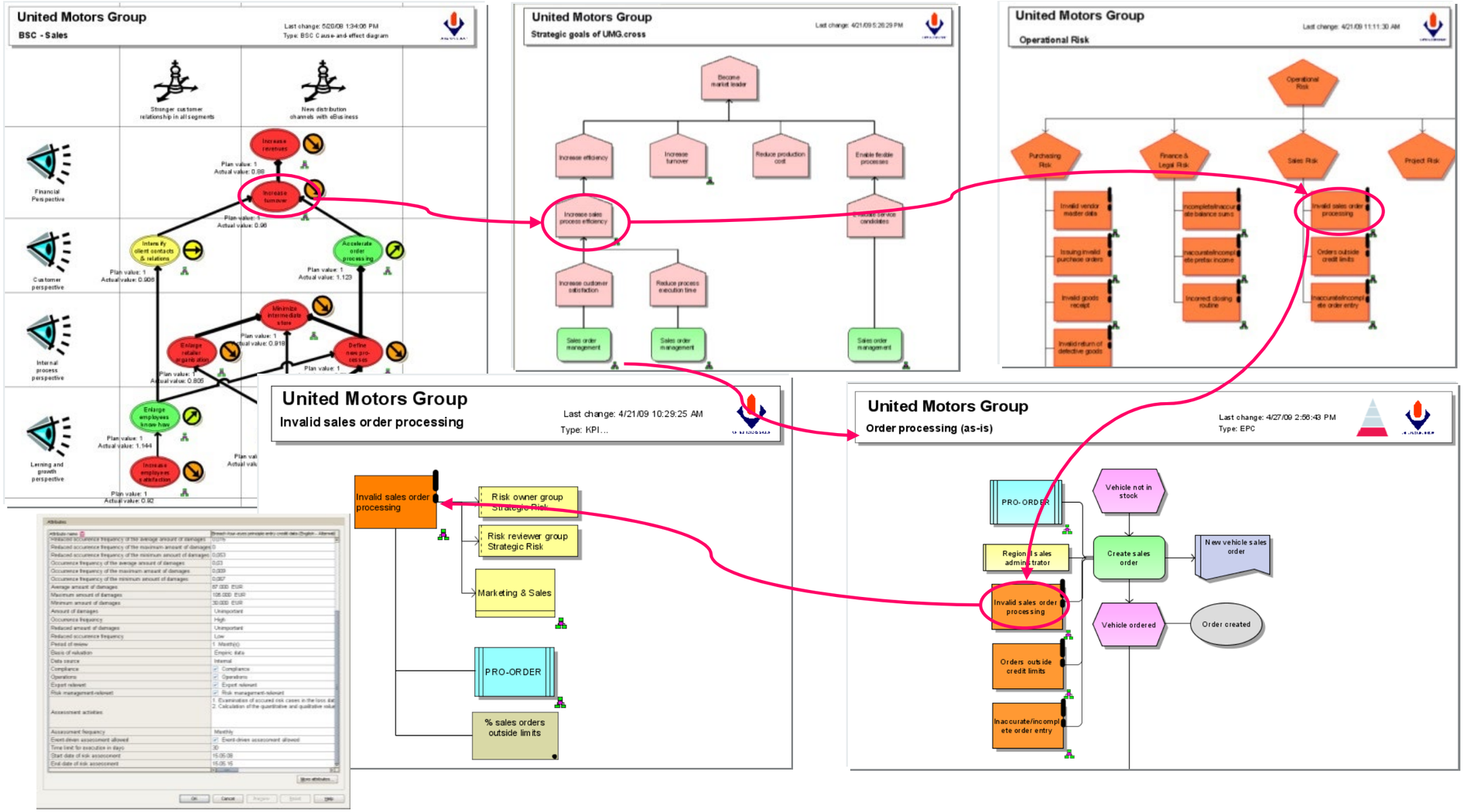
- Eficacia y eficiencia de las operaciones.
- Disminución del riesgo.
- Fiabilidad de la información financiera.
- Cumplimiento de las leyes y normas que son aplicables.

Estas categorías se interrelacionan entre sí.

Ecosistema del control interno



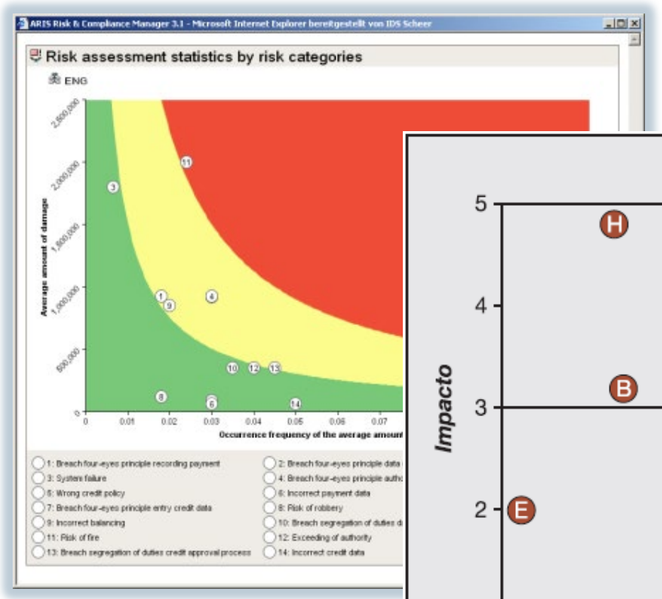
Evaluación de riesgos

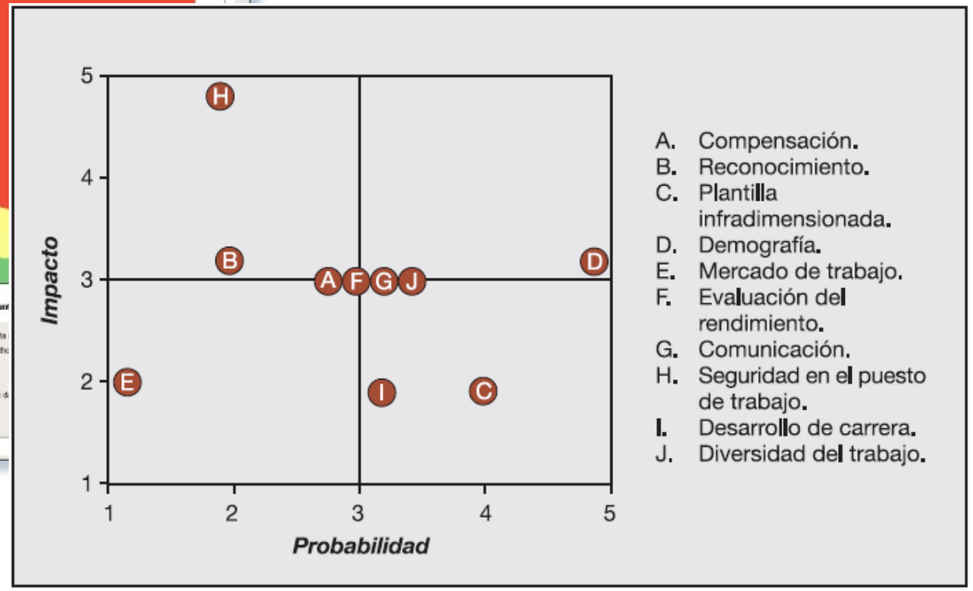


Evaluación del riesgo

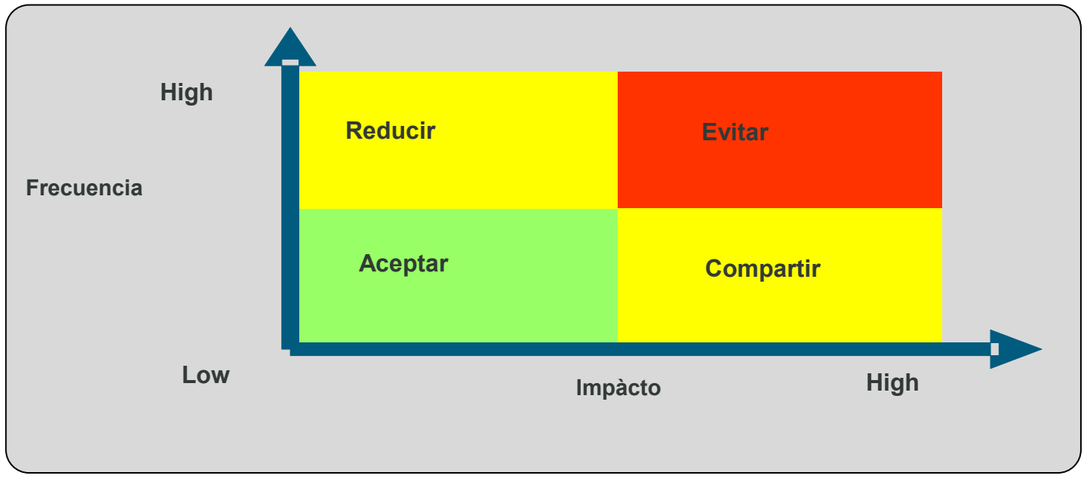
Una empresa evalúa los riesgos que afectan a su objetivo de mantener una plantilla de calidad. La probabilidad se considera en términos de porcentaje de rotación a lo largo de un determinado periodo y el impacto en términos del coste de ineficacia operativa y de sustitución, formación y desarrollo de los empleados. El código de color resalta los riesgos con una mayor probabilidad de materialización, así como aquellos con una mayor probabilidad de tener un efecto significativo en los objetivos.

	Tema	Descripción del riesgo	Probabilidad	Impacto
A	Compensación	La insatisfacción de los empleados con la compensación recibida conduce a un mayor índice de rotación de la plantilla.	Posible	Moderado
B	Reconocimiento	Los empleados no se sienten reconocidos, lo que supone una menor concentración en las tareas y tasas superiores de error	Improbable	Leve
C	Plantilla infra-dimensionada	Los empleados están utilizados en exceso y hacen un número considerable de horas extra. Los empleados se marchan a trabajar a otras organizaciones con un mejor equilibro entre la vida profesional y la personal.	Probable	Moderado
D	Demografía	El cambio en la composición demográfica del grupo de empleados provoca una mayor rotación.	Prácticamente seguro	Moderado
E	Mercado de trabajo	Aumento de la demanda de empleados de la empresa por parte de empresas de contratación.	Improbable	Moderado
F	Evaluación del rendimiento	La insatisfacción de los empleados con las medidas y procesos de evaluación del rendimiento provoca un descenso de la motivación, el enfoque hacia objetivos no críticos y la pérdida de personas que se van a empresas percibidas como preferidas.	Posible	Moderado
G	Comunicación	Una comunicación ineficiente entre los empleados y la dirección provoca la aparición de mensajes contradictorios y la búsqueda de un empleo alternativo.	Posible	Moderado



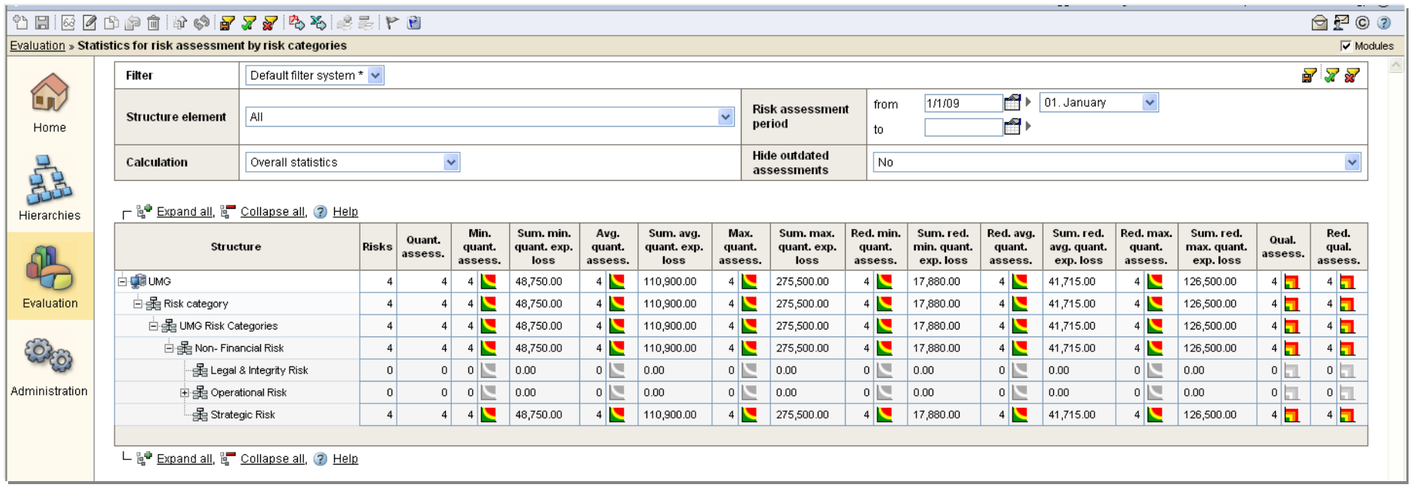


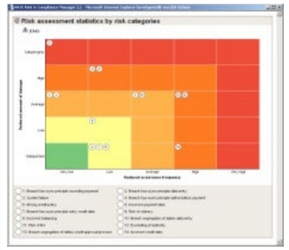
Respuesta a los riesgos

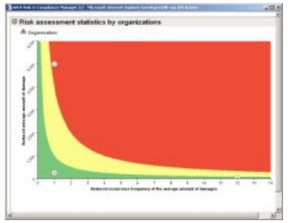


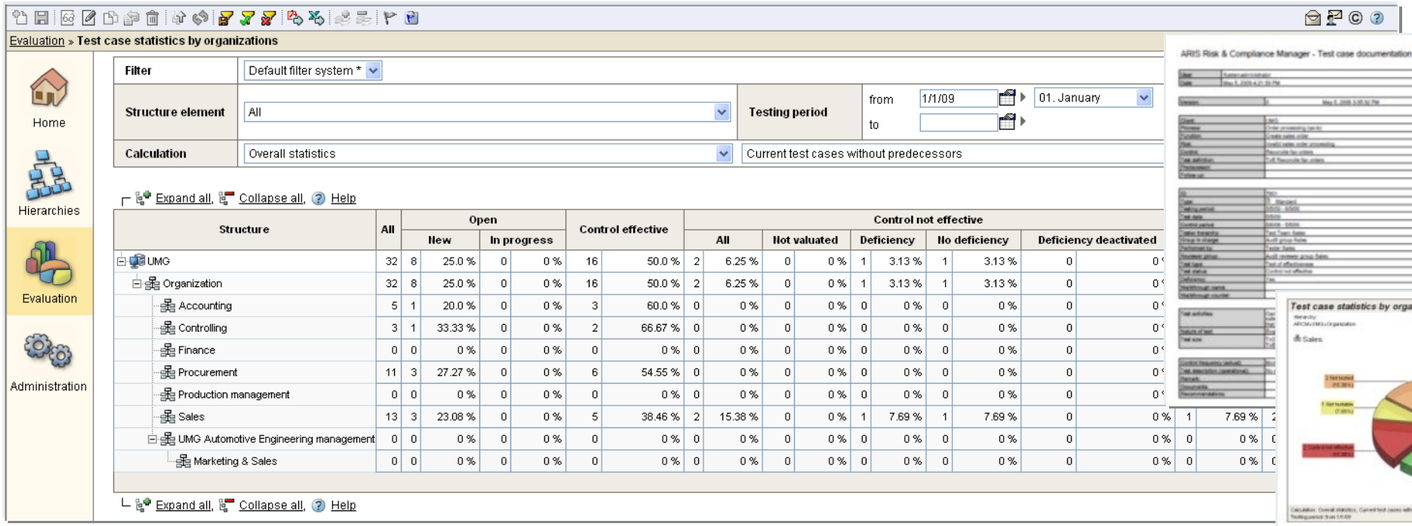
Evitar	Compartir
• Prescindir de una unidad de negocio, línea de producto o segmento geográfico. • Decidir no emprender nuevas iniciativas/actividades que podrían dar lugar a riesgos.	• Adoptar seguros contra pérdidas inesperadas significativas. • Entrar en una sociedad de capital riesgo/sociedad compartida. • Establecer acuerdos con otras empresas. • Protegerse contra los riesgos utilizando instrumentos del mercado de capital a largo plazo. • Externalizar procesos de negocio. • Distribuir el riesgo mediante acuerdos contractuales con clientes, proveedores u otros socios del negocio.
Reducir	**Aceptar**
• Diversificar las ofertas de productos. • Establecer límites operativos. • Establecer procesos de negocio eficaces. • Aumentar la implicación de la dirección en la toma de decisiones y el seguimiento. • Reequilibrar la cartera de activos para reducir el índice de riesgo con respecto a determinados tipos de pérdidas. • Reasignar el capital entre las unidades operativas.	• Provisionar las posibles pérdidas. • Confiar en las compensaciones naturales existentes dentro de una cartera. • Aceptar el riesgo si se adapta a las tolerancias al riesgo existentes.

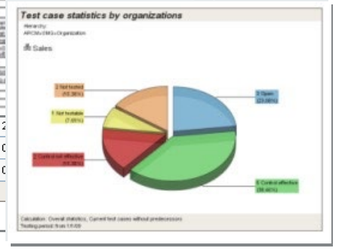
Supervisión









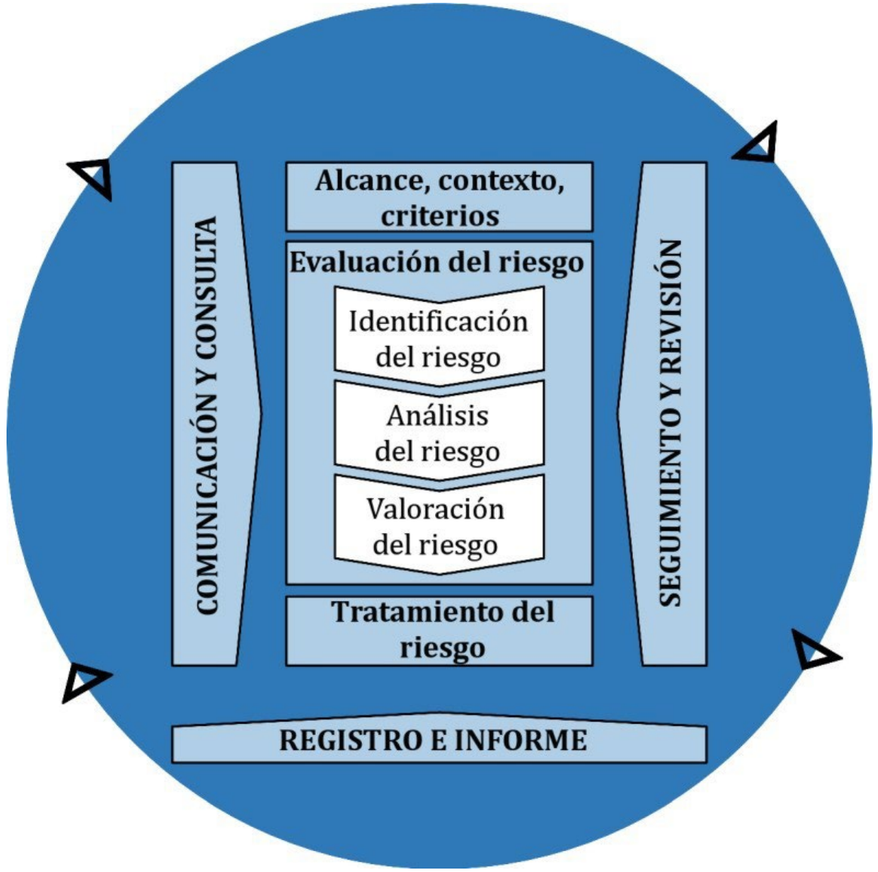


RIESGOS DE CIBERSEGURIDAD

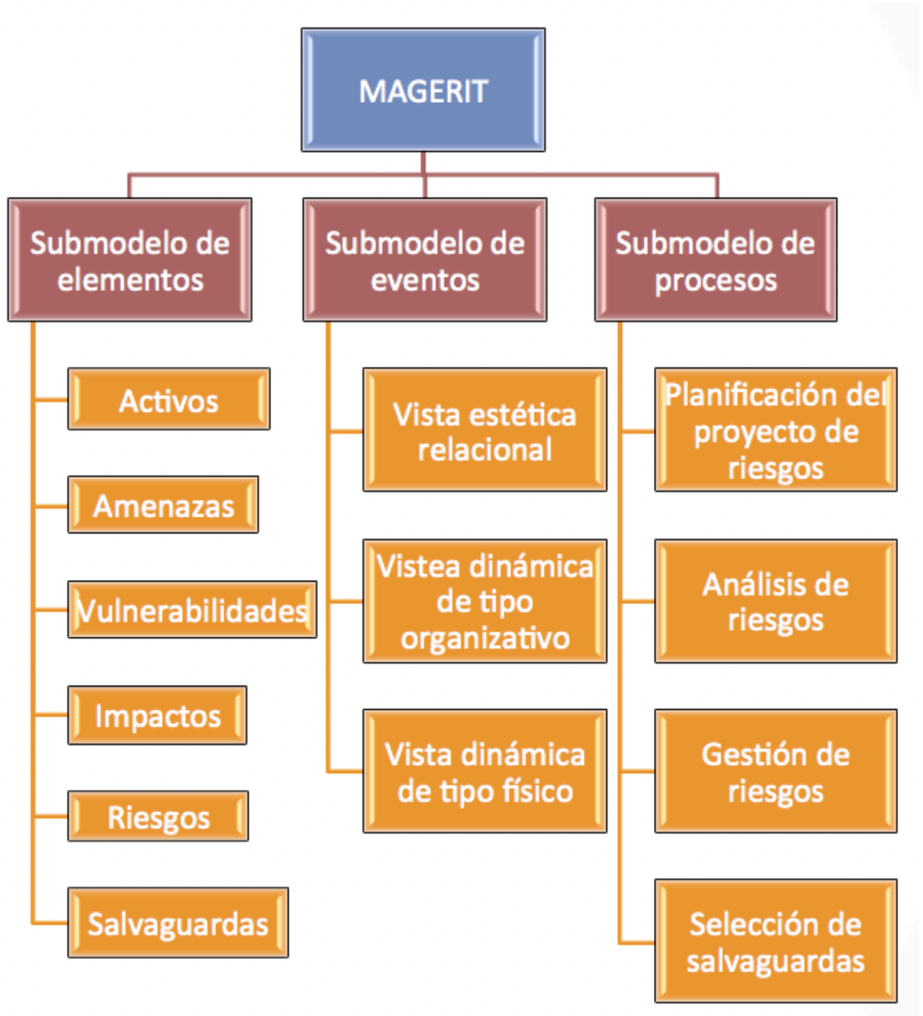
Riesgos de ciberseguridad

ISO 31000:2018
Gestión de Riesgos

La norma ISO 31000 proporciona principios y directrices genéricos sobre la gestión de riesgos. Se centra en el marco conceptual, los procesos y los principios que son aplicables a cualquier tipo de organización o contexto.



Riesgos de ciberseguridad



MAGERIT

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Desarrollada por el Centro Criptológico Nacional de España, esta metodología se centra en la gestión de riesgos de seguridad de la información.

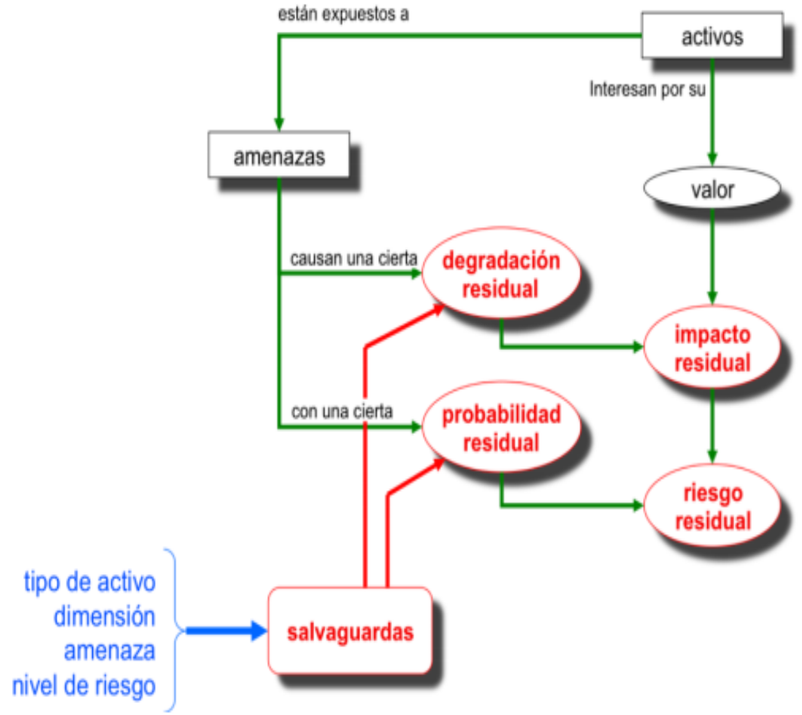


Ilustración 10. Elementos de análisis del riesgo residual

Riesgos de ciberseguridad

1.ISO 31000:2018: Gestión de Riesgos: La norma ISO 31000 proporciona principios y directrices genéricos sobre la gestión de riesgos. Se centra en el marco conceptual, los procesos y los principios que son aplicables a cualquier tipo de organización o contexto.

2.MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información): Desarrollada por el Centro Criptológico Nacional de España, esta metodología se centra en la gestión de riesgos de seguridad de la información.

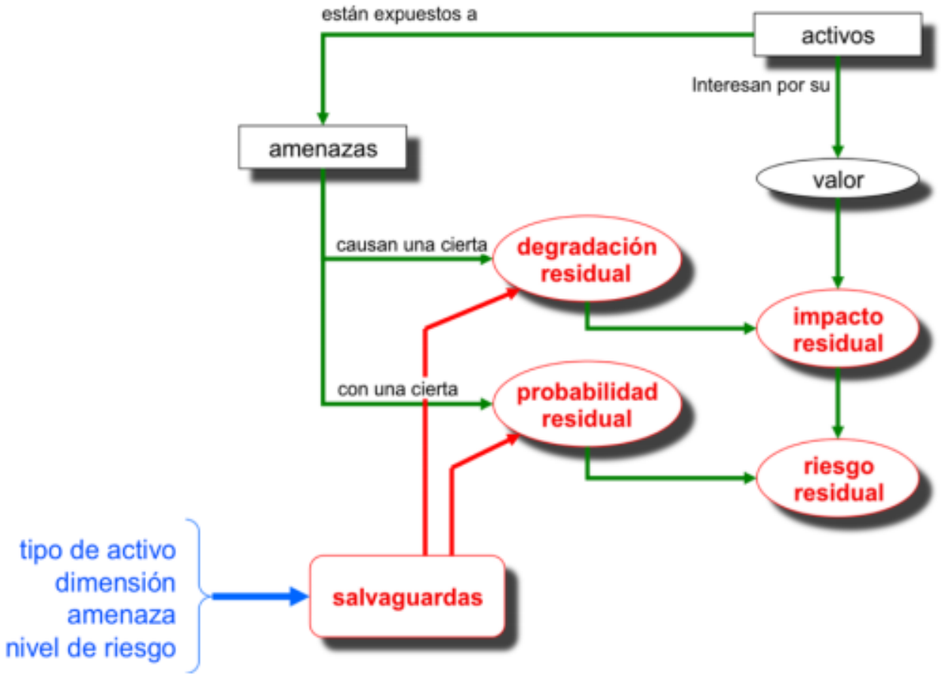


Ilustración 10. Elementos de análisis del riesgo residual

Riesgos de ciberseguridad

“Para poder protegernos hay que conocer bien a que actores y a que amenazas estamos expuestos”

Amanazas

ENISA THREAT LANDSCAPE 2023
October 2023

Figure 2: Breakdown of analysed incidents by threat type (July 2022 till June 2023)

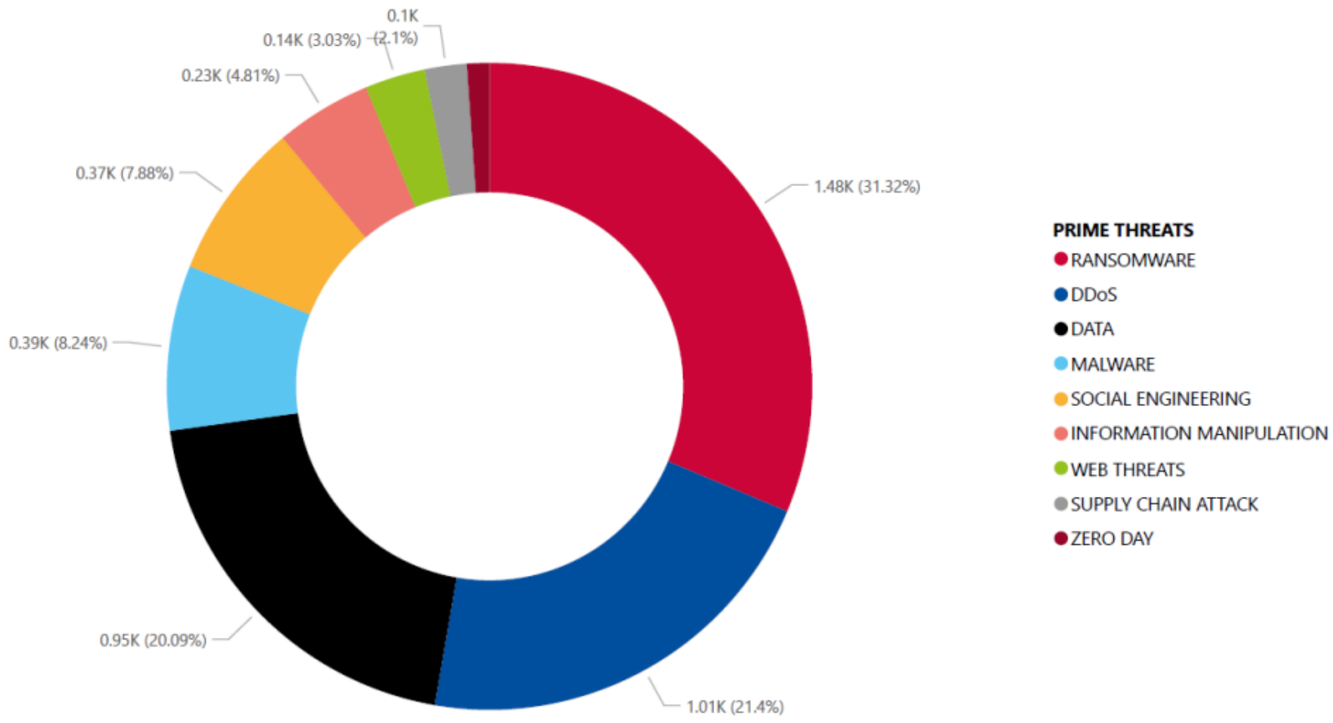
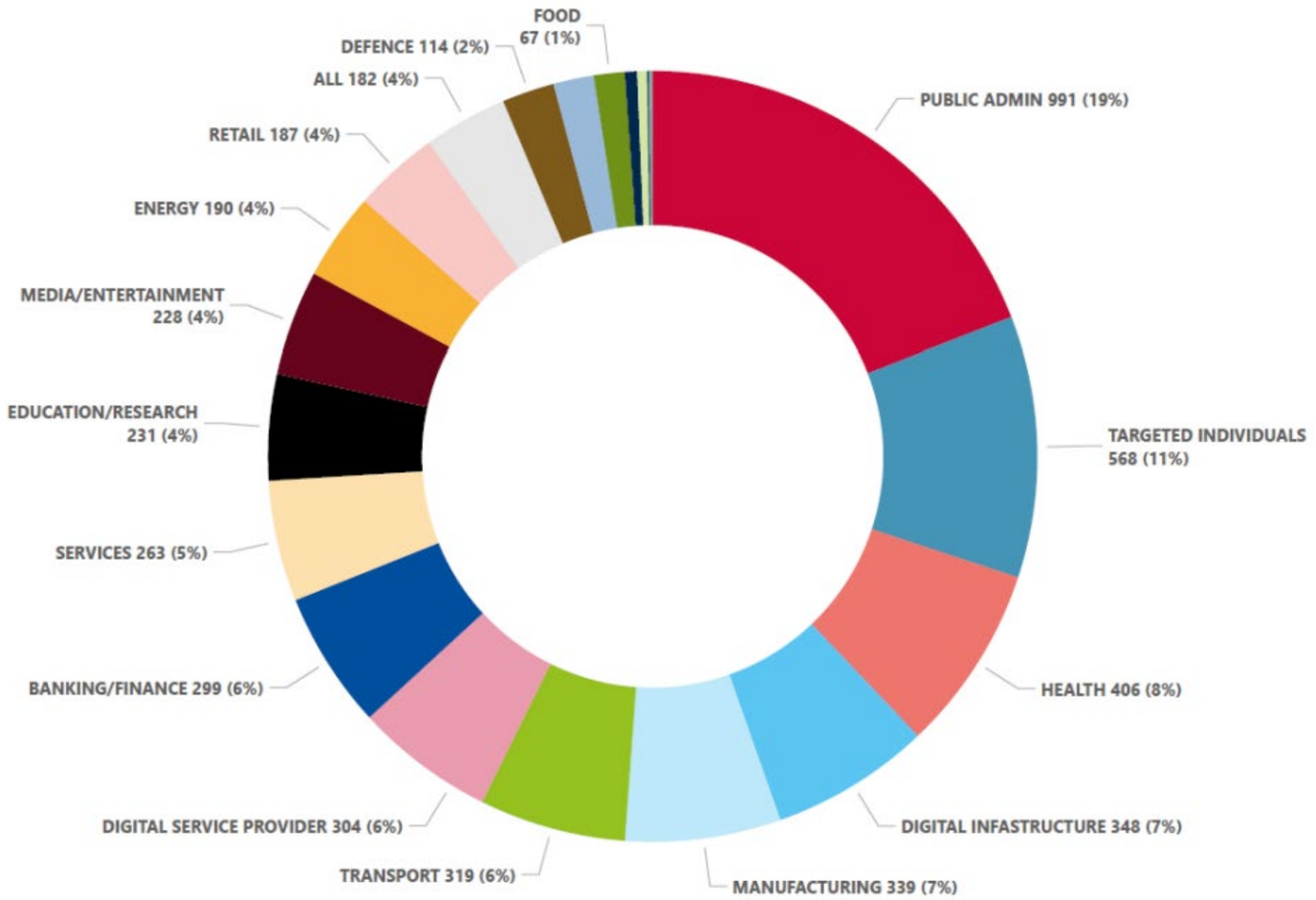


Figure 2: Breakdown of analy

Amenazas por sector

Figure 6: Targeted sectors per number of incidents (July 2022 - June 2023)



Actores de amenazas

Figure 8: Threat actor by sector

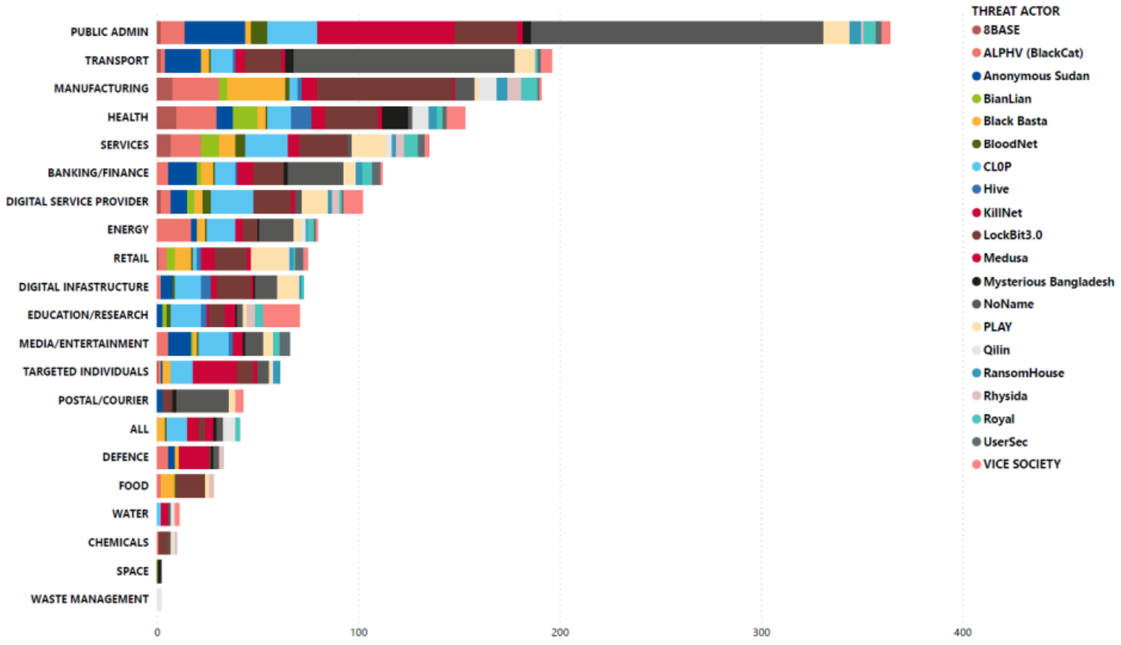
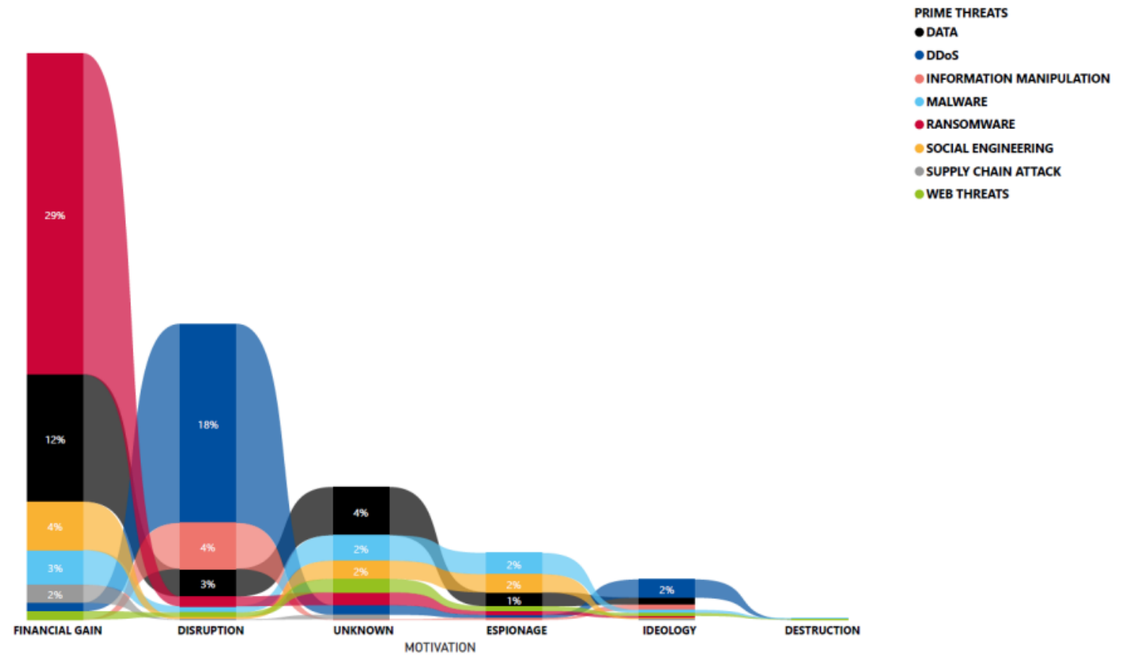


Figure 10: Motivation of threat actors per threat category



Tendencias de las amenazas

- **El ransomware y las amenazas contra la disponibilidad (DDos)** ocuparon los primeros puestos durante el periodo analizado.
- Varios actores de amenazas han profesionalizado aún más sus **programas As-a-Service**.
- **Uso indebido de herramientas legítimas** principalmente para eludir la detección durante el mayor tiempo posible.
- Las **técnicas de extorsión** las organizaciones delictivas han ido evolucionando. No sólo utilizaron tácticas y métodos novedosos para infiltrarse en los entornos, sino que también profundizaron en enfoques alternativos para presionar y extorsionar a las víctimas.
- **La geopolítica** sigue teniendo un fuerte impacto en las operaciones cibernéticas.
- **Aumento de las operaciones por parte de las fuerzas de seguridad**, como el desmantelamiento de la infraestructura informática del grupo de ransomware Hive o Trickbot.
- Cl0p aumentó en el primer semestre de 2023 con la **militarización de dos zero-days**.
- Una de las mayores amenazas de malware siguen siendo los **ladrones de información (Stealers)** como Agent Tesla, Redline Stealer y FormoBook.

Tendencias de las amenazas

- **El phishing** vuelve a ser el vector más común para el acceso inicial.
- **El compromiso del correo electrónico comercial (BEC)** sigue siendo uno de los medios favoritos de los atacantes para obtener beneficios económicos.
- **Las brechas de seguridad basadas en robo de información** sigue en aumento.
- El impacto disruptivo y la adopción exponencial de **chatbots IA generativa** como ChatGPT, Microsoft Bing y Google Bard están cambiando la sutileza y forma de atacar de los criminales.
- Los **ataques DDoS** son cada vez mayores y más complejos, se están desplazando hacia las redes móviles y el IoT.
- Las **“Deep Fakes" y la manipulación de la información** mediante inteligencia artificial siguen siendo motivo de preocupación. Aemás, ha sido un elemento clave de la guerra de Rusia contra Ucrania.
- Los grupos de amenazas tienen un interés creciente en los **ataques a la cadena de suministro** y muestran una capacidad cada vez mayor utilizando a los empleados como puntos de entrada.

Impactos

IMPACTO DIGITAL

- se refiere a sistemas dañados o no disponibles, archivos de datos corruptos o exfiltración de datos o alguna intrusión maliciosa anunciada.

IMPACTO ECONÓMICO

- se refiere a la pérdida financiera directa sufrida, el daño a la seguridad nacional que puede ser causados por la pérdida de material importante o la petición de un rescate.

IMPACTO SOCIAL

- se refiere a cualquier efecto sobre el público en general o a una perturbación generalizada que pueda tener un impacto en la sociedad (por ejemplo, incidentes que perturben el sistema nacional de salud de un país, filtración de cualquier dato de datos personales, números de la seguridad social, direcciones, etc.).

IMPACTO EN LA REPUTACIÓN

- se refiere a la posibilidad de publicidad negativa o una percepción pública adversa de la entidad que ha sido víctima de un incidente. entidad víctima de un ciberincidente.

IMPACTO FÍSICO

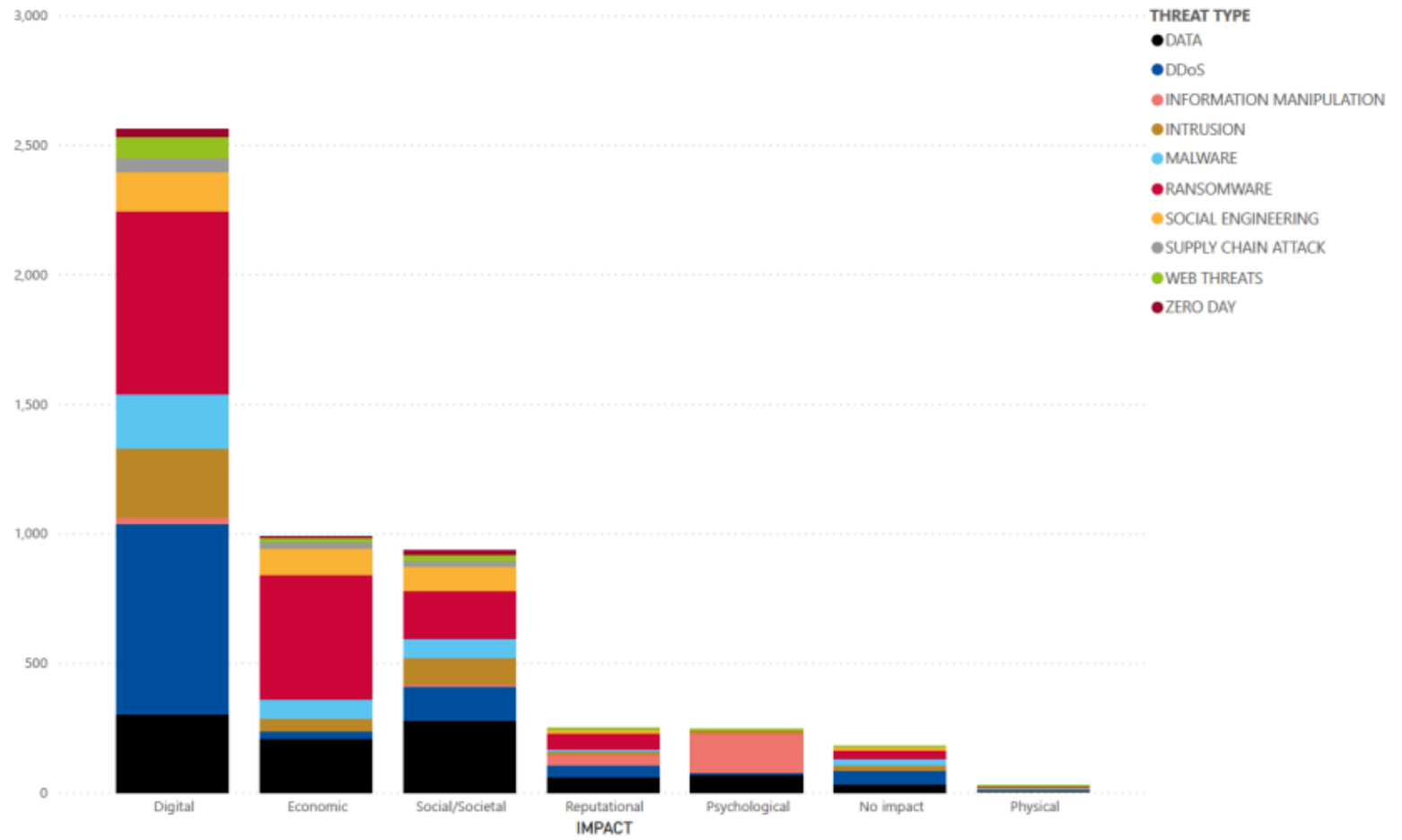
- se refiere a cualquier tipo de lesión o daño a empleados, clientes o pacientes.

IMPACTO PSICOLÓGICO

- se refiere a cualquier tipo de confusión, malestar, frustración, preocupación o ansiedad causada a empleados, clientes o pacientes, o al público en general.

Impactos

Figure 9: Threat type breakdown by Impact



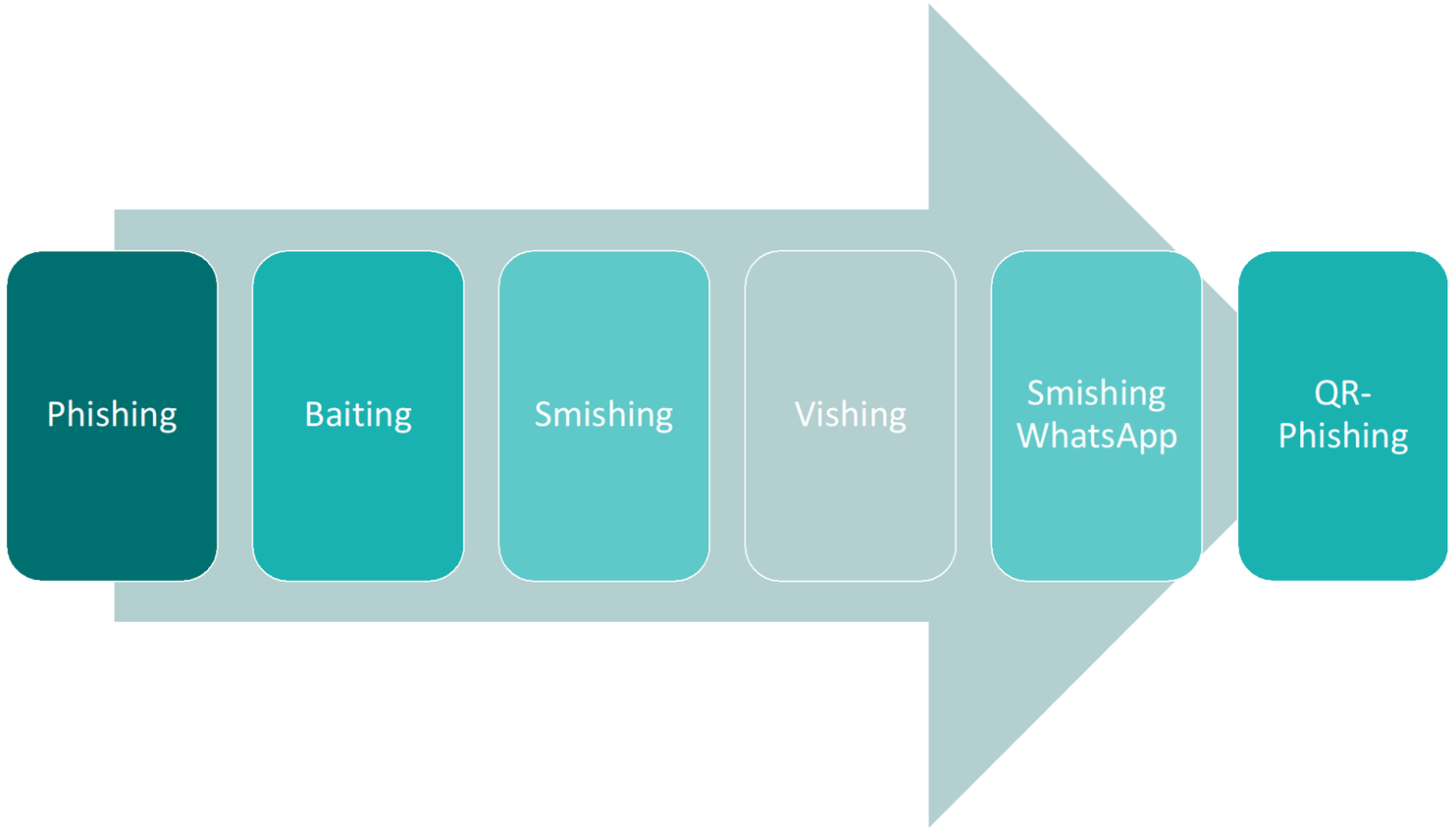
Vectores de amenaza

Usuario

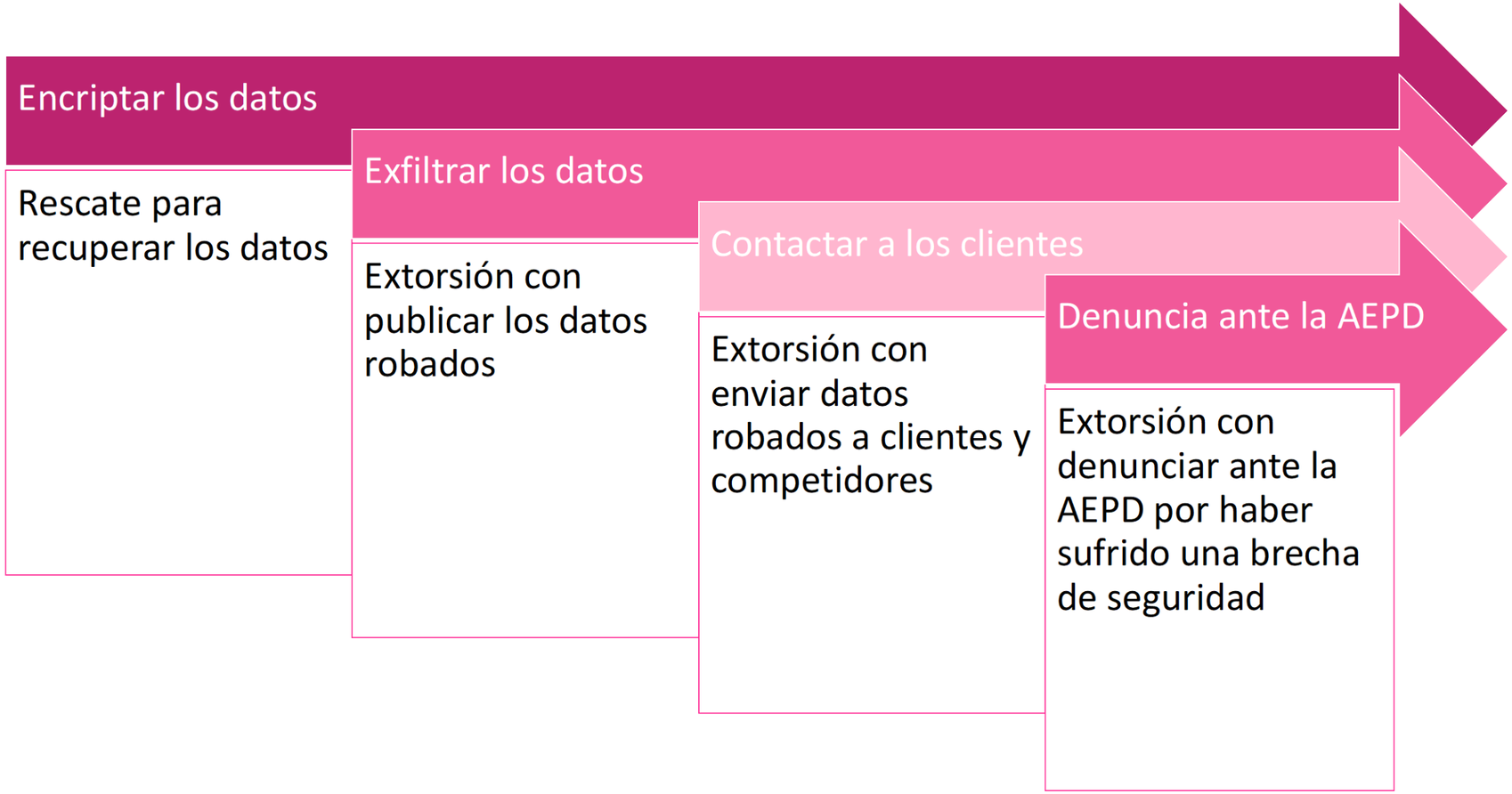
Vulnerabilidad

Cadena de suministro

Ataques al usuario



Ransomware


Encriptar los datos
Rescate para recuperar los datos
Exfiltrar los datos
Extorsión con publicar los datos robados
Contactar a los clientes
Extorsión con enviar datos robados a clientes y competidores
Denuncia ante la AEPD
Extorsión con denunciar ante la AEPD por haber sufrido una brecha de seguridad

Riesgos normativos

¿Y si asumimos la brecha de seguridad?
¿Estamos preparados para responder correctamente?

Cada vez tenemos nuevas normativas y regulaciones que las empresas deben aplicar.

La UE está promoviendo nuevas regulaciones:

- ❑ GDPR
- ❑ DORA
- ❑ NIS2
- ❑ Cyber Resilience Act

Cyber Resiliencia

¿Y si asumimos la brecha de seguridad? ¿Estamos preparados para responder correctamente? ¿Somos Cyber-resilientes?

¿Aplicamos la ISO 22301? ¿Tenemos un Plan de Continuidad de Negocio? ¿Tenemos un Plan de Recuperación ante Desastres? ¿Sabemos gestionar las comunicaciones en caso de crisis? ¿Sabemos los RPO y DPO de nuestros procesos? ¿Hemos probamos los DRP?

La normativa DORA pretende que las empresas sean 'CYBER-RESILIENTES'

- La EBA, ESMA, EIOPA y AES crearán un marco único de gestión y supervisión a nivel europeo.
- El objetivo es reforzar la exigencia de los supervisores sobre riesgos digitales y establecer pruebas de los sistemas TICs.
- Unificar y mejorar la gestión de riesgos de ciberseguridad y TIC
- El alcance: Todos los actores del Sector Financiero en diferentes fases.

Ataques al usuario

¿Qué se va a revisar en DORA?

- Sistemas, protocolos y herramientas
- Respuesta y recuperación de incidentes
- Políticas de seguridad
- Aprendizaje y evolución
- Comunicación de incidentes
- Adopción de nuevos estándares
- Respuesta ante incidentes
- Pruebas de resiliencia operativa
- Gestión del riesgo de terceros
- Acuerdos de intercambio de información

Siguientes pasos

Servicios al CISO

- Ciso-as-a-Service y Virtual-CISO
- Programa de seguridad
- Gestión de Riesgos
- CyberCompliance & CyberResilience
- Controles de seguridad

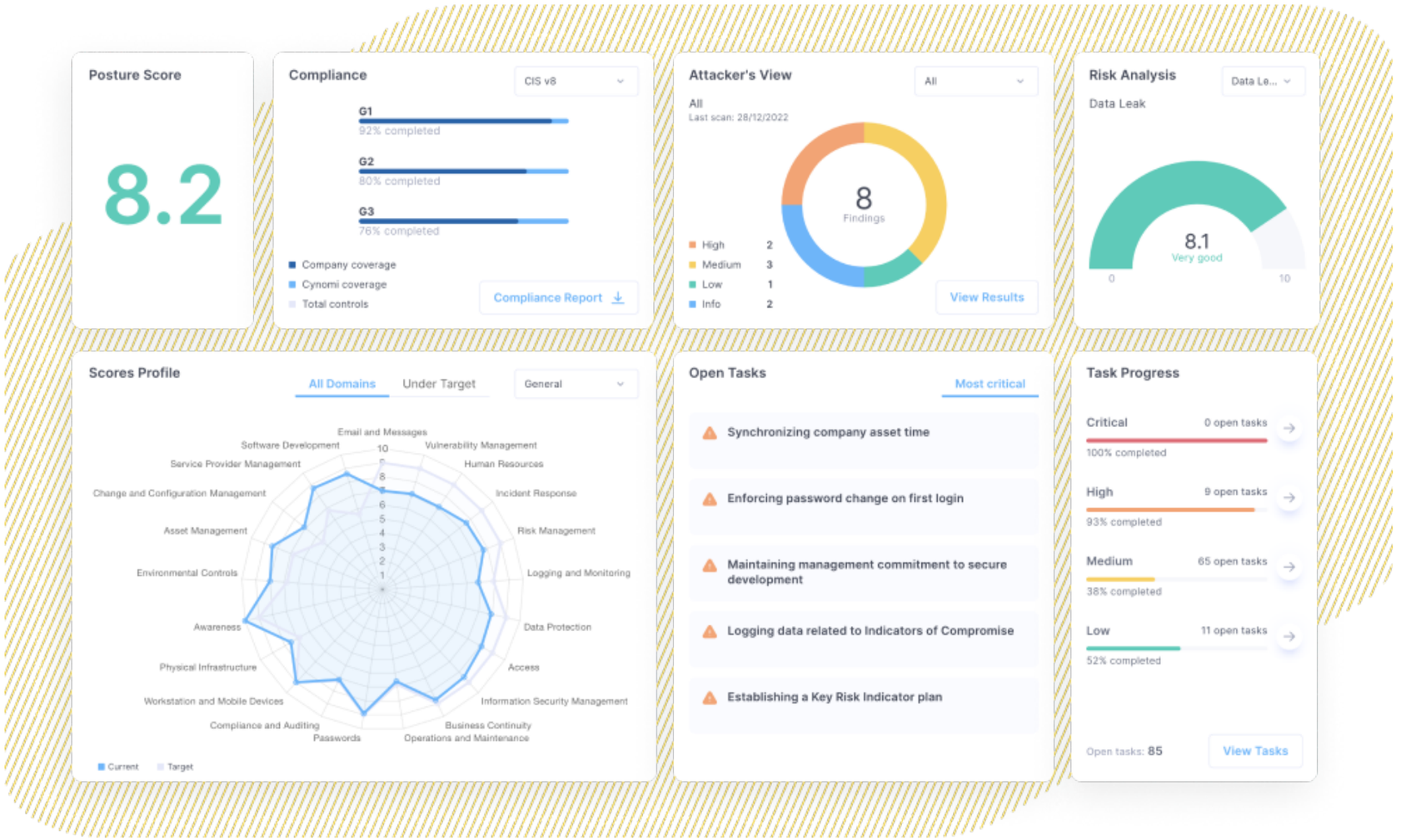
Formación y concienciación

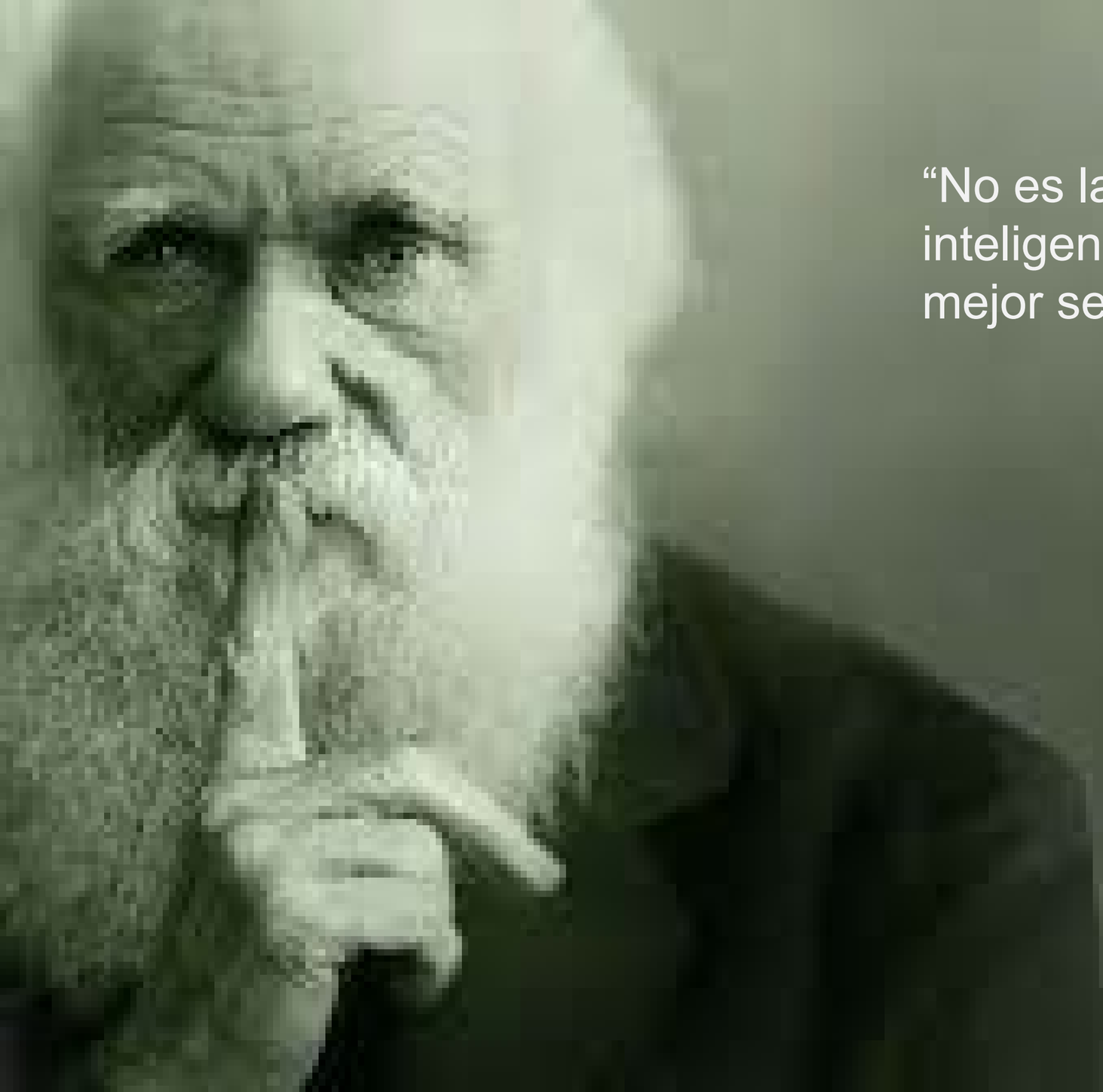
- Formación técnica
- Técnicas de hardening
- Concienciación a empleados
- Simulaciones de ataques

Auditorías

- Técnicas (Red, Web, Sistemas)
- Cumplimiento normativo
- Superficie de ataque

Plataforma Cynomi





“No es la especie más fuerte, ni la más inteligente, la que sobrevive, sino la que mejor se adapta al cambio“

Charles Darwin

corus

www.corusconsulting.com