Gestión de ciber riesgos

May/2023

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

ISACA
Quito - Ecuador

Roberth D. Chávez J.

- Gerente Senior de Asesoría en Riesgos en **Deloitte** (2006 a 2020)
- Vicepresidente en **Isaca – Cap. Quito** (2016-2018)
- Gerente de Auditoría Interna de TI en **Banco Pichincha** (2020-2022)
- Gerente de Ciber Riesgos en **Banco Pichincha** (2022 - actualidad)
- **Certificaciones**:
  - CISM
  - PMP
  - CISA
  - Master ISO 27001
  - Risk Manager ISO 31000

Antecedentes

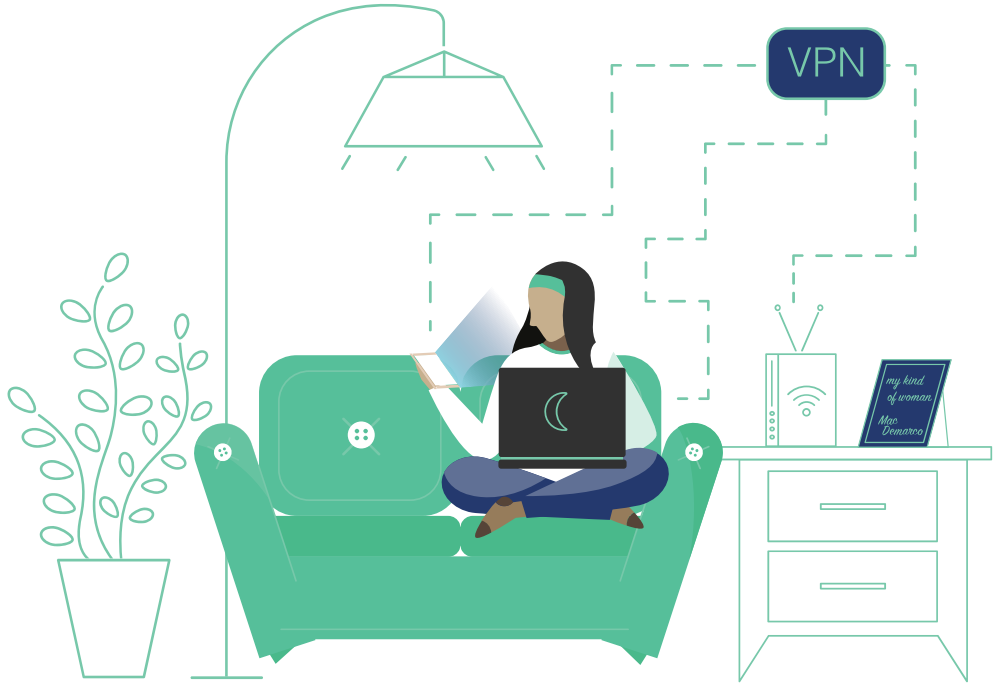
Ataques Ciber más comunes

Malware

Ataques DoS

Phishing

Spoofing



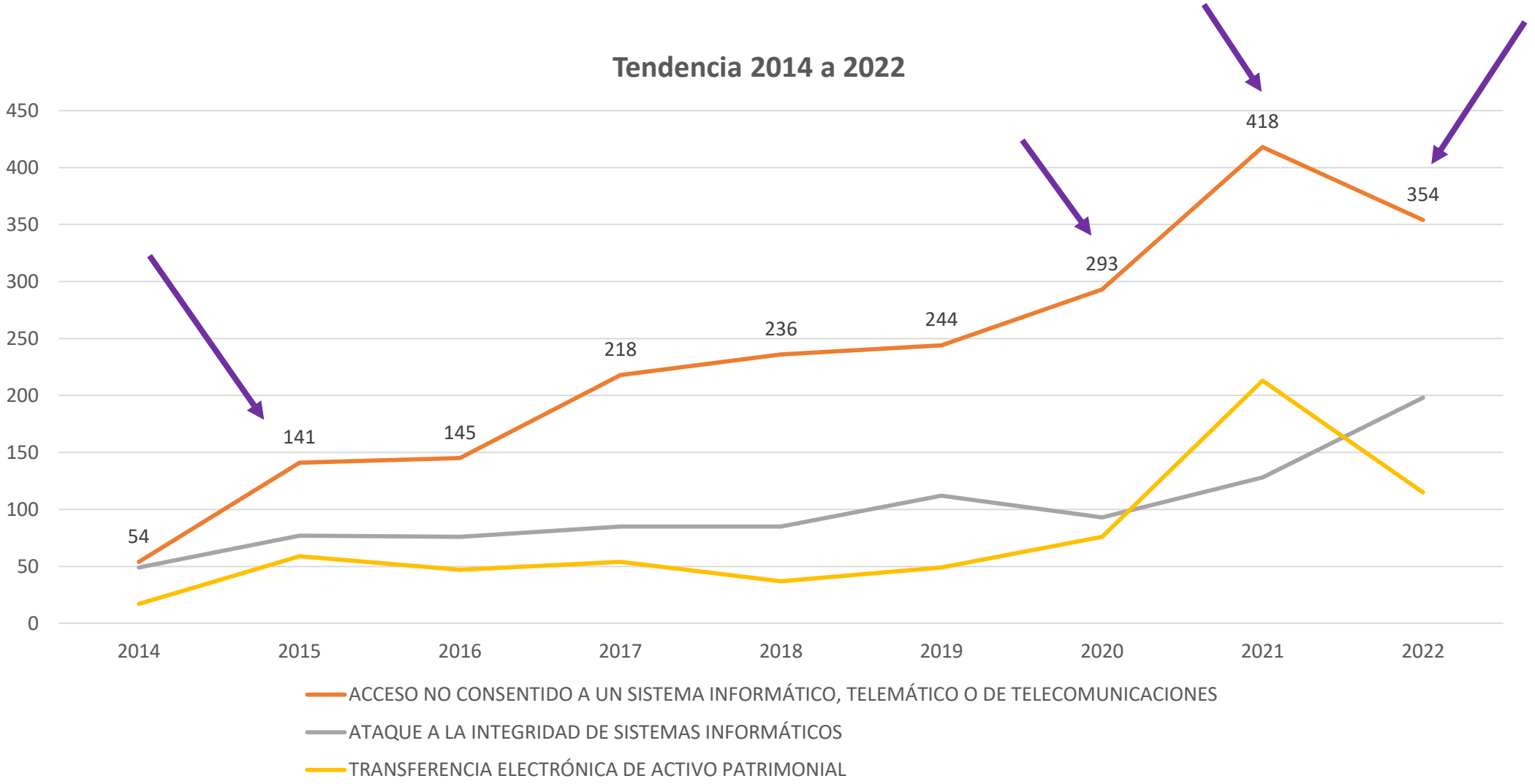
Ataques basados en identidades

Ataque por inyección código

Ataque en cadena suministro

Insiders

Antecedentes - Ecuador



Gestión de Ciber Riesgos

01 **Establecer criterios**

Establecer impacto, probabilidad y nivel de riesgo.

02 **Identificar activos**

Se trata de activos de información, no es lo mismo que un activo fijo.

03 **Identificar amenazas y vulnerabilidades**

Identificar amenazas y vulnerabilidades enfocado en ciber.

04 **Evaluar nivel de riesgos y controles**

Determinar el impacto y probabilidad y la eficacia de controles

05 **Determinar riesgo residual**

Para aquellos riesgos donde el control no es suficiente, se requiere un tratamiento

Gestión de Ciber Riesgos

Impacto → Mide la consecuencia de materialización de un evento en términos del giro de negocio.

Cuantitativo

Impacto = $2,300.000

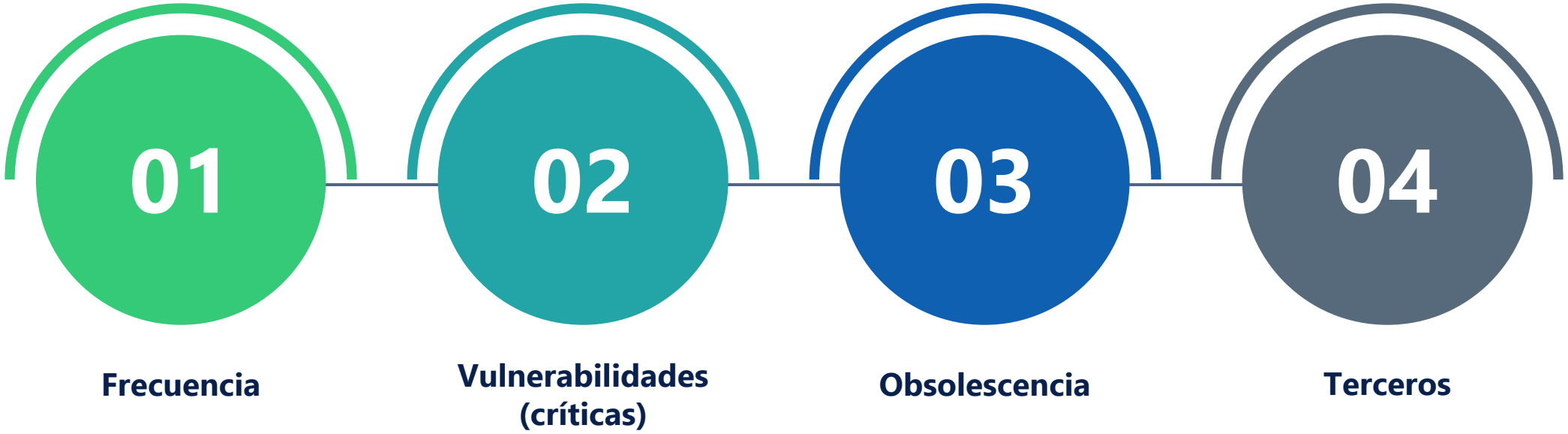
Cualitativo

Regulatorio = Alto, Medio ó Bajo
Eficiencia = Alto, Medio ó Bajo

Gestión de Ciber Riesgos

Probabilidad

Mide la posibilidad de ocurrencia de un evento que pueda derivar en un ciber incidente.



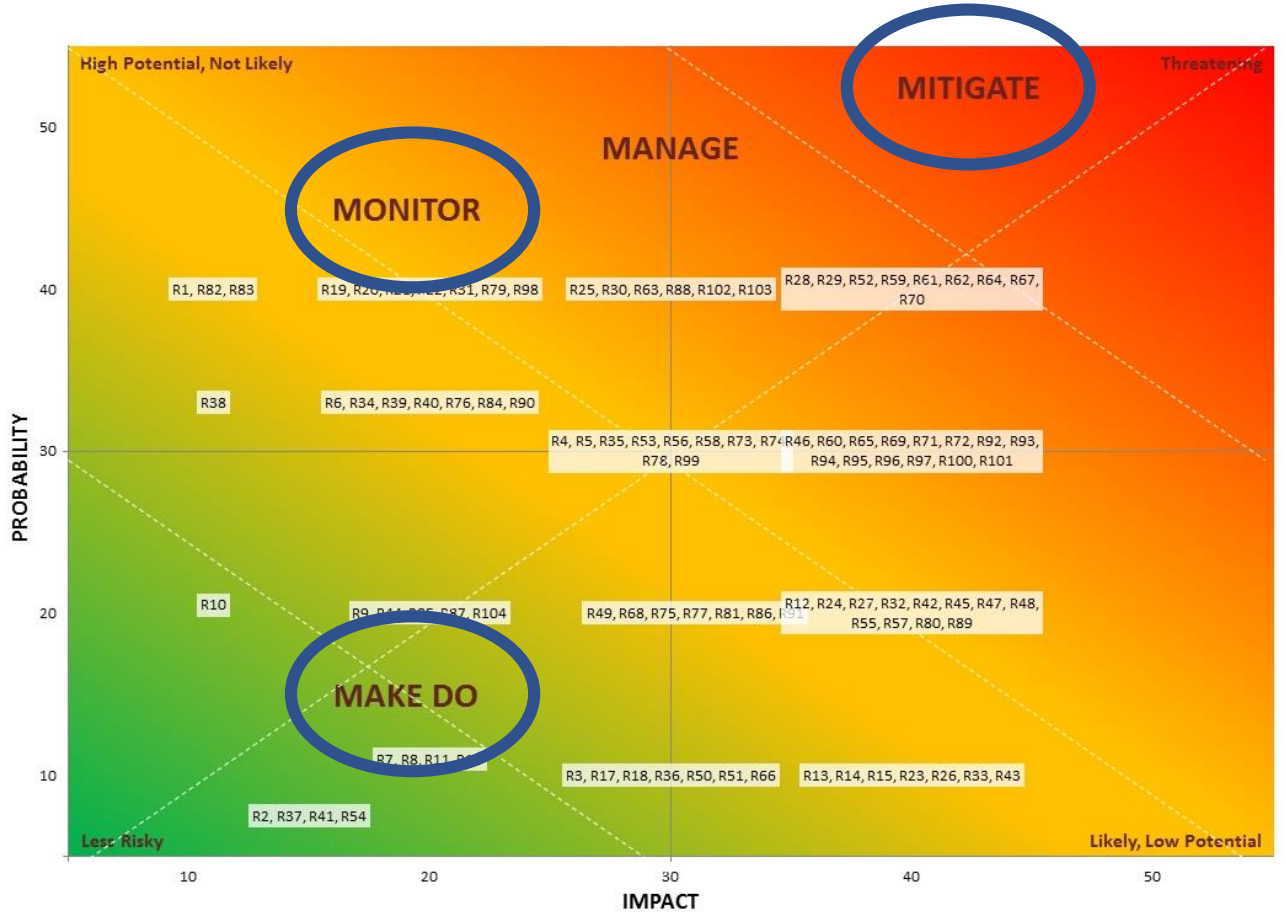
Gestión de Ciber Riesgos

Nivel de riesgo

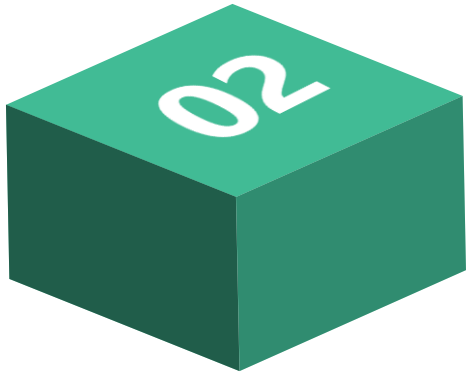
Estima la combinación de impacto y probabilidad aceptable a fin de dar una respuesta al riesgo.

Gestión de Ciber Riesgos

Nivel de riesgo



Gestión de Ciber Riesgos



Activos →

Considerar más fuentes para identificar esto:

- **Reportes de vulnerabilidades**
- **Informes de auditoría interna, externa y entes de control**
- **Boletines de fabricantes (Zero days)**
- **Feeds de inteligencia de amenazas (IOCs)**

Gestión de Ciber Riesgos

Amenazas
Vulnerabilidades

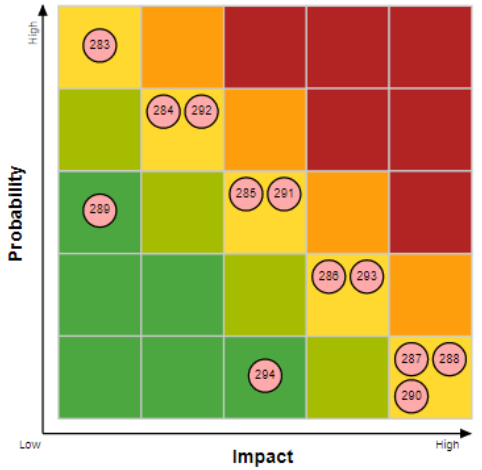
Considerar más fuentes para identificar esto:

- **Reportes de vulnerabilidades**
- **Informes de auditoría interna, externa y entes de control**
- **Boletines de fabricantes (Zero days)**
- **Feeds de inteligencia de amenazas (IOCs)**

Gestión de Ciber Riesgos

Estimar nivel de riesgo

Se estima el IMPACTO y PROBABILIDAD por cada escenario de riesgo:



Gestión de Ciber Riesgos

Estimar eficacia controles

Es algo que usualmente no se realiza y genera muchas interpretaciones. Se evalúa 2 componentes:

- **Diseño** (como el control está diseñado para mitigar el riesgo: i) naturaleza, ii) oportunidad, iii) automatización, iv) documentación.
- **Eficacia** (como el control está operando: i) cobertura, y ii) control interno)

Gestión de Ciber Riesgos

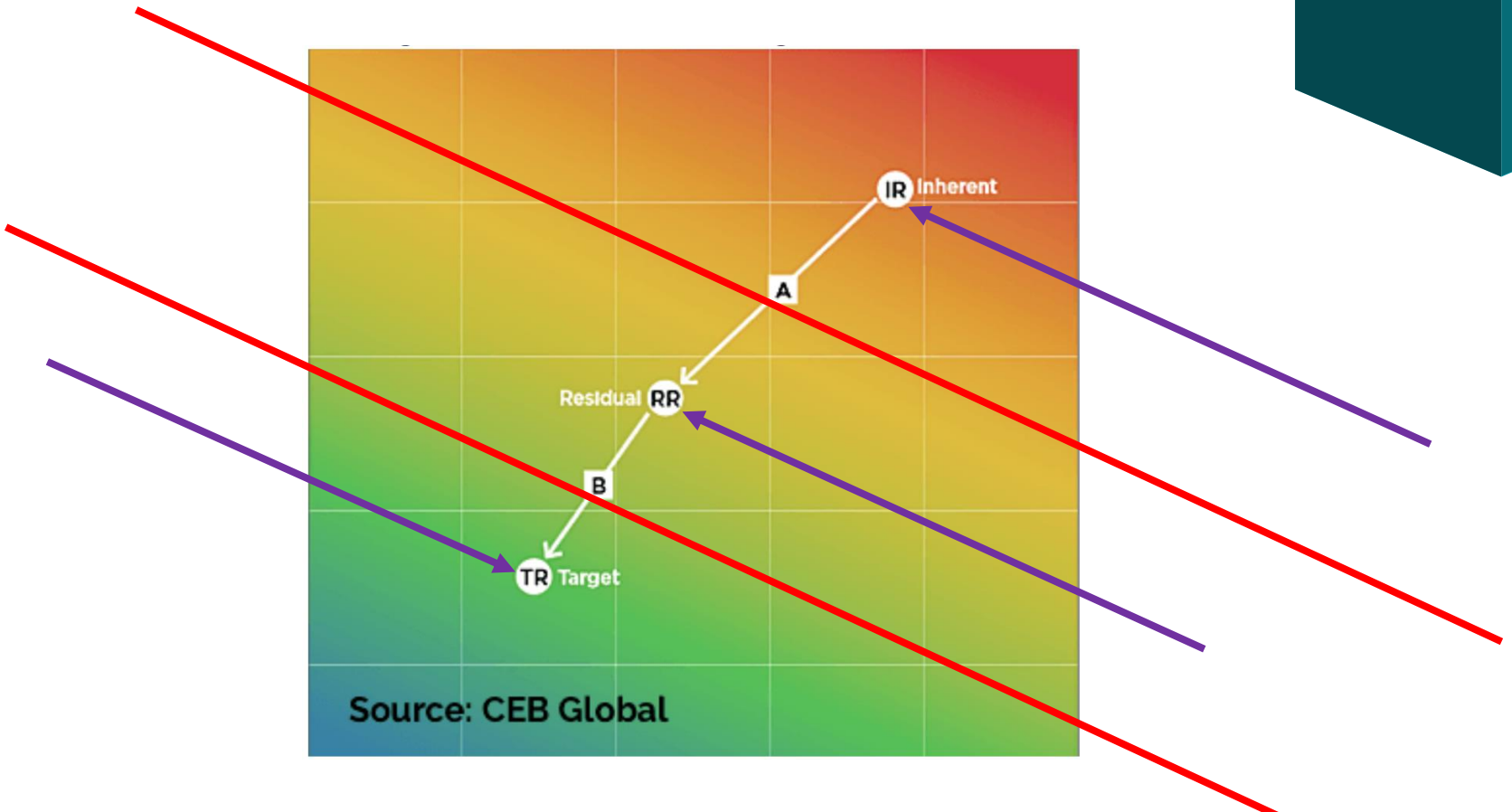
Riesgo residual

Es el riesgo que permanece luego de que los controles han sido aplicados:

$$R_{inherente} - Controles = R_{residual}$$

Gestión de Ciber Riesgos

$R_{inherente} - Controles = R_{residual}$



Gestión de Ciber Riesgos

- La gestión de ciber riesgos se podría planificar, pero el 80% surge producto de:
    - **Eventos de ciberseguridad** (críticos)
    - **Incidentes** de ciberseguridad
    - Revisiones o auditorías **internas** o **externas**
    - Novedades en la operación
    - **Reportes de vulnerabilidades**
- ¿Qué se debe actualizar? **Probabilidad y/o Eficacia de controles**

Conclusiones

- La ciberseguridad requiere un enfoque más especializado, sin necesidad de crear silos para la gestión de riesgos.
- Errores típicos:
  - Sesgo cognitivo
  - Subestimación
  - Optimismo
- A pesar de que la ciberseguridad es un subconjunto de la seguridad de información, el uso de tecnologías emergentes, servicios nube, IOTs, RPA, etc; requiere una atención más ágil en la cual se verifiquen debilidades especializadas (SME).

Preguntas y Respuestas