Unidad 9: La mitigación del riesgo
BLOQUE III – La gestión del ciberriesgo como un proceso

Grado en Ingeniería de la Ciberseguridad, curso 2022-2023

CONTENIDOS

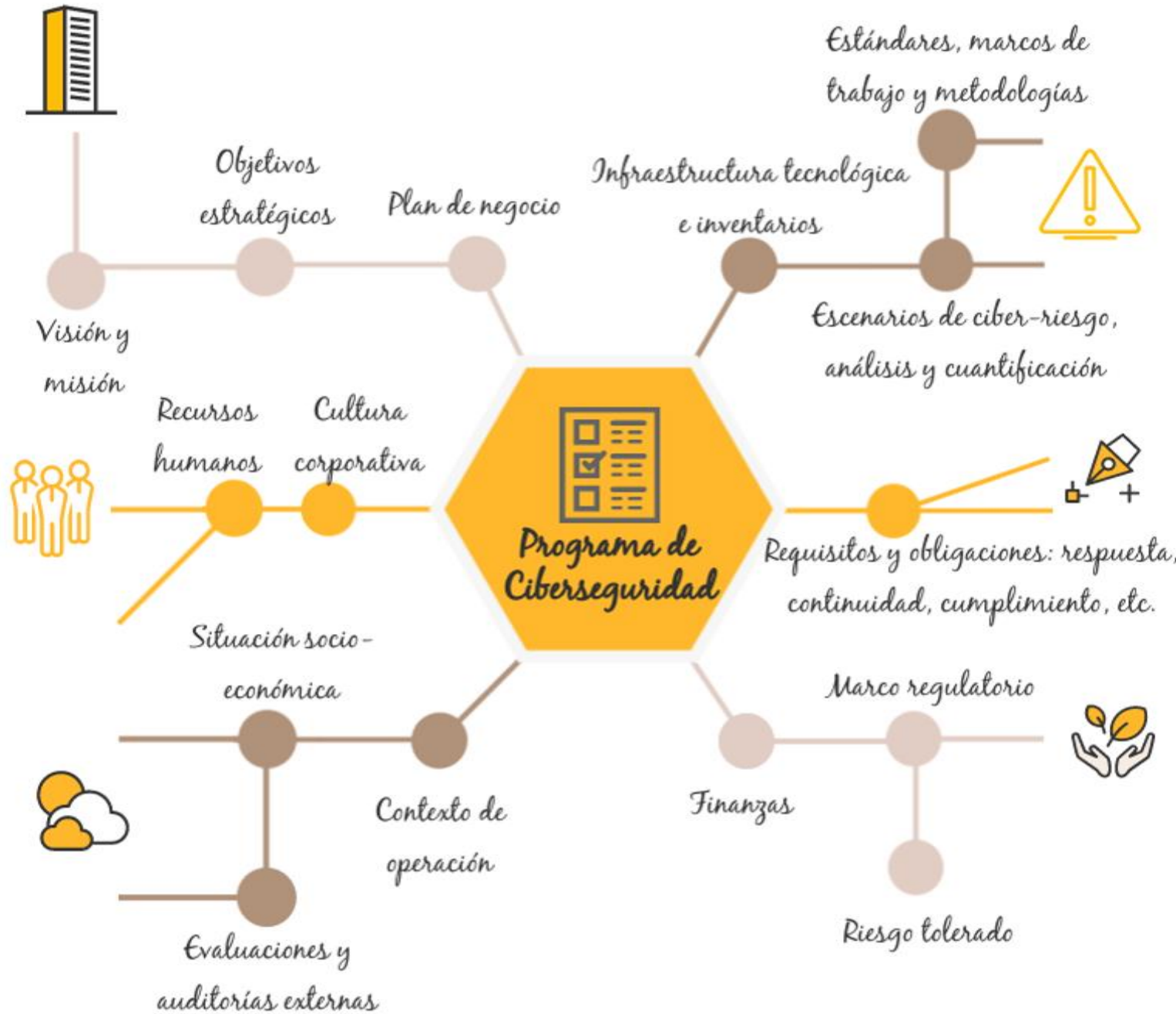
1. Estrategias y planes de mitigación.
2. Modelos de control.
3. Gestión de la cadena de suministro.
4. Retornos de inversión.

1. Estrategias y planes de mitigación

- Una vez identificados, analizados y cuantificados los ciberriesgos se puede pasar a tratarlos con diferentes estrategias: aceptar, evitar, mitigar, transferir.
- En la estrategia de mitigación el objetivo es reducir el ciberriesgo inherente reduciendo la probabilidad o el impacto de los riesgos.
- Normalmente esta estrategia es la seleccionada para tratar riesgos con probabilidad alta.
  - Si el impacto es bajo, al reducir la probabilidad de podrá pasar a gestionar el riesgo residual con una estrategia de aceptación.
  - Si el impacto es alto, al reducir la probabilidad se podrá pasar a aplicar una estrategia de transferencia. O se podrá intentar reducir también este impacto para pasar a realizar aceptación.

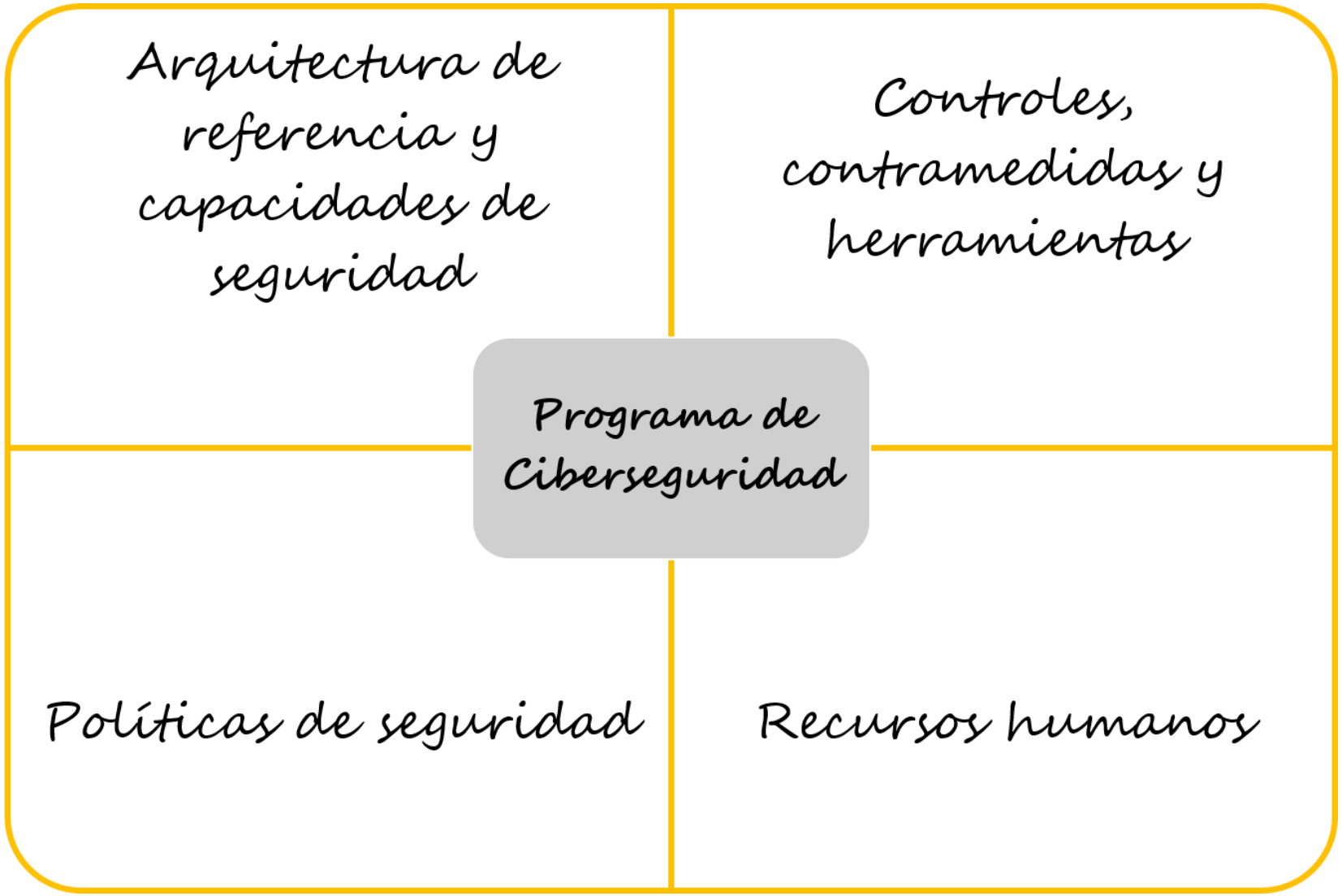
1. Estrategias y planes de mitigación

- La mitigación completa es imposible.
- La aplicación de la estrategia de mitigación de manera eficiente se basa en un Cybersecurity Program.
  - O Information Security Management Program, ISMP.
- Conjunto de documentos que, teniendo en cuenta la tolerancia al riesgo de la organización y los ciberriesgos cuantificados así como la regulación nacional e internacional, el contexto de operación, los estándares y mejores prácticas existentes y los recursos disponibles, recogen cómo la organización debe aplicar estrategias de mitigación concretas.

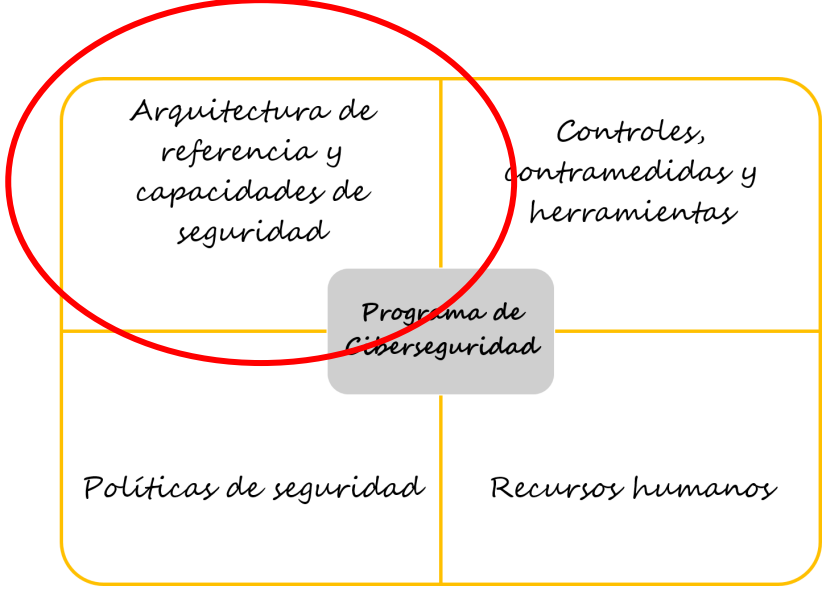

Estándares, marcos de trabajo y metodologías
Objetivos estratégicos
Plan de negocio
Infraestructura tecnológica e inventarios
Visión y misión
Escenarios de ciber-riesgo, análisis y cuantificación
Recursos humanos
Cultura corporativa
Programa de Ciberseguridad
Requisitos y obligaciones: respuesta, continuidad, cumplimiento, etc.
Situación socio-económica
Marco regulatorio
Contexto de operación
Finanzas
Evaluaciones y auditorías externas
Riesgo tolerado

1. Estrategias y planes de mitigación

- El director de seguridad suele ser el responsable de elaborar este programa y de presentarlo al comité de dirección para conseguir aprobación y presupuesto.
- El programa debe tener un ciclo de vida, no es un documento estático que se define, se aprueba y se guarda en un cajón.
- Refleja las prioridades que el director de seguridad ha decidido para la mitigación de los ciberriesgos.
- Para que el programa sea manejable, suele estructurarse en diferentes módulos y documentos.


Arquitectura de referencia y capacidades de seguridad
Controles, contramedidas y herramientas
Programa de Ciberseguridad
Políticas de seguridad
Recursos humanos

Una arquitectura de referencia describe los bloques y componentes esenciales de la infraestructura tecnológica ideal, teniendo en cuenta el inventario de activos que deben protegerse, así como las decisiones de diseño y despliegue que permiten lidiar con las amenazas identificadas.



¿Capacidades? Agnósticas en cuanto a tecnología o herramienta:

- Seguridad física.
- Segmentación y segregación de la red corporativa.
- Protección del perímetro.
- Acceso remoto seguro.
- Identificación, Autenticación, Autorización y Auditoría (IAAA) de usuarios.
- Protección de datos.
- Detección de intrusiones.
- Auditoría y trazabilidad.

MUY TRADICIONALES

Capacidades habituales en entornos actuales (web, mobile, cloud, IoT):

- Gestión de dispositivos y *end-points*.
- Identificación, Autenticación, Autorización y Auditoría (IAAA) de usuarios.
- Protección de las comunicaciones.
- Protección de datos.
- Orquestación segura de servicios.
- *AppSec* y desarrollo seguro de aplicaciones y APIs.
- Detección de anomalías y eventos.
- Monitorización continua.
- Repuesta ante incidentes y recuperación.

Faltarían las capacidades relativas a los recursos humanos, a la evaluación y planificación o a las adquisiciones y gestión de la cadena de suministro, que no tienen tanta relación con la tecnología sino con las personas y los procesos y por lo tanto, no aparecen explícitamente cuando dibujamos la arquitectura de referencia. Pero también tienen que estandarizarse.

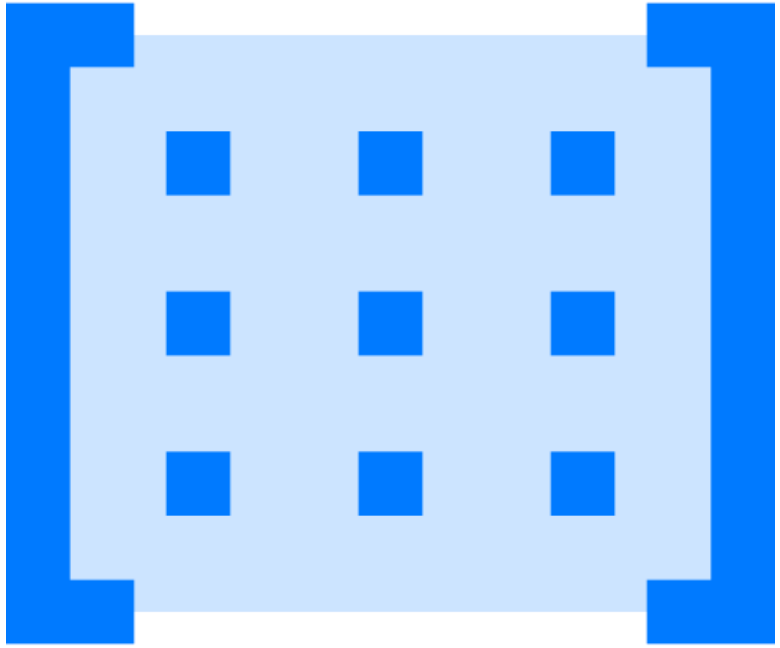
1. Estrategias y planes de mitigación

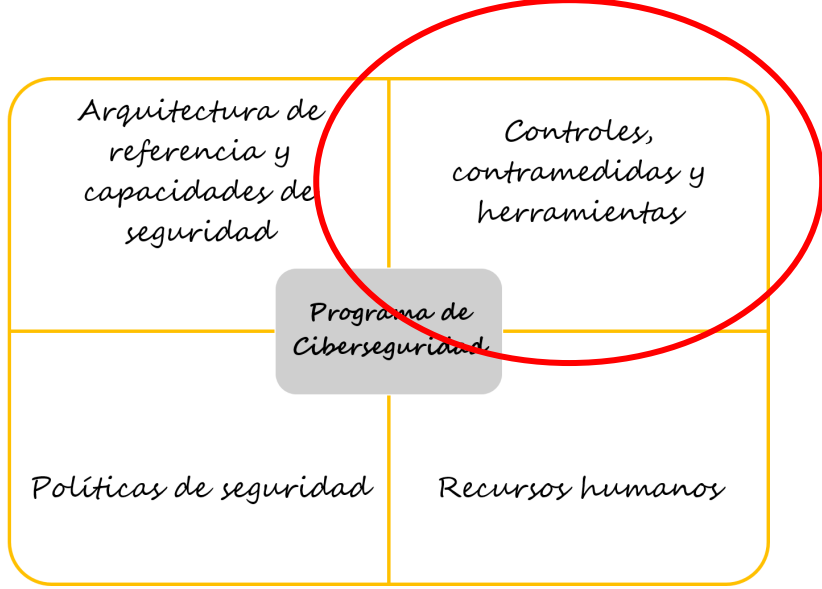
- ¿Cómo decido las capacidades? Y ¿cómo las priorizo?
  - Normalmente se trabaja con un marco de trabajo, estándar, documento de buenas prácticas.
  - Y a partir de un análisis de riesgos (normalmente, realizado siguiendo una metodología).
- Esto ya nos suele fijar una manera de trabajar.

1. Estrategias y planes de mitigación

- En cuanto a la toma de decisiones de priorización, hay diferentes estrategias:
  - Primero las mitigaciones relacionadas con los riesgos más altos que hemos decidido mitigar.
  - Primero las mitigaciones que más cantidad de riesgo mitigan o que a más escenarios/activos afectan.
  - Primero la mitigaciones más rentables (las que mitigan más riesgo por euro invertido).
  - Primero las que mitigan más cantidad de riesgo en un plazo menor.

Una vez identificada una determinada capacidad de seguridad que debe incluir la arquitectura de referencia de la organización, ésta se puede desplegar de diferentes maneras, incorporando diferentes controles, contramedidas o herramientas de seguridad.

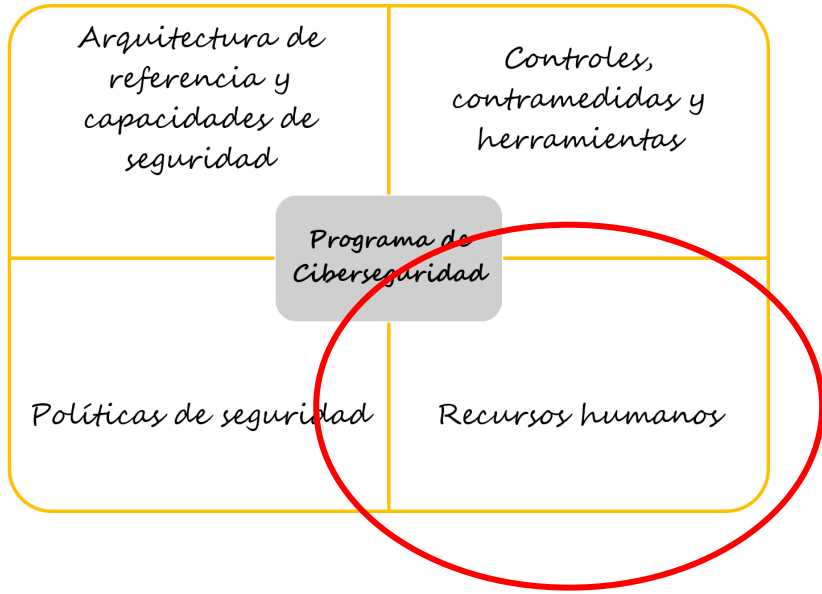




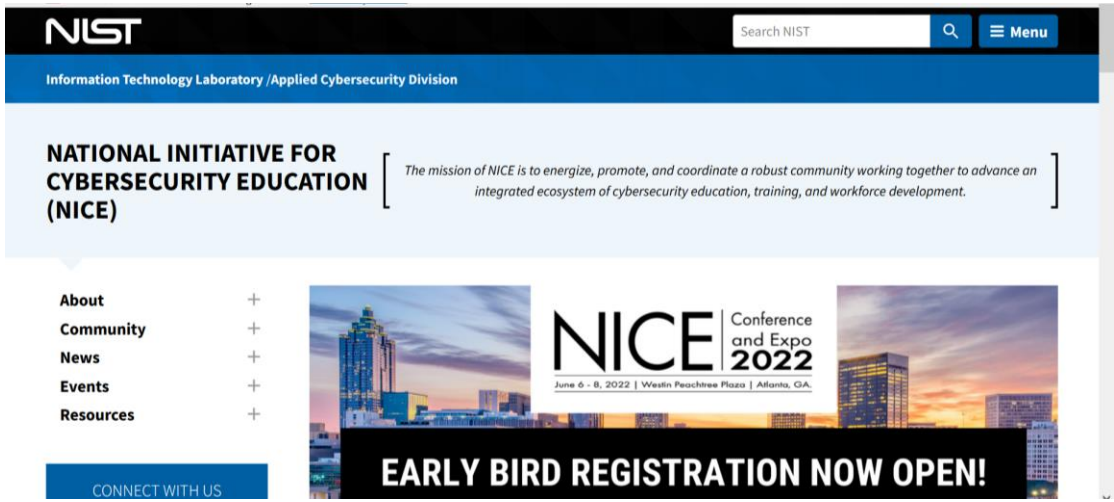
Se recomienda trabajar con matrices de cobertura, para que todas las capacidades queden cubiertas por al menos un control, y para evitar redundancias en la arquitectura.

Para trabajar con nomenclaturas unificadas, los marcos de trabajo, documentos de buenas prácticas, etc. (unidad 3) ayudan mucho.

Es conveniente que el Programa identifique a los miembros del equipo responsable y les asigne roles y responsabilidades concretas en los proyectos de los sucesivos planes directores.



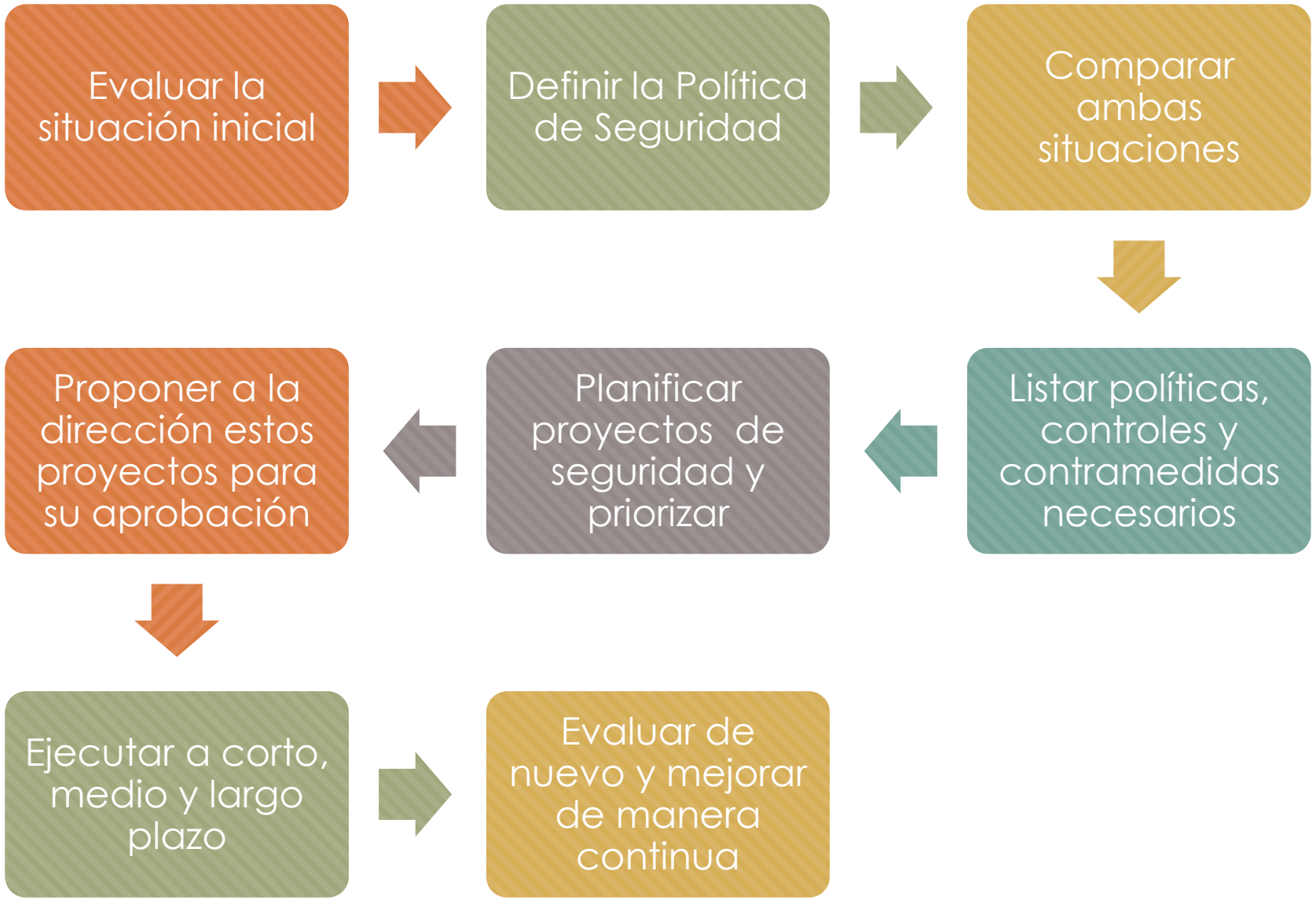
1. Determinar las competencias y habilidades necesarias para adoptar cada uno de los roles necesarios.
2. Determinar las competencias y habilidades que tienen los miembros del equipo.
3. Identificar las diferencias y planificar la formación o certificaciones que es necesario proporcionar a los miembros del equipo.
4. Identificar y planificar las nuevas contrataciones y/o sub-contrataciones necesarias para cubrir las competencias y habilidades que no quedará cubiertas internamente en el plazo necesario.



1. Estrategias y planes de mitigación

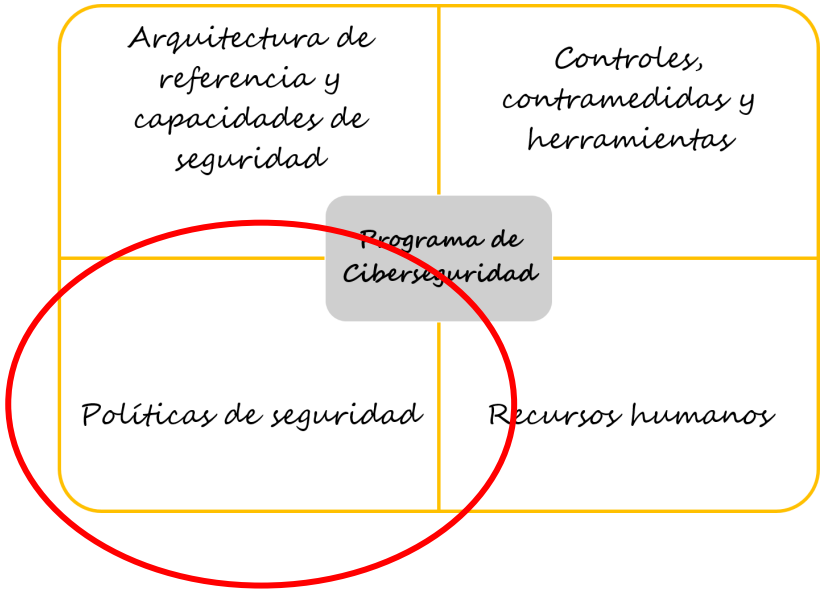
- El programa de seguridad es una planificación a largo plazo, define una estrategia, nos guía hacia una situación ideal.
- Normalmente en el corto plazo se trabaja con planes directores de seguridad.
  - Estos planes identifican la situación actual y planifican el trabajo a 12 ó 18 meses vista (como mucho).
- La estrategia de muchas organizaciones actuales se realinea con ciclos muy rápidos y el riesgo evoluciona también cada vez más en ciclos cortos, así que no tiene sentido intentar programar y planificar en el área de la seguridad a un plazo mucho mayor.

¿Os acordáis de Introducción a la Ciberseguridad en 1º?

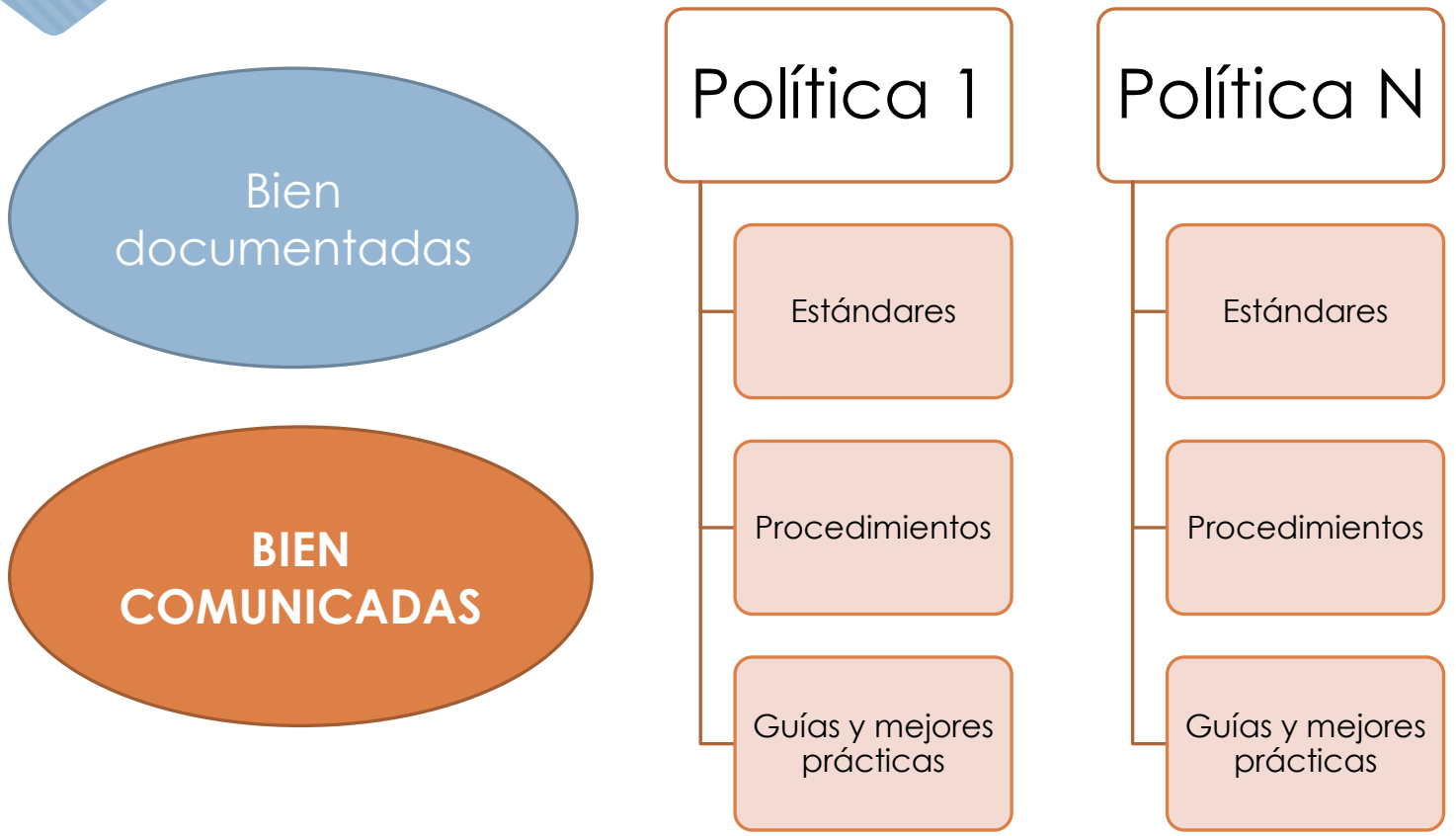


2. Modelos de control

¿Os acordáis de Introducción a la Ciberseguridad en 1º?



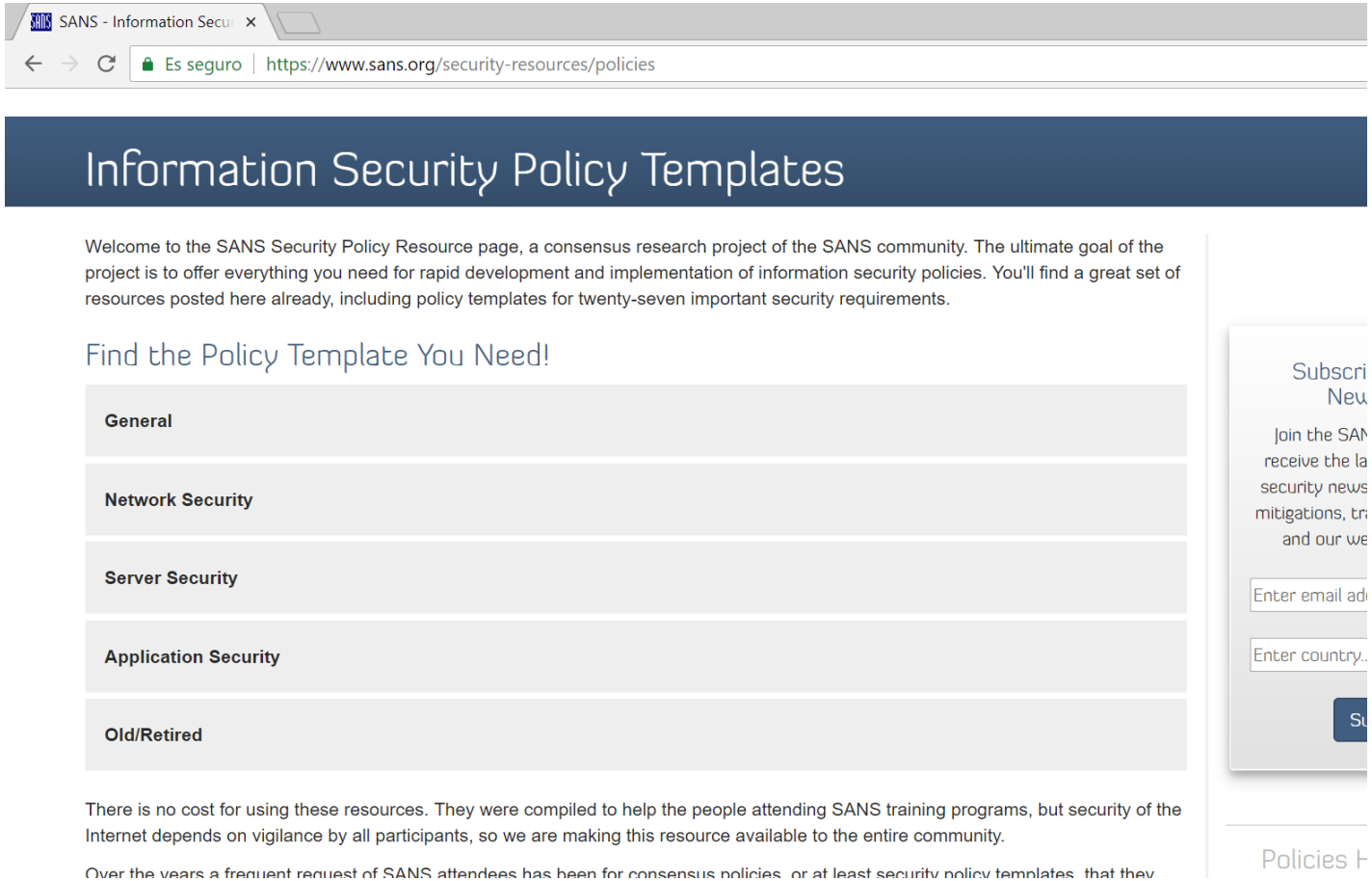
2. Modelos de control



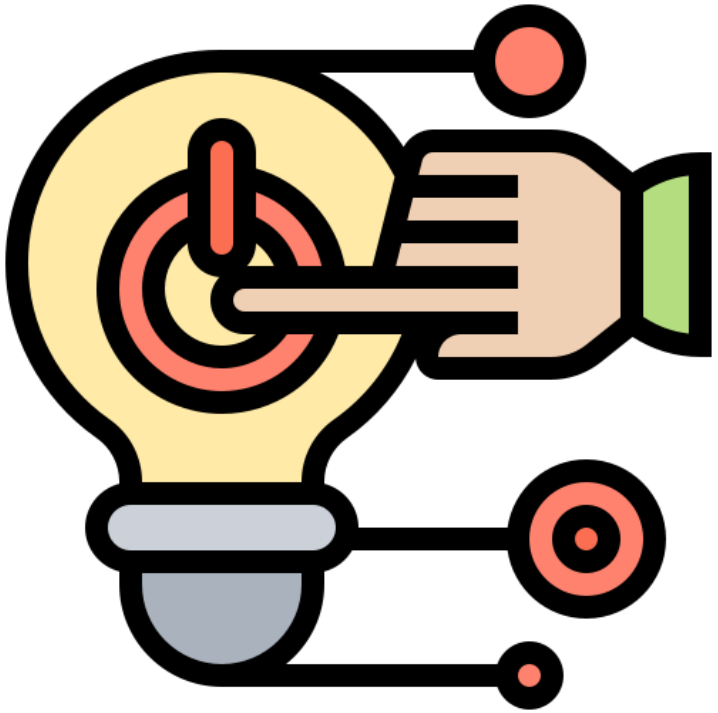
2. Modelos de control

- **Título de la Política:** Enunciado corto y de fácil comprensión que proporciona una línea de acción desde la dirección.
- **Estándares**: Traducción de estas políticas a detalles concretos de uso de HW y SW para los usuarios.
- **Procedimientos**: Instrucciones concretas acerca de cómo cumplir las políticas teniendo en cuenta los estándares. Suelen definir planes de instalación, testeo, administración, configuración, etc. para administradores y otros responsables.
- **Guías y mejores prácticas:** Completan los estándares y procedimientos con sugerencias que no son de obligado cumplimiento pero que pueden el trabajo de administradores y usuarios, etc.

2. Modelos de control



3. Gestión de la cadena de suministro



CASO 2

4. Retornos de inversión

- ROI (Return On Investment):

$$\text{ROI} = \frac{Beneficios - Gastos}{Gastos}$$

¿Cómo cuantificamos los beneficios de una inversión en mitigaciones de seguridad?

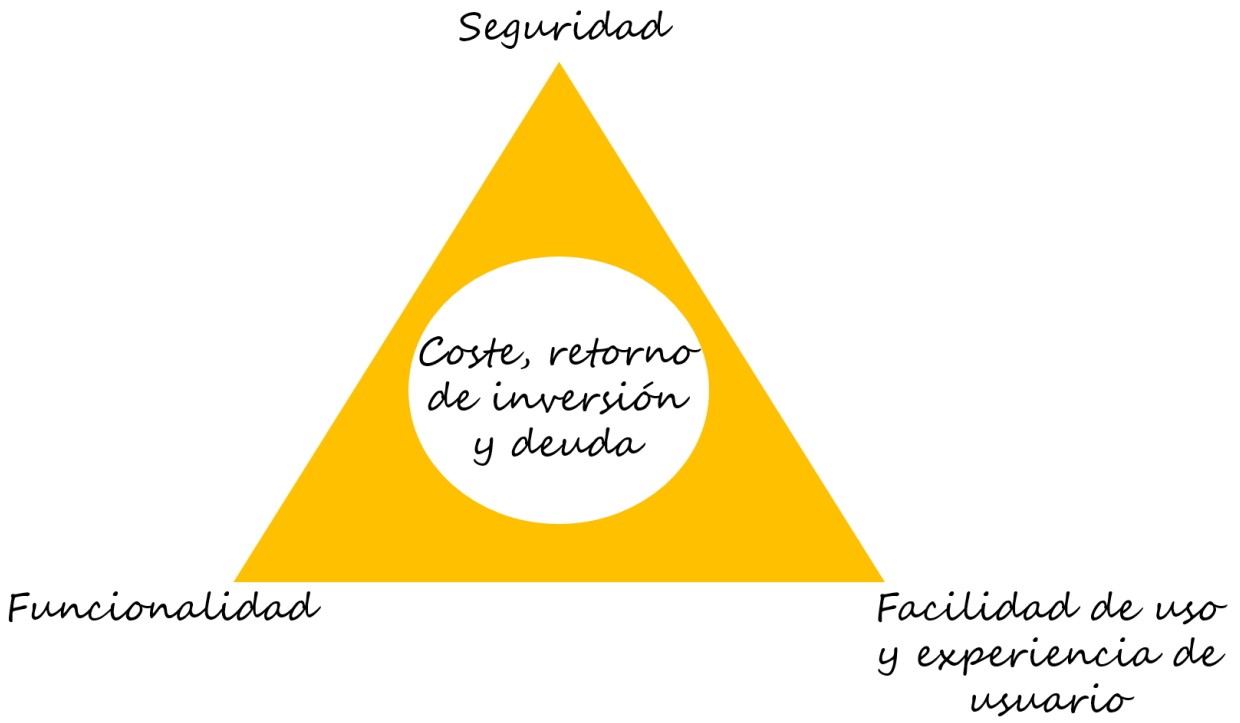
¿Y los gastos? Cuidado, que no pueden ser sólo los de adquisición….

4. Retornos de inversión

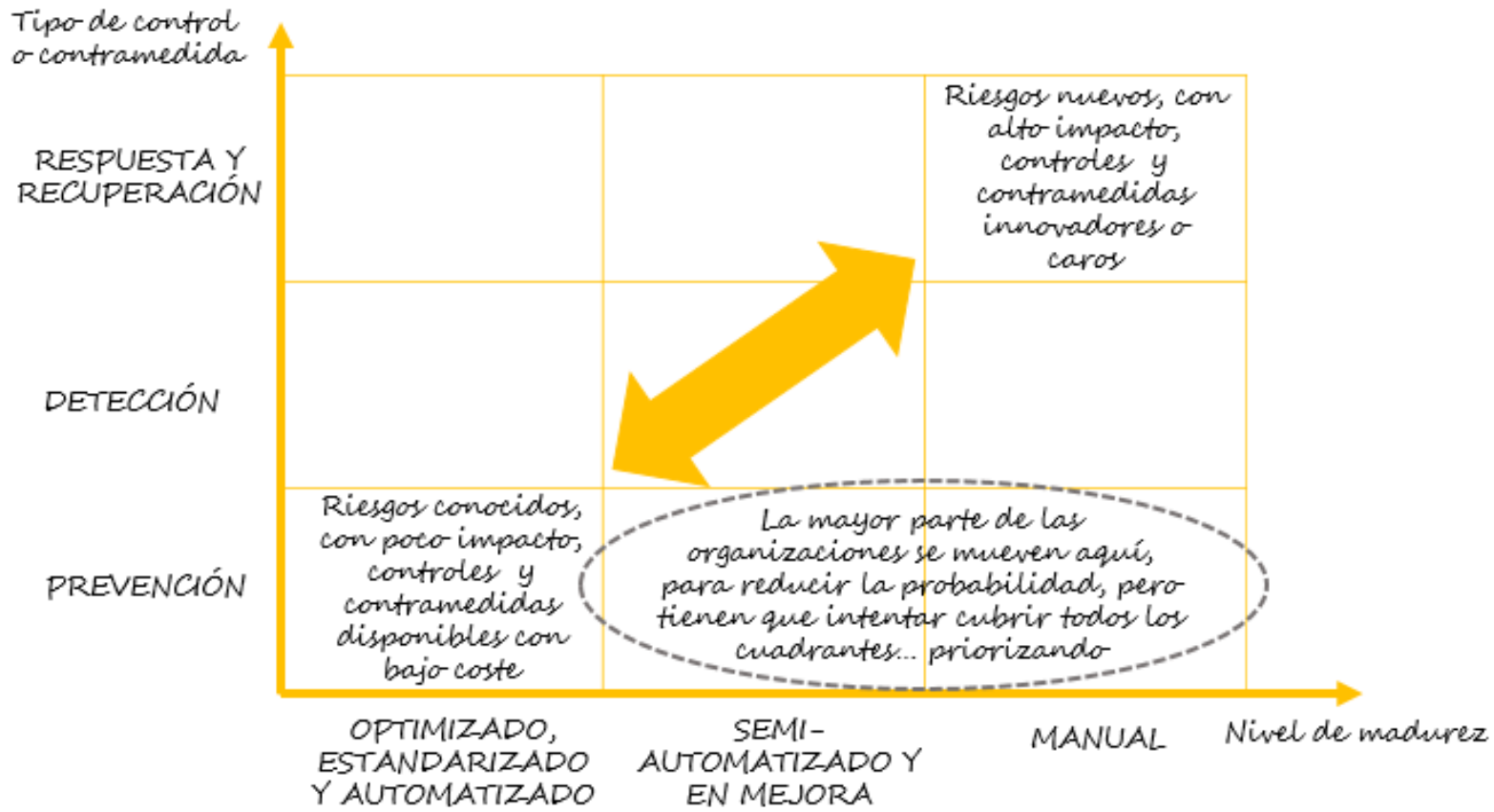
No es lo mismo invertir 10.000 € en un control que reduce el riesgo inherente en un 10% que hacerlo en uno que lo reduce en un 30%.

El problema es que en el cálculo del ROI es relativamente sencillo tener en cuenta lo que ganamos al realizar la inversión pero no lo que perdemos en cuanto a funcionalidad, experiencia de usuario, etc.

Cuidado además, se debe tener en cuenta el TCO, no sólo el coste inicial de las mitigaciones.



4. Retornos de inversión



4. Retornos de inversión

- Otro concepto interesante es el de deuda técnica en relación con la ciberseguridad.
  - TDR o Technical Debt Ratio.
- El TDR se calcula dividiendo el coste de resolución de la deuda (el coste que implica arreglar lo que está mal) entre el coste total de la infraestructura en la que ésta se ha creado.

Para leer e investigar…

- Dutta, Ashutosh, and Ehab Al-Shaer. ""“What”,“Where”, and “Why” Cybersecurity Controls to Enforce for Optimal Risk Mitigation." *2019 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2019.
- Martinez, Jabier, et al. "Security Debt: Characteristics, Product Life-Cycle Integration and Items." 2021 IEEE/ACM International Conference on Technical Debt (TechDebt). IEEE, 2021.

Referencias

- Fotografías
  - https://unsplash.com
- Iconos
  - https://www.flaticon.es/