

enise



inteco



Instituto Nacional
de Tecnologías
de la Comunicación

Centros de Operación de la seguridad

La clave está en los procesos

T25 Externalización de servicios seguros

Marcos A. Polanco Velasco, CISSP, CISM, CISA, ITIL

Director

Ironwall

Ironwall
STRATEGIC SECURITY SYSTEMS



1. Introducción
2. Problemática actual
3. Seguridad gestionada basada en sistemas sociotécnicos
4. Conclusiones





Instituto Nacional
de Tecnologías
de la Comunicación

1. Introducción



**Capacidad
técnica**



**Disciplina
operativa**

Errar es humano

- ✓ El 42% de los fallos de seguridad (security breaches) son ocasionados por errores humanos
- ✓ El 80% de los cortes de servicio son ocasionados por errores de las personas o en los procesos, sobre todo en la gestión de cambios





Instituto Nacional
de Tecnologías
de la Comunicación

2. Problemática actual



Errores comunes en la operación de la seguridad

Tres factores asociados a los errores

✓ Tecnológico

✓ Humano

✓ Organizacional

Los errores humanos pueden derivar en tres tipos de problemas de seguridad

✓ Errores de configuración al instalar productos

✓ Incapacidad de dar seguimiento a las configuraciones de los sistemas

✓ Incapacidad de reconocer cuando un ataque está sucediendo

Este tipo de errores tienen un impacto al negocio y por lo tanto son un riesgo

Impacto sobre la eficiencia y eficacia

Las organizaciones que NO siguen mejores prácticas invierten entre el 35y 45% de su tiempo en la recuperación de servicios y trabajo no planeado ni programado

La probabilidad de fracaso al realizar un cambio sin gestionarlo, controlarlo y monitorizarlo es del 30%

La naturaleza del perfil genera otros problemas

Normalmente nos enfocamos más a los aspecto técnicos

Características del perfil técnico, altamente especializado, como la seguridad lo requiere

- ✓ No le gusta documentar
- ✓ No le gusta seguir procedimientos
- ✓ Quiere resolver los problemas
- ✓ No siempre mide el impacto de sus acciones

Conocimiento concretado en unas cuantas personas específicas

Falta de documentación

Ejemplo reciente

En agosto de este año Cisco.com experimentó un corte de servicio por más de 2 horas debido a un error humano

Al aplicar un cambio común dentro de las actividades de mantenimiento, el cual tuvo resultados no previstos

enISE



inteco



Instituto Nacional
de Tecnologías
de la Comunicación

3. Seguridad gestionada basada en sistemas sociotécnicos (SST)



Los sistemas sociotécnicos

Un sistema que contempla las tecnologías y las personas así como sus implicaciones organizacionales y culturales como parte de un sistema integral donde cada subsistema interactúa con los demás y por lo tanto influye en ellos

Un sistema sociotécnico surge cuando las interacciones cognitivas y sociales son medidas por tecnologías de la información

Los sistemas sociotécnicos

La Ciberseguridad es una mezcla compleja de interacciones tecnológicas y sociales dentro de una organización

El desempeño de la organización para alcanzar su objetivo está en función de su capacidad de encajar estos dos sistemas (tecnológico y social)

Los sistemas sociotécnicos

Características

- ✓ Misión específica
- ✓ Funciones específicas
- ✓ Personas
- ✓ Organización humana
- ✓ Evolución constante para mayor eficiencia

Componentes del sistema sociotécnico de un SOC

✓ Modelo metodológico



✓ Modelo tecnológico



✓ Modelo Operacional



✓ Modelo Organizacional

Modelo Organizacional

Roles

Funciones

Responsabilidades

Interacciones

Planes de formación

Matrices de escalado

Modelo Operacional

Procesos asociados al talento humano

✓ Reclutamiento

✓ Formación

✓ Operativa

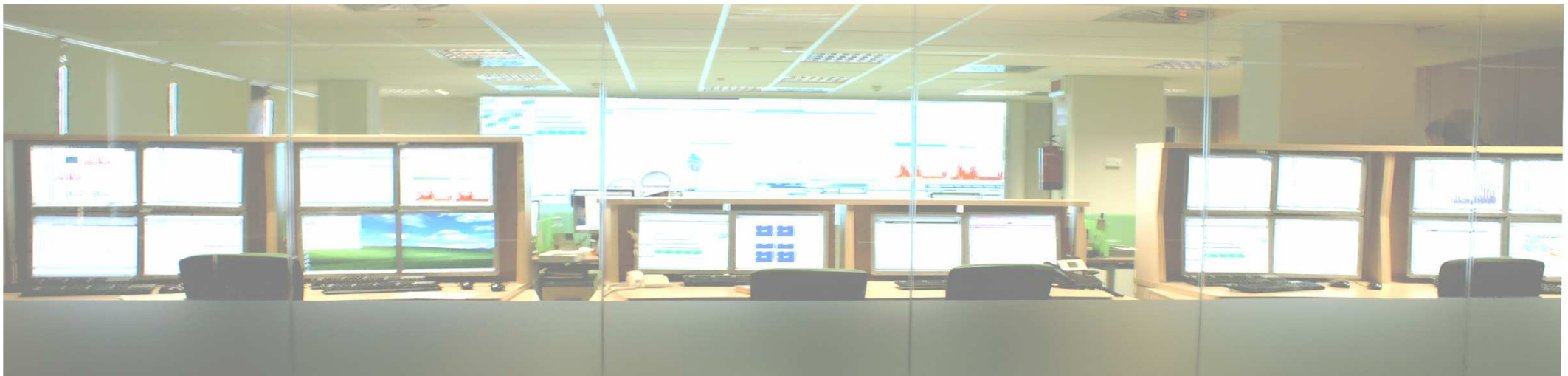
✓ Técnica

✓ Retención

Procesos de Monitorización

✓ Recolección, análisis e informe de eventos, actividades sospechosas e incidentes

✓ Gestión de eventos de seguridad



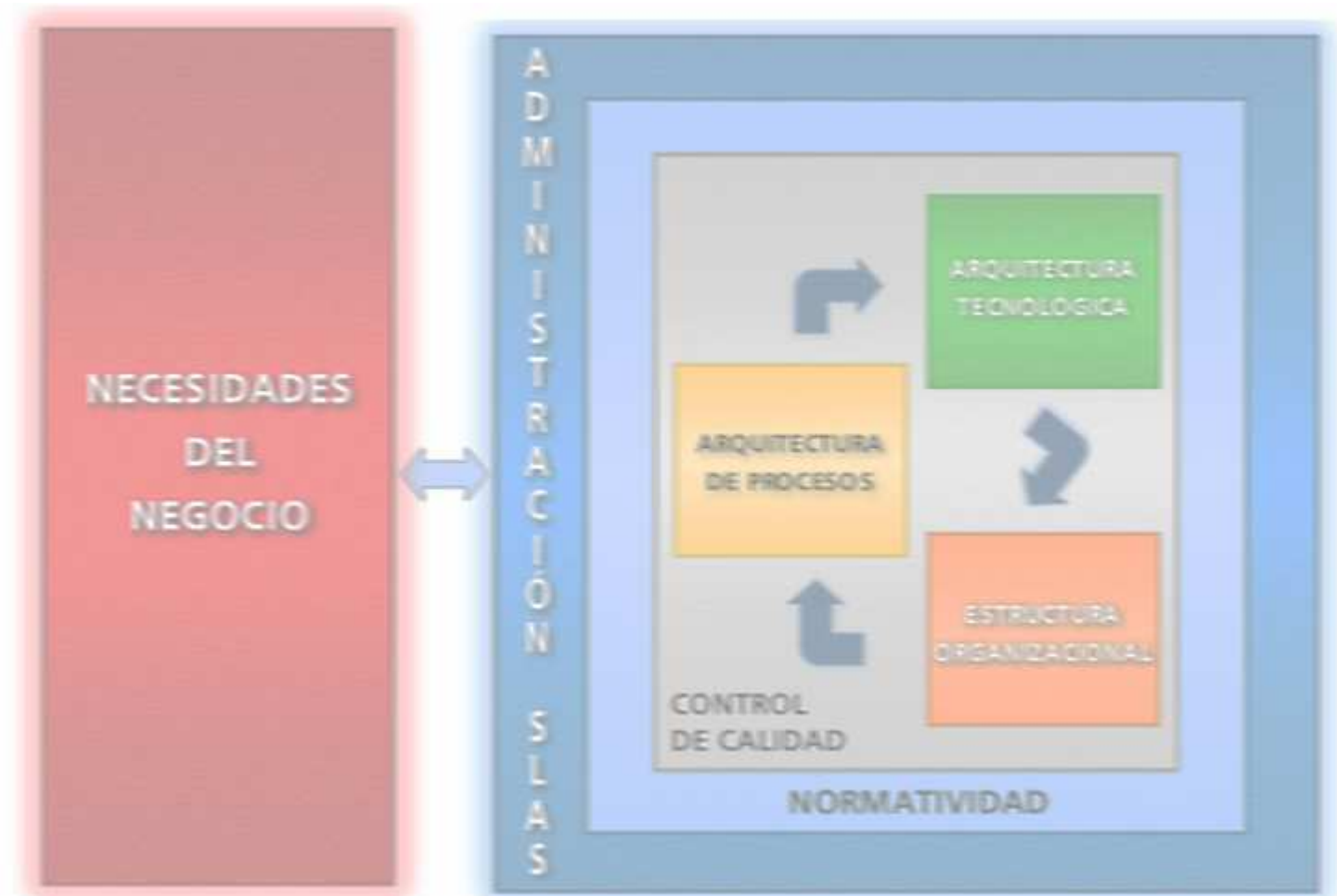
Modelo Metodológico

ITIL/ISO20000

ISO27000

CERT/CC

ISO9000



Modelo Tecnológico

Todos los sistemas para la operación

- ✓ Sistemas de correlación
- ✓ Sistemas de monitorización
- ✓ Sistemas de service desk
- ✓ Sistemas de gestión de logs
- ✓ Sistemas de análisis forense
- ✓ Sistemas de inteligencia

Funciones del sistema

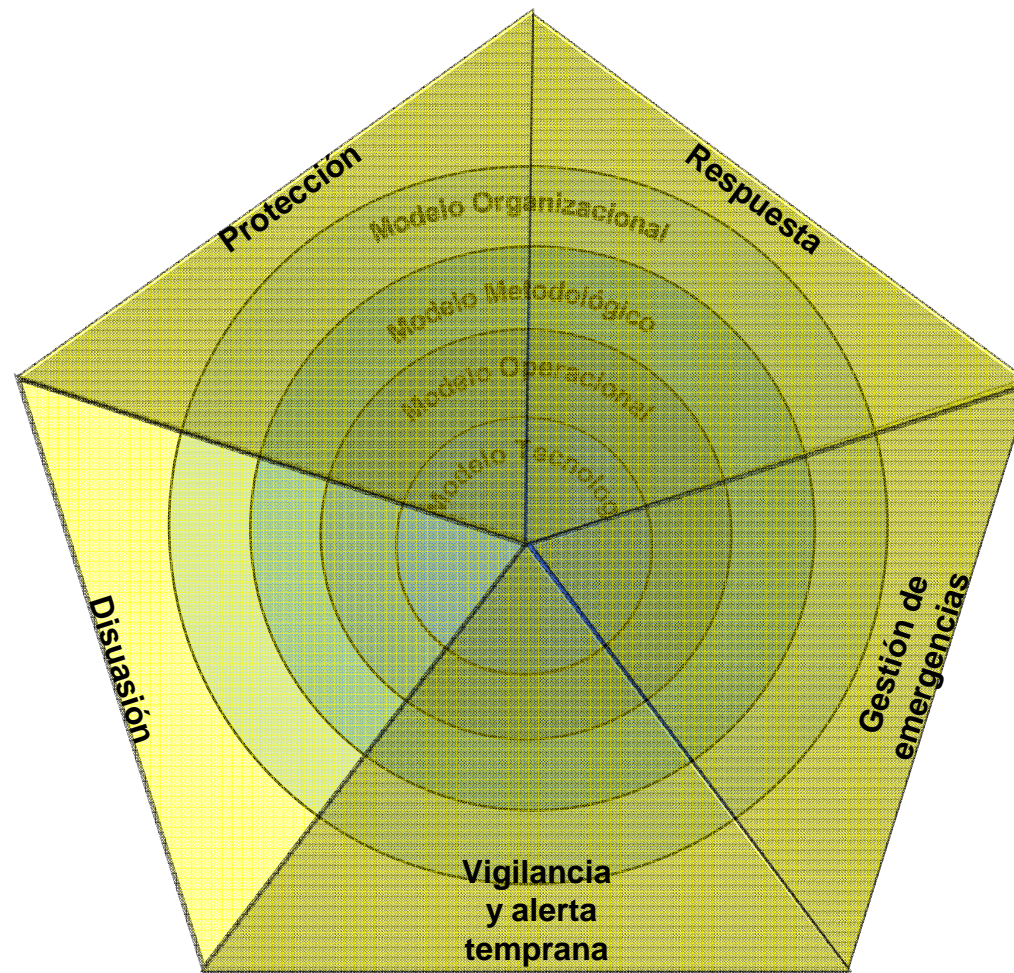
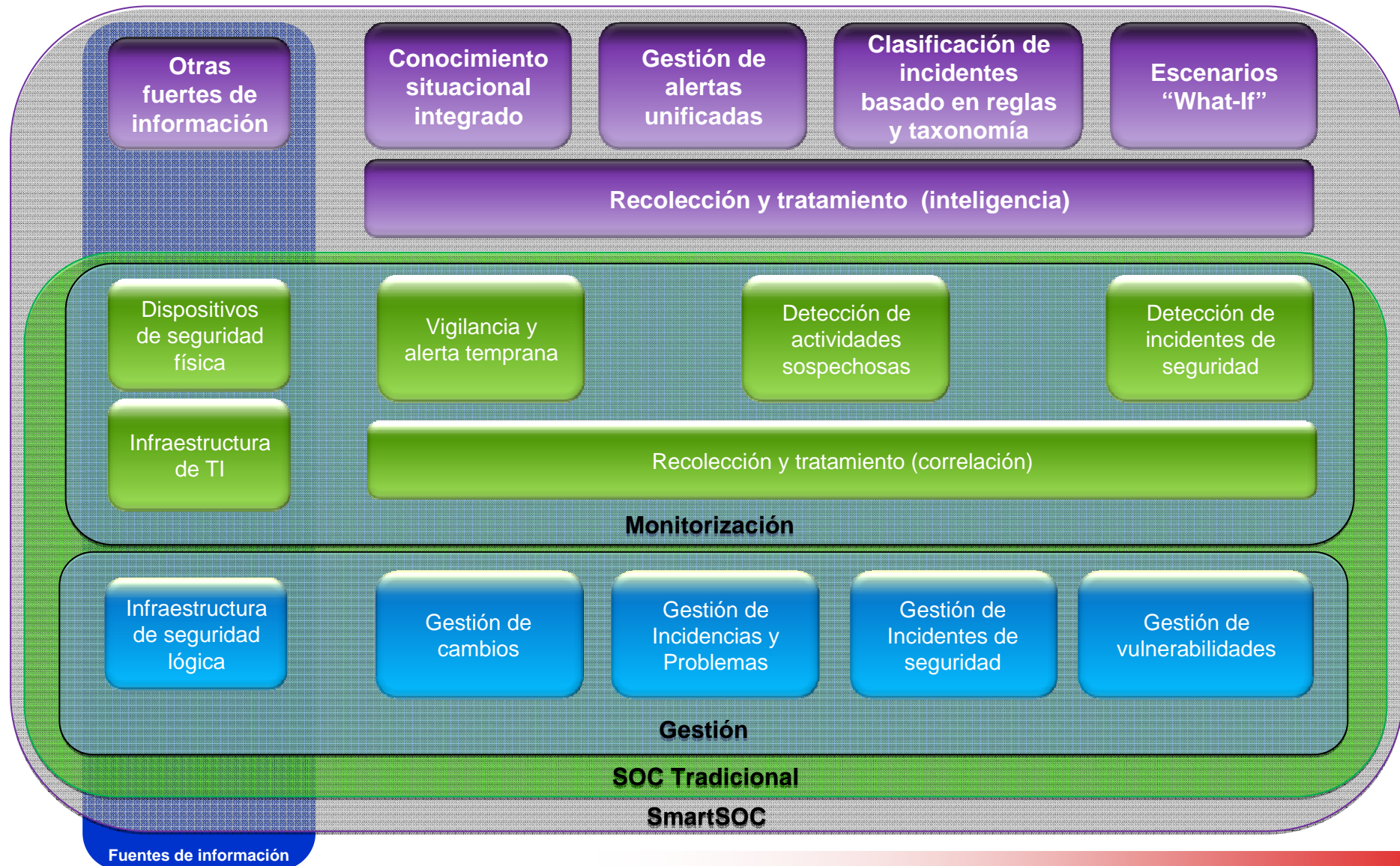


Diagrama conceptual





Instituto Nacional
de Tecnologías
de la Comunicación

4. Conclusiones



Capacidad técnica vs Disciplina operativa

- ✓ Capacidad técnica sin disciplina operativa dará problemas
- ✓ Disciplina operativa sin capacidad técnica también



La disciplina operativa

- ✓ Uno de los principales retos de los proveedores de seguridad gestionada (además de lograr un alto conocimiento técnico)
- ✓ De igual forma, si decidimos montar nuestro propio SOC , no debemos olvidarla
- ✓ La automatización de los procesos donde sea posible para garantizar una ejecución ordenada y consistente
- ✓ Al buscar un proveedor es importante ver su nivel de madurez operativa, es decir, su disciplina así como su metodología

Sistemas sociotécnicos

- ✓ Considerar todos los aspectos sociales y tecnológicos para un enfoque adecuado
- ✓ Al contar con una plataforma de operación basada en sistemas sociotécnicos es mucho más fácil evolucionar los servicios de seguridad gestionada hacia sistemas de inteligencia

Muchas gracias

