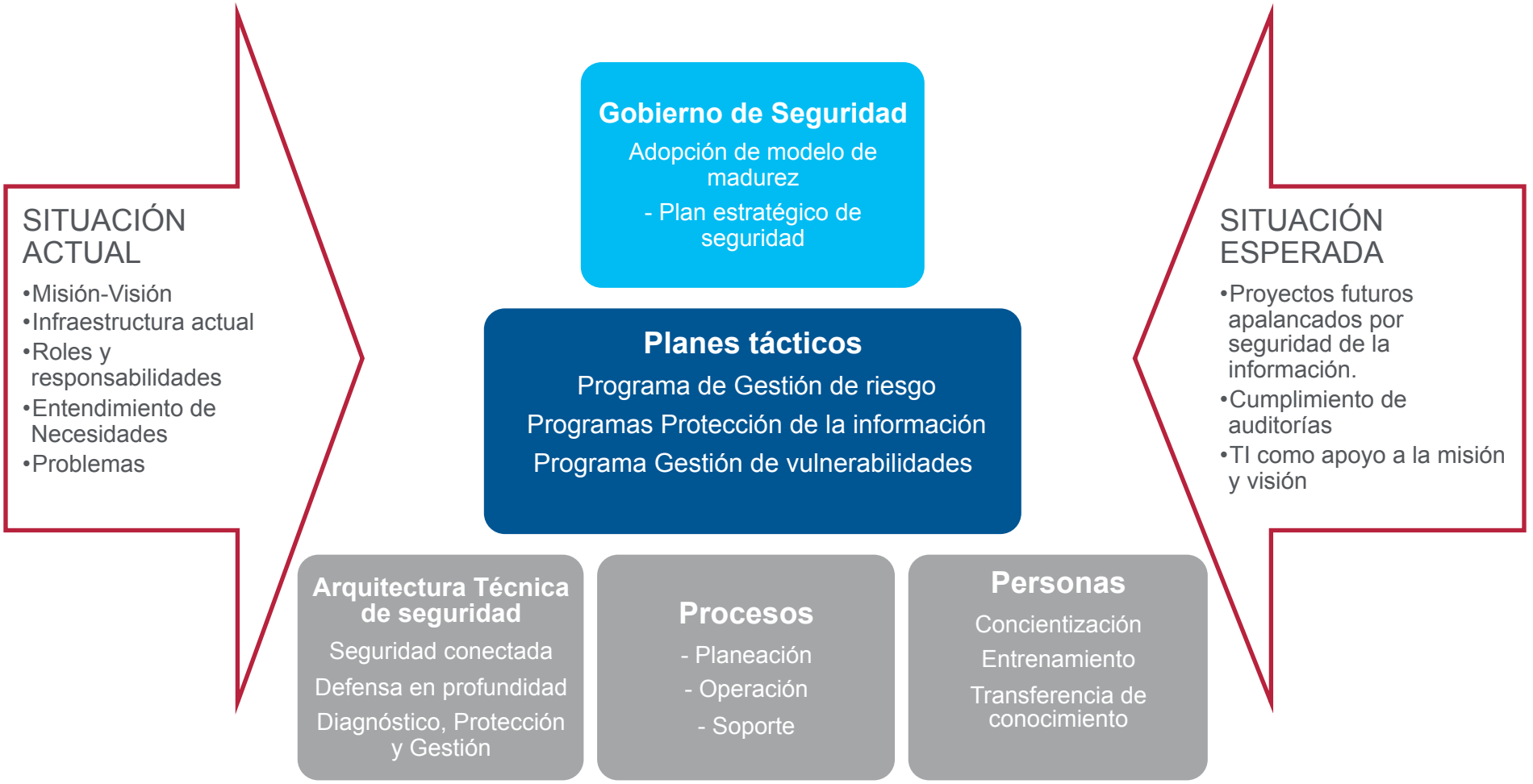
intel Security

Diagnóstico de Seguridad Informática

Evaluación para solución de problemas y cumplimiento de objetivos estratégicos

TM

Alcance


SITUACIÓN ACTUAL
•Misión-Visión
•Infraestructura actual
•Roles y responsabilidades
•Entendimiento de Necesidades
•Problemas
Gobierno de Seguridad
Adopción de modelo de madurez
- Plan estratégico de seguridad
Planes tácticos
Programa de Gestión de riesgo
Programas Protección de la información
Programa Gestión de vulnerabilidades
Arquitectura Técnica de seguridad
Seguridad conectada
Defensa en profundidad
Diagnóstico, Protección y Gestión
Procesos
- Planeación
- Operación
- Soporte
Personas
Concientización
Entrenamiento
Transferencia de conocimiento
SITUACIÓN ESPERADA
•Proyectos futuros apalancados por seguridad de la información.
•Cumplimiento de auditorías
•TI como apoyo a la misión y visión

Matriz de Madurez de ciberseguridad

Modelo de madurez de Ciber - resistencia									
intel Security	Basico o reactivo		Establecido		Avanzado y Proactivo		Optimizado		intel Security
	Procesos no estandarizados		Procesos establecidos y se repiten para evaluarse		Se está en constante mejora Los SLAs son un indicador		Procesos automatizados y alineados a los objetivos de la organización		
Procesos									
Promedio Nivel de avance		8%		0%		0%		0%	
Personas									
Promedio Nivel de avance		7%		0%		0%		0%	
	Reactivo y Manual		Basado en Herramientas		Modelo Integrado		Defensa Dinámica		Resistencia organizacional
	Se tienen herramientas actuando de forma parcial		Las herramientas están definidas y hacen su trabajo de forma completa		Hay integración y colaboración para mejorar la visibildiad y contexto		Se tiene un modelo predictivo y se tiene defensas dinámicas adaptables		Se identifican incidentes, se toman acciones de forma automática. El modelo es preventivo y se soportan procesos de negocio
Tecnología									
Perímetro		7%		3%		0%		0%	0%
Contenido avanzado		0%		0%		0%		0%	0%
Host y servicios (Correo y Web)		38%		10%		0%		0%	0%
Aplicación		0%		0%		0%		0%	0%
Datos		0%		0%		0%		0%	0%
SIEM - Gestión		0%		0%		0%		0%	0%
Promedio Nivel de avance		1%		1%		0%		0%	0%

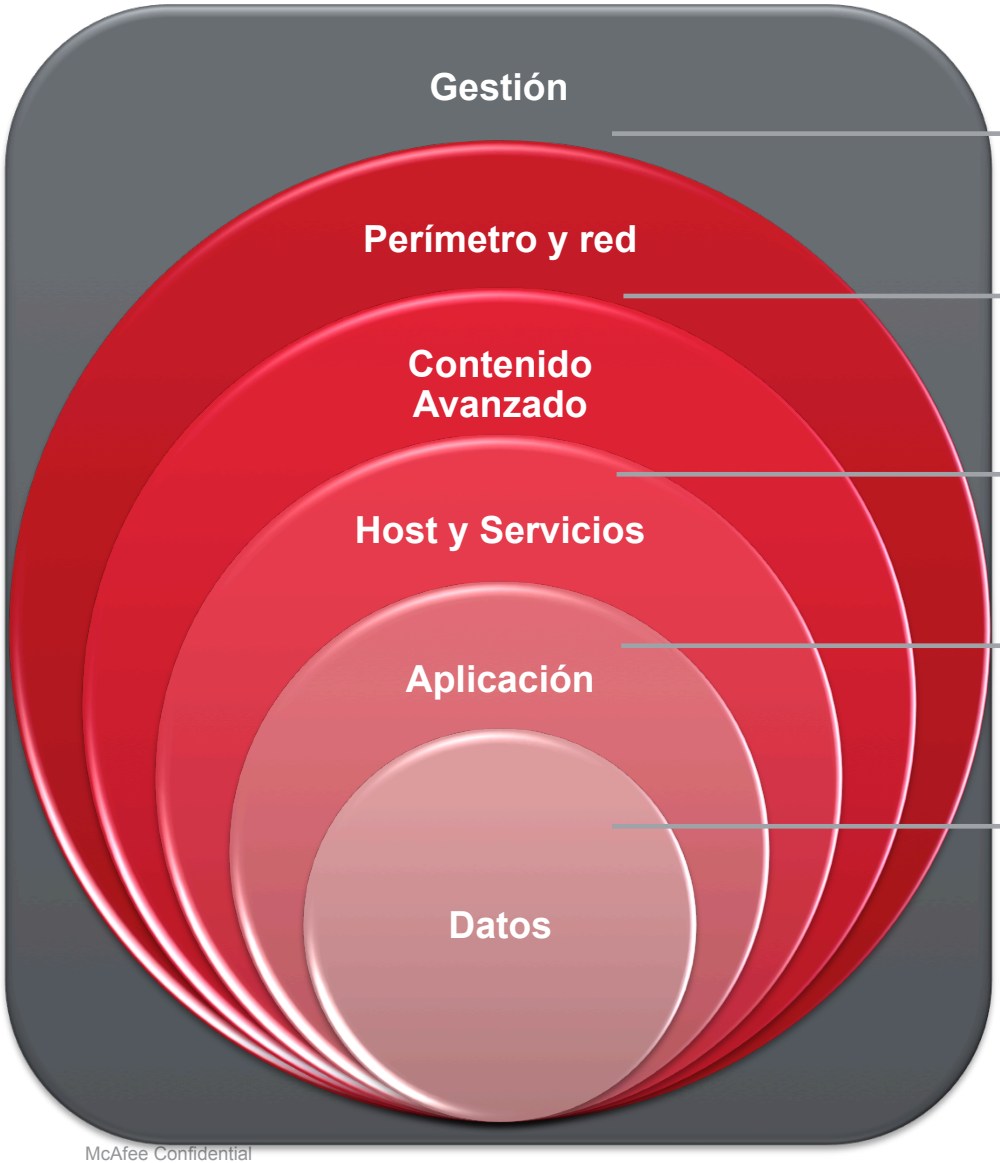
Modelo basado en marco de referencia COBIT de madurez de Tecnología de la información.

Permite identificar el nivel actual de seguridad y realizar mediciones de avances

Se traza el camino para llegar a un modelo de alto nivel de seguridad,, sostenible en el tiempo

Anillos de seguridad tecnológica

Defensa en profundidad



Visibilidad, monitoreo y correlación
Alertas tempranas y nivel de riesgo

Control de acceso y anomalías
Segmentación y filtros de tráfico de red

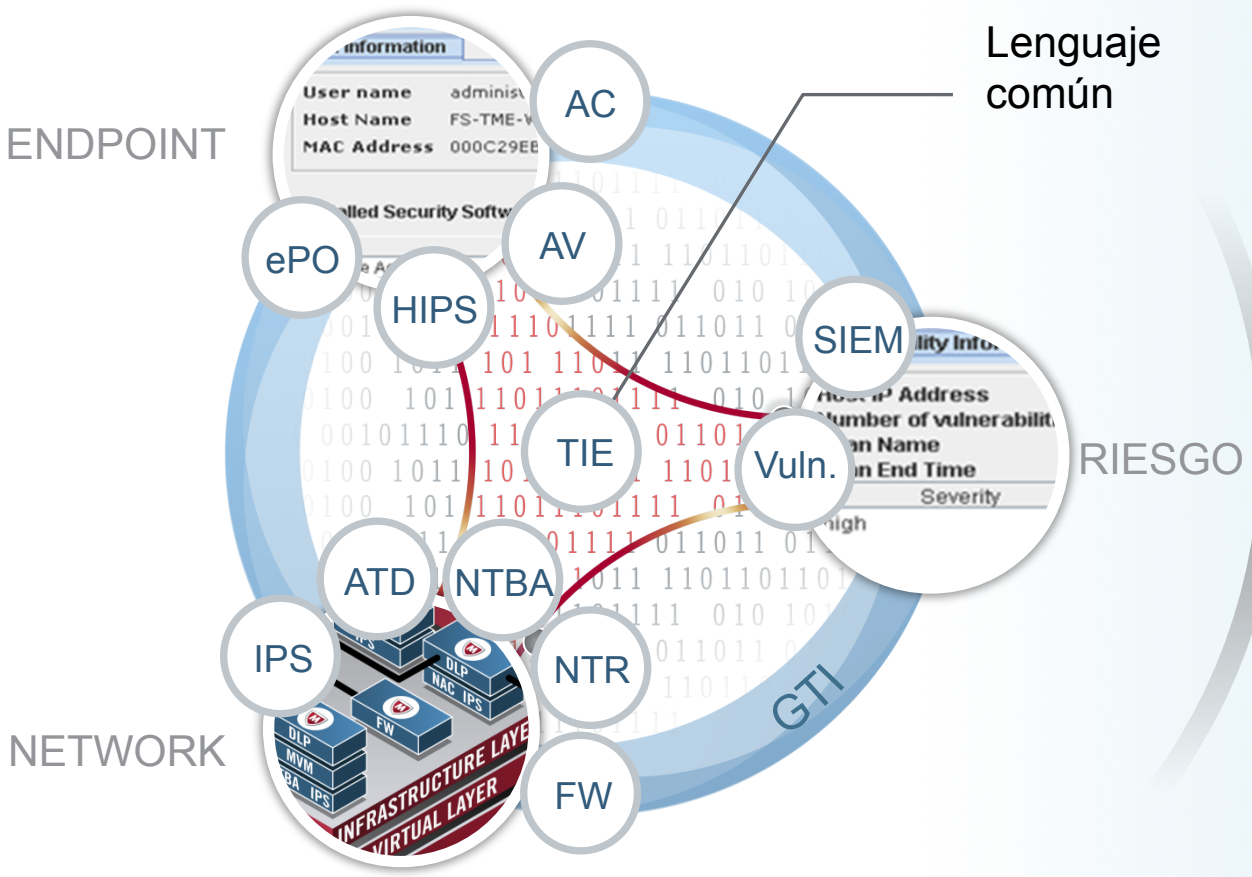
Detección de amenazas avanzadas persistentes e inteligencia adaptativa

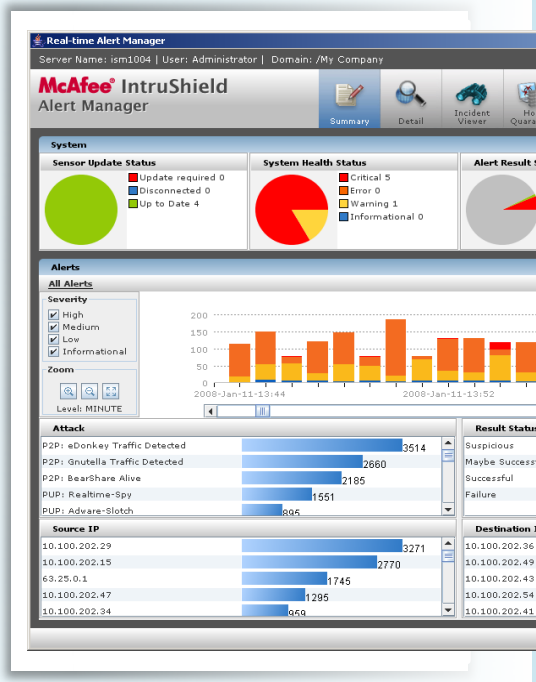
Protección de estaciones finales y servidores (contexto local)

Protección de aplicaciones (Aplicaciones claves)

Autenticación y acceso seguro
Clasificación y control de información sensible

Valor de la integración





Tecnologías de seguridad interconectadas

Inteligencia en las soluciones

Respuesta y entendimiento en tiempo real

Beneficios

Promesa de valor de la optimización y mejora, soportado por la propuesta de Intel Security

DISPONIBILIDAD
Optimización de los recursos actuales

- Garantizar disponibilidad de la red y recursos
- Gestión enriquecida para soportar el crecimiento
- Ahorro de la ocupación de los actuales canales de comunicación (MPLS e Internet)
- Mejora en los tiempos de respuesta de aplicaciones

INTEGRIDAD
Trazabilidad y gestión de cambios

- Minimizar el daño o alteración de la información
- Trazabilidad y autorización de cambios
- Configuraciones consistentes y seguras

CONFIDENCIALIDAD
Protección tráfico y datos

- Comunicaciones seguras
- Priorización de tráfico
- Minimización de suplantación o robo de identidad o de los datos
- Acceso seguro