TOGAF y Gestión de Requisitos en Infraestructura Crítica

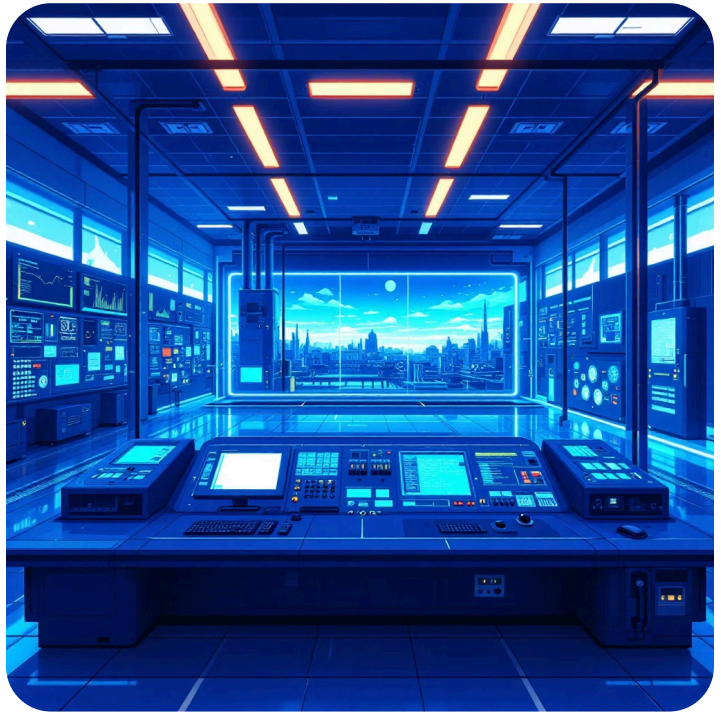
Caso práctico: **HidroTech** - Integración metodológica para ciberseguridad en servicios públicos de agua potable

HidroTech: Contexto Estratégico

Infraestructura Crítica

Empresa de servicios públicos responsable del suministro de agua potable para la ciudad

- Sistemas de control industrial (OT)
- Dosificación química automática
- Bombas de presión distribuidas



Riesgos Críticos Identificados

Integridad

Manipulación de químicos en el proceso de tratamiento

Impacto: Salud pública comprometida

Disponibilidad

Fallo en el suministro de agua potable

Impacto: Continuidad urbana afectada

Cumplimiento

Adherencia a normativas ISA/IEC 62443

Imperativo: Evolución sin interrupciones

La Sinergia TOGAF: Fase H + Gestión de Requisitos

> La interdependencia crítica entre la Fase H de TOGAF y la Gestión de Requisitos forma la base de la resiliencia operacional en infraestructura crítica

Gestión de Requisitos: Del "Qué" al "Cómo"

01

Identificación

Determinar la necesidad de protección más alta según criticidad del activo

02

Gestión

Traducir requisitos a soluciones de Arquitectura Tecnológica específicas

03

Validación

Confirmar eficacia sin comprometer la disponibilidad operacional

Requisito Crítico Implementado

Necesidad Identificada

> "Los comandos de dosificación química del SCADA deben ser inmutables y estar firmados digitalmente para asegurar la integridad del agua"

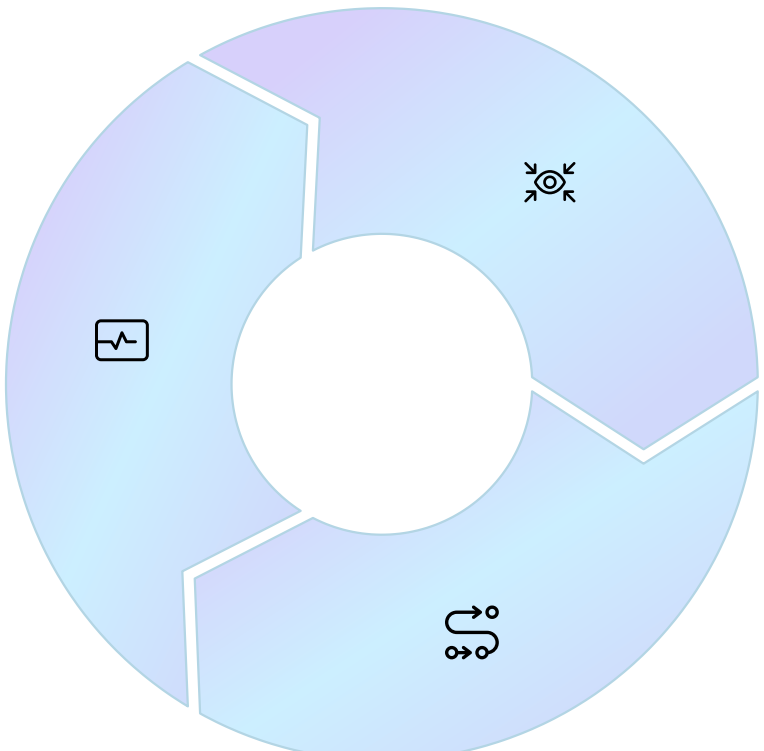
Solución Arquitectónica

- Firewalls Industriales con DPI
- Módulo de Firma Digital en SCADA
- Tiempo de respuesta < 50ms

Fase H: Gestión del Cambio Arquitectónico

Monitoreo

Vigilancia continua de cambios internos y externos



Evaluación

Análisis de impacto en arquitectura actual

Activación ADM

Inicio de nuevos ciclos cuando es necesario

Escenarios de Activación del ADM

Innovación (Medidores IoT)

Cambio: Miles de nuevos puntos de acceso inalámbrico

Impacto: Superficie de ataque ampliada

Acción: Sistema IAM para dispositivos

Amenaza Externa (Ransomware)

Evento: Ataque similar desactiva bombas

Evaluación: Arquitectura de respaldos insuficiente

Solución: DRP aislado

Auditoría (Acceso Remoto)

Hallazgo: Política de proveedores deficiente

Urgencia: Revisión inmediata requerida

Implementación: Jump Box con PoLP

Arquitectura de Respuesta Resiliente

Detección

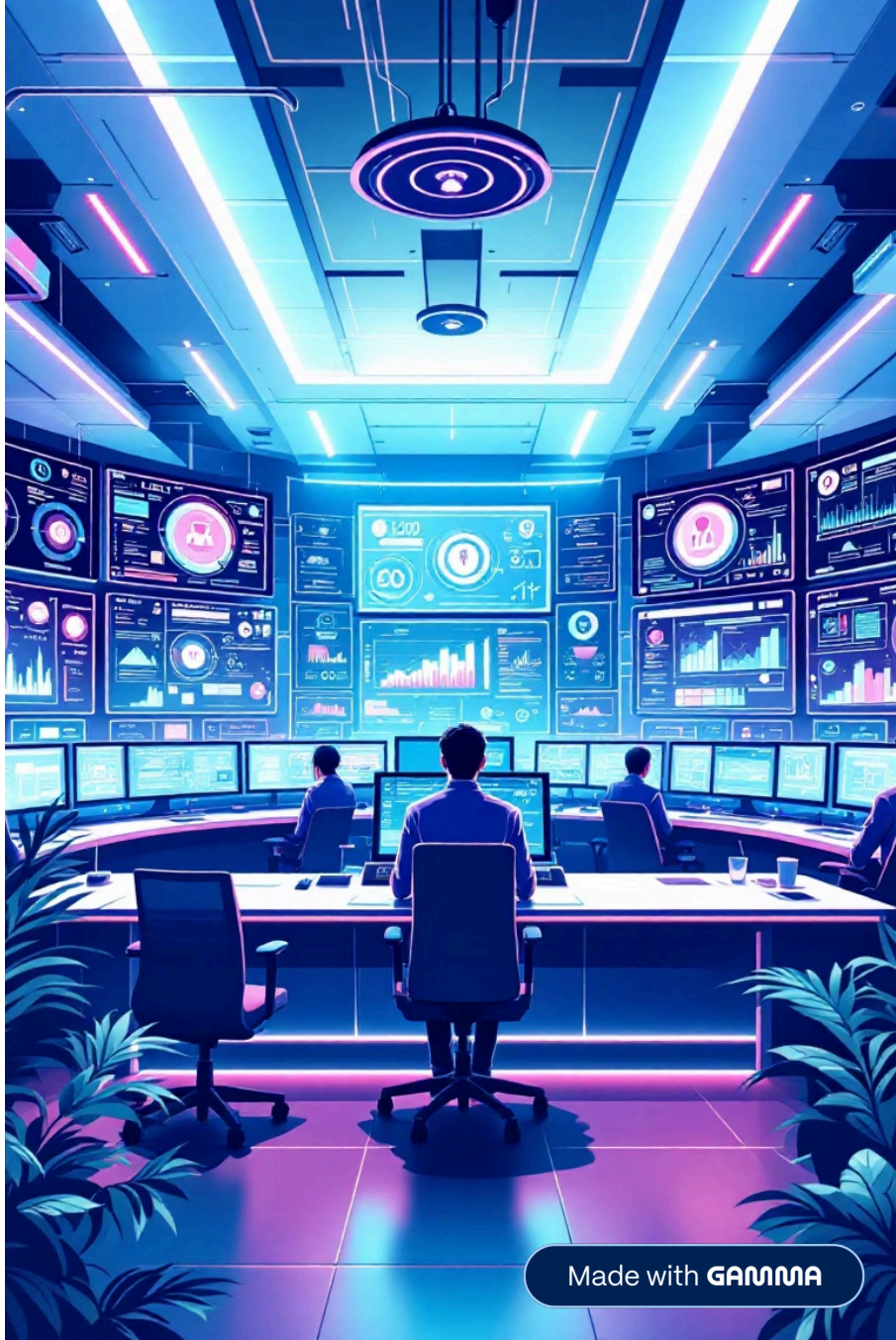
Monitoreo 24/7 de amenazas y cambios operacionales

Respuesta

Activación automática de protocolos de seguridad

Recuperación

Restauración controlada sin comprometer la continuidad



Conclusión: Resiliencia Operacional

Marco Integrado TOGAF

La sinergia entre Fase H y Gestión de Requisitos asegura:

- Protección de la salud pública
- Continuidad del servicio crítico
- Evolución tecnológica segura
- Cumplimiento normativo continuo

> La arquitectura de ciberseguridad se convierte en un habilitador estratégico, no en una barrera operacional