VI CONGRESO INTERNACIONAL
DE CIBERSEGURIDAD, PREVENCIÓN
DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA
Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

MAS ALLA DE LA ALERTA

IA y la Autogestión de Crisis en la Banca Moderna

Rodrigo Castellanos

Country Manager — Panamá

+15 años en ciberseguridad defensiva y respuesta a incidentes

rcastellanos@devel.group

02:47 AM

Tu teléfono suena.

¿Cuántos han vivido algo similar?

VI CONGRESO INTERNACIONAL
DE CIBERSEGURIDAD, PREVENCIÓN
DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA
Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

Más Allá de la Alerta

IA y la Autogestión de Crisis en la Banca Moderna

Rodrigo Castellanos

Anatomía de un Incidente Bancario

7 flujos que se activan simultáneamente al confirmar un incidente

Contención Técnica

Evaluación de Impacto

Notificación Interna

Comunicación a Regulador

Preservación de Evidencia

Gestión de Terceros

Documentación Continua

Se activan en paralelo — no en secuencia

¿Cuántos de estos flujos tiene su organización automatizados hoy?

Lo que el Regulador Exige en un Incidente

Regulaciones activadas simultáneamente en un incidente de fraude interno

Acuerdo 3-2012

Riesgo TI y Seguridad de la Información

Notificación a SBP mediante formulario. Monitoreo de usuarios privilegiados.

Acuerdo 001-2022

Protección de Datos Personales Bancarios

Comunicar al titular y a SBP en incidentes significativos de datos personales.

Acuerdo 11-2018

Riesgo Operativo

Evento de riesgo operativo por acción deliberada de personal. Registro obligatorio.

Ley 81 de 2019

Protección de Datos Personales

Informar al titular lo más pronto posible cuando datos hayan sido sustraídos.

En un incidente de fraude interno con exfiltración de datos, se activan TODAS simultáneamente.

La Brecha entre la Regulación y la Realidad

Lo que pide el regulador	Lo que la mayoría hace	Lo que debería ser
Notificación al regulador mediante formulario establecido	Redacción manual post-incidente. Demora en preparación y envío.	Borrador generado en tiempo real. Listo para revisión y envío.
Documentación de todas las acciones de respuesta	Logs manuales, incompletos, reconstruidos después del incidente.	Documentación automática continua durante todo el incidente.
Evaluación de impacto a clientes afectados	Análisis manual que tarda días. Alcance impreciso.	Correlación automática con bases afectadas + estimación de impacto.

Ejemplo — 3 de más de 20 requisitos regulatorios mapeados

80%

del dolor de un incidenteno es técnico.

Es operativo y regulatorio.

¿Y si la documentación se escribiera sola mientras gestionas el incidente?

La disciplina precede a la automatización.

Si automatizas el caos,
solo tienes caos más rápido.

Niveles de Autonomía AI en Seguridad

¿Hasta dónde puede llegar su organización?

Agente Autónomo
AI actúa con guardrails.
Humano supervisa y audita.

Agente Supervisado
AI propone acciones,
humano aprueba antes de ejecutar.

Filtro
AI procesa volumen,
humano valida lo relevante.

Herramienta
Humano pide, AI responde.
Uso manual, caso por caso.

← **La mayoría está aquí**

4 Capas de Asistencia AI en Respuesta a Incidentes

COMUNICACIÓN

Borradores de notificación adaptados al contexto: regulador, comité de crisis, clientes afectados.

DOCUMENTACIÓN

Reportes regulatorios generados en tiempo real. Timeline de acciones automático. Nada se pierde.

ORQUESTACIÓN

Acciones priorizadas basadas en procedimientos pre-aprobados. Contención → evidencia → notificación.

CORRELACIÓN

Contextualización de la alerta: sistemas afectados, datos en juego, impacto al negocio.

HUMANO

Valida
Decide
Ejecuta

La AI prepara. El humano tiene la última palabra.

Regulación + AI: **El Antes y el Después**

Requisito SBP	⚠ Sin AI	✓ Con AI
Notificación a regulador mediante formulario	Redacción manual post-incidente. Demora en preparación.	Borrador generado en tiempo real. Listo para revisión.
Documentación de acciones de respuesta	Logs manuales, incompletos. Reconstruidos después.	Documentación automática continua durante el incidente.
Evaluación de impacto a clientes	Análisis manual. Días de trabajo. Alcance impreciso.	Correlación automática + estimación de impacto.

El mapeo completo cubre más de 20 requisitos regulatorios

Ejercicio Práctico

Fraude Interno con Acceso Privilegiado — Respuesta Asistida por AI

ESCENARIO

Actor: Administrador de BD senior, 8 años en la organización
Datos: 47,000 registros de clientes corporativos (saldos >$100K)
Método: Extracción durante ventanas de mantenimiento (3 semanas)
Exfiltración: Copia a dispositivo USB personal
Acceso: Legítimo — usuario autorizado con permisos activos

Pregunta a la sala: ¿Revocan acceso de inmediato o investigan primero?

Dashboard
Incidentes
Regulatorio
Reportes
Configuración

Resumen Operativo

Período activo — 18 Marzo 2026

3	1	87%	12
ACTIVOS	PEND. REGULATORIO	CUMPLIMIENTO	ESTE MES

INCIDENTES RECIENTES

Todos | Activos | Críticos

ID INCIDENTE	SEVERIDAD	DESCRIPCIÓN	FECHA	ESTADO
INC-2026-0046	• ALTO	Phishing — campaña dirigida corp.	09-Mar	• ACTIVO
INC-2026-0045	• MEDIO	Malware detectado en endpoint	07-Mar	• CERRADO
INC-2026-0044	• ALTO	Violación política DLP — RRHH	05-Mar	• CERRADO
INC-2026-0043	• MEDIO	Acceso fallido reiterado VPN	02-Mar	• CERRADO

+ NUEVO INCIDENTE

La Escalera de Madurez AI en Banca

2026

AI asiste y filtra

Documenta en tiempo real,
reduce ruido,
asiste al analista con información
contextual.

2027

AI propone y orquesta

Genera reportes regulatorios,
recomienda
acciones priorizadas, humano
aprueba.

2028+

AI ejecuta con gobernanza

Contención automática
con guardrails,
humano supervisa y audita
resultados.

Los bancos que empiecen hoy tendrán ventaja competitiva en cumplimiento regulatorio.

La disciplina precede a la automatización.

Procedimientos formales. Documentos operativos.
Cada uno con dueño. Cada uno auditado.

Sobre esa base se construye AI con gobernanza.

4 Ideas para Llevarse Hoy

1. El mayor dolor de un incidente no es técnico — es orquestación, documentación y comunicación bajo presión.

2. AI no reemplaza a su equipo. Lo potencia. Un analista con AI bien diseñado equivale a cinco durante una crisis.

3. No necesitan presupuestos millonarios. Necesitan procesos sólidos y la voluntad de construir.

4. Sus instrucciones de AI son propiedad intelectual. Protéjanlas como protegen su código fuente.

VI CONGRESO INTERNACIONAL
DE CIBERSEGURIDAD, PREVENCIÓN
DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

Rodrigo Castellanos

rcastellanos@devel.group

Todo lo que compartí hoy es la punta del iceberg.

Si quieren explorar cómo se ve esto en su contexto específico,
estoy disponible aquí en el congreso.