Ciudad de Guatemala, 29 de abril de 2,026

Gremial de Tecnología e Innovación

Cámara de Industria de Guatemala

Circular Multisectorial de Tecnología

Recientemente ha trascendido a nivel nacional una serie de incidentes de ciberseguridad que han afectado a diversas instituciones dentro del territorio de Guatemala.

Ante esta situación, nuestra gremial y el sector de tecnologías de la información deseamos manifestar nuestra total disposición de colaborar con todos los sectores del país en la construcción de entornos digitales más seguros y resilientes para la protección de la información.

Reconocemos la importancia estratégica de que los servicios de información operen con normalidad, continuidad y confiabilidad, ya que de ello depende el adecuado funcionamiento de empresas, instituciones y servicios esenciales para la ciudadanía.

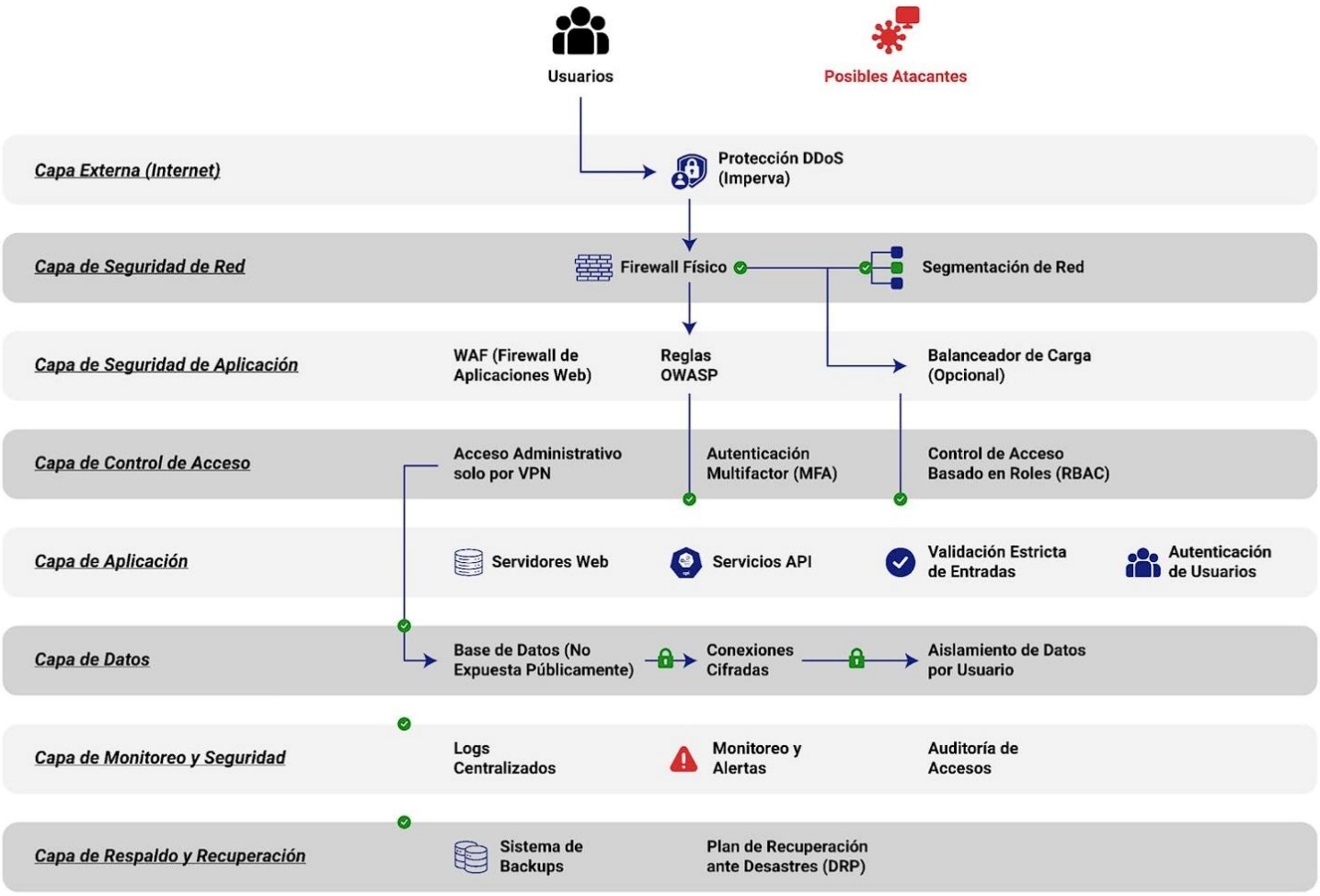
En ese sentido, nuestros socios, colegas y miembros de cámara hemos tomado la determinación de mantener una actualización constante de información técnica y profesional, poniéndola al servicio de la sociedad civil, del sector privado y del sector público.
Estamos convencidos de que en la unidad reside una fortaleza invaluable.

Como guatemaltecos, queremos aportar nuestra experiencia y conocimiento para fortalecer las defensas de nuestros sistemas de información, así como contribuir al desarrollo y continuidad operativa de nuestras organizaciones e instituciones.

Como primera medida, recomendamos revisar y fortalecer al máximo la seguridad de todos los entornos tecnológicos expuestos a Internet, adoptando controles preventivos, correctivos y de monitoreo continuo. En particular, sugerimos considerar las mejores prácticas internacionalmente reconocidas contenidas en la norma ISO/IEC 27001, referente global en sistemas de gestión de seguridad de la información.

Adicionalmente, recomendamos implementar arquitecturas tecnológicas robustas y segmentadas para sistemas web, basadas en principios de defensa en profundidad, alta disponibilidad, control de accesos, monitoreo permanente y planes de continuidad operativa.
Reiteramos nuestra disposición de apoyar técnicamente a los distintos sectores del país, promoviendo una cultura de prevención, respuesta coordinada y mejora continua frente a las amenazas digitales actuales.

"EJEMPLO DE SEGURIDAD PARA APLICATIVOS WEB"



Alejandro José Gudiel Estrada
Juan Carlos Rodríguez Paniagua
Socios fundadores de Homeland S.A.

Homeland
Software and Apps
www.homeland.com.gt

Pablo Barrera – Socio Fundador, ES Consulting.

ES CONSULTING

1. Resumen ejecutivo

Síntesis del incidente y alcance de este comunicado

Un actor de amenazas externo ha reivindicado públicamente el compromiso de los sistemas de varias entidades gubernamentales que resguardan datos sensibles de ciudadanos. Las estimaciones apuntan a millones de registros de identidad civil y datos biométricos y al registro vehicular del país. Adicionalmente, los atacantes afirman haber establecido persistencia en la infraestructura comprometida.

El incidente se suma a incidentes recientes en otras instituciones del Estado (DIGECAM, Ministerio de Trabajo, entre otras). Este comunicado está dirigido a organizaciones de cualquier industria —entidades financieras, industria, comercio electrónico, retail, salud, educación y gobierno— porque la consecuencia operativa es transversal: la información de identidad de la población guatemalteca debe asumirse comprometida y ningún proceso crítico debería depender exclusivamente de PII estática ni de validación en línea contra fuentes hoy bajo sospecha de integridad.

El comunicado propone una respuesta escalonada en tres horizontes —0–72 horas, 1–2 semanas y 30–90 días— y entrega escenarios de amenaza específicos por sector, además de acciones por dominio de control aplicables a cualquier organización.

2. Contexto de los incidentes

Ante el posible compromiso reportado contra RENAP y SAT (no verificado) se enmarca en una serie creciente de incidentes contra instituciones del Estado guatemalteco. Aún cuando el alcance final está bajo investigación oficial, la posición prudente para todas las industrias es operar bajo el supuesto del **peor escenario** hasta que las propias instituciones afectadas confirmen el alcance real, contengan al atacante y restablezcan garantías de integridad de sus sistemas.

La premisa rectora de este comunicado es que datos como DPI, NIT, dirección, fecha de nacimiento, filiación, biometría dactilar y facial, teléfono, correo, vehículos registrados y certificados electrónicos de propiedad deben tratarse como información públicamente disponible para fines de fraude. Cualquier control que dependa exclusivamente de estos atributos pierde efectividad y puede generar una falsa sensación de seguridad.

La siguiente tabla resume las fuentes reportadas como vulneradas, los datos potencialmente expuestos y la implicación operativa principal para cualquier organización.

Fuente reportada	Datos potencialmente expuestos	Implicación principal
RENAP	Identidad civil completa: nombres, DPI, fechas y lugares de nacimiento, filiación, actas de nacimiento, matrimonio y defunción. Datos biométricos (huella, rostro).	La fuente oficial de validación de identidad ya no puede tratarse como íntegra ni confidencial.
SAT	Registros vehiculares: NIT, propietarios, direcciones fiscales, placas, números de chasis y motor, certificados electrónicos de propiedad.	Suplantación con perfil patrimonial real, ingeniería social creíble, fraude documental.
Antecedentes recientes	DIGECAM: datos personales, registros de licencias y armas. Mintrab "Tu Empleo": hojas de vida, datos salariales y académicos. Otras instituciones del sector público y académico.	Perfilamiento de víctimas de alto valor; ingeniería social muy personalizada.

Hipótesis de trabajo recomendada

Asumir que cualquier dato que la organización podía pedir como "prueba de identidad" —DPI, NIT, dirección, fecha de nacimiento, nombre de la madre, placa vehicular, certificado de propiedad— es información que el atacante ya posee con alta probabilidad.

Asumir además que la integridad de respuestas provenientes de servicios gubernamentales comprometidos puede estar afectada hasta que las propias instituciones afectadas confirmen lo contrario.

3. Escenarios de amenaza por sector

La explotación de los datos comprometidos no se limita al sector financiero. La siguiente sección describe los escenarios más probables por industria. Cada organización debe evaluar su exposición específica en función de su modelo de negocio, canales y arquitectura tecnológica.

3.1 Entidades financieras

El sector financiero es objetivo prioritario por la monetización directa del fraude. Los datos comprometidos facilitan la apertura de cuentas, solicitudes de crédito, account takeover, smishing y vishing creíble.

Escenario de amenaza	Vector probable	Control mitigante
Validaciones contra RENAP manipuladas	Persistencia del atacante en la infraestructura de RENAP que altere o devuelva respuestas falsas a consultas de validación de identidad.	No depender de RENAP como única fuente; cruce con burós, score interno y validación presencial reforzada.

Escenario de amenaza	Vector probable	Control mitigante
Apertura de cuentas con identidad ajena	Onboarding 100% digital con DPI, biometría y filiación obtenidos del volcado.	Doble factor humano + tecnológico, fricción adicional, validación cruzada en burós y telcos.
Crédito vehicular fraudulento	Solicitudes con NIT, placa y certificado de propiedad reales obtenidos del volcado SAT.	Validación física del vehículo, comparación con bases de gravámenes, llamada al cliente por canal verificado.
Account takeover por SIM swap	Suplantación con DPI ante operador móvil para portar la línea.	Migrar OTP a app/FIDO2; detectar cambio reciente de SIM antes de operaciones críticas.
Vishing al call center	Atacante presenta DPI, NIT, dirección y vehículos del cliente como “prueba” de identidad.	Step-up por canal seguro; prohibir validar solo con datos hoy públicos.

3.2 Industria

El sector industrial enfrenta amenazas en su cadena de suministro, procesos B2B y operación tecnológica (OT). Los datos filtrados permiten suplantar a proveedores, clientes y empleados clave.

Escenario de amenaza	Vector probable	Control mitigante
Suplantación de proveedores y clientes B2B	Correos con NIT, dirección fiscal y datos de contactos legítimos solicitando cambios de cuenta bancaria de pago.	Verificación dual por canal alterno; políticas estrictas de cambio de datos bancarios; doble aprobación financiera.
Fraude de factura (Business Email Compromise)	Correos altamente personalizados con datos reales de operaciones recientes obtenidos por phishing previo o filtraciones.	DMARC/DKIM/SPF estrictos, alerta visual a correos externos, autenticación reforzada para finanzas.
Espionaje industrial dirigido	Spear-phishing a personal técnico con datos personales correctos para incrementar credibilidad.	Capacitación, simulacros, MFA en correo y VPN, segmentación de redes operacionales (OT).
Compromiso de cadena de suministro	Atacantes usan identidad real de proveedores para infiltrar accesos o software malicioso.	Inventario de proveedores críticos, validación de actualizaciones de software,

Escenario de amenaza	Vector probable	Control mitigante
		accesos de proveedores con MFA y monitoreo.
Ataques a infraestructura OT	PII expuesta de operadores y técnicos para spear-phishing dirigido a sistemas industriales.	Aislamiento OT-IT, monitoreo específico ICS, controles físicos sobre acceso a operadores.

3.3 Comercio electrónico (e-commerce)

Las plataformas digitales con onboarding en línea y pagos no presenciales son especialmente vulnerables. Los atacantes combinan PII real con tarjetas robadas o credenciales reutilizadas.

Escenario de amenaza	Vector probable	Control mitigante
Fraude de tarjeta no presente	Datos personales reales se combinan con tarjetas robadas para sortear validaciones AVS.	3D Secure 2.0, scoring antifraude, biometría conductual, listas internas de PII expuesta.
Toma de cuenta de comprador	Credenciales reutilizadas + datos personales correctos para responder preguntas de seguridad.	MFA obligatoria, detección de credential stuffing, monitoreo de cambios de envío y método de pago.
Fraude de devoluciones (refund fraud)	Atacante con identidad real solicita reembolsos o cambios de envío.	Verificación de identidad para cambios sensibles, límites a montos sin verificación, ML antifraude.
Phishing con marca suplantada	Correos con datos reales del cliente y referencias a compras legítimas.	DMARC, monitoreo de dominios similares, comunicación proactiva a clientes.
Cuentas creadas con datos reales para abuso	Perfiles falsos con DPI y NIT real para abusar de promociones, evadir restricciones o lavar dinero.	Validación documental, prueba de vida, detección de dispositivos y patrones recurrentes.

3.4 Comercios y retail

El retail físico y omnicanal sufre fraudes en programas de lealtad, financiamiento en punto de venta y devoluciones. Los datos personales correctos vencen los controles tradicionales.

Escenario de amenaza	Vector probable	Control mitigante
Fraude en programas de lealtad	Acceso con datos reales para vaciar puntos, millas o saldos prepago.	MFA en cuenta de fidelidad, alertas de redención, límites diarios.
Fraude en crédito de consumo y financiamiento en tienda	Solicitudes de crédito en punto de venta usando DPI real ajeno.	Validación biométrica con liveness, llamada al cliente registrado, verificación con buró.
Apertura de cuentas comerciales fraudulentas	Uso de NIT y dirección fiscal reales para abrir cuentas de crédito a nombre de empresas.	Validación con representante legal por canal verificado, inspección física para cuentas significativas.
Fraude de pagos sin presencia física	Compras telefónicas o por chat usando datos personales correctos.	Autenticación 3DS, límites por canal, escalamiento manual sobre umbral.
Devoluciones y cambios fraudulentos	Reclamos con datos reales del comprador legítimo.	Vinculación de devolución al método de pago original, identificación física en tienda.

3.5 Sector salud

El sector salud combina alto valor de los datos clínicos con criticidad operativa. La PII filtrada amplifica fraudes médicos, ransomware con extorsión, y acceso indebido a expedientes.

Escenario de amenaza	Vector probable	Control mitigante
Fraude médico y de seguros	Reclamos de seguros y servicios usando identidad real de pacientes para obtener atención, medicamentos o reembolsos.	Autenticación reforzada en portales de pacientes, validación biométrica en atención, auditoría de patrones.
Acceso indebido a historiales clínicos	Suplantación para obtener historial clínico, recetas o resultados de exámenes.	MFA en portales, registro de accesos, alertas a paciente sobre consultas a su expediente.
Recetas fraudulentas de medicamentos controlados	Uso de DPI real para obtener recetas o medicamentos restringidos.	Receta electrónica con autenticación del médico, verificación cruzada con farmacia, MFA.
Ransomware con extorsión basada en PII	Compromiso de sistemas hospitalarios y amenaza de	Backups segmentados e inmutables, EDR/XDR, plan de

Escenario de amenaza	Vector probable	Control mitigante
	filtración con datos sensibles ya validados públicamente.	continuidad clínica, ejercicios de respuesta.
Phishing dirigido a personal de salud	Correos con datos reales de pacientes, médicos o trámites para obtener acceso a sistemas.	Capacitación específica, simulacros, MFA, segmentación de cuentas administrativas.

3.6 Sector educativo

Universidades, colegios y plataformas educativas manejan datos de menores, expedientes académicos y trámites con alto impacto. La filtración facilita suplantación de estudiantes y fraude académico.

Escenario de amenaza	Vector probable	Control mitigante
Suplantación de estudiantes	Inscripciones, exámenes en línea o trámites usando DPI y datos académicos reales.	Identificación reforzada en exámenes (cámara, biometría conductual), verificación presencial en momentos clave.
Fraude académico (títulos y certificados)	Emisión o validación de títulos falsos basados en identidad real.	Verificación digital firmada criptográficamente, registros centralizados, validación cruzada con autoridades.
Acceso indebido a expedientes académicos	Suplantación de padres, estudiantes o personal para obtener notas, registros o realizar cambios.	MFA en portales, registro de accesos, autorización por canal verificado para cambios sensibles.
Phishing y fraude de pago de matrículas	Correos con datos reales del estudiante solicitando pagos o cambios de cuenta.	Comunicación oficial por canal único, alertas visuales a correos externos, doble validación de pagos.
Compromiso de plataformas y datos de menores	Acceso a información de niñas, niños y adolescentes con consecuencias graves de privacidad.	Cifrado en reposo, controles de acceso estrictos, minimización de datos, supervisión parental adecuada.

3.7 Sector gobierno

Las instituciones públicas son simultáneamente víctimas y responsables. La persistencia atacante reportada exige acciones excepcionales de remediación y recuperación de la confianza ciudadana.

Escenario de amenaza	Vector probable	Control mitigante
Suplantación ciudadana en trámites	Realización de trámites a nombre de terceros con datos personales y biometría comprometidos.	Autenticación multifactor reforzada, prueba de vida activa, validación cruzada entre instituciones.
Fraude electoral y manipulación del padrón	Uso de DPI real para inscripciones o cambios indebidos en registros electorales.	Auditoría continua del padrón, controles biométricos en empadronamiento, transparencia de logs.
Acceso indebido a registros públicos sensibles	Consulta o modificación de registros mercantiles, propiedad, antecedentes, etc.	Trazabilidad estricta, MFA, separación de funciones, monitoreo de patrones anómalos.
Ataques a infraestructura crítica nacional	PII filtrada usada para spear-phishing dirigido a operadores de servicios esenciales.	Programas nacionales de concientización, MFA obligatoria, segmentación de redes críticas.
Persistencia atacante en sistemas comprometidos	Mantenimiento de accesos ocultos a pesar de remediación de vulnerabilidades conocidas.	Caza de amenazas (threat hunting), reconstrucción de sistemas desde imágenes confiables, auditoría forense exhaustiva.

4. Plan de acción inmediato (0–72 horas)

Las siguientes diez acciones deben evaluarse y, en su mayoría, ejecutarse en las próximas 72 horas. Cada organización debe asignar responsable nominal, hora de inicio y hora límite, y reportar avance al comité de crisis.

#	Acción inmediata (próximas 72 horas)	Responsable sugerido
1	Convocar comité extraordinario de crisis cibernética con dirección general, riesgo, legal, operaciones, tecnología, seguridad y comunicación.	Dirección General / CISO / Riesgo
2	Suspender o reforzar con doble control todo proceso que dependa exclusivamente de validación contra RENAP en línea (alta de clientes, pacientes, estudiantes, proveedores, beneficiarios) hasta tener garantía de integridad de la fuente.	CISO / Operaciones / Cumplimiento
3	Activar nivel de alerta elevado en SOC, fraude y monitoreo. Aumentar sensibilidad de reglas de account takeover, alta de	CISO / Seguridad de la Información

#	Acción inmediata (próximas 72 horas)	Responsable sugerido
	beneficiarios, cambios de contacto y operaciones digitales no presenciales.	
4	Eliminar de inmediato cualquier validación de identidad en canales humanos basada únicamente en DPI, NIT, dirección, fecha de nacimiento o nombre de la madre. Actualizar guiones y políticas de atención.	Operaciones / Atención al Cliente
5	Aplicar autenticación reforzada (step-up) obligatoria a operaciones críticas: cambio de contacto, restablecimiento de contraseña, alta de beneficiarios, transferencias o transacciones sobre umbral, cambios en historiales clínicos o académicos.	CISO / TI
6	Verificar exposición de datos de clientes, pacientes, estudiantes, empleados y proveedores en los volcados; marcar internamente registros como “PII expuesta” y aplicar controles reforzados sin avisar al exterior.	CTI / Inteligencia de Amenazas
7	Bloquear preventivamente flujos 100 % no presenciales para alta de nuevos usuarios, clientes o cuentas con privilegios sensibles hasta endurecer los controles de identidad.	Operaciones / TI
8	Verificar requerimientos legales y contractuales que pudieran verse afectados.	Cumplimiento / Legal / CISO
9	Lanzar comunicación masiva a clientes, pacientes, estudiantes o usuarios alertando sobre el incremento inminente de phishing, vishing y mensajes con datos personales correctos. Reforzar el “qué nunca pedirá la organización”.	Comunicación / CISO
10	Reforzar concientización interna mediante alerta urgente al personal: incremento esperado de spear-phishing dirigido, especialmente a perfiles con privilegios elevados o acceso a datos sensibles.	Recursos Humanos / CISO

5. Plan a corto y medio plazo

Una vez estabilizada la respuesta inmediata, las siguientes acciones consolidan la postura defensiva y cierran las brechas estructurales que el incidente ha expuesto.

Plazo	Acción	Responsable
1–2 sem.	Reentrenar modelos de detección de fraude y de identidad sintética con la hipótesis explícita de PII y biometría comprometidas. Aplicable a banca, e-commerce, telcos, aseguradoras y cualquier organización con onboarding digital.	Analítica / Fraude / CISO
1–2 sem.	Rediseñar guiones de atención telefónica, presencial y por chat; capacitar al personal en ingeniería social específica al incidente con simulacros frecuentes.	Operaciones / Capacitación
1–2 sem.	Establecer fuentes alternativas de validación de identidad: burós, telcos, score conductual interno, validación presencial reforzada. Documentar la nueva arquitectura.	CISO / Arquitectura / Negocio
30–60 d	Migrar autenticación crítica de SMS-OTP a TOTP en aplicación o llaves FIDO2/WebAuthn en operaciones de alto riesgo y accesos privilegiados internos.	CISO / TI
30–60 d	Ejecutar ejercicios de mesa con escenario realista del incidente; documentar lecciones y ajustar planes de respuesta y continuidad.	Gestión de Riesgo / CISO
30–90 d	Auditar accesos de terceros y proveedores; rotar credenciales privilegiadas y revisar segmentación de red.	CISO / TI / Compras
30–90 d	Actualizar la matriz de riesgo tecnológico incorporando el escenario del compromiso y formalizar el plan de continuidad asociado.	Riesgo / Cumplimiento
30–90 d	Revisar políticas de retención y minimización de datos personales; eliminar PII innecesaria y cifrar lo que sea indispensable conservar.	CISO / Cumplimiento / Negocio

6. Acciones específicas por dominio de control

Estas acciones son aplicables a organizaciones de cualquier sector. La intensidad y ritmo de implementación dependerá del nivel de exposición y madurez de cada institución.

6.1 Identidad y autenticación

- Reevaluar todo flujo que valide identidad contra RENAP en línea: añadir capas independientes (burós, validación con telco, score conductual interno) y exigir doble coincidencia antes de aprobar.
- Si la organización usa biometría comparada contra plantillas RENAP o derivadas, suspender ese factor como único determinante y exigir factor adicional independiente.
- Migrar la autenticación de operaciones de alto riesgo y accesos privilegiados internos de SMS-OTP a TOTP en aplicación o llaves FIDO2/WebAuthn.
- Implementar detección de anomalías por dispositivo, geolocalización, comportamiento conductual y reputación de IP como capa permanente.
- Eliminar gradualmente las preguntas de seguridad basadas en PII estática en todos los canales digitales y telefónicos.

6.2 Onboarding y verificación de identidad (KYC equivalente)

- Añadir fricción graduada a todo onboarding 100 % digital (clientes, pacientes, estudiantes, proveedores, empleados): límites operativos iniciales, retraso en emisión de credenciales físicas, periodo de observación intensiva los primeros 30 a 60 días.
- Reforzar verificación documental con análisis forense del DPI: detección de plantillas, manipulación, copias y deepfakes.
- Exigir prueba de vida activa (no estática) y, cuando sea posible, validar con preguntas dinámicas que solo el usuario legítimo pueda responder por su historial.
- Incorporar modelos de detección de identidad sintética: correlación entre antigüedad del DPI y profundidad de historial, antigüedad del número telefónico, dirección compartida, reutilización de dispositivos.
- Aplicar fricción adicional en operaciones inmediatamente posteriores al alta: limitar montos o privilegios, observar el patrón inicial.

6.3 Detección de fraude y abuso

- Reentrenar y recalibrar modelos con la hipótesis explícita de PII y biometría comprometidas; aumentar sensibilidad en eventos de cambio de contacto, restablecimiento de contraseña, alta de beneficiarios y operaciones críticas en línea.
- Mantener una lista interna de “PII expuesta” para registros cuyos datos se identifiquen en los volcados públicos, con controles más estrictos sin afectar la experiencia visible.
- Aplicar reglas específicas a productos o trámites vinculados con datos SAT comprometidos (crédito vehicular, transferencias de propiedad, trámites tributarios).
- Activar correlación entre alta reciente y comportamiento atípico en los primeros 30 días con escalamiento automático.

6.4 Canales humanos: atención, call center, agencias y ventanillas

- Eliminar de los guiones cualquier validación de identidad basada únicamente en DPI, NIT, dirección, fecha de nacimiento, nombre de la madre o datos vehiculares.
- Obligar autenticación por canal seguro: notificación push a la app, OTP a dispositivo registrado, videollamada con verificación visual o presencia física antes de operaciones sensibles.
- Capacitar al personal frontal en ingeniería social específica al incidente; ejecutar simulacros frecuentes mientras dure la crisis.
- Establecer protocolo de escalamiento cuando el solicitante demuestre identidad con un volumen inusual de datos personales correctos en circunstancias atípicas.

6.5 Inteligencia de amenazas y cooperación sectorial

- Reforzar el monitoreo de dark web, Telegram y foros donde se comercializan estas bases; correlacionar hallazgos con la base de usuarios propios y empleados con privilegios.
- Compartir indicadores de compromiso, tipologías y patrones emergentes con el CSIRT-GT, regulador sectorial correspondiente y pares de la industria a través de los canales formales.
- Documentar internamente cada caso confirmado o sospechoso de fraude derivado del incidente para alimentar reglas, modelos y posicionamiento sectorial conjunto.
- Mantener vigilancia activa sobre comunicados oficiales de RENAP, SAT, CSIRT-GT y reguladores para reaccionar oportunamente a actualizaciones del alcance.

6.6 Comunicación con clientes, pacientes, estudiantes y usuarios

- Comunicación proactiva en las próximas 24 a 72 horas advirtiendo sobre el incremento inminente de phishing y vishing con datos verdaderos. No atribuir el incidente a la organización; mantener tono institucional y de servicio.
- Reforzar el mensaje de “qué nunca pedirá la organización”: claves, OTP, PIN, instalación remota de aplicaciones, transferencias a cuentas “de seguridad”.
- Promover el uso de alertas, bloqueo inmediato desde la app, autenticación reforzada y verificación de canales oficiales.
- Habilitar canal prioritario para víctimas potenciales de suplantación que requieran orientación o atención reforzada.

6.7 Gobernanza, regulación y resiliencia

- Documentar formalmente la respuesta a este escenario en la matriz de riesgo y en los registros de cumplimiento exigidos por el regulador sectorial correspondiente.

- Ejecutar tabletop exercise en las próximas dos semanas con el escenario real: “Datos de identidad y biométricos de la población se asumen comprometidos y la fuente oficial de validación está bajo investigación; ¿qué hace la organización en las primeras 72 horas, en 7 días y en 30 días?”
- Actualizar el plan de respuesta a incidentes para incluir flujos específicos de víctimas de suplantación: atención prioritaria, registro forense, coordinación con la fiscalía y restitución.
- Apoyar institucionalmente, vía cámaras y asociaciones sectoriales, los esfuerzos para acelerar la aprobación de un marco de ciberseguridad nacional y de protección de datos personales.

6.8 Higiene de seguridad interna

- Auditar de inmediato accesos de terceros y proveedores; aplicar principio de menor privilegio y revisión de cuentas de servicio.
- Forzar rotación de credenciales privilegiadas y revisión de segmentación de red; revisar gestión de parches en sistemas expuestos.
- Verificar capacidad de logging y forense para reconstruir incidentes con suficiente granularidad temporal.
- Reforzar concientización al personal interno: la filtración pública también facilita spear-phishing dirigido a empleados con privilegios elevados (ejecutivos, administradores de sistemas, áreas financieras y de seguridad).

7. Indicadores que merecen vigilancia reforzada

Durante las próximas 8 a 12 semanas, los equipos de seguridad, fraude y operaciones deberían vigilar especialmente los siguientes siete indicadores, contrastándolos con la línea base previa al incidente.

- **1. Tasa de altas digitales:** intentos de creación de cuentas, perfiles, expedientes o accesos en línea respecto al promedio histórico.
- **2. Eventos de cambio de credenciales:** volumen de restablecimientos de contraseña, cambios de número telefónico, correo registrado y altas de beneficiarios o destinatarios.
- **3. Reportes de usuarios externos:** llamadas o correos sospechosos que mencionan datos personales correctos, agrupados por canal y tipología.
- **4. Casos de SIM swap:** incidentes confirmados o sospechosos y cruces con operadores móviles.
- **5. Anomalías de inicio de sesión:** nuevos dispositivos, geolocalizaciones inusuales, horarios atípicos, múltiples intentos fallidos.
- **6. Discrepancias en trámites con datos SAT/RENAP:** solicitudes con datos correctos pero patrón inconsistente con el perfil del titular legítimo.

-
- **7. Aparición de credenciales o PII en mercados clandestinos:** datos corporativos, de usuarios o empleados que aparezcan publicados o a la venta.

8. Contactos y referencias clave

Mantener canales abiertos con los siguientes actores facilita la respuesta coordinada y el cumplimiento de obligaciones de notificación.

Entidad / Recurso	Función relevante en este incidente
Superintendencia de Bancos (SIB)	Reporte y supervisión para entidades financieras.
Asociación Bancaria de Guatemala (ABG) y BANCERT	Mesa sectorial bancaria, intercambio de tipologías y posición conjunta ante medios y reguladores.
RENAP / SAT	Fuentes bajo investigación de integridad. Mantener seguimiento de comunicados oficiales antes de reanudar la dependencia operativa de sus servicios.
Ministerio Público – Fiscalía contra el Delito Cibernético	Denuncia y persecución penal de fraudes, suplantación de identidad y ataques informáticos.
Operadores móviles del país	Coordinación reforzada para detección y mitigación de SIM swap; canales bilaterales de consulta de antigüedad y cambios recientes.
Burós de crédito	Fuente complementaria de validación de identidad y comportamiento crediticio, especialmente útil ante el compromiso de fuentes oficiales.
Reguladores sectoriales	MSPAS (salud), MINEDUC (educación), Superintendencia de Telecomunicaciones, MINECO, Cámaras empresariales y demás autoridades sectoriales para reportes específicos por industria.