6.6.1- Haga lo que hicimos en aula: Usar IA de manera segura

Se aborda las mejores prácticas para utilizar la IA de forma segura, evitando filtraciones de información sensible y garantizando el cumplimiento de las directrices internas.

Para esta ocasión se ha utilizado el caso del Banco Quetzal en Guatemala, presentando la siguiente situación:** una analista del área de riesgos pega en un ChatGPT gratuito una hoja con 2,000 clientes (nombre, DPI, NIT, teléfono, correo, saldos y mora) para "encontrar patrones de morosidad". Otro colega pide a la IA que revise código de la banca móvil que tiene una clave de API incrustada. Un tercero sube el borrador de una campaña de tarjetas que se lanza el próximo mes.

Es filtración de entrada en tres frentes: datos personales, credenciales e información estratégica.

**1. Identificar y separar documentos que contengan credenciales, datos personales, datos sensibles en información estratégica que den ser protegidos.

- **Credenciales:** claves de API, cadenas de conexión a la base del core bancario, certificados.
- **Datos personales:** nombre, DPI, NIT, teléfono, correo, dirección, ID de cliente.
- **Datos sensibles:** salud (seguros asociados), menores (cuentas de ahorro infantil), procesos judiciales o disciplinarios.
- **Información estratégica:** campañas por lanzar, tasas y negociaciones con cifras, código de la banca móvil, arquitectura de seguridad, contratos, presentaciones de la junta directiva, reportes de operaciones sospechosas.

Cada categoría va en repositorios separados, con acceso por rol.

**2. Establecer criterios para reconocer y evitar el envío de datos confidenciales a modelos de IA.

Si el archivo contiene cualquiera de esas cuatro categorías, no sale a una herramienta pública. La pregunta de control es: *¿esto es confidencial? Si lo es, no lo ingreso o lo anonimizo.* Las consultas generales sí se permiten.

**3. Implementar un protocolo para la anonimización o enmascaramiento de información sensible antes de su uso.

- **Enmascaramiento:** "Juan Pérez, DPI 2xxx…" pasa a "Cliente 1".
- **Minimización:** rango de edad en vez de fecha de nacimiento, y rangos de saldo (Q5,000–Q10,000) en vez del monto exacto.
- **Datos sintéticos o muestra reducida:** 50 registros ficticios en vez de la cartera completa.

La analista de riesgos obtiene los mismos patrones de morosidad sin exponer a nadie.

**4. Configurar sistemas y herramientas que garanticen el almacenamiento seguro y la retención adecuada de los registros de acceso a la IA.

- Prohibir cuentas personales de IA para trabajo del banco y desconectar integraciones como Gmail.
- Usar un plan corporativo con políticas de retención y eliminación, auditoría y regiones de datos definidas por contrato.
- Aplicar segmentación, cifrado y monitoreo continuo para detectar accesos no autorizados.
- Los bancos con datos críticos (tarjetas, cuentas) deben conservar control sobre dónde viven los datos, incluso con centros de datos propios.

**5. Realizar revisiones manuales de los resultados para verificar errores, alucinaciones o fallas en el cumplimiento y la propiedad intelectual.

Toda salida se revisa como si fuera a publicarse:
- Verificar cifras, fuentes y fragmentos.
- Buscar alucinaciones.
- Confirmar autoría y licencias antes de usar texto o imágenes en una campaña.
- Pasar por Compliance y Jurídico antes de publicar cualquier material externo.

**6. Adoptar recursos corporativos y contractuales que aseguren la integración segura con datos internos y garanticen el cumplimiento de las normativas de protección de datos aplicables.

- Contrato empresarial con el proveedor de IA que fije retención, regiones y accesos.
- Conectores oficiales (SharePoint, Drive, CRM) con permisos definidos, en lugar de copiar y pegar.
- Política interna explícita de qué se puede y qué no, con flujo de revisión.

Marco legal a verificar

- Según un informe de 2026, Guatemala no tiene una ley específica de protección de datos personales; en agosto de 2025 se presentó la Iniciativa 6572, que está en estudio en el Congreso.
- Un análisis anterior señala que la Ley de Libre Acceso a la Información Pública es la única que regula datos personales y sensibles.

- Para bancos, un referente es la Resolución JM-104-2021, el Reglamento para la Administración del Riesgo Tecnológico, de la Superintendencia de Bancos.
- Además, el Decreto 15-2026 es la nueva ley antilavado, relevante para cualquier dato de transacciones sospechosas.

Que no exista una ley general no reduce el riesgo: el banco sigue respondiendo ante la SIB, sus clientes y sus contratos, y la información financiera es de las más sensibles.