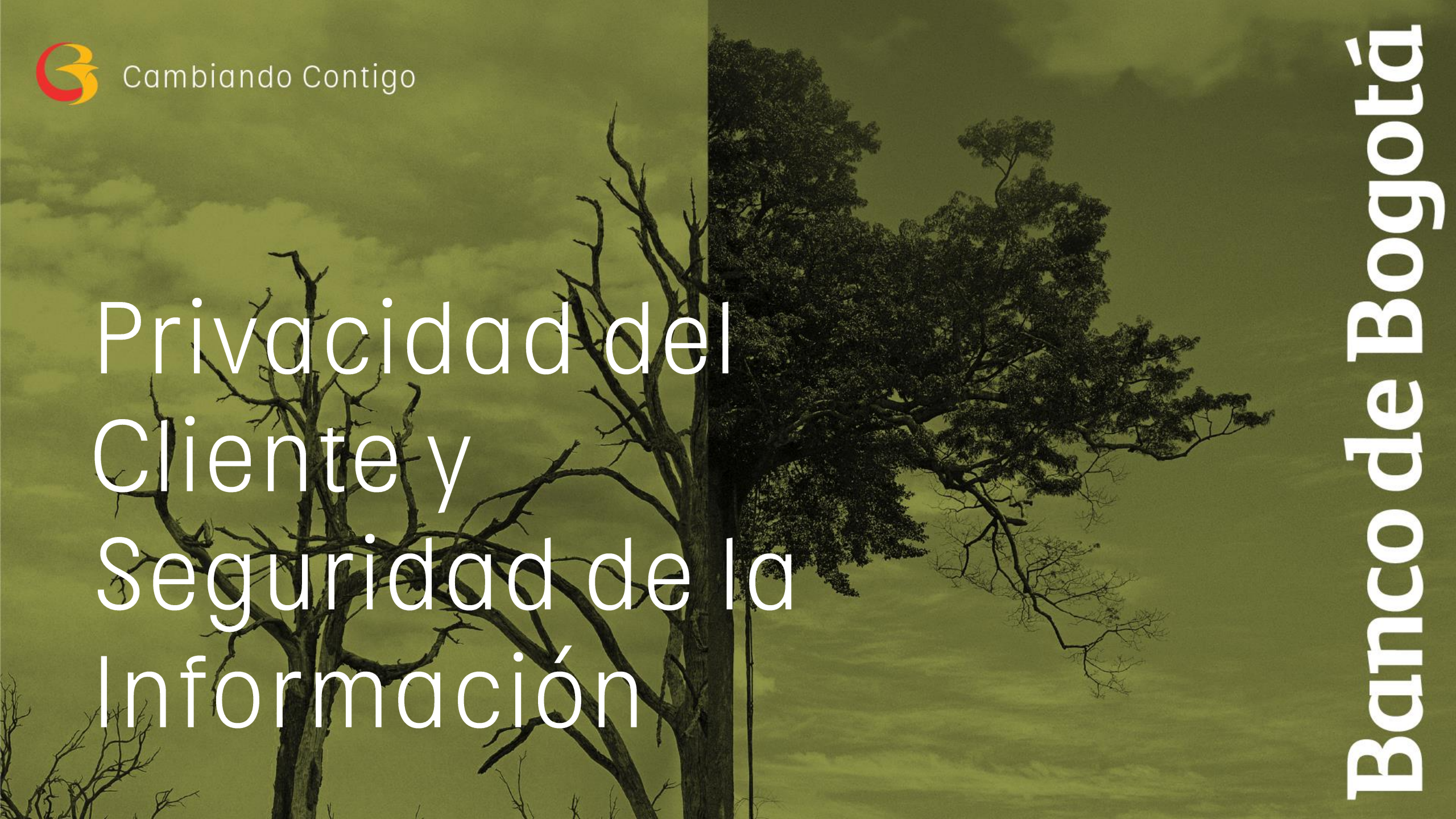
Cambiando Contigo
Privacidad del Cliente y Seguridad de la Información
Banco de Bogotá

¿El entorno informático de nuestra organización qué tan seguro y confiable es para nuestros clientes?

La *gestión de riesgos relacionados con la recopilación, retención y uso de datos sensibles, confidenciales o de propiedad de los clientes es un asunto que impacta la sostenibilidad del negocio directamente* desde el entorno social de uno de los grupos de interés más relevantes del sector financiero y a su vez de su cadena de valor; *abordar este asunto desde la estrategia de la organización mediante políticas y prácticas seguras* relacionadas con la infraestructura informática, formación del equipo de trabajo y otros mecanismos proporciona un entorno seguro en cuanto al manejo de información *garantizando la seguridad de los datos de los clientes y usuarios*.

Banco de Bogotá

Privacidad del Cliente y Seguridad de la Información

TEMAS SESIÓN DE FORMACIÓN

(50 Min) buenas prácticas para la gestión de la información
- ✓ Conceptos de Riesgo
- ✓ 5 puntos clave para la política de Seguridad de la Información.

(30 Min) valoración de los Controles
- ✓ 3 Formas de valorar la calidad de los controles.

(40 Min) Caso de estudio
Documentación y análisis de un evento de seguridad de la información.

Categoría: Capital Social

Privacidad del Cliente y Seguridad de la Información

5 puntos clave para una política de Seguridad de la Información.

1. Evaluación de riesgos y análisis de amenazas:

- ✓ Comienza por identificar y evaluar los riesgos y amenazas a los que se enfrenta tu organización en relación con la seguridad de la información.
- ✓ Realiza un análisis de vulnerabilidades para comprender las debilidades en tus sistemas y procesos.
- ✓ Clasifica la información según su importancia y sensibilidad para priorizar la protección de los activos más críticos.

Categoría: Capital Social

Privacidad del Cliente y Seguridad de la Información

5 puntos clave para una política de Seguridad de la Información.

2. Definición de políticas y procedimientos:

- ✓ Establece políticas de seguridad de la información claras y específicas que aborden los riesgos identificados y los requisitos legales y regulatorios aplicables.
- ✓ Crea procedimientos detallados para implementar estas políticas y garantizar que se sigan de manera consistente en toda la organización.
- ✓ Asegúrate de que todos los empleados estén al tanto de estas políticas y procedimientos y reciban capacitación periódica sobre seguridad de la información.

Categoría: Capital Social

Privacidad del Cliente y Seguridad de la Información

5 puntos clave para una política de Seguridad de la Información.

3. Control de acceso y autenticación:

- ✓ Implementa controles de acceso adecuados para garantizar que solo las personas autorizadas tengan acceso a la información crítica.
- ✓ Utiliza autenticación multifactor (MFA) para aumentar la seguridad de las cuentas y sistemas.
- ✓ Revoca inmediatamente los privilegios de acceso cuando un empleado deje la organización o cambie de roles.

Banco de Bogotá

Privacidad del Cliente y Seguridad de la Información

5 puntos clave para una política de Seguridad de la Información.

4. Protección contra amenazas cibernéticas:

- ✓ Mantén actualizados los sistemas y software con parches de seguridad y actualizaciones regulares.
- ✓ Utiliza soluciones de seguridad, como firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS).
- ✓ Implementa una estrategia de gestión de incidentes de seguridad para responder de manera efectiva a incidentes como brechas de datos.

Privacidad del Cliente y Seguridad de la Información

5 puntos clave para una política de Seguridad de la Información.

5. Monitoreo y auditoría continua:

- ✓ Establece un sistema de monitoreo de seguridad en tiempo real para detectar y responder a posibles amenazas.
- ✓ Realiza auditorías periódicas de seguridad de la información para evaluar la eficacia de tus políticas y procedimientos.
- ✓ Mantén registros detallados de incidentes de seguridad, actividades de usuario y cambios en la configuración para la revisión y análisis posteriores.

Privacidad del Cliente y Seguridad de la Información

La seguridad es un proceso continuo que requiere **adaptación constante** a medida que evolucionan las amenazas y tecnologías. Por lo tanto, es importante revisar y actualizar regularmente tu política de seguridad de la información para mantenerla efectiva y relevante.

Privacidad del Cliente y Seguridad de la Información

¿Qué se debe Garantizar?

Confidencialidad: Se garantiza que la información es accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: Se garantiza que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con la misma, toda vez que se requiera.

Privacidad del Cliente y Seguridad de la Información

VALORACIÓN DE CONTROLES.

CONTROL:

Medida que afecta el estado del riesgo, se deben segmentar en los controles que me impactan la probabilidad y los que me impactan la consecuencia, severidad o impacto de la materialización del mismo.

METODOLOGÍAS DE VALORACIÓN DE CONTROLES.

1. Grado del Control
2. Integralidad del Control
3. Solidez

Privacidad del Cliente y Seguridad de la Información

Atributos y Variables de un Control

Características o propiedades del control que NO afectan su valoración

ATRIBUTOS DEL CONTROL

Estado (Implementado, Propuesto, en proceso)
Tipo de Control (Preventivo, Protección, Correctivo, Transferencia)
Garantía del Seguro (Muy Importante)
Cumplimiento Legal (Muy Importante)

Propiedades del control que SI afectan su valoración.

VARIABLES DEL CONTROL

Responsable (Existe, No existe)
Naturaleza del Control (Manual, Automático)
Documentación
Frecuencia
Evidencia de cumplimiento
Idoneidad del Responsable del control
Alcance
Vulnerabilidad
Complejidad

Privacidad del Cliente y Seguridad de la Información

VALORACIÓN DE CONTROLES.

METODOLOGÍA 1, GRADO DEL CONTROL.

Es un valor que se asigna al control Y/O al conjunto de controles para determinar en qué nivel de implementación y ejecución se encuentra, de forma cualitativa se avalúan algunas variables del control para que el dueño del riesgo determine el grado del control.

1. DÉBIL
2. MODERADO
3. FUERTE
4. AUSENCIA DE CONTROL

Privacidad del Cliente y Seguridad de la Información

VALORACIÓN DE CONTROLES.

METODOLOGÍA 2, INTEGRALIDAD

DISEÑO 40%

¿Está definido el responsable del control? (40%)
SÍ: 100
NO: 0

¿Está documentado, actualizado y formalizado? (30%)
SÍ: 100
NO: 0

¿El control es Manual, Mixto o Automático? (30%)
MANUAL: 50
MIXTO: 80
AUTOMÁTICO: 10

EFICACIA 60%

¿El control se ejecuta? (30%)
SÍ: 100
OCASIONALMENTE: 50
NO: 0

¿El resultado de la aplicación del control es confiable y cumple con su objetivo? (70%)
SÍ: 100
CASIONALMENTE: 50
NO: 0

Materialidad (Criterio de Importancia)
¿La omisión de este control afecta: Garantía de seguro, normatividad legal externa, normatividad interna y/o fraude?
SÍ: Muy Importante
NO: Se evalúa el impacto hacia el riesgo

Categoría: Capital Social

Privacidad del Cliente y Seguridad de la Información

VALORACIÓN DE CONTROLES.

METODOLOGÍA 3, SOLIDEZ

DISEÑO DEL CONTROL		
Existe un responsable asignado	SI Existe	NO Existe
Ejecutor del control	SI Existe	NO Existe
Clase control (Correctivo, Detectivo, Preventivo)	Adecuado	Inadecuado
Naturaleza (Manual, Automático, dependiente de TI)	Definido	NO Definido
Frecuencia o Periodicidad del Control	Adecuado	Inadecuado
Documentación	Documentado	NO Documentado
Actividades que componen el control	Adecuadas	Inadecuadas

EJECUCIÓN DEL CONTROL
FUERTE
MEDERADO
DEBIL

Banco de Bogotá

Privacidad del Cliente y Seguridad de la Información

VALORACIÓN DE CONTROLES.

METODOLOGÍA 3, SOLIDEZ

Características del Diseño de los Controles y su Evaluación	
Descripción	**Características evaluables asociadas al diseño del control: Responsable, Tipo de control (correctivo, detectivo o preventivo), Naturaleza (manual, automático, manual dependiente de TI), Frecuencia / Periodicidad (diario, semanal, mensual, bimestral, trimestral, semestral, anual), Documentación y Actividades que componen el Control** • Evaluación del diseño del control (Muy Adecuado, Adecuado o inadecuado), teniendo en cuenta la siguiente lógica: • Responsable: Existe un responsable asignado = 1, No existe un responsable asignado=0 • Tipo de control (correctivo, detectivo o preventivo): Es adecuado = 1, Es inadecuado= 0 • Naturaleza (manual, automático, manual dependiente de TI): Definido = 1, No definido=0

Privacidad del Cliente y Seguridad de la Información

Características del Diseño de los Controles y su Evaluación	
Descripción	• Frecuencia / Periodicidad (diario, semanal, mensual, bimestral, trimestral, semestral, anual): Es adecuada = 3, Es inadecuada = 0 • Documentación: Está documentado = 1, No está documentado = 0 • Actividades que componen el Control: Son adecuadas = 3, Son inadecuadas = 0 ✓ R1: Si la sumatoria de todas las variables es igual a 10, el diseño del control es Muy Adecuado. ✓ R2: Si la sumatoria de todas las variables es menor a 10, pero la Frecuencia / Periodicidad del control es adecuada (3) y las actividades que componen el control son adecuadas (3), el diseño del control es Adecuado. ✓ R3: Si no se cumplen las condiciones del R1 o las condiciones del R2, el diseño del control es Inadecuado.
Diseño del control	Características asociadas al diseño del control, para que a través de su evaluación se pueda obtener la calificación del diseño del control, como Muy Adecuado, Adecuado o Inadecuado.

Privacidad del Cliente y Seguridad de la Información

VALORACIÓN DE CONTROLES.

METODOLOGÍA 3, SOLIDEZ

Modificar la Evaluación de la Ejecución de los Controles	
Descripción	El modelo Propone la ejecución de los controles, a través de las siguientes categorías: • Fuerte • Moderado • Débil
Ejecución	Evaluación de la ejecución de los controles de acuerdo con las anteriores categorías, para que en conjunto con la evaluación del diseño del control se pueda calcular la solidez del control.

Privacidad del Cliente y Seguridad de la Información

METODOLOGÍA 3, SOLIDEZ

Cálculo de la **solidez del control** como **Fuerte**, Moderado o **Débil**, de acuerdo con la calificación del diseño y de la ejecución del control. Para realizar este cálculo se debe tener en cuenta la siguiente lógica:

- ✓ Si **Diseño del control** = Inadecuado, entonces la **Solidez del control** = Débil
- ✓ Si **Diseño del control** = Muy Adecuado y **Ejecución del control** = Fuerte, entonces la **Solidez del control** = Fuerte
- ✓ Si **Diseño del control** = Muy Adecuado y **Ejecución del control** = Moderado, entonces la **Solidez del control** = Moderado
- ✓ Si **Diseño del control** = Muy Adecuado y **Ejecución del control** = Débil, entonces la **Solidez del control** = Débil
- ✓ Si **Diseño del control** = Adecuado y **Ejecución del control** = Fuerte, entonces la **Solidez del control** = Moderado
- ✓ Si **Diseño del control** = Adecuado y **Ejecución del control** = Moderado, entonces la **Solidez del control** = Moderado
- ✓ Si **Diseño del control** = Adecuado **Ejecución del control** = Débil, entonces la **Solidez del control** = Débil

CASO DE ESTUDIO

Título del Caso de Estudio:

"Evento de Seguridad de la Información en la Empresa **UNICORN**: Un Desafío de Seguridad y Privacidad de la Información''

Contexto:

UNICORN es una empresa que fabrica productos electrónicos de consumo. La empresa maneja información crítica de los clientes, incluidos datos de tarjetas de crédito y registros de garantía de productos. A pesar de su tamaño pequeño, **UNICORN** tiene una presencia significativa, con un sitio web de comercio electrónico y una base de datos que almacena información de clientes.

Evento:

- Un día, el equipo de seguridad de **UNICORN** descubre que ha ocurrido un evento que afecta la seguridad de los datos.
- Se sospecha que la información de los clientes, incluidos los números de tarjetas de crédito, han sido hurtados.
- La empresa tiene la responsabilidad de investigar el incidente, mitigar los daños y tomar medidas para evitar futuras violaciones.

CASO DE ESTUDIO

Preguntas clave para el análisis:

1. **¿Cómo ocurrió el evento?** Se puede explorar la cadena de eventos que llevó a la violación de datos, incluidas las vulnerabilidades en el sistema, las prácticas de seguridad deficientes o el comportamiento del empleado.

2. **¿Cuáles son las consecuencias?** Discutir las implicaciones legales, financieras y de reputación de la brecha de datos para UNICORN y sus clientes.

3. **¿Cómo se podría haber evitado le evento?** Analizar las medidas de seguridad que la empresa podría haber implementado para prevenir la violación.

4. **¿Qué debería hacer UNICORN a continuación?** Destacar las acciones correctivas que la empresa debe tomar para mitigar los daños, notificar a los clientes afectados y fortalecer sus políticas y prácticas de seguridad.

5. **¿Qué lecciones se pueden aprender de este incidente?** Destacar las lecciones clave que otras organizaciones pueden extraer de este caso de estudio para mejorar su propia seguridad y privacidad de la información.