



# Qué Hacer Si Hay un Compromiso de Seguridad

Programa de Seguridad de Información de Cuentas (AIS)

Febrero del 2006

**Administración de Riesgo**

Región América Latina y el Caribe





Introducción.....3  
Reportes de Violaciones de Seguridad.....4  
Pasos y Requisitos para las Entidades Comprometidas .....5  
Pasos y Requisitos para Bancos Miembros .....7  
Lineamientos de Investigación Forense .....8  
Apéndice A – Modelo del Reporte de Respuesta a un Incidente de Seguridad.....10

## Introducción

Reconocer qué constituye un incidente de seguridad es crucial para minimizar el impacto que un compromiso de seguridad podría tener en su organización. En general, un incidente de seguridad se podría definir como un ataque electrónico deliberado a los sistemas de comunicaciones o procesamiento de información. Trátese de un incidente iniciado por un empleado disgustado, un competidor malicioso o un delincuente cibernético mal intencionado, los ataques deliberados frecuentemente causan daños e interrupciones similares o mayores a los que puede causar cualquier desastre natural. La forma en que usted responde y maneja un ataque a los sistemas de información de su empresa determina lo bien que usted podrá controlar los costos y las consecuencias que podrían derivarse de dicho ataque. Por estas razones, el alcance de sus preparativos para manejar un incidente de seguridad y colaborar con Visa ALC tiene una importancia vital para la protección de la información clave de su compañía.

En caso de ocurrir un incidente de seguridad, los comercios o agentes deben actuar inmediatamente para investigar el suceso, limitar la exposición de los datos de los tarjetahabientes, notificar a su banco y a Visa y reportar los hallazgos de su investigación. Esta guía, titulada “Qué Hacer Si Hay un Compromiso de Seguridad” contiene instrucciones que le dicen paso por paso lo que debe hacer al responder a un incidente de seguridad. Además de las instrucciones generales que aquí se dan, es posible que Visa requiera una investigación que incluye, sin limitación, brindar acceso a los locales de la empresa y a todos los documentos y registros pertinentes, incluyendo copias de los análisis.

## Reportes de Violaciones de Seguridad

En caso de una violación de la seguridad, el *Reglamento Operativo de Visa ALC* requiere que los Miembros reporten inmediatamente dicha violación y cualquier sospecha de pérdida o la pérdida o robo confirmado de cualquier material o registro que pueda contener datos de los tarjetahabientes. Inmediatamente al completar la investigación el Miembro debe demostrar su capacidad o la capacidad de sus comercios o agentes para prevenir la pérdida o robo de información sobre transacciones en el futuro, de conformidad con los requisitos del Programa de Seguridad de la Información de Cuentas (AIS). Visa ALC o un tercero independiente aceptable para Visa deberá verificar esta capacidad llevando a cabo una revisión de seguridad posterior.

Si Visa determina que una entidad ha sido deficiente o negligente a la hora de mantener en forma segura la información de las cuentas o al reportar o investigar la pérdida de esta información, Visa podría requerir acción correctiva inmediata.

Si un comercio o su agente no cumplen con los requisitos de seguridad o no corrigen un problema de seguridad, Visa podrá:

- Multar al Banco Miembro,
- Imponer restricciones al comercio o su agente, o
- Prohibir permanentemente al comercio o a su agente la participación en programas de Visa.

## Pasos y Requisitos para las Entidades Comprometidas

Los comercios y proveedores de servicio que sospechen o hayan experimentado una violación de seguridad confirmada deben tomar medidas rápidas para ayudar a prevenir daños adicionales y cumplir con los requisitos del Programa de Seguridad de la Información de Cuentas (AIS).

1. **Inmediatamente contener y limitar la exposición.** Prevenir la pérdida de otros datos llevando a cabo una investigación exhaustiva del compromiso de seguridad de la información confirmado o que se sospecha. A fin de facilitar la investigación:
  - No acceda a los sistemas comprometidos ni los altere (por ejemplo, no se conecte a la máquina y cambie la contraseña, no se conecte como ROOT).
  - No apague la máquina comprometida. Por el contrario, aíslas los sistemas comprometidos de la red (es decir, desconecte el cable).
  - Preserve las bitácoras y registros electrónicos como evidencia.
  - Registre todas las acciones que implemente.
  - Si usa una red inalámbrica, cambie el SSID en el AP y otras máquinas que podrían estar utilizando esta conexión, con la excepción de cualquier sistema que usted crea comprometido.
  - Manténgase en alerta de ALTA seguridad y monitoree todos los sistemas de Visa.
2. **Alerte inmediatamente a todas las entidades necesarias. Asegúrese de contactar a:**
  - Su grupo de seguridad de la información y equipo de respuesta a incidentes internos.
  - Su banco comercial.
  - Inmediatamente al Grupo de Control de Fraude de Visa al teléfono (305) 328-1713.
  - Su departamento de policía local.
3. **Proporcione todos los números de las cuentas Visa comprometidas al Grupo de Control de Fraude de Visa dentro de un plazo de 24 horas.** Todas las cuentas potencialmente comprometidas deberán proporcionarse y transmitirse según las instrucciones que le dé el Grupo de Control de Fraude de Visa. Visa distribuirá los números de las cuentas comprometidas a los Emisores y asegurará el carácter confidencial de la información de la entidad e información que no sea de índole pública.
4. **Dentro de un plazo de cuatro días hábiles de la fecha del compromiso de seguridad reportado:**
  - Proporcione a Visa el documento con el Reporte de Respuesta a un Incidente de Seguridad. (Vea el Apéndice A para obtener el modelo del reporte.)

- Dependiendo del nivel de riesgo y elementos de datos obtenidos, realice una revisión forense independiente, llene el cuestionario de cumplimiento y realice un escán de vulnerabilidad a discreción de Visa.

## Pasos y Requisitos para Bancos Miembros

1. Reporte inmediatamente a Visa la sospecha de pérdida o robo o pérdida o robo confirmado de datos de tarjetahabientes de Visa. Los Miembros deben comunicarse inmediatamente con el Grupo de Control de Fraude de Visa al teléfono (305) 328-1713.
2. Obtenga de la entidad comprometida los números de las cuentas que están en riesgo. Dentro de un plazo de 48 horas informe a Visa si la entidad estaba cumpliendo con el Programa de Seguridad de la Información de Cuentas (AIS) en el momento de ocurrir el incidente, y, si es así, proporcione prueba apropiada.
3. Participe en todas las discusiones con la entidad comprometida y Visa ALC.
4. Asegure que se contrate a un evaluador de seguridad aprobado por Visa para llevar a cabo la investigación forense.
5. Obtenga de la entidad toda la información disponible sobre el compromiso de seguridad.
6. Determine si se ha contenido el compromiso de seguridad.
7. Informe a Visa ALC el estado de la investigación dentro de un plazo de 48 horas.
8. Asegure que la entidad haya dado los pasos necesarios para prevenir la pérdida o robo de otros datos de las cuentas en el futuro, de conformidad con los requisitos del Programa de Seguridad de la Información de Cuentas (AIS).

## Lineamientos de Investigación Forense

En caso de ocurrir un compromiso de seguridad, Visa ALC o el Miembro Adquirente de Visa contratará a una firma de seguridad independiente para que realice una investigación forense de las entidades comprometidas dentro de un plazo de 24 horas del compromiso de seguridad. Se deberán implementar las siguientes acciones como parte de la investigación forense:

### **Determinar qué información del tarjetahabiente está en riesgo. Ello incluye:**

- El número de cuentas en riesgo, identificar las cuentas almacenadas y comprometidas en todos los sistemas de prueba, desarrollo y producción.
- Tipo de información de cuenta en riesgo:
  - Número de cuenta
  - Fecha de vencimiento
  - Nombre del tarjetahabiente
  - Dirección del tarjetahabiente
  - Valor de Verificación de Tarjeta 2 (CVV2)
  - Pista 1 y Pista 2
  - Bloques de PINes
- Identificar cualquier dato exportado por el intruso.
- Proporcionar fechas y plazos para los números de cuenta almacenados y comprometidos
- Si es aplicable, el equipo de investigación forense ejecutará un Packet-Sniffer en la red de la entidad.

**Determinar si la aplicación de pago está reteniendo todos los datos de la pista, incluyendo bloques de PIN.**

### **Realizar una validación y evaluación del incidente de seguridad:**

- Establecer cómo ocurrió el compromiso de seguridad.
- Establecer el origen o causa de dicho compromiso.
- Determinar la fecha o plazo del compromiso de seguridad.
- Revisar toda la red para identificar todos los sistemas comprometidos o afectados, considerando los ambientes de comercio electrónico, corporativos, de prueba, de desarrollo y producción, así como conexiones de redes privadas virtuales (VPN), módem, DSL y cable de módem, y cualquier conexión a terceros.
- Determinar si se ha contenido el compromiso de seguridad.

**Verificar si se almacenan el Valor de Verificación de Tarjeta 2 (CVV2) y la Pista 1 y la Pista 2.** Examinar todas las posibles ubicaciones—incluida la aplicación de pago—para determinar si se almacenan los datos del Valor de Verificación de Tarjeta 2 (CVV2), Pista 1 o Pista 2, sea en formato encriptado o sin encriptar, por ejemplo, en tablas y bases de datos de producción o de respaldo, bases de datos utilizadas para el desarrollo, bitácoras de aplicaciones, bitácoras de transacciones, ambientes temporales o de prueba, o si hay datos de ambiente de prueba en las máquinas de los ingenieros de software, etc.

**Si una aplicación de pago está almacenando los datos completos de la pista, identificar el nombre del proveedor, el nombre del producto y la versión del producto.**

**Si es aplicable, revisar la seguridad en los puntos de conexión final de VisaNet y determinar el riesgo.**

**Preservar toda la evidencia electrónica potencial en una plataforma que sea apropiada para la revisión y el análisis de un tribunal, si fuera necesario.**

**Realizar un escán remoto de vulnerabilidad del sitio o sitios de la entidad conectados a Internet.**

## Apéndice A – Modelo del Reporte de Respuesta a un Incidente de Seguridad

Las normas de contenido y formato del reporte se delinean a continuación y deberán seguirse al completar el *Reporte de Respuesta a un Incidente de Seguridad*. Una vez completado, el reporte deberá enviarse a Visa y al banco comercial. Visa clasificará el reporte como “Visa Secret” o “Información Secreta de Visa”.

### I. Resumen Ejecutivo:

- Proporcione una descripción general del incidente.
- Incluya el Nivel de Riesgo (Alto, Mediano, Bajo) durante el análisis forense.
- Especifique si se ha contenido ya el compromiso de seguridad.

### II. Antecedentes

### III. Estado de Seguridad de Datos de la Industria de Tarjetas de Pago

- Tomando como base los hallazgos de la investigación forense, liste los requisitos de seguridad de datos de la industria de tarjetas de pago que no se estaban cumpliendo.

### IV. Descripción General de la Infraestructura de Red

- Incluya un diagrama de la red.

### V. Procedimientos de Investigación

- Incluya las herramientas forenses utilizadas durante la investigación.

### VI. Hallazgos

- Especifique el número de cuentas en riesgo e identifique las cuentas almacenadas y comprometidas.
- Indique el tipo de información de la cuenta que está en riesgo:
  - Número de cuenta
  - Fecha de vencimiento
  - Nombre del tarjetahabiente
  - Dirección del tarjetahabiente
  - Valor de Verificación de Tarjeta 2 (CVV2)
  - Pista 1 y Pista 2
  - Bloques de PIN
- Identifique todos los sistemas analizados. Incluya lo siguiente:
  - Sistemas de Nombres de Dominio (DNS)
  - Direcciones de Internet (IP)

- Versión del sistema operativo (OS)
  - Función de sistema(s)
- Identifique todos los sistemas comprometidos. Incluya lo siguiente:
  - Sistemas de Nombres de Dominio (DNS)
  - Protocolos de Internet (IP)
  - Versión del Sistema Operativo (OS)
  - Función de sistema(s)
- Indique las fechas o plazos del compromiso de seguridad.
- Describa cualquier tipo de dato exportado por el intruso.
- Explique el origen o causa del compromiso y cómo se estableció.
- Incluya evidencia de que todas las ubicaciones de bases de datos potencialmente comprometidas han sido verificadas a fin de asegurar que no hay datos del Valor de Verificación de Tarjeta 2 (CVV2), Pista 1 o Pista 2 almacenados en ningún lugar, sea en formato encriptado o sin encriptar (por ejemplo, en tablas o bases de datos de producción o de respaldo duplicadas, bases de datos utilizadas para el desarrollo, datos de ambientes temporales o de prueba en las máquinas de los ingenieros de software, etc.).
- Si una aplicación de un tercero almacena los datos completos de la pista, identifique lo siguiente:
  - Nombre del Proveedor
  - Información de Contacto
  - Nombre del Producto
  - Versión del Producto
  - Nombre(s) del registro o de los registros de la aplicación donde se retienen datos completos de la pista
  - Razón para almacenar y cuánto tiempo se retienen los datos completos de la pista
- Si el proveedor facilitó un parche o utilidad para borrar los datos completos de la pista, identifique el Nombre del Producto, Versión de Producto/Parche o Utilidad, y dé una breve descripción del parche o utilidad.
- Si un revendedor brinda soporte al producto, identifique lo siguiente:
  - Nombre del Revendedor
  - Información de Contacto
- Si es aplicable, revise la seguridad en los puntos de conexión final de VisaNet y determine el riesgo.

## VII. Acción de la Entidad Comprometida

**VIII. Recomendaciones**

**IX. Contactos de la Entidad y Evaluador de Seguridad que Realiza la Investigación**