Universidad Interamericana de Puerto Rico
Oficina del Presidente

# GUÍAS, NORMAS Y PROCEDIMIENTOS PARA LA PREVENCIÓN DEL ROBO DE IDENTIDAD

**DOCUMENTO NORMATIVO F-1009-019R**

## Introducción

El robo de identidad es un fenómeno social que puede afectar no sólo a la Universidad como institución sino también a sus estudiantes, empleados y acreedores. Por ello, las leyes federales y estatales exigen que ciertas instituciones, entre ellas las universidades, establezcan programas y procedimientos para la prevención, detección y mitigación de los efectos del robo de identidad.

En este documento se establecen las guías, normas y procedimientos para lograr esos propósitos en la Universidad Interamericana de Puerto Rico.

## I. Base legal

Este documento normativo sobre la prevención del robo de identidad se promulga en virtud de la autoridad conferida al Presidente de la Universidad por la Junta de Síndicos en los Estatutos de la Universidad.

Se apoya, además, en la Ley de Transacciones Crediticias Justas y Precisas o "Fair and Accurate Credit Transactions Act" (FACTA), su reglamentación sobre alertas "Red Flags", y las definiciones de la "Federal Trade Commision" (FTC) 16 C.F.R. §. 681.2.

## II. Propósito

Este documento normativo tiene el propósito de establecer las guías, normas y procedimientos del plan para detectar, identificar y mitigar el robo de identidad de las cuentas identificadas de la Institución que así lo precisen.

## III. Alcance

Este documento normativo tendrá vigencia en todas las unidades del Sistema Universitario.

## IV. Definiciones

4.1 Administrador – el Administrador del programa de prevención de robo de identidad.

4.2 Acreedor – entidad que regularmente extiende, renueva o prorroga crédito.

4.3 Alertas "Red Flags" – patrón de conducta, práctica o actividad específica que indica la posible existencia de robo de identidad.

4.4 Cliente – persona con una cuenta cubierta con el acreedor.

4.5 Crédito – derecho otorgado por un acreedor a un deudor de diferir el pago de una deuda; de incurrir en deuda y diferir su pago o de comprar propiedad o servicios y diferir el pago.

4.6 Cuentas cubiertas:

4.6.1 Cualquier cuenta que la Universidad tenga primariamente para propósitos económicos, que incluya múltiples pagos o transacciones.

4.6.2 Cualquier otra cuenta que la Universidad tenga para la cual exista algún riesgo razonable para los consumidores o clientes o para la seguridad y fortaleza de la Universidad en torno al robo de identidad.

4.7 Información identificable – nombre o número que se utiliza solo o en conjunto con cualquier otra información, para identificar a una persona en específico, tales como: nombre, dirección, número de teléfono, número de seguro social, fecha de nacimiento, número de licencia de conducir, número de registro de un extranjero residente, número de pasaporte, número de identificación patronal o de la persona que pague contribución sobre ingresos, el número de identificación único electrónico, o la dirección del protocolo de Internet de la computadora.

4.8 Junta de Síndicos – la Junta de Síndicos de la Universidad Interamericana de Puerto Rico, Inc.

4.9 Presidente – el Presidente de la Universidad Interamericana de Puerto Rico.

4.10 Programa – programa de prevención del robo de identidad, según se describe en el Anejo A.

4.11 Robo de identidad – fraude que se comete utilizando la información identificable de otra persona.

4.12 Universidad o Institución – la Universidad Interamericana de Puerto Rico, Inc.

## V. Responsabilidades

5.1 Presidente

5.1.1 El Presidente designará a un oficial de la Universidad para que sirva como Administrador del Programa.

5.1.2 Someterá a la Junta de Síndicos, para su aprobación, los cambios que sean necesarios para mantener actualizado el Plan para la prevención del robo de Identidad.

5.2 Rectores y Decanos de Escuelas profesionales

5.2.1 Los rectores y decanos de las escuelas profesionales designarán el Oficial responsable del Programa en su unidad para desarrollar e implantar los métodos específicos y el protocolo apropiado para cumplir con lo establecido en este documento normativo.

5.3 Administrador

5.3.1 El Administrador desarrollará, implantará y mantendrá al día el Programa de Prevención del robo de identidad en todo el Sistema Universitario.

5.3.2 Ejercerá la supervisión apropiada y efectiva del Programa e informará al Presidente en torno a sus resultados.

5.3.3 Coordinará con el apoyo de los oficiales de las unidades el ofrecimiento de adiestramientos a los empleados en torno a los siguientes asuntos relacionados con el Programa:

a. Detección de alertas.
b. Pasos que se deben seguir para la detección, prevención y mitigación de robo de identidad.
c. Preparación de informes relacionados con el robo de identidad.

5.3.4 Revisará periódicamente el Programa para identificar los cambios que sean necesarios, relacionados con:

a. Tecnologías en desarrollo.
b. Riesgos de robo de identidad.
c. Métodos de robo de identidad.
d. Detección de robo de identidad.
e. Métodos de prevención y mitigación.
f. Tipos de cuentas que tiene la Institución.
g. Acuerdos contractuales de negocios de la Universidad con otras entidades.
h. Requerimientos legales en el área de robo de identidad.

5.3.5 Consultará con el personal universitario que sea necesario para asegurar el cumplimiento con el Programa.

5.3.6 Presidirá un grupo de trabajo compuesto por un representante de la Vicepresidencia de Asuntos Académicos, de Gerencia y Finanzas, del Centro de Cómputos y de la Oficina Jurídica.

5.3.7 Presentará las recomendaciones de cambios al Presidente para su aprobación.

5.4 Oficial del Programa

5.4.1 Persona designada en cada unidad del Sistema para desarrollar e implantar los métodos específicos y el protocolo apropiado para cumplir con las disposiciones de este documento.

5.5 Empleados

5.5.1 Los empleados con funciones relevantes al Programa deberán asistir a adiestramientos para conocer y monitorear las diferentes alertas relacionadas con las cuentas de la Universidad (tipos de cuentas, métodos de apertura y acceso a cuentas y para aprender sobre experiencias anteriores en torno al robo de identidad). En particular deberán conocer y monitorear las siguientes categorías:

a. Notificaciones y advertencias de agencias que proveen informes de crédito

- Informe de fraude que se acompaña al informe de crédito.
- Notificación o informe de una agencia crediticia sobre la congelación de crédito de un cliente o solicitante de crédito.

- Notificación o informe de una agencia crediticia sobre una alerta en una cuenta activa de un solicitante.
- Indicación en un informe de crédito de alguna actividad que sea inconsistente con el patrón o actividad usual de un cliente.

b. Documentos sospechosos

- Documento de identificación o tarjeta que parezca haber sido falsificada, alterada o que no sea auténtica.
- Documento de identificación o tarjeta en la que la fotografía de una persona o su descripción física no sea consistente con la persona que presenta la identificación.
- Otro documento que contenga información que no sea consistente con la información que se tenga un cliente (por ejemplo un cheque con la firma aparentemente falsificada).
- Solicitud de servicio que aparenta haber sido alterada o falsificada.

c. Información personal de identificable como sospechosa

- Información presentada para identificación presentada que resulte inconsistente con otra información que el cliente provee (por ejemplo: fecha de nacimiento inconsistente).
- Información presentada para identificación que sea inconsistente con otra fuente de información, como una dirección que no coincida con los documentos provistos por el estudiante.
- Información presentada para identificación igual a la que aparece en otras solicitudes que resultaron ser fraudulentas.
- Información presentada para identificación que sea consistente con actividad fraudulenta (como un número de teléfono que no es válido o una dirección de facturación ficticia).
- Número de seguro social presentado, que sea idéntico al provisto por otro estudiante o cliente.
- La persona deja de proveer información personal de identificación completa en su solicitud, aún después que se le requiera que la provea (a excepción del número de seguro social que por ley no deber ser requerido).
- Información para la identificación de una persona que no es consistente con la información que existe en su expediente.

d. Actividad sospechosa en una cuenta, o uso poco común de una cuenta

- Cambio de dirección para una cuenta seguido de una solicitud de cambio de nombre del dueño de la cuenta.
- Uso de una cuenta de una manera que no es consistente con su uso anterior (mucha actividad de repente en la cuenta).
- Correspondencia enviada a un estudiante que ha sido repetidamente devuelta por no poderse entregar.
- Notificación a la Universidad de que el estudiante no está recibiendo la correspondencia enviada.
- Notificación a la Universidad de que en una cuenta se está llevando a cabo una actividad no autorizada.
- Violación del sistema de seguridad computarizado de la Universidad.
- Acceso no autorizado a una cuenta o uso de la información de una cuenta.

e. Otras alertas

- Notificación a la Universidad de parte de un estudiante de que ha sido víctima de robo de identidad, o de que alguna agencia del orden público u otra entidad, ha abierto o mantiene una cuenta fraudulenta.

f. Los empleados deberán conocer los pasos que deben seguir, una vez estén adiestrados para las alertas anteriores.

## VI. Procedimiento para la detección de alertas

6.1 Nuevas cuentas

Para poder detectar cualquiera de las alertas identificadas anteriormente, relacionadas con la apertura de cuentas nuevas, el personal de la Universidad llevará a cabo los siguientes pasos para obtener y verificar la identidad de la persona que abre la cuenta:

a. Solicitar información para identificar a la persona: nombre, fecha de nacimiento, dirección residencial, licencia de conducir u otra identificación con retrato.
b. Verificar la identidad del estudiante (revisar la licencia de conducir y otra tarjeta de identificación con retrato).
c. Contactar al estudiante en otra ocasión para verificar si la información es correcta.

6.2 Cuentas existentes

Para poder detectar cualquiera de las alertas identificadas anteriormente para una cuenta ya existente, el personal de la Universidad tomará los siguientes pasos a fines de monitorear las transacciones realizadas en una cuenta:

a. Verificar la identificación de los clientes cuando soliciten información (en persona, por teléfono, por facsímil, o por correo electrónico).
b. Verificar la validez de las solicitudes de cambio de dirección.

## VII. Mitigación de robo de identidad

7.1 Cuando el personal de la Universidad detecte o identifique alguna de las alertas descritas en este documento, deberá tomar los pasos necesarios y apropiados para reaccionar, mitigar el robo de identidad, dependiendo de la naturaleza y el grado de riesgo de la alerta, incluyendo, pero no limitándose a lo siguiente:

7.1.1 Continuar el monitoreo de la cuenta para recoger evidencia de robo de identidad.

7.1.2 Contactar al estudiante.

7.1.3 Cambiar la contraseña o dispositivo de seguridad que permita el acceso a las cuentas.

7.1.4 Notificar a las agencias pertinentes del orden público pertinentes.

## VIII. Contratos con proveedores de servicios

Cuando la Universidad contrate a un proveedor de servicios para que realice una actividad relacionada con una o varias de las cuentas, la Universidad verificará que el proveedor de servicio realice la actividad de acuerdo con las políticas y procedimientos razonables designados para detectar, prevenir y mitigar el riesgo de robo de identidad.

## IX. Cláusula de confidencialidad sobre prácticas específicas

Se considerará confidencial cualquier documento que se haya producido o que se produzca para desarrollar o implementar el Programa según se describe en el Anejo A, el cual describe prácticas o procedimientos específicos.

## X. Separabilidad

Si cualquier parte o sección de estas guías, normas y procedimientos es declarada nula por una autoridad competente, tal decisión no afectará las restantes.

## XI. Derogación o enmiendas

Estas guías, normas y procedimientos enmiendan el documento normativo F-1009-019 y cualesquiera otras directrices que estén en conflicto con lo aquí dispuesto. Este documento puede ser enmendado o derogado por el Presidente de la Universidad.

## XII. Vigencia

Estas guías, normas y procedimientos tendrán vigencia inmediata a partir de la aprobación y firma del Presidente.

## XIII. Aprobación

Manuel J. Fernós, Lcdo.
Presidente

24 de marzo, 2011
Fecha (D-M-A)

ymc

Anejo

**ANEJO A**

**Universidad Interamericana de Puerto Rico**
**Oficina Central del Sistema**

# PROCEDIMIENTO PARA LA IMPLANTACIÓN DEL PROGRAMA DE PREVENCIÓN, DETECCIÓN Y MITIGACIÓN DEL ROBO DE IDENTIDAD EN LAS CUENTAS CUBIERTAS DE LA UNIVERSIDAD INTERAMERICANA DE PUERTO RICO

## Introducción

La Universidad, en armonía con su misión educativa, tiene el compromiso firme de cumplir cabalmente con las disposiciones de ley y velar por los mejores intereses de la comunidad universitaria y de la propia Institución. Como parte de este compromiso la Junta de Síndicos aprobó que se estableciera, documentara y mantuviera un programa preventivo para la identificación, detección y mitigación a riesgos de robo de identidad. Este documento normativo reafirma la política institucional y provee el mecanismo para la implantación del Programa.

## I. Base legal

Este Programa de prevención, detección y mitigación del robo de Identidad se promulga conforme a los requisitos establecidos en el documento normativo: *Guías, normas y procedimientos para la prevención del robo de Identidad*, Documento Normativo F-1009-019.

Se apoya, además, en la *Ley de transacciones crediticias justas y precisas*, también conocida como el "Fair and Accurate Credit Transactions Act of 2003 (FACTA)" y su reglamentación sobre alertas "Red Flags Rule of 2007", 16 C.F.R. §681.2 que enmiendan el "Fair Credit Reporting Act (FCRA)", 15 U.S.C. § 1681m(e).

## II. Propósito

Este documento tiene el propósito de establecer un programa coordinado para la prevención, detección y mitigación de los efectos del robo de identidad de las cuentas cubiertas identificadas por la Universidad. El programa incorporará, según proceda, los procedimientos que controlan los riesgos razonablemente previsibles. Incluirá, además, el procedimiento para:

2.1 Identificar alertas rojas "Red Flags" de las cuentas cubiertas;

2.2 Detectar las alertas rojas "Red Flags" que se identifiquen en el Programa;

2.3 Prevenir y mitigar adecuadamente cualquier alerta roja "Red Flag" que se detecte;

2.4 Asegurar que el Programa se actualice periódicamente para reflejar los cambios en los factores de riesgo para las cuentas cubiertas de la Universidad y para la seguridad y solidez de los acreedores de la Universidad.

## III. Alcance

Este documento tendrá vigencia en todas las unidades del Sistema, inclusive en los centros de servicios, empresas auxiliares y cualquier otra dependencia de la Universidad.

## IV. Definiciones

Además de adoptarse las definiciones establecidas en el documento *Guías, normas y procedimientos para la prevención del robo de identidad*, en este Documento los siguientes términos y expresiones tendrán el significado que se indica a continuación:

4.1 Alertas rojas "Red Flags" - patrón de conducta, práctica o actividad específica que indica la posible existencia de robo de identidad.

4.2 Cliente - persona con una cuenta cubierta con la Universidad.

4.3 Cuentas cubiertas:

(a) cualquier cuenta que la Universidad tenga primariamente para propósitos económicos, que incluya múltiples pagos o transacciones.

(b) cualquier otra cuenta que la Universidad tenga para la cual exista algún riesgo razonable para los consumidores o clientes o para la seguridad y fortaleza de la Universidad en torno al robo de identidad.

Las cuentas cubiertas en la Universidad incluyen, pero no se limitan a:

4.3.1 Expediente académico de estudiantes.

4.3.2 Préstamos estudiantiles, como el programa de salud (HPSL, NSL), Stafford, préstamos directos, Perkins e Institucionales.

4.3.3 Pago diferido de matrícula.

4.3.4 Reembolsos de balances créditos.

4.4 Ejecutivo Principal - El Presidente de la Universidad, el Rector de cada Recinto, el Decano de la Facultad de Derecho y el Decano de la Escuela de Optometría.

4.5 Información identificable - Información que puede ser utilizada para identificar a una persona y que, al ser divulgada de forma inadecuada, pueda causar daño o perjuicio a la persona. Esto incluye, pero no se limita a:

- Nombre completo
- Número de seguro social
- Número que se utiliza solo o en conjunto con cualquier otra información para identificar a una persona en específico
- Dirección
- Número de teléfono
- Fecha de nacimiento
- Número de licencia de conducir
- Número de registro de un extranjero residente
- Número de pasaporte
- Número de identificación patronal
- Número de registro único electrónico
- Dirección del protocolo de internet de la computadora
- Tarjetas de crédito
- Los documentos requeridos para crear expedientes de estudiantes, tales como:
  - Solicitud debidamente cumplimentada
  - Transcripciones de crédito
  - Resultados de pruebas de admisión
  - Certificado de Inmunización
  - Cartas de recomendación
  - Certificado de antecedentes penales
  - Tarjeta de residencia
  - En caso de estudiantes extranjeros,
    - Afidávit del auspiciador
    - Carta bancaria
    - Pasaporte y Visa

4.6 Robo de identidad - Fraude que se comete utilizando la información identificable de otra persona.

4.7 Unidad del Sistema - La Oficina Central, cada uno de los recintos, la Facultad de Derecho, la Escuela de Optometría y cualquier otra unidad que se establezca en el futuro.

## V. Identificación de alertas rojas "Red Flags" relevantes

El Programa considera los siguientes factores de riesgo en la identificación de alertas rojas relevantes:

5.1 Documentos sospechosos.

5.1.1 Tarjeta de identificación que parezca alterada, falsificada o no auténtica.

5.1.2 Documento con información que no sea consistente con la información que la Universidad tenga de la persona o cliente (ejemplo: firma falsificada, apellidos diferentes, direcciones diferentes, entre otros).

5.1.3 Identificación donde la fotografía de la persona no sea consistente con la persona que la presenta.

5.1.4 Solicitud de servicio con información identificable incompleta.

5.1.5 Tarjeta de identificación de estudiante o de seguro social presentada que no sea el del estudiante o del cliente.

5.2 Notificaciones y advertencias de agencias que proveen informes de crédito.

5.2.1 Informe de fraude que se adjunta al informe de crédito.

5.2.2 Notificación o informe de una agencia crediticia sobre la congelación de crédito de un cliente o solicitante de crédito.

5.2.3 Notificación o informe de una agencia crediticia sobre una alerta en una cuenta activa de un solicitante.

5.2.4 Indicación en un informe de crédito de alguna actividad que sea inconsistente con el patrón o actividad usual de un cliente.

5.3 Información personal que se identifica como sospechosa.

5.3.1 Información presentada para identificación que resulte inconsistente con otra información que el cliente o estudiante provee (por ejemplo: fecha de nacimiento inconsistente).

5.3.2 Información presentada para identificación que sea inconsistente con otra fuente de información, como una dirección que no coincida con los documentos provistos por el estudiante o cliente.

5.3.3 Información presentada para identificación igual a la que aparece en otras solicitudes que hayan resultado fraudulentas.

5.3.4 Información presentada para identificación que sea consistente con actividad fraudulenta (como un número de teléfono que no sea válido o una dirección de facturación ficticia).

5.3.5 Número de seguro social presentado que sea idéntico al provisto por otro estudiante o cliente.

5.3.6 Información personal de identificación incompleta en la solicitud, aun después que se le requiera que la provea (a excepción del número de seguro social que por ley no debe ser requerido).

5.3.7 Información para la identificación de una persona que no sea consistente con la información que existe en su expediente.

5.3.8 Alertas recibidas del Departamento de Educación Federal a través del "Institutional Student Information Record" (ISIR), el cual contiene toda la información contenida en la Solicitud Gratuita de Ayuda Económica (FAFSA).

5.3.9 Cambios solicitados en el formulario de activación de depósito directo.

5.4 Actividad sospechosa o uso poco común de una cuenta.

5.4.1 Cambio de dirección para una cuenta, seguido de una solicitud de cambio de nombre del dueño de la cuenta.

5.4.2 Uso de una cuenta que no sea consistente con el uso anterior (mayor o menor uso de la cuenta).

5.4.3 Correspondencia enviada a un estudiante o cliente que haya sido devuelta repetidamente por no poderse entregar.

5.4.4 Notificación a la Universidad de que el estudiante o cliente no está recibiendo la correspondencia enviada.

5.4.5 Notificación a la Universidad de que en una cuenta se está llevando a cabo una actividad no autorizada.

5.4.6 Violación del sistema de seguridad computadorizado de la Universidad.

5.4.7 Acceso no autorizado a una cuenta o uso de la información de una cuenta.

5.5 Otras alertas.

Notificación a la Universidad de parte de un estudiante o cliente de que ha sido víctima de robo de identidad, o de que alguna agencia del orden público u otra entidad ha abierto o mantiene una cuenta fraudulenta.

## VI. Procedimiento para la detección de alertas rojas "Red Flags" en cuentas nuevas y cuentas existentes

Se deberá seguir el siguiente procedimiento:

6.1 Requerir que el estudiante o cliente provea información adicional para identificar a la persona, como fecha de nacimiento, dirección, licencia de conducir u otra identificación con retrato vigente.

6.2 Verificar la identidad a través de la licencia de conducir u otra identificación con foto emitida por el gobierno estatal o federal, al proveer una identificación al estudiante.

6.3 Verificar la identidad del estudiante o de la persona que provee su sustento, si solicita información de la cuenta o del expediente del estudiante.

6.4 Verificar la validez de la solicitud de cambio de dirección e información de la cuenta del estudiante o cliente.

6.5 Verificar el uso de una cuenta cubierta cuando no sea consistente con su uso normal (actividad constante de una cuenta).

6.6 Solicitar autorización por escrito del estudiante, que incluya su identificación o la del solicitante, antes de someter información a una tercera persona. Esta divulgación está regulada por el Documento Normativo I-1209-007 "*Procedimiento para la divulgación de información a terceros*".

6.7 Requerir información personal identificable y consistente, que permita la validación de la transacción.

## VII. Prevención y mitigación

Cada empleado o contratista que realice trabajos para la Universidad deberá cumplir con las siguientes directrices:

7.1 Cumplir con las *Guías, normas y procedimientos para la prevención del robo de identidad*, Documento Normativo F-1009-019.

7.2 Manejar la información confidencial en forma segura, según se establece en los Documentos Normativos I-1209-006 "*Normas sobre la confidencialidad de la información*" y el G-0207-027 "*Guías, normas y procedimientos para la protección de la privacidad de la información del consumidor*".

7.3 Divulgar la alternativa que tiene el estudiante de excluir su información del directorio del Directorio de Estudiantes y Ex alumnos, según se establece en el Documento Normativo E-0809-002 "*Reglamentación de la Universidad Interamericana de Puerto Rico sobre el directorio de estudiantes y ex alumnos*".

7.4 Cumplir con la *Normativa institucional contra el fraude*, Documento Normativo F-1106-012.

7.5 Triturar todo documento que contenga información personal identificable.

7.6 Limitar el código de acceso del estudiante a una vigencia anual. El mismo debe ser creado por el estudiante con una combinación de caracteres específicos (números, letras y signos).

7.7 Asegurar el cumplimiento del proceso de autorización y uso de contraseñas para garantizar la seguridad y la confidencialidad de la información. Se detalla la información en el "*Reglamento de contraseñas de la Universidad Interamericana de Puerto Rico*, Documento Normativo I-1009-002R".

7.8 No proveer información identificable o confidencial a través de llamada telefónica.

7.9 Comunicarse con el estudiante para verificar la información.

7.10 Continuar el monitoreo de la cuenta para recoger evidencia de robo de identidad.

7.11 Cambiar periódicamente la contraseña o el dispositivo de seguridad que permita el acceso a las cuentas.

7.12 Toda información identificable transmitida a través de correos electrónicos de la Universidad deberá estar encriptada al ser transmitida electrónicamente y contener el siguiente mensaje:

*"Este mensaje puede contener información confidencial y/o propietaria de la Universidad Interamericana de Puerto Rico y la misma está dirigida a la persona u organización a la cual originalmente fue enviada. Cualquier uso por otros está estrictamente prohibido. Si usted no es la persona u organización a la que se dirige este correo electrónico, y el mismo ha llegado por error, infórmelo al remitente y destruya el mismo".*

7.13 Notificar el robo de identidad a las agencias responsables del cumplimiento de ley correspondiente.

7.14 Manejar la información contenida en los documentos impresos (distribución en papel) considerando las siguientes medidas:

7.14.1 Cumplir con las disposiciones del *Reglamento para la Administración de Documentos en la Universidad Interamericana de Puerto Rico*, Documento Normativo F-AD-005-2001.

7.14.2 Cualquier dato personal o sensitivo deberá almacenarse en gavetas, archivos, o bóvedas mientras no se esté utilizando.

7.14.3 Las gavetas, archivos, o bóvedas que contengan información identificable deberán ponerse bajo llave o combinación al cierre de cada día o cuando no haya supervisión en el lugar.

7.14.4 Los escritorios, áreas de trabajo, impresoras, facsímiles y áreas comunes de trabajo deberán estar libres de documentos que puedan tener información identificable o sensitiva.

7.14.5 Las pizarras, tablones de discusión y presentaciones deberán de estar libres de información identificable al cierre de cada día o cuando no haya supervisión.

7.14.6 Cuando los documentos o expedientes se tengan que compartir entre oficinas se proveerá sólo la información necesaria para cumplir con la solicitud de la oficina peticionaria.

7.15 Contratos con proveedores de servicios.

Cuando la Universidad contrate proveedores de servicios, tales como agencias de cobros, agencias de facturación, entre otros, para que realicen una actividad relacionada con una o varias de las cuentas cubiertas, se requerirá lo siguiente:

7.15.1 Que en el contrato se especifique que el proveedor realizará el servicio de acuerdo con las directrices y procedimientos designados en este documento para detectar, prevenir y mitigar el riesgo de robo de identidad.

7.15.2 Que notifique al Administrador del Programa de la Universidad cualquier alerta roja "Red Flag" que haya detectado al ofrecer sus servicios.

## VIII. Administración del Programa

8.1 La responsabilidad general para el desarrollo, implantación y actualización de este programa recae en el Administrador del Programa. El Administrador del Programa será responsable de:

8.1.1 Administrar el Programa en el nivel institucional.
8.1.2 Revisar los informes de personal con respecto a la detección de las alertas y las medidas para prevenir y mitigar el robo de identidad.
8.1.3 Determinar los pasos de prevención y mitigación que deben darse en circunstancias particulares, teniendo en cuenta los cambios periódicos del Programa.
8.1.4 Coordinar, con el apoyo de los oficiales de las unidades, el ofrecimiento de adiestramientos adecuados para la formación del personal relacionado con el Programa.
8.1.5 Coordinar, con el oficial de cada unidad, los adiestramientos del personal con funciones relevantes al Programa para conocer y monitorear las diferentes cuentas cubiertas y aprender a detectar y mitigar cuando se detecte una alerta roja "Red Flag".
8.1.6 Preparar y someter un informe anual al Presidente que incluya una evaluación de la efectividad del Programa, los incidentes y el manejo de los mismos, las monitorias y recomendaciones, y la actualización del Programa.

8.2 Responsabilidades de los oficiales de las unidades del Sistema.

8.2.1 Comunicar a los decanos y directores, los requisitos del Programa y la manera en que éstos impactan sus programas.
8.2.2 Colaborar con el Administrador en la revisión y actualización del Programa.
8.2.3 Colaborar con el Administrador en los adiestramientos del personal con funciones relevantes al Programa.

8.3 Responsabilidades de los supervisores de oficina con funciones relevantes al Programa.

8.3.1 Procurar que se adiestre a los empleados de sus áreas o departamentos sobre los requisitos del Programa.
8.3.2 Velar por que los empleados de sus áreas o departamentos cumplan con los requisitos del Programa.
8.3.3 Tomar las medidas necesarias y apropiadas para mitigar el robo de identidad.

8.4 Nombramiento de un oficial de cada unidad por el ejecutivo principal de la unidad. El oficial designado comunicará los requisitos del Programa a los decanos y directores y la manera que impacta sus programas. Los ejecutivos principales, los decanos y los directores, a su vez, son responsables de adiestrar a los empleados de sus áreas o departamentos sobre los requisitos de este Programa.

8.5 Actualización del Programa.

Este programa será revisado y actualizado periódicamente para reflejar los cambios en los riesgos de las cuentas cubiertas identificadas y para fortalecer el Programa de la Universidad contra el robo de identidad. Al menos una vez al año, el Administrador del Programa deberá reunirse con el oficial responsable del programa de cada unidad para considerar sus experiencias relacionadas con el robo de identidad y con los cambios en: la identificación de métodos de robo de identidad, la detección y prevención de robo de identidad; los tipos de cuentas que la Universidad mantiene, y los acuerdos de negocio de la Universidad con otras entidades. Después de considerar estos factores, el Administrador determinará si se justifican los cambios en el Programa, incluyendo la lista de alertas. Si se justifican, el Administrador actualizará el Programa.

8.6 Adiestramientos a Empleados.

El Administrador del Programa coordinará con el oficial designado de cada unidad los adiestramientos del personal con funciones relevantes al Programa, para conocer y monitorear las diferentes cuentas cubiertas y aprender a detectar y mitigar cuando se detecta una alerta roja "Red Flag".

8.7 Supervisión de los proveedores de servicios.

El ejecutivo principal adoptará las medidas necesarias para garantizar que los servicios de los proveedores que realicen una actividad con una o más cuentas cubiertas, se lleve a cabo de conformidad con directrices y procedimientos diseñados para detectar, prevenir y mitigar el robo de identidad.

## IX. Separabilidad

Si cualquier parte o sección de este Programa es declarado nulo por una autoridad competente, tal decisión no afectará las restantes secciones de este documento.

CRI