ESTÁNDARES DE PROTECCIÓN INFORMACIÓN DE IDENTIFICACIÓN PERSONAL

Control de versiones

	Fecha	Modificado por	Aprobado por	Cambios
1.0	1 de octubre de 2017	N/A	Acceso a la Información Confidencial del Cliente – Comité Directivo Ejecutivo	Publicación inicial
1.1	30 de enero de 2019	**Carol Aybar** Asesora No Financiera de Banca Digital y Nuevas Iniciativas	**Grant Mick** Vicepresidente Sénior, Controles Internos **Nicole Frew** Vicepresidenta Sénior, Controles Internos	(1) Se solicitará una confirmación por escrito a todos los empleados que trabajen de forma remota (página 12) (2) Se excluirá a los empleados que sean móviles (es decir, sin ubicación física fija ni en las instalaciones del Banco ni en casa) de las visitas programadas o no programadas en sitio en la ubicación de trabajo alternativa (página 15) (3) Se agregó la opción de inspección en línea para las actividades de monitoreo de personal que trabajan de forma remota (páginas 15 y 16) (4) Las actividades de monitoreo de personal que trabaja de forma remota cambiaron a cada 180 días en lugar de cada 120 días (página 16)
2.0	6 de agosto de 2021	**Sargon Youhanna** Banca Canadiense Asesor No Financiero de Banca Digital y Nuevas Iniciativas **Rodrigo Caballero Colin** Gerente Sénior, Gestión del Cumplimiento Regulatorio Banca Internacional - Control Interno		(1) Enlaces actualizados de las Políticas y Procedimientos correspondientes en todo el documento (2) Se creó la nueva sección Imprimir en casa (page 8) (3) Se creó la nueva sección de herramientas de colaboración (Teams/Zoom) (página 10) (4) Se incorporó la sección 3.3, “Monitoreo adicional para los empleados que permanentemente trabajan de forma remota” en la sección 2.3 “Trabajo desde casa” para consolidar los requisitos en una sola sección (página 15)

		Tejinder Litt Gerente Sénior, Iniciativas Operacionales y Regulatorias Control Regulatorio y Operacional de Gestión Patrimonial		(5) Se revisó el requisito impuesto a los gerentes de sucursales para ya no mantener el Registro de Inspección de Monitoreo, ya que el programa de Monitoreo Reforzado de Empleados brinda los controles de apoyo para el monitoreo sistemático de PII (página 16) (6) Se agregó un Monitoreo Reforzado de Empleados en la sección 3.1 (página 17) (7) Se actualizó la frecuencia de revisión del acceso lógico para que no exceda lo seis meses, a diferencia de tres meses, para adaptar el plazo y completar las conciliaciones manuales de las unidades de negocio más grandes (página 18)
2.1	22 -Sep-2021		**Grant Mick** Vicepresidente Sénior, Controles Internos - Banca Canadiense **Carolina Parra** Vicepresidenta Sénior de PLD y Controles Internos - Banca Internacional **Rosemary Chan** Vicepresidenta Sénior, Control Interno y Asuntos Regulatorios	(1) Aprobación final

Índice

1. Reseña

Los clientes y empleados depositan su confianza en The Bank of Nova Scotia (el "Banco" o "Scotiabank") para mantener su Información de Identificación Personal segura y protegida, y esperan que esta confianza sea respetada. Cada empleado y tercero externo contratado por el Banco es responsable de toda la Información de Identificación Personal que tenga en su poder o custodia, incluida la información personal divulgada a terceros con fines de procesamiento o para la ejecución de otras funciones administrativas.

Los Estándares de Protección de Información de Identificación Personal (los "Estándares") describen los requisitos mínimos que deben seguir los empleados con acceso excesivo a información sensible de los clientes en Banca Canadiense, Banca Internacional y Gestión Patrimonial Global para proteger y salvaguardar la Información de Identificación Personal de los clientes y empleados. Si bien el riesgo de incidentes y violaciones a la privacidad no puede eliminarse completamente, puede gestionarse efectivamente para reducir de manera significativa el riesgo de provocar algún daño a Scotiabank, a sus clientes, empleados y otras personas. Algunas violaciones a la privacidad incluyen:

Para los clientes, empleados y otras personas afectadas:

- Robo de identidad, fraude y apropiación de cuenta;
- Pérdida de la capacidad crediticia, pérdida del derecho de movilidad o empleo;
- Pérdida de activos personales, pérdida financiera, negación de beneficios;
- Daño a la reputación, vergüenza, humillación, discriminación, inconveniencia; e
- Injusticia, amenazas, victimización, chantaje o daño físico.

Para Scotiabank:

- Responsabilidad legal por pérdidas o litigios de alto costo;
- Costos de remediación, carga administrativa, multas y sanciones;
- Daño a los activos del Banco, incluyendo la marca y la reputación;
- Interrupción al propósito y misión del negocio;
- Deterioro de la capacidad de prestar servicios y cumplir con los objetivos de negocios;
- Pérdida de propiedad intelectual; y
- Pérdida de la confianza pública.

1.1 Alcance

Los Estándares son aplicables a todos los empleados de Banca Canadiense, Banca Internacional y de Gestión Patrimonial Global[1] (empleados de Banca Personal, Pequeñas Empresas y Gestión Patrimonial, incluyendo Sucursales, Centros de Contacto, Operaciones y Cobranzas) que tienen acceso a la información confidencial de los clientes, incluyendo a los empleados de las subsidiarias de propiedad o control total.

Cuando se requiera, el Banco cumplirá con la legislación local específica, regulaciones del sector o regulaciones internas que impongan obligaciones mayores o adicionales a los estándares en este documento.
En situaciones cuando recién se ha establecido el control de una subsidiaria y podría haber inicialmente una falta de conformidad con los estándares descritos en este documento, la Línea de Negocio evaluará las deficiencias y elaborará planes de acción para asegurar su rectificación oportuna.

Los terceros que procesan o trabajan con Información de Identificación Personal en nombre del Banco, deben cumplir como mínimo, con los estándares contenidos en este documento.[2]

Los Estándares se aplican a la información sobre todos los clientes y empleados, independientemente del tipo de productos o servicios que recibe el cliente o empleado.

[1] Incluye a los empleados con cualquier estado de empleo: tiempo completo, tiempo parcial, temporales o casuales (p. ej., pasantes, empleados del programa de formación y empleo (co-op)) y contratistas, cuando corresponda.

[2] Los controles de privacidad, confidencialidad y de seguridad de la información de terceros deben ser proporcionales o mejores que las propias política, procedimientos y controles del Banco. Para obtener más información, consultar el Manual de Gestión de Riesgos con Terceros.

1.2 Definición de Información de Identificación Personal

La Información de Identificación Personal (PII) se refiere a cualquier tipo de información que permite inferir de manera directa o indirecta la identidad de cualquier cliente o empleado, incluyendo cualquier información que esté "vinculada" o sea "vinculable" a dicha persona. La "información vinculada" es información que se puede relacionar con otra información de una persona. Por ejemplo, si en dos bases de datos diferentes cada una contiene un número de seguro social, entonces alguien que tiene acceso a ambas bases de datos podría enlazar la información e identificar personas más fácilmente.

La PII se clasifica dependiendo de su nivel de sensibilidad. Para obtener información sobre las clasificaciones de PII, consultar la Lista de control de elementos de datos de privacidad.

Para fines de este documento, todos los Estándares son aplicables a cualquier tipo de PII, sin importar su clasificación.

1.3 Uso de palabras clave para indicar el requisito

- Debe: Esta palabra o los términos "se requiere" o "deberá", significa que la definición es un requisito indispensable de la especificación.

- No debe: Esta frase o el término "prohibido" o la frase "no deberá" significa que la definición es una prohibición absoluta de la especificación.

- Debería: Esta palabra, o el adjetivo "recomendado", significa que podrían existir razones válidas en circunstancias particulares (p. ej., técnicas, regulatorias, legales u otra razón de mayor importancia) para descartar un estándar en particular, pero se deben entender todas las repercusiones que esto podría tener y evaluar cuidadosamente antes de decidirse por un curso de acción diferente.

- No debería: Esta frase, o la frase "no recomendado" indica que puede haber razones válidas en circunstancias específicas para que el comportamiento específico sea aceptable, pero antes de adoptar cualquier comportamiento con esta descripción, deberían comprenderse todas las repercusiones y sopesarse cuidadosamente el caso.

1.4 Revisión periódica

Los Estándares descritos en este documento serán revisados con regularidad y modificados cuando sea necesario en función de cualquier cambio relevante en las regulaciones, el ambiente de negocios, las nuevas tecnologías, el perfil de riesgo del Banco o en otros casos los cuales se determine que se requiera.

Las unidades de Riesgo Operacional dentro de la primera línea de defensa llevan a cabo las revisiones y los cambios a estos Estándares, con la asesoría y recomendaciones de la Oficina Institucional de Privacidad (EPO), Control y Seguridad de la Información (IS&C), Recursos Humanos, Riesgo Operacional Global y la Oficina del Programa del Código de Conducta.

1.5 Incidentes y violaciones a la privacidad

En caso de un presunto incidente de privacidad o confirmación de este, dicho incidente o violación deberá ser escalado a la gerencia inmediatamente por medio de la cadena de comunicación descrita en el Procedimiento de Gestión de Incidentes y Violaciones de la Privacidad de Scotiabank.

1.6 Políticas y procedimientos relacionados

Los Estándares descritos en este documento deberán basarse y se deben leer con las políticas y los procedimientos siguientes:

- Marco de Gestión del Riesgo de Privacidad de Scotiabank
- Manual de Privacidad
- Política de Privacidad del Empleado
- Código de Conducta de Scotiabank
- Código de Conducta para el uso de Internet y del Correo Electrónico - Parte del Código de Conducta de, Principio 4
- Procedimiento de Gestión de Incidentes y Violaciones de la Privacidad de Scotiabank
- Estándar de Clasificación de Seguridad de la Información y los Sistemas
- Política de Seguridad de la Información de Scotiabank
- Política de Opciones de Trabajo Flexible - AskHR – Política de Opciones de Trabajo Flexible (Canadá)
- Marco de Gobierno de Seguridad de la Información de Scotiabank

1.7 Pautas de S&C y GTS

Es necesario que revise el siguiente material a través de los enlaces que se proporcionan a continuación:

- Trabajar desde casa – Guía de mejores prácticas, que incluye una lista de "lo que se debe y no se debe hacer" mientras se trabaja desde casa.
- Hoja de consejos de contraseñas para IS&C –consejos sobre cómo generar una contraseña segura.
- Consejos de Concientización sobre la Ciberseguridad para phishing, ciberhigiene, contraseñas y viajes.

Las pautas de seguridad para computadoras portátiles dan consejos sobre cómo cuidar las computadoras portátiles, teléfonos inteligentes y tabletas.

Protege tus dispositivos, que proporciona consejos independientes sobre la protección de tu red doméstica, WiFi, seguridad de los dispositivos Bluetooth y más.

Directiva de CISO sobre Teletrabajo en Scotiabank cuando se invoca el BCP define los requerimientos para las computadoras del Banco y las computadoras de casa de los empleados que se utilizan para el teletrabajo cuando se ponen en marcha los Planes de Continuidad del Negocio (BCP).

Para cualquier otra política, procedimiento y guía, consultar la Oficina Institucional de Privacidad (EPO). Para cualquier otra política, directiva, estándares y procesos de información relacionada, consultar el Portal de Seguridad y Control de la Información.

2. Estándares

Es responsabilidad de todos los empleados estar familiarizados con estos Estándares, las demás políticas y pautas, otras pautas relacionadas que se aplican directamente a sus propias unidades de negocio o funciones de apoyo clave, y reportar cualquier caso real o cualquier sospecha de posible violación de estas pautas.

2.1 Protección de información en formato físico

Los empleados deben proteger toda la PII en su posesión o custodia. A continuación, se destacan los requerimientos estándar mínimos para garantizar la seguridad de los documentos físicos que contengan PII en las estaciones de trabajo (p. ej., cubículos en oficinas, escritorios, salas de conferencia o reuniones, sala de impresión o en la oficina en casa):

Tema	Estándares
Limpieza del escritorio y manejo de papel	• Para evitar un manejo indebido o pérdida de la PII, se deberá evitar imprimir o escribir dicha información o que estas actividades sean mínimas. • Para evitar el acceso no autorizado a la PII: o No se deberán dejar expedientes ni documentos que contengan PII en los escritorios mientras no está alguien ahí: ▪ Si los expedientes o documentos no están siendo utilizados o si la estación de trabajo va a estar desocupada durante un largo periodo (p. ej., durante el almuerzo, reuniones, etc.), se deberá guardar dicha documentación en los cajones o archivos. ▪ Al término de la jornada laboral, se deberán guardar los expedientes y documentos en cajones y archivos protegidos. o Cuando se trabaja en salas de reuniones, las pizarras que contienen PII, deberán borrarse y toda la información impresa deberá ser retirada de la sala al final de la reunión. o Los documentos que contienen PII no deberán ser eliminados utilizando contenedores no seguros (p. ej., basura o recipientes de reciclaje abiertos); los documentos que ya no se necesiten se deberán triturar o desechar utilizando contenedores oficiales de eliminación o trituración cerrados.
Impresión, escaneo y fax seguros	• El acceso a impresora, fax, copiadora o escáner se deberá dar basado en una necesidad para el negocio. En todos los demás casos, el acceso a impresoras y dispositivos multifuncionales deberá estar inhabilitado. • Debido a que las impresoras personales no están equipadas con las mismas funciones de seguridad con las que cuentan los dispositivos multifuncionales más sofisticados, su uso será permitido únicamente de acuerdo con las necesidades del negocio y en casos excepcionales. • Para evitar dejar documentos desatendidos que tengan PII en dispositivos como impresoras compartidas/fax/copiadoras/escáneres/dispositivos multifuncionales, se deberá implementar la autenticación del usuario (p. ej., autenticación por NIP o tarjeta de acceso). • Para evitar el envío de PII a personas no deseadas, los documentos escaneados deberán ser enviados directamente a la dirección de correo electrónico del usuario de Scotiabank y no a una carpeta compartida. Queda prohibida la transmisión directa del escáner/dispositivo multifuncional a direcciones externas de correo electrónico, así como la transferencia de archivos a destinos externos. • Debido a que la confidencialidad no puede garantizarse, el uso de fax será la excepción y no la norma. La PII solo podrá ser transmitida vía fax cuando el tiempo sea un factor crítico y los demás otros medios (correo interno, correo electrónico o sistema postal) no satisfagan las necesidades del negocio. o Antes de enviar un documento que contenga PII vía fax, se deberán tener en consideración los siguientes puntos: ▪ ¿Existe una necesidad de recepción inmediata de la información? ▪ ¿Cuál es el impacto si la información es enviada a la persona equivocada por error (p. ej., marcar a un número de fax erróneo)? o Para cada transmisión vía fax, la carátula de fax de Scotiabank deberá

	incluir la Notificación de Confidencialidad estándar (consultar el Anexo A). ○ Al enviar un fax, se deberá contactar al destinatario por anticipado (especialmente en el caso de transmisiones por primera vez o para números no usados frecuentemente) para alertarlo sobre el próximo fax y para verificar la recepción completa de la transmisión. ○ Para garantizar la protección de los faxes recibidos fuera del horario laboral, las máquinas de fax deben estar programadas para no imprimir fuera del horario laboral utilizando la función "Auto Receive to Memory" (recepción automática en la memoria). ○ Si se envía un fax erróneamente al destinatario equivocado, los empleados deberán: ▪ Identificar y ponerse en contacto con el destinatario no deseado y enviar a un mensajero que recupere la documentación, o como alternativa, pedir a dicho destinatario que destruya el fax no deseado. ▪ Escalar el error a la gerencia y consultar los Procedimientos de Gestión de Incidentes y Violaciones de la Privacidad de Scotiabank para más detalles. • La PII deberá ocultarse, de ser posible, antes de cada transmisión (p. ej., ocultando la PII que no sea relevante/aplicable al enviar el fax o cuando se realice un escaneado; o seleccionando solamente las páginas específicas sin PII al momento de imprimir). • Todos los documentos no vigilados que se queden en la impresora/fax/dispositivos multifuncionales deberán ser triturados o colocados en contenedores oficiales de eliminación/trituración cerrados.
Imprimir en casa	**Imprimir en casa:** • Imprimir en casa - Queda prohibido imprimir desde casa y no se permite imprimir documentos del Banco desde ningún dispositivo al trabajar desde casa. • Esto incluye imprimir desde, estaciones de trabajo, computadoras portátiles mini, dispositivos móviles, y desde aplicaciones y servicios prestados desde Citrix Access Gateway. Queda prohibido conectar una impresora personal de forma inalámbrica o por medio de una conexión física a dichos dispositivos. **Opciones para tomar en consideración:** • Utiliza un monitor en casa para ver la información en una pantalla separada. • Si tienes un monitor especializado en tu lugar de trabajo y necesitas acceso a él, completa el formulario "Take Custody of IT or Office Assets - Home or Offsite" (custodia de activos de TI o de oficina – en casa o fuera de la oficina) en Scotia Service Now con respecto a todos los activos retirados de los espacios de trabajo. **Proceso de excepción:** • Llena la "Solicitud de Excepción por Prevención de Pérdida de Datos (DLP)" con la información de la marca, modelo, número de serie/UID de la impresora, nombre del host, modelo de la computadora portátil/computadora de escritorio en las

	"notas de trabajo" de la solicitud y marca la solicitud como "USB Read". Podrás obtener todo esto en la herramienta de información del Sistema BNS en tu estación de trabajo. • La solicitud deberá ser aprobada por tu gerente, el vicepresidente sénior del área de tu línea de negocio, además de que será revisada también por la función 1B de tu área. • Una vez aprobada, tu servicio de TI se pondrá en contacto contigo para habilitar la funcionalidad de impresión, que solo estará activa durante un plazo de 3 meses. • Además, tendrás que asegurarte del manejo adecuado de la información personal y confidencial, incluyendo la trituración y eliminación segura de la información impresa en casa. • En caso de preguntas relacionadas con la impresión en casa, ponte en contacto con it.servicedesk@scotiabank.com

2.2 Protección de información en formato electrónico

Los empleados deben asegurarse de tomar las medidas de seguridad adecuadas para proteger los dispositivos electrónicos portátiles que sean propiedad del Banco: computadoras (personales y de escritorio) y dispositivos electrónicos móviles (teléfonos celulares, tabletas y almacenamiento extraíble). Los siguientes son los requisitos mínimos a los cuales deberán apegarse todos los empleados:

Tema	Estándares
Almacenamiento de datos y transmisión electrónica segura	• Para evitar una posible filtración y uso indebido de PII, el almacenamiento de esta información en formatos no estructurados (p. ej., documentos en MS Word, hojas de cálculo, bases de datos, PDF, etc.) debe evitarse a menos que exista una razón de negocios válida. En dichos casos, se aplicarán los siguientes criterios: o La PII deberá ocultarse o bloquearse en los documentos almacenados en plataformas o repositorios con imágenes si la PII no es relevante o necesaria para apoyar la tarea de negocios. o La PII no deberá ser guardada en campos de ingreso de datos de texto libre (p. ej., secciones de comentarios o notas) porque estos campos no pueden ser ocultados ni protegidos. • La PII solo podrá ser transmitida por medio de correo electrónico si recibir/enviar la información es esencial para las necesidades del negocio. Para asegurar la protección de la información mientras se utiliza el correo electrónico como canal de venta, se deberán seguir los siguientes estándares: o La transmisión externa de PII hacia o desde los clientes deberá realizarse utilizando el sistema de correo electrónico seguro de Scotiabank. Para orientación sobre cómo enviar y recibir correos electrónicos seguros, se debe consultar la Guía del Empleado sobre el Correo Electrónico Seguro de Scotiabank (instrucciones para clientes sobre cómo recibir o responder correos electrónicos seguros); y o Si se envía un correo electrónico por error a un destinatario equivocado, los empleados deberán: a) Utilizar la opción "recuperar" para obtener y borrar el correo electrónico del buzón del destinatario equivocado. Si esta opción falla (después de

Tema	Estándares
	usar esta opción llegará un correo electrónico de confirmación detallando si la recuperación tuvo éxito o no), entonces: i) Identificar y contactar al destinatario equivocado y pedirle que borre permanentemente el correo electrónico no deseado. ii) Escalar el error a la gerencia, consultando los Procedimientos de Gestión de Incidentes y Violaciones de la Privacidad de Scotiabank para obtener detalles.
Computadoras de escritorio, portátiles y dispositivos electrónicos móviles	• Con el fin de evitar que personas no autorizadas vean, accedan o utilicen indebidamente PII por medio de computadoras de escritorio, portátiles y dispositivos electrónicos móviles: o Deberá evitarse el uso de computadoras portátiles o dispositivos electrónicos móviles en lugares públicos concurridos (p. ej., cafeterías, aeropuertos, etc.). Como mínimo, deberán utilizarse pantallas de privacidad si existe una necesidad de negocios para trabajar en lugares públicos concurridos. o Las computadoras de escritorio y las tabletas con acceso a PII ubicadas en áreas públicas dentro de las oficinas del Banco deben contar con una pantalla de privacidad. o Las computadoras portátiles deben protegerse por medio un cable de seguridad durante el horario laboral. Dado que los cables de seguridad no son convenientes fuera del horario laboral, las computadoras portátiles deberán guardarse en un cajón o gabinete seguro al final del día. ▪ Si un cable de seguridad no está disponible o su uso no es factible (p. ej., escritorios sin ganchos de seguridad), las computadoras portátiles deberán guardarse durante ausencias prolongadas (p. ej., pausas para comer, reuniones, etc.). Los cables de seguridad y las pantallas seguras se podrán obtener en IT&S Store. o Cuando no se utilicen, los dispositivos electrónicos móviles deberán guardarse en cajones o gabinetes seguros. o Las computadoras (de escritorio y portátiles) siempre deberán mantenerse fuera de sesión cuando los empleados no estén en sus escritorios y al final de cada jornada laboral. • Para evitar software malicioso (malware) o virus, solo se permitirá la instalación de software autorizado y registrado en los dispositivos propiedad del Banco.
Herramientas de colaboración y pautas para el uso de Zoom	• Con el fin de apoyar tus necesidades de colaboración y comunicación en línea, favor de utilizar las herramientas aprobadas por el Banco: **MS Teams** y/o **Skype**. Las pautas se aplican a todas las jurisdicciones, excepto donde dichas herramientas no hayan sido aprobadas por los organismos reguladores locales: México, Perú, Brasil y Uruguay. • Cuando utilices aplicaciones de video aprobadas por el Banco: o *Obtén el consentimiento, ejerce una retención adecuada, restringe el intercambio de PII, aplica un trasfondo de pantalla (probablemente cubierto en la sección general de conferencia por video), y ten cuidado al compartir la pantalla.* o *Zoom no es un software aprobado por Scotiabank y supone un riesgo alto de seguridad y privacidad para el Banco.*

Tema	Estándares
	○ **Queda prohibido el uso de Zoom** **Si te piden que participes en una reunión por Zoom para realizar negocios del Banco, por favor sigue este proceso de excepción:** • No te unas a la reunión convocada por el tercero externo haciendo clic en el enlace de conferencia. • Llama usando el número de conferencia que aparece en la invitación de la reunión utilizando tu teléfono móvil o Skype. • De manera alternativa, ofrece ser el anfitrión de una llamada por **MS Teams y/o Skype** para comunicarte con los participantes de la reunión. • Pide al organizador de la reunión que comparta los archivos vía correo electrónico antes de la reunión. No obstante, si requieres un acceso total a Zoom, por ejemplo, para participar en llamadas de reunión importantes que sean convocadas por los clientes u organizaciones externas por medio de Zoom, por favor solicita una excepción vía ServiceNow. **Consulta:** Herramientas de colaboración aprobadas por el Banco y pautas de Zoom Instrucciones sobre cómo solicitar la funcionalidad de grabación Memorando de privacidad de Microsoft Teams Tecnología: Trabajar desde casa: Mejores prácticas
Medios de almacenamiento extraíbles	Los medios de almacenamiento extraíbles son cualquier tipo de dispositivo de almacenamiento que puede ser extraído de una computadora mientras el sistema está en operación. **Solicitudes de excepción:** Las personas que puedan demostrar una necesidad de negocios podrían solicitar la funcionalidad de autocifrado, que podrá ser modificada por medio de una excepción que sea aprobada. Favor de consultar el documento de solicitud de excepción, que puede encontrarse en el siguiente enlace; Solicitud de excepción Algunos ejemplos son: memorias extraíbles portátiles USB (también conocidas como unidades USB, dispositivos US o memorias USB), tarjetas de memoria digitales seguras o tarjetas SD, reproductores portátiles MP3 o reproductores de música MPEG tales como iPods, teléfonos celulares y teléfonos inteligentes, cámaras digitales que admiten el almacenamiento de datos u otro medio de almacenamiento de datos extraíble o no extraíble. Los siguientes son los requisitos y pautas mínimas de seguridad para el uso de medios de almacenamiento extraíbles: • El uso de medios de almacenamiento extraíbles deberá establecerse con base en las necesidades del negocio y deberá ser autorizado por la gerencia. En todos los demás casos, los puertos de las tarjetas USB y de memoria deberán ser inhabilitados en las computadoras de escritorio, portátiles y en los dispositivos

Tema	Estándares
	electrónicos móviles. • Únicamente podrán usarse los medios de almacenamiento extraíbles protegidos y cifrados que proporcione el Banco. • Si los medios de almacenamiento extraíbles se utilizan para transferir PII, las contraseñas deberán ser comunicadas al destinatario por medio de canales de comunicación alternativos (p. ej., otro USB cifrado vía paquetería o contraseña comunicada vía telefónica). • Para evitar software malicioso (malware) o virus, cualquier medio extraíble recibido de un tercero será escaneado en búsqueda de malware antes de ser usado (consulta con tu grupo de apoyo de TI para conocer las opciones disponibles). • Para evitar robo o pérdida, los medios extraíbles no deben dejarse desatendidos. Cuando no estén en uso, deberán guardarse en un lugar seguro (p. ej., cajón, gabinete de archivos, caja fuerte). • Todos los presuntos incidentes tales como dispositivos perdidos, presunto acceso no autorizado a algún dispositivo, deberán ser reportados inmediatamente a la gerencia, haciendo referencia a los Procedimientos de Gestión de Incidentes y Violaciones de la Privacidad de Scotiabank. Para obtener más información, consultar la Directiva CISO: Seguridad de Medios de Almacenamiento Extraíbles de IS&C.

Control de acceso lógico	Con el fin de asegurar la responsabilidad de las acciones de una persona y para asegurar que solo los usuarios autorizados a utilizar un sistema del Banco lo hagan, se asignará una ID de usuario y contraseña únicas a todos los empleados que accedan a los sistemas e información del Banco (podrían asignarse múltiples ID y contraseñas únicas si se le otorga al empleado acceso a múltiples sistemas y aplicaciones). La protección de acceso lógico es común en todas las plataformas, por los tanto, estos Estándares tienen por objeto aplicarse en todos los casos: • Para minimizar el riesgo del acceso no autorizado a los sistemas y aplicaciones del Banco: o Las contraseñas no deberán ser escritas en papel o almacenadas electrónicamente. o Los ID de usuarios y contraseñas nunca se deberán compartir con supervisores, colegas, familia ni con nadie. o Queda estrictamente prohibido acceder a los sistemas, aplicaciones e información utilizando el ID o contraseña de otro empleado. Las contraseñas deberán cambiarse al menos cada 180 días y siempre que exista algún indicio de alguna posible vulnerabilidad del sistema o contraseña. Favor de consultar los requisitos de las contraseñas especificados en el Estándar de Autenticación de Usuarios. Si se sospecha que existe o se identifica cierta vulnerabilidad, se deberá informar inmediatamente a Control y Seguridad de la Información: Correo electrónico: Cyber.Security@scotiabank.com Línea de asistencia de ciberseguridad: 1-833-970-1239 (número gratuito global)

	• Para minimizar el riesgo de acceso no autorizado o uso indebido de la información almacenada en las herramientas EUC[3], se deberán implementar los controles de acceso lógico (p. ej., restringir el acceso a una carpeta específica o documentos por función de trabajo, acceso solo para lectura, restringir la impresión, etc.) y ser monitoreados periódicamente.
Controles de acceso a redes remotas	El acceso remoto a las redes de Scotiabank utilizando las computadoras portátiles asignadas y dispositivos electrónicos móviles solo será permitido de conformidad con el Estándar de Seguridad de Redes (sección de acceso remoto a las redes de Scotiabank) exclusivamente para hacer negocios en nombre del Banco. Es importante acatar todos los requisitos de seguridad que se describen a continuación: • Con el fin de minimizar la exposición de PII a partes no autorizadas, el acceso remoto a la red del Banco solo será otorgado de acuerdo con las necesidades del negocio y será autorizado por la gerencia según corresponda. • Solo se utilizará la tecnología de Red Privada Virtual (VPN) aprobada por el Banco. • Solo se permitirá el acceso autorizado a los sistemas y proporcional a los privilegios regulares del empleado. • Queda prohibido inhabilitar, cambiar o alterar la configuración del software de acceso remoto en los dispositivos propiedad del Banco. • Para evitar que los hackers accedan a la información contenida en las computadoras portátiles y dispositivos electrónicos, queda prohibido conectarse a internet usando una red Wi-Fi no segura (p. ej., Wi-Fi gratuito en restaurantes, cafeterías y aeropuertos). Todas las conexiones inalámbricas a internet deben realizarse utilizando un cifrado reforzado (p. ej., WPA2).
Acceso a sitios web externos con capacidades de transmisión de información	• El acceso directo a los servicios de correo web (por ejemplo, Gmail, Yahoo Mail, Hotmail) se bloquea en todas las computadoras portátiles y de escritorio del Banco. • Otros dispositivos corporativos como teléfonos y tabletas no se verán afectados por el cambio; podrás seguir utilizando las aplicaciones de correo web en ellos. • No se harán excepciones. Con el fin de proteger la PII se aplicarán los siguientes estándares mínimos: • El acceso a los sitios web externos se basará en las necesidades del negocio y será autorizado por la gerencia. En los demás casos, quedará restringido. • Para aquellas funciones que requieren acceso a sitios web externos: o El uso de un proveedor de servicios externos (p. ej., una plataforma digital de servicio a clientes que unifique los mensajes de texto, redes sociales y chat por medio de aplicaciones) se tomará en consideración. o Los sitios de redes sociales y las plataformas de mensajería instantánea nunca deberán ser utilizados para reenviar o recibir PII. o Se prohíbe el acceso a aplicaciones o plataformas de almacenamiento de datos personales en la nube. Con respecto a los servicios de nube informática autorizados por el Banco, consultar la Directiva CISO sobre subcontratación en la nube. **Nota:** El uso que hagan los empleados de la tecnología de información y los servicios de Scotiabank puede ser vigilado en cualquier momento para identificar actividades inusuales, inadecuadas o sospechosas que puedan indicar un incumplimiento del

	Código de Conducta de Scotiabank. Esto incluye el monitoreo de correos electrónicos u otras comunicaciones (p. ej., mensajes instantáneos, publicaciones, etc.) y el contenido de tu computadora de escritorio, portátil o dispositivos electrónicos móviles.
Dispositivos electrónicos personales	Los dispositivos electrónicos personales se refieren (p. ej., no asignados por el Banco) a los teléfonos celulares, teléfonos inteligentes, computadoras portátiles, tabletas, iPods o reproductores de MP3, cámaras, dispositivos de grabación portátiles, relojes inteligentes u otros dispositivos personales con la capacidad de grabar o almacenar imágenes, video o audio. • Debido a que los dispositivos electrónicos personales no están equipados con la misma seguridad que los dispositivos propiedad del Banco, el almacenamiento o transmisión de PII en dispositivos personales queda prohibido sin importar la razón. • En un entorno laboral con acceso excesivo a PII o información confidencial, cada oficina ejecutiva podría implementar los siguientes controles, según sea necesario: o Los dispositivos electrónicos personales y pertenencias personales (bolsos, mochilas, bolsas de computadoras portátiles, etc.) deberán guardarse en cajones o gabinetes en todo momento. o El uso de dispositivos personales está restringido a áreas accesibles sin tarjetas de acceso (p. ej., espacios comunes, cafeterías o vestíbulos de entrada del edificio) o en espacios designados (p. ej., salas de reuniones, cabinas telefónicas, etc.). o La instalación o el uso de cámaras web personales o tecnología similar están prohibidos en cualquier área, excepto si se cuenta con la aprobación de la gerencia y la Unidad de Seguridad e Investigación.
Eliminación segura de dispositivos electrónicos	• Para la destrucción segura de los dispositivos electrónicos (computadoras portátiles, dispositivos electrónicos móviles y medios de almacenamiento extraíble), consultar la Eliminación segura de equipos y medios de almacenamiento en el Estándar de Protección de Datos o previa solicitud enviando un correo electrónico a asksecurity@scotiabank.com.

[3] Las aplicaciones utilizadas por el usuario final (EUC) se refieren a los sistemas que permiten a los no programadores (p. ej., el usuario final en lugar del departamento de TI) crear aplicaciones de trabajo. Las hojas de cálculo y bases de datos son los ejemplos más comunes.

2.3 Controles de trabajo remoto

Los empleados que trabajan de forma remota (p. ej., realizando negocios fuera del Banco o desde casa, hoteles, conferencias, otras oficinas del Banco, etc.) deberán ejercer un cuidado adicional para proteger la PII que tengan en su posesión o que esté bajo su custodia. Para proteger la información de personas no autorizadas, incluyendo familiares y amigos, se deberán seguir los siguientes requisitos:

Tema	Estándares

Protección de información en formato físico y electrónico	• Al trabajar fuera de la oficina, solo se deberá llevar la más mínima cantidad de información requerida. Salvo que la gerencia lo autorice, solo deberán llevarse copias y no documentos originales.
	• Al viajar, los documentos y dispositivos electrónicos portátiles siempre deberán estar a la mano. Las computadoras portátiles deberán llevarse como equipaje de mano y no como equipaje documentado.
	• Para evitar el robo o pérdida de documentos y dispositivos electrónicos portátiles que contengan PII:
	  ○ Los documentos y dispositivos electrónicos portátiles no deberán dejarse desatendidos dentro de autos ni otros medios de transporte, habitaciones de hotel, salas de conferencia, salas de reuniones, escritorios, impresoras o fotocopiadoras.
	  ○ Cuando no se utilicen o cuando se dejen desatendidos por un largo periodo (p. ej., durante comidas, actividades fuera del sitio, etc.), toda la documentación y dispositivos electrónicos portátiles deberán guardarse en un cajón o gabinete seguro.
	  ▪ En caso de dejarse en la habitación del hotel o en casa, los documentos y los dispositivos electrónicos portátiles deberán dejarse en una caja fuerte o en un cajón o gabinete con llave.
	• Para proteger la PII al trabajar desde casa cuando los proveedores de servicios (p. ej., internet, telefonía, mantenimiento del hogar, etc.) o visitantes (amigos y familiares) estén temporalmente ahí:
	  ○ El lugar de trabajo designado en caso debe estar protegido si el espacio quedará desatendido durante la visita.
	  ○ Si el espacio de trabajo en casa se encuentra en un área abierta (p. ej., sin puertas), todos los documentos y dispositivos electrónicos portátiles que contengan PII, deberán guardarse y deberá cerrarse la sesión en la computadora.
	  ○ No se deberá perder de vista a los proveedores de servicios o visitantes.
	  ○ Por razones de privacidad y seguridad, los empleados no deberán agendar reuniones de trabajo en su oficina en casa. Si existe la necesidad de tener una interacción personal, los empleados deberán volver temporalmente al espacio de trabajo tradicional (p. ej., las oficinas del Banco).
	• Para prevenir el acceso no autorizado a PII en caso de pérdida, los teléfonos inteligentes y tabletas deben estar programadas para bloquearse después de cierto periodo de inactividad. Se deberá requerir una contraseña, NIP o patrón para desbloquear el dispositivo, con un número determinado de intentos.

Tema	Estándares
Acuerdo de trabajo permanente en sitios alternos	La gerencia de la Línea de Negocio deberá llevar a cabo actividades de diligencia debida adicional al aprobar a los empleados con acceso a PII que trabajan regularmente desde un sitio alterno. Estos son los requisitos mínimos que deben ser implementados además de todos los requisitos indicados en la política Opciones de Trabajo Flexible ("FWO") (para las Unidades de Negocio locales) y las políticas locales de trabajo flexible en las Unidades de Negocio internacionales: • Con el fin de evaluar de mejor manera la idoneidad de un candidato y concientizarlo sobre las políticas y procedimiento de privacidad del Banco, los empleados que soliciten trabajar regularmente desde casa en un sitio alterno deberán: o Tener al menos 1 año de experiencia en su puesto actual. Además, los candidatos deberán tener una experiencia laboral mayor (p. ej., más de 3 años de experiencia general). o Haber completado de manera exitosa todos los cursos obligatorios relacionados del Banco (Código de Conducta, Privacidad, PLD/PFT, etc.). o No haber tenido ninguna conducta indebida en materia de privacidad en los últimos 12 meses. • Para proteger adecuadamente la PII, el sitio alterno u oficina en casa deberá ser un lugar cerrado dedicado a ese fin (p. ej., no deberá compartirse con nadie más) y con cerraduras en las puertas, ventanas y cajones o gabinetes, además de cumplir con la política FWO. o Además, los empleados deberán otorgar su consentimiento por escrito para recibir visitas programas y no programadas en sitio y en línea a cargo de la gerencia en el sitio alterno de trabajo para determinar si el sitio se apega a los estándares mínimos[4]. Con respecto a las unidades de negocio o jurisdicciones con sus propios estándares, se deberá dar un seguimiento a nivel local. • Todos los empleados que trabajan remotamente deben proporcionar una confirmación por escrito de que han leído y comprendido, y se apegan a estos estándares. • Los Scotiabankers deben seguir los estándares que aparecen a continuación cuando trabajen de forma remota o desde casa: • Tomar medidas razonables para instalar un espacio de trabajo en un área privada. • Utilizar solamente los dispositivos del Banco para las actividades de negocios, evitar el uso de dispositivos personales en cualquier circunstancia, incluyendo el envío de información de negocios a las cuentas de correo electrónico personales para imprimir documentos. • Mantener segura toda la información de propiedad exclusiva del Banco para prevenir el acceso no autorizado. • Prestar atención a los dispositivos que tienen asistentes virtuales inteligentes (p. ej., Google Home, Amazon Alexa, etc.), y procurar que no estén dentro del rango de escucha cuando tengan conversaciones de negocios. • Tomar las precauciones apropiadas para mantener la confidencialidad si vives con un cliente del Banco, alguien que trabaja en un banco de la competencia o un proveedor. • Para determinar si el acuerdo debe darse por terminado debido a

	circunstancias de incumplimiento de alguno de los requisitos o estándares mínimos, la gerencia deberá involucrar a Relaciones con los Empleados y seguir la Política de Conducta Indebida de los Empleados (Global).

[4] Excluyendo a los empleados móviles que trabajan visitando clientes en sitios alternos como parte de sus funciones laborales.

2.4 Controles de acceso físico

Las instalaciones de Scotiabank están debidamente protegidas para evitar el acceso no autorizado o involuntario, de acuerdo con el nivel de sensibilidad y riesgo. Cada área física del Banco se clasifica como "estrictamente segura", "segura", "protegida" o "común", con base en el valor de la información, materiales, equipo u otros recursos que se usan o almacenan dentro de esa área (para más detalles consultar los Estándares Comunes - Control de Acceso Físico de IS&C.

Estos son los requisitos mínimos de todas las áreas, a excepción de las comunes:

Tema	Estándares
Acceso a las áreas estrictamente seguras, seguras y protegidas	• Se prohíbe el acceso a las áreas estrictamente seguras, seguras y protegidas usando la tarjeta de acceso, código o llaves de acceso de otro empleado. • Las tarjetas y llaves de acceso no deben dejarse desatendidas. En caso de pérdida, deberá reportarse inmediatamente a la gerencia y al mostrador de seguridad de las instalaciones. • Para prevenir el acceso no autorizado, como mínimo, los visitantes (p. ej., personas que no sean del Banco o empleados de otros departamentos – el personal de limpieza regular y las personas que llenan las máquinas de comida y café con tarjetas de acceso autorizadas no se consideran visitantes) deben ser escoltados por un guardia de seguridad o por un miembro del personal en todo momento. Todos los visitantes deberán seguir el protocolo establecido para ingresar a las instalaciones. • Permitir el acceso a una persona no autorizada a un lugar (p. ej., empleados que abren una puerta y la mantienen abierta para otras personas) queda prohibido. Todos los empleados que ingresan a áreas distintas a las áreas comunes deberán utilizar su tarjeta de acceso válida.

3. Actividades de monitoreo

Cada empleado es responsable de la seguridad y protección de toda la información de identificación personal bajo su custodia. Además, la gerencia de la línea de negocios es responsable del diseño, documentación e implementación de las actividades de control de seguimiento a fin de asegurar que los empleados estén cumpliendo con los estándares mínimos descritos en este documento.

3.1 Monitoreo continuo

Tema	Estándares
Actividades de supervisión diarias	De conformidad con el nivel de exposición de PII, la gerencia debe establecer un proceso adecuado de monitoreo. Para Banca Canadiense y Gestión Patrimonial Global esto incluye, como mínimo, recorridos aleatorios durante el día e inspecciones al final del día. Otras jurisdicciones deberán establecer la frecuencia de monitoreo requerida. El propósito es garantizar que: • Los documentos y archivos que contienen PII no deben dejarse desatendidos en escritorios, impresoras o dispositivos multifuncionales. • Las computadoras de escritorio y computadoras portátiles se deben desconectar cuando los empleados no se encuentren en sus puestos de trabajo.

	• Todos los dispositivos portátiles, dispositivos de almacenamiento extraíbles, credenciales de acceso y llaves utilizadas para acceder a la PII se deben guardar de forma segura y nunca se deben dejar desatendidos cuando no se utilizan. • Los gabinetes de archivos que contengan documentos con PII deben mantenerse cerrados en todo momento cuando no se utilizan y cuando el puesto de trabajo se deja desatendido y bloqueado al final de cada día de trabajo. • Las pizarras que contienen PII se deben borrar y toda información impresa y electrónica (p. ej., las llaves USB asignadas por el Banco) debe ser retirada de las salas de reuniones al final de cada reunión. • Las tabletas con acceso a PII que se utilizan en áreas públicas tengan pantallas de privacidad. • Las computadoras portátiles están protegidas con un cable de seguridad o se encuentran guardadas en gavetas seguras cuando se dejan desatendidas por largos períodos de tiempo durante las horas de trabajo. • El uso de dispositivos personales debe apegarse al Código de Conducta de Scotiabank y podrían tener restricciones adicionales, según la unidad de negocio o requisitos jurisdiccionales. • Los empleados que ingresan a las áreas estrictamente seguras, seguras o protegidas utilizan credenciales de acceso válidas y deben mantener las puertas de las instalaciones cerradas para personas no autorizadas. • La información que ya no se requiere o que se deja desatendida en impresoras o dispositivos multifuncionales se coloca en contenedores de trituradoras oficiales o en contenedores de desechos confidenciales cerrados. • Las computadoras de escritorio se deben desconectar y las computadoras portátiles se guardan de forma segura al final de la jornada laboral. • Si se identificaron incidentes o violaciones de la privacidad durante las inspecciones, estos se deben atender de acuerdo con los Procedimientos de Gestión de Incidentes y Violación de Privacidad de Scotiabank.
Monitoreo Mejorado de Empleados	• El Programa mejorado de monitoreo a empleados se está implementando a nivel institucional con el fin de actuar como un control adicional de detección e identificar a los empleados que podrían acceder a información personal sin ningún motivo de negocios razonable. El objetivo es proteger, detectar e investigar incidentes de privacidad, interés, mala conducta y abuso del acceso. o Las unidades de negocio deben investigar y responder cualquier correo electrónico de alerta que reciban del equipo de Monitoreo Mejorado. Si existen posibles incidentes o violaciones de privacidad, los gerentes y supervisores deberán seguir las pautas relacionadas con la Política de Conducta Indebida del Empleado (Global) (consultar la sección 4).

3.2 Monitoreo del acceso lógico y físico

Tema	Estándares
Registros o reportes de acceso	Con el fin de garantizar que los controles de acceso lógico y físico funcionen de manera adecuada y el acceso se retire oportunamente, la gerencia de la Línea de Negocio deberá mantener y revisar los registros o reportes internos de acceso detallando todos los privilegios de acceso autorizado. Como mínimo, el registro o reporte debe incluir la siguiente información por usuario: • Lista de todos los privilegios de acceso otorgados a la persona. • Si la aprobación fue otorgada de manera excepcional. • Estado de acceso (p. ej., activo, inactivo, suspendido, etc.). • Tipo de acceso (permanente, temporal, de emergencia). Si es temporal, se debe registrar una fecha de finalización. • Estado laboral (por ejemplo, a tiempo completo, a tiempo parcial, por contrato, etc.). Los registros o reportes de acceso no deberán incluir contraseñas, claves de cifrado u otra información que exija secrecía.
Revisiones periódicas	Los registros y reportes de acceso lógico y físico deben revisarse y actualizarse periódicamente para validar que: • El acceso se retire oportunamente a los empleados que han sido transferidos[5] o despedidos; o se suspenda el acceso al personal con ausencia prolongada. • Para usuarios temporales, el acceso se elimine en la fecha de finalización registrada en la solicitud de acceso inicial. Si se autorizó una prórroga, la gerencia debe garantizar que se proporcionó un motivo válido. • Se elimine a los usuarios inactivos luego de un período de inactividad prolongado. Los usuarios que han estado inactivos por más de 3 meses deben ser notificados y evaluados para determinar si el acceso debe continuarse, suspenderse o eliminarse. Si la inactividad se debe a que el empleado tiene una ausencia prolongada, el acceso debe suspenderse. • Con respecto al acceso lógico, la revisión deberá llevarse a cabo de acuerdo con la frecuencia definida en los procedimientos de control de los sistemas de acceso lógico de la unidad, sin exceder un periodo de revisión semestral (o según lo especificado en los Estándares comunes para el control de acceso lógico de IS&C), comparando los registros o reportes internos de acceso lógico con las listas de Recursos Humanos (p. ej., reporte de Servicios de Información de Recursos Humanos (HRIS)). • Con respecto al acceso físico, la revisión deberá llevarse a cabo mensualmente (o según lo especificado en los Estándares Comunes de Control de Acceso Físico de IS&C), comparando los registros o reportes internos de acceso y los reportes de Recursos Humanos con los reportes elaborados por el Custodio del Área Física[6] que muestran quién tiene acceso al área.
Reporte de excepciones	Además de la revisión de registros o reportes internos, la Línea de Negocio deberá elaborar un proceso de reporte de excepciones para capturar y validar las siguientes excepciones: • Usuarios con un acceso prolongado que sea mayor a la duración máxima especificada en la solicitud inicial. • Usuarios con acceso fuera de los parámetros preestablecidos basados en funciones específicas de trabajo (es decir, acceso aprobado de forma excepcional). • Acceso solicitado y/o aprobado por personas que no figuran en la lista

	de solicitantes o aprobadores autorizados. • Solicitudes de acceso repetido para el mismo usuario de manera excepcional en los últimos 12 meses. Para todas las excepciones se deberá proporcionar una justificación detallada para ayudar a la gerencia a evaluar la validez de la excepción. Como mínimo, este reporte deberá ser elaborado y ejecutado semestralmente.
Supervisión de herramientas de informática de usuario final	Se deberá otorgar el acceso a las herramientas EUC según sea necesario, asignando diferentes privilegios para restringir el acceso por función. Además, la gerencia deberá crear y mantener un inventario de todas las herramientas EUC y ser almacenado en un servidor de archivos central. Deberá realizarse una revisión periódica (semestralmente como mínimo) para garantizar que el acceso a las herramientas EUC sea retirado cuando los empleados sean transferidos o despedidos. Consultar el Estándar sobre el Cómputo de Usuario Final para obtener más información con respecto a los controles que deben implementarse por la gerencia de la Línea de Negocio.

[5] Los empleados transferidos también incluyen los empleados que fueron transferidos a un equipo diferente dentro de la misma unidad o departamento y que podrían necesitar acceso a diferentes sistema o aplicaciones, o a diferentes instalaciones del Banco.

[6] El Custodio del Área Física es la unidad o persona responsable de autorizar la solicitud de privilegios de acceso al área y de asegurarse de que los controles adecuados de acceso físico estén operando.

4. Conducta indebida de los empleados

Es una condición para la continuidad del empleo que los empleados demuestren los valores de Scotiabank, apegarse a las políticas y procedimientos del Banco, y cumplir con las leyes y regulaciones aplicables. A fin de determinar las medidas apropiadas que debe adoptarse cuando se produce una excepción a cualquiera de los estándares, consultar la Política de Conducta Indebida de los Empleados (Global) de Scotiabank.

Este proceso se aplica a todos los empleados de Banca Canadiense, Banca Internacional y Gestión Patrimonial Global en todo el mundo, salvo cuando la legislación local disponga un proceso alternativo.

Anexo A: Aviso de Confidencialidad

Si bien cada unidad de negocio es responsable del diseño general de su portada de fax, se deberán colocar los siguientes Avisos de Confidencialidad en la parte inferior de cada portada de fax. Para las transmisiones de fax en Canadá, el uso de los avisos en inglés y francés es obligatorio. Para Banca Internacional, el uso de cualquier aviso que se sea diferente al idioma oficial del país es opcional.

English

THE BANK OF NOVA SCOTIA - NOTICE OF CONFIDENTIALITY

The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, re-transmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender immediately by telephone (collect if required). A courier will be sent to retrieve the documents or, alternatively, immediately destroy this transmission, including all attachments, without copying, distributing or disclosing same.

Français

BANQUE SCOTIA - AVIS DE CONFIDENTIALITÉ

L'information transmise est strictement réservée à la personne ou à l'organisme auquel elle est adressée et peut être de nature confidentielle. Toute lecture, retransmission, divulgation ou autre utilisation de cette information, ou toute action prise sur la foi de cette information, par des personnes ou organismes autres que son destinataire est interdite. Si vous avez reçu cette information par erreur, veuillez contacter son expéditeur immédiatement par téléphone (à frais virés si nécessaire). Un messager passera prendre le(s) document(s) ou, supprimez immédiatement cette information, y compris toutes pièces jointes, sans en avoir copié, divulgué ou diffusé le contenu.

Español

BANCO SCOTIABANK – AVISO DE CONFIDENCIALIDAD

La información transmitida está destinada únicamente a la persona o entidad a la que se dirige y puede contener información confidencial y/o privilegiada. Cualquier revisión, retransmisión, difusión u otro uso o toma de cualquier acción basada en esta información por personas o entidades distintas del destinatario previsto está prohibido. Si recibió esto por error, póngase en contacto con el remitente inmediatamente por teléfono (con cargo al Banco si es requerido). Un mensajero será enviado para recuperar los documentos o, alternativamente, destruya inmediatamente esta transmisión, incluyendo todos los anexos, sin copiarlos, distribuirlos o divulgarlos.

Colocación recomendada del Aviso de Confidencialidad