ANEXO CLÁUSULAS DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRATOS

1.0 Control de acceso lógico

Para garantizar el cumplimiento de los requisitos de Scotiabank sobre el control de la seguridad para el acceso, el Proveedor deberá:

(a) proteger la confidencialidad de todas las contraseñas o claves de acceso asignadas al Proveedor por Scotiabank;

(b) contar con una política de contraseñas en virtud de la cual su personal, incluidos los subcontratistas, que puedan tener acceso a los sistemas del Proveedor o de Scotiabank o a cualquier dato de Scotiabank cambien las contraseñas inmediatamente después de recibirlas y posteriormente las cambien cada noventa (90) días o con mayor frecuencia, y eviten contraseñas triviales o evidentes; y

(c) oportunamente retirar los privilegios de acceso lógico al personal del Proveedor, incluidos los subcontratistas (si el Proveedor está autorizado a utilizar dichos subcontratistas en el Acuerdo celebrado entre el Proveedor y Scotiabank) que, ya sea por transferencia interna o cese de la relación con el Proveedor, o de ser el caso, los subcontratistas correspondientes, dejan de estar involucrados en el procesamiento de la información y datos de Scotiabank.

2.0 Responsabilidades del personal

Para garantizar el cumplimiento de los requisitos de Scotiabank referentes a la responsabilidad de los empleados, el Proveedor deberá:

(a) certificar que todos los dispositivos utilizados por los empleados del Proveedor o sus subcontratistas que estén conectados al ambiente de procesamiento de Scotiabank cumplan y sigan cumpliendo los siguientes requisitos:
   i. deben aplicarse y estar al día los paquetes de actualizaciones (service pack) más recientes y todos los parches de seguridad aplicables a todos los sistemas operativos y software residentes en los dispositivos;
   ii. los dispositivos deben tener el software estándar de la industria contra programas maliciosos (malware) instalado, funcionando y actualizado con el último archivo de firma; y
   iii. el dispositivo debe tener instalado y activo un producto de seguridad tipo cortafuego (firewall) personal y estándar de la industria.

(b) certificar que sus empleados y subcontratistas reciban información profesional y capacitación de sensibilización sobre ciberseguridad al momento de la contratación y posteriormente de forma periódica.

3.0 Seguridad de los servidores

Para asegurar la integridad, confidencialidad y disponibilidad de todos los servidores utilizados para procesar la información y datos de Scotiabank, y para mitigar la amenaza, riesgo e impacto

del uso indebido y abuso externos o internos de las plataformas de servidores, el Proveedor deberá:

(a) proteger el acceso a todos los servidores, como mínimo, mediante una combinación de la identificación (ID) del usuario y la contraseña secreta;
(b) cambiar todas las contraseñas de los servidores que vienen de fábrica antes del comienzo del procesamiento y cambiarlas posteriormente cada noventa (90) días o más frecuentemente;
(c) asegurar que los servidores se encuentren ubicados en zonas físicamente seguras;
(d) reforzar la seguridad de todos los servidores utilizados para procesar, almacenar o transmitir datos e información de Scotiabank, debiendo dicho reforzamiento incluir, entre otros, la eliminación de todos los privilegios y servicios salvo aquellos que sean esenciales para la ejecución de las operaciones para las que están instalados dichos servidores;
(e) implementar herramientas de análisis de la seguridad de los servidores para informar periódicamente sobre el estado de cada servidor y verificar que todas las configuraciones, parámetros y opciones estén conformes con el estado de reforzamiento acordado para ese dispositivo y para detectar cambios no autorizados a partir de la línea base de la configuración aprobada del servidor;
(f) registrar toda la actividad de acceso del servidor y almacenar los datos de dicha actividad de una manera apropiada por un período mínimo de quince (15) meses; y
(g) revisar periódicamente (al menos una vez al año) todos los controles de seguridad del servidor definidos anteriormente para asegurarse de que todavía estén vigentes.

4.0 Desarrollo de Software

Para garantizar el cumplimiento de los requisitos de Scotiabank y de las mejores prácticas de la industria para los códigos seguros, el Proveedor deberá:

(a) Incorporar el análisis Estático y Dinámico de los códigos de seguridad en el ciclo de vida del desarrollo del software;

(b) Mitigar los problemas de seguridad identificados durante el análisis Estático y Dinámico de los códigos antes de pasarlos al entorno de producción.

5.0 Seguridad de los archivos de datos y bases de datos

Para asegurar la integridad, confidencialidad y seguridad en general de todas las bases de datos y archivos de datos utilizados para almacenar información y datos de Scotiabank, el Proveedor deberá:

(a) almacenar la información "Confidencial" de Scotiabank (por ejemplo, contraseñas, datos de los clientes, etc.) en un formato cifrado de conformidad con las mejores prácticas de la industria;
(b) ubicar todos los servidores de bases de datos, servidores de archivos y repositorios que contengan datos de Scotiabank en un área físicamente segura;
(c) restringir todo el acceso físico y lógico a las bases de datos, archivos de datos e información y datos almacenados en éstos, así como a cualquier sistema o componente de la red relacionado con el procesamiento de transacciones según un esquema basado solo en la “necesidad de conocer o usar” del negocio;

(d) proteger todos los accesos a las bases de datos y archivos de datos utilizando, como mínimo, una combinación de la identificación del usuario y la contraseña secreta;
(e) cambiar todas las contraseñas de las bases de datos que vienen de fábrica antes del comienzo del procesamiento y cambiarlas posteriormente cada noventa (90) días;
(f) registrar toda la actividad de acceso a las bases de datos y archivos de datos, y almacenar los datos de dicha actividad de una manera apropiada por un período mínimo de quince (15) meses;
(g) registrar toda la actividad de transacciones y almacenar los datos de dicha actividad de una manera apropiada durante al menos tres (3) años desde la fecha de cada transacción;
(h) manejar todas las copias de respaldo de todos los registros de las bases de datos y archivos de datos de conformidad con medidas estrictas de seguridad y controles de acceso, ejerciendo controles idénticos o similares a los empleados para las bases de datos y los archivos de datos principales;
(i) implementar herramientas de análisis de la seguridad de las bases de datos para revisar periódicamente las configuraciones de las bases de datos y garantizar el cumplimiento de las configuraciones de base esperadas;
(j) eliminar y destruir de una manera adecuada y segura todas las instancias de cualquier información o datos de Scotiabank y material impreso conexo para asegurar que las transacciones y demás datos no puedan ser recuperados por personas no autorizadas; y
(k) revisar en forma periódica (al menos una vez al año) todos los controles de seguridad de la base de datos definidos anteriormente para asegurar que continúan vigentes.

6.0 Seguridad de la red

Para mitigar la amenaza, riesgo e impacto de intrusiones, abuso o uso indebido del sistema o la red, el Proveedor deberá:

(a) instalar, configurar y activar un sistema integral de protección contra intrusiones (en la red y el host), de conformidad con las mejores prácticas de la industria, para que en forma continua evite, detecte e informe la ocurrencia de ataques no autorizados a la red y en contra de sus sistemas, incluidos, entre otros, intentos de penetración, ataques por denegación de servicio y sondeos excesivos;
(b) instalar cortafuegos (firewall) para redes basados en las mejores prácticas de la industria entre los servidores y las puertas de enlace (gateways) a la red pública de modo que excluyan los protocolos de comunicación que no sean necesarios para procesar el tráfico de Internet;
(c) registrar toda la actividad de los cortafuegos y puertas de enlace y almacenar los datos de dicha actividad de una manera apropiada por un período mínimo de dieciocho (18) meses;
(d) proteger los datos contra la divulgación no autorizada durante su tránsito a través de redes públicas a Scotiabank, o sus agentes autorizados, o sus clientes, para garantizar la seguridad de los datos que sean propiedad de Scotiabank o estén relacionados con Scotiabank; y
(e) aplicar las técnicas criptográficas, "Transport Layer Security" (TLS) versión 1.2 o 1.3 para la autenticación mutua de certificados (del cliente al servidor o de servidor a servidor), y una longitud mínima de clave de 128 bits o una norma equivalente basada en las mejores prácticas de la industria.

7.0 Protección contra programas maliciosos [Malware]

Para mitigar la amenaza, riesgo e impacto de los virus informáticos, gusanos, troyanos y otros tipos de software malicioso, colectivamente llamado "malware", el Proveedor deberá:

(a) instalar, configurar, activar y mantener actualizado un software antivirus y antiespías (anti-spyware) basado en las mejores prácticas de la industria, en todos los servidores, dispositivos, computadoras portátiles y estaciones de trabajo que procesen o almacenen las transacciones y cualquier otro dato de Scotiabank;

(b) configurar dicho software anti-malware para invocarlo automáticamente en el arranque y ejecutarlo interactivamente de forma continua, en todos los dispositivos donde esté instalado; e

(c) presentar reportes sobre incidentes relacionados con programas maliciosos (específicos de Scotiabank y que presentan la posibilidad de afectar de manera crítica sus sistemas) a Scotiabank dentro de un plazo no mayor a 24 horas, tras la confirmación del Proveedor de que el incidente es específico de Scotiabank y tiene la posibilidad de afectar de manera crítica sus sistemas.

8.0 Vulnerabilidades de la seguridad e instalación de parches de seguridad

Para mitigar la amenaza, riesgo e impacto de las vulnerabilidades de la seguridad en el sistema o red, el Proveedor deberá:

(a) desarrollar e implementar un proceso para investigar continuamente las fuentes fiables de advertencias sobre vulnerabilidades de la seguridad emergentes;

(b) identificar vulnerabilidades específicas que puedan impactar los ambientes operativos o plataformas utilizados por el Proveedor en nombre de Scotiabank;

(c) evaluar la criticidad de una vulnerabilidad en relación con las operaciones generales del Proveedor y Scotiabank, a fin de determinar la conveniencia de instalar el correspondiente parche de seguridad; y

(d) probar e instalar oportunamente los parches de seguridad.

9.0 Alerta y escalamiento de problemas y gestión de incidentes de seguridad

En el caso de pérdida, acceso no autorizado, o divulgación no autorizada de la Información Confidencial de Scotiabank, Información Personal de Scotiabank, u otros datos de Scotiabank (cada uno de ellos una “Violación de Seguridad de los Datos”), el proveedor inmediatamente y tan pronto como sea posible, después de determinar que se ha producido una Violación de la Seguridad de los Datos:

(a) notificar a Scotiabank las violaciones de seguridad de los datos por correo electrónico: cyber.security@scotiabank.com y por teléfono al 1-833-970-1239 (línea internacional gratuita) o 1-416-288-3568; y
(b) investigar la violación de seguridad de los datos y proporcionar a Scotiabank la información detallada sobre la violación de seguridad de los datos.

10.0 Control de cambios

Para garantizar el cumplimiento de los requisitos de Scotiabank y de las mejores prácticas de la industria para el control de cambios, el Proveedor deberá:

(a) desarrollar, probar y documentar cada cambio de conformidad con la gestión de cambios y las normas, procedimientos y procesos de control, preservando la integridad lógica continua de los datos, programas y rastros de auditoría.

11.0 Respaldo y recuperación

Para garantizar el cumplimiento de los requisitos de Scotiabank y de las mejores prácticas de la industria para el respaldo y la recuperación, el Proveedor deberá:

(a) implementar medidas de respaldo adecuadas, incluido el almacenamiento de los archivos de datos de respaldo en lugares seguros fuera del sitio de procesamiento, para permitir la recuperación eficiente del sistema;

(b) facilitar la reanudación de las aplicaciones críticas y actividades de negocios de una manera oportuna después de una emergencia o desastre; y

(c) mantener un plan de recuperación de desastres documentado para cada sistema crítico relacionado con Scotiabank y para las aplicaciones de negocios, y probarlo anualmente.