POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA TERCEROS

DAVIVIENDA

CONTENIDO

I. OBJETIVOS.

Establecer los lineamientos de Seguridad de la Información para la protección de la información del Banco, sus clientes y personas relacionadas cuando se implementan servicios o proyectos a través de terceros.

II. ALCANCE.

El presente documento aplica al Banco Davivienda, Filiales y a todos los proveedores que presten algún tipo de servicio al Banco. Al mencionar Banco se hace referencia al Banco y sus Filiales

III. DEFINICIONES.

IV. RESPONSABILIDADES DE LOS SUPERVISORES DE CONTRATO.

1. Aspectos legales.

Toda vinculación de terceros con el Banco debe estar formalmente determinada a través de un documento con alcance legal y este debe contar con el visto bueno del área jurídica del Banco.

2. Supervisor del contrato.

El supervisor del contrato es responsable de garantizar que se cumplan las políticas, normas y estándares de seguridad de la información. Cuando el servicio que prestará el tercero involucre intercambio periódico de información, el supervisor debe formalizarlo a través de los acuerdos (documentos legales) que el área jurídica del Banco ha diseñado en conjunto con el Departamento de Seguridad de la Información.

V. ESTRUCTURA Y ASPECTOS DE GOBIERNO.

1. Mejores prácticas.

El tercero deberá aplicar las mejores prácticas establecidas en los estándares nacionales e internacionales relacionadas con el objeto contractual y debe garantizar que sus Sistemas de Gestión (Calidad, Riesgo, Seguridad, etc.) se encuentren plenamente alineados e integrados a dichos estándares y mejores prácticas.

2. Propiedad de la información.

Toda la información entregada a los terceros es propiedad exclusiva de BANCO DAVIVIENDA S.A. En consecuencia, dicha información no podrá ser utilizada por el Tercero para fines diferentes al desarrollo del servicio especificados, ni compartida sin previa autorización por parte del BANCO DAVIVIENDA.

3. Confidencialidad.

El Tercero debe comprometerse a que sus directivos, funcionarios, asociados y, en general, todo el personal a su cargo o bajo su dirección, en ningún momento, de ninguna manera, directa o indirectamente, divulgarán o comunicarán a ninguna persona natural o jurídica información alguna relacionada con los negocios de la parte que ha suministrado la información, que haya sido suministrada por el Banco, incluyendo sin que esto implique limitación a: información comercial, tecnológica, científica, de propiedad intelectual, secretos comerciales, especificaciones técnicas, tecnología, información sobre el personal, datos financieros actuales y estimados, estadísticas, presupuestos, políticas, correspondencias, contratos y costos financieros, impuestos, historias del personal, procedimientos y/o información contable de la parte que suministro la información, y cualquier otra información perteneciente al Banco o relacionada con los negocios de éste, sus planes, su forma de conducirlos, procesos o cualquier otro dato de cualquier otra clase.

El Tercero debe devolver la información, todos los documentos, manuales, libros, correspondencia, publicaciones, útiles y demás bienes de propiedad de BANCO DAVIVIENDA relacionados con el objeto del servicio que este presta al Banco, a la terminación del contrato y/o cuando así lo solicite BANCO DAVIVIENDA.

4. Auditabilidad.

El Tercero permitirá al Banco llevar a cabo la realización de visitas de auditoria (s), con el objetivo de verificar el cumplimiento de controles y procedimientos propios del Tercero. El BANCO deberá comunicar de forma escrita (incluida e-mail) al Tercero la fecha y hora en que se llevará a cabo la (s) respectiva (s) auditoría (s) con una antelación mínima de veinticuatro (24) horas respecto de la fecha y hora exacta en las cuales se empezará cada auditoría en particular.

Cuando el Servicio prestado por el Tercero apoye procesos críticos del negocio, el Tercero deberá entregar al Banco previa la firma del contrato un informe escrito, emitido y firmado por un Auditor Certificado, el cual, debe contener el resultado del proceso de evaluación de los controles de Tecnología y Controles de procesos relacionados con las actividades desarrolladas por el Tercero para el cumplimiento del contrato. El anterior certificado deberá ser aceptado de forma escrita por el Banco.

5. Gestión de riesgo del proveedor.

Cuando el servicio del tercero sea para procesos críticos de negocio, el Tercero deberá tener implementado un sistema de gestión de riesgo de información y emitir informes periódicos a Davivienda sobre los indicadores de gestión, evaluación de controles y los procesos de mitigación de riesgos identificados.

6. Organización de seguridad de la información.

El tercero debe contar con un área o función encargada de la gestión de seguridad de la información, teniendo en cuenta que toda la información que Banco comparta con los terceros es de carácter confidencial, tercero se sujetará a las siguientes obligaciones:

A. El Tercero será responsable de establecer y mantener un programa de seguridad de la información incluyendo seguridad física de elementos físicos, diseñado para:

---

1. Garantizar la seguridad y confidencialidad de la información confidencial.

2. Proteger contra las amenazas anticipadas o riesgos a la seguridad o integridad de la Información Confidencial.

3. Proteger contra el acceso o uso no autorizados de la Información Confidencial.

4. Garantizar el borrado seguro de la Información Confidencial.

5. El Tercero deberá desarrollar procedimientos para gestionar cualquier incidente de acceso no autorizado y/o violación que amenace la seguridad de la Información Confidencial del Banco y lo notificará al Banco inmediatamente tenga conocimiento del mismo.

6. El Tercero podrá modificar sus procedimientos de seguridad de la información incluyendo seguridad física de elementos físicos, en cualquier momento durante la vigencia del contrato, de conformidad con las normas aplicables y buenas prácticas de seguridad de la información, previa notificación y aprobación por parte del Banco. Esta aprobación se emitirá 30 días después de la notificación de dicho cambio.

VI. ASPECTOS OPERACIONALES.

1. Inventario de tecnología.

El Tercero deberá contar con documentación actualizada de inventario de la infraestructura tecnológica asignada a Davivienda con los respectivos diagramas de la red.

2. Incidentes de seguridad.

El Tercero deberá contar con un procedimiento de gestión de incidentes de seguridad documentado, implementado y en ejecución, este debe estar alineado con el procedimiento de gestión de incidentes del Banco.

3. Monitoreo de seguridad.

El Tercero debe contar con un procedimiento de Monitoreo de Seguridad documentado, implementado y en ejecución. Este debe tener como alcance la totalidad de la infraestructura que será utilizada por el Banco para almacenar, trasportar y procesar la información de la solución técnica ofrecida por el Tercero. Las alertas generadas por el procedimiento deben ser insumo del proceso de gestión de incidentes del tercero.

4. Continuidad de negocio.

El Tercero deberá contar con planes de recuperación ante desastres documentados, implementados y probados y deberán incluir escenarios específicos para Davivienda, así como contemplar escenarios de perdida de continuidad en la prestación de servicios por parte de los terceros del Tercero.

5. Acuerdos de niveles de servicio.

Se deberán establecer acuerdos de niveles de servicio, claramente definidos, medibles, obligatorios y adecuados a los requerimientos de Seguridad de la Información.

6. Componentes de infraestructura de seguridad.

Cuando los procesos del Banco involucrados en la solución se clasifiquen como procesos críticos o gestionen información confidencial, el Tercero debe contar con componentes de infraestructura de seguridad interna y perimetral como lo son: Firewalls, IDS, IPS, Antivirus, DLP, Filtro de Navegación, Filtro de Correo, Herramienta de Control de Puertos, Anti- DDOS, Anti-Malware, Web Application Firewall, Herramientas para correlación de eventos, monitoreo de seguridad y monitoreo de integridad de archivos.

En todos los casos cuando el servicio involucre la utilización correo electrónico el Tercero debe contar con componentes de seguridad como: DLP, AntiSpam, herramientas para: verificación de reputación y URLs para links adjuntos, bloqueo por tipo de archivos adjuntos y SandBox para análisis y control de malware.

7. Seguridad de información en ciclo de desarrollo de software.

El Tercero debe utilizar estándares para desarrollo seguro de software, estos deben estar basados en las mejores prácticas de la industria y deben incluir en todo el ciclo de vida seguridad de la información.

8. Revisión de código fuente.

Con el propósito de identificar vulnerabilidades en la codificación y en la definición de los requisitos, el Tercero debe contar con un procedimiento implementado par la revisión del código fuente. Esta revisión deberá realizarse antes de que el software sea implementado en el ambiente de producción. La revisión deberá incluir entre otros, aspectos como: Identificación de usuarios, autenticación y protección de datos, Autorizaciones de acceso, Lectores de formato, Operaciones no seguras en cadenas, Búfferes y punteros, Códigos de conversión de datos, Lógica empleada en la interpretación de datos, Código involucrado en la generación de mensajes de error, validación de no inclusión de código malicioso, validación de la utilización de herramientas autorizadas por el Banco y cumplimiento con las normas y estándares para desarrollo de software del Banco.

9. Ambientes de desarrollo, laboratorio y producción.

El Tercero debe contar con separación de ambientes tecnológicos de desarrollo, laboratorio y producción. En todos los ambientes tecnológicos se debe contar con sistemas de control de acceso. Debe haber una total separación de funciones del personal que desempeña cargos en cada uno de los ambientes tecnológicos. No debe existir conectividad entre las máquinas de los ambientes de desarrollo, laboratorio y producción.

10. Datos de prueba.

Los datos de producción no se deben utilizar en ambientes de desarrollo o laboratorio, en especial los datos confidenciales de los clientes del Banco. Los datos de prueba utilizados en ambientes de desarrollo y laboratorio deben eliminarse de los aplicativos y tablas antes de ser activados en el ambiente de producción. En casos especiales en que se requiera contar con datos de producción para certificar cambios en ambientes de laboratorio o pruebas, se debe garantizar el enmascaramiento o modificación de datos considerados como Confidenciales.

11. Desarrollo de software con codificación segura.

El desarrollo de software que realice el Tercero para Banco deberá estar basado en directrices de codificación seguras como OWASP Guide, SANS CWET Top 25 o CERT Secure coding, entre otras. Con el propósito de evitar vulnerabilidades de codificación comunes en los procesos de desarrollo de software, dichos procesos de desarrollo deben incluir la revisión y gestión de las siguientes vulnerabilidades: Errores de inyección de código como errores de inyección SQL, errores de inyección de comandos de OS, LDAP y Xpath. Desbordamiento de buffer, Almacenamiento cifrado inseguro, Comunicaciones inseguras y Manejo inadecuado de errores. Estos controles deben exigirse como parte de las políticas de seguridad de la información que deben ser cumplidas por los Proveedores encargados de desarrollar código para el Banco o sus Filiales.

12. Desarrollo de aplicaciones WEB.

En desarrollo de aplicaciones WEB tanto de uso interno como externo, las directrices de codificación segura adicionalmente deberán incluir: Validación de todos los parámetros antes de su inclusión con el propósito de evitar errores por comandos entre distintos sitios (XSS). Evitar un control de acceso inapropiado (tal como referencias no seguras a objetos directos, no restricción de acceso a URL y exposición completa de los directorios). Falsificación de solicitudes entre distintos sitios (CSRF). Estos controles deben exigirse como parte de las políticas de seguridad de la información que deben ser cumplidas por los Proveedores encargados de desarrollar código para el Banco o sus Filiales.

13. Desarrollo de aplicaciones WEB públicas.

Con el propósito de identificar vulnerabilidades en la codificación y en la definición de los requisitos, el Tercero debe contar con un procedimiento implementado par la revisión del código fuente. Esta revisión deberá realizarse antes de que el software sea implementado en el ambiente de producción. La revisión deberá incluir entre otros, aspectos como: Identificación de usuarios, autenticación y protección de datos, Autorizaciones de acceso, Lectores de formato, Operaciones no seguras en cadenas, Búfferes y punteros, Códigos de conversión de datos, Lógica empleada en la interpretación de datos, Código involucrado en la generación de mensajes de error, validación de no inclusión de código malicioso, validación de la utilización de herramientas autorizadas por el Banco y cumplimiento con las normas y estándares para desarrollo de software del Banco.

14. Control de cambios.

El Tercero deberá cumplir con el procedimiento de gestión de cambios de TI establecido en Davivienda.

15. Controles de cambio a parámetros.

El Tercero deberá ofrecer un mecanismo de generación de alertas hacia Davivienda en tiempo real cuando se realice cualquier modificación de parámetros y configuración de software (base y aplicativo) y hardware.

16. Administración de copias respaldo.

El Tercero deberá contar con procedimientos documentados, implementados, probados y aprobados por Davivienda para:

- Mecanismos de cifrado para copias de respaldo.
- La generación de copias de respaldo de software y/o de información.
- Pruebas de restauración de copias de respaldo.
- Almacenamiento externo de copias de respaldo.

17. Infraestructura de seguridad perimetral e interna.

El tercero debe contar con dispositivos y herramientas de seguridad que protejan su red de datos.

18. Infraestructura de seguridad perimetral e interna.

El tercero debe establecer controles para la entrega de la información confidencial del Banco y utilizar herramientas o mecanismos de destrucción segura de la misma conforme a las mejores prácticas de la industria.

19. Pruebas de vulnerabilidad.

Cuando el tercero preste servicios para actividades de informática y/o desarrollos por ejemplo software, equipos de comunicación, enlaces, entre otros, se exige a El Tercero exclusividad, confidencialidad, cumplimiento de los estándares y requisitos de Seguridad de la Información de EL BANCO, y principalmente debe realizar:

A. Con una periodicidad mínima de dos (2) veces por año, ejecutar pruebas de vulnerabilidad que generen un diagnóstico del nivel de seguridad existente en la infraestructura de tecnología del Tercero.

B. El Tercero debe informar los resultados de las diferentes pruebas de vulnerabilidad, la gestión de remediación de las identificadas y entregar la evidencia a EL BANCO cada vez que sean ejecutadas.

C. Implementar procedimientos a seguir cuando se encuentra evidencia de alteración o manipulación de equipos o información.

D. Para los contratos que contemplen prestación de servicios de desarrollo y/o hosting de sitios web del Banco se exige a EL TERCERO:

---

1. Para los sitios web informativos ejecutar pruebas de vulnerabilidad con una periodicidad mínima de dos (2) veces por año.

2. Para los sitios web transaccionales ejecutar pruebas de vulnerabilidad con una periodicidad mínima de cuatro (4) veces por año.

3. EL Tercero debe informar los resultados de las diferentes pruebas de vulnerabilidad, la gestión de remediación de las identificadas y entregar la evidencia a EL BANCO cada vez que sean ejecutadas.

VII. CONTROL DE ACCESO LÓGICO.

1. Gestión de usuarios.

Todo servicio prestado por un tercero deberá cumplir con los procedimientos de gestión de usuarios establecidos en Davivienda.

2. Autenticación fuerte.

Cuando los procesos del Banco involucrados en la solución se clasifiquen como procesos críticos o gestionen información confidencial, deben existir mecanismos de autenticación fuerte (Dos Factores) para los accesos a la solución ofrecida por el Tercero con el propósito de minimizar el riesgo de suplantación de usuarios.

3. Control de acceso lógico.

El Banco definirá los procedimientos de control de acceso a los datos, el cual deberá estar restringido de acuerdo a los roles y perfiles definidos y principio de menor necesidad de conocer. Los usuarios y privilegios serán aprobados por el Banco tanto para usuarios finales y de administración.

4. Segmentación a nivel de red.

Cuando los procesos del Banco involucrados en la solución se clasifiquen como procesos críticos o gestionen información confidencial, el proveedor del servicio deberá garantizar que los componentes de infraestructura asignados al Banco y los datos en reposo y en tránsito estén correctamente aislados por medio de segmentación de red.

5. Cifrado de información.

La información gestiona por la solución provista por el proveedor debe incluir el cifrado de la información en todos los puntos de transmisión (Entre Servidores del mismo segmento, entre servidores del proveedor y el Banco) y en todos los puntos de almacenamiento.

La información de las bases de datos en debe protegerse mediante mecanismos de cifrado.

6. Protocolos seguros.

Para trasmisión de información entre cualquier componente tecnológico el proveedor debe utilizar protocolos de comunicación seguros y estos deben ser aprobados por el Banco.

7. Custodia y gestión de llaves de cifrado de información.

La custodia y gestión de llaves de cifrado de información debe estar a cargo del Banco.

8. Actualización de información

Si por requerimientos del Banco la solución ofrecida por el proveedor necesita actualizar algún campo de información sobre sistemas de información del Banco, estas actualizaciones deben ser analizadas y aprobadas por el Banco y en todo caso primarán los procedimientos de actualización de información que el Banco ya tiene establecidos.

9. Entrega de información.

La información contenida en las bases de datos de la solución ofrecida por el proveedor debe ser entregada periódicamente al Banco y en la estructura definida por el Banco. Esta periodicidad deberá ser definida en conjunto por el área del negocio y el área de tecnología que lidere el proyecto.

VIII. CONTROL DE ACCESO FÍSICO EN INFRAESTRUCTURA DEL TERCERO.

El Tercero deberá contar con mecanismos y procedimientos que permitan proteger las áreas que contienen información y medios de procesamiento de información y su perímetro frente a accesos no autorizados.

1. Ubicación y protección física.

Para proveer una adecuada protección contra acceso no autorizado y garantizar que se cuente con los debidos controles ambientales, los componentes de infraestructura de la solución deben estar ubicados dentro del centro de cómputo, estos deben contar con un sistema de control de acceso al sitio. (Tarjetas de proximidad, mecanismos de control de acceso biométrico, entre otros).

2. Vigilancia.

Para prevenir accesos no autorizados el centro de cómputo debe contar con vigilancia privada 7x24 y con un sistema de cámaras de para todo el sitio.

3. Visitantes.

Para garantizar una debida gestión de acceso de visitantes debe existir un procedimiento para de autorización y registro de visitantes y terceros. Los visitantes y terceros siempre deben estar acompañados de funcionarios autorizados.

4. Controles ambientales.

Con el propósito de proteger los componentes de infraestructura de la solución por alteraciones ambientales se deben tener un sistema de aire acondicionado y controles para humedad y temperatura.

5. Respaldo eléctrico.

Para garantizar un correcto y estable suministro eléctrico para los componentes de infraestructura de la solución se debe contar con un sistema de respaldo de energía eléctrica que incluya, entre otros, UPS y Planta eléctrica.

6. Prevención de incendios.

El centro de cómputo debe contar con un sistema de detección de incendios que incluya alerta por sensores de humo y/o temperatura.

IX. CUMPLIMIENTO NORMATIVO Y REGULATORIO.

1. Cumplimiento normativo.

El Tercero debe cumplir todos los requerimientos y exigencias establecidas por la normatividad legal vigente y por la Superintendencia Financiera de Colombia, siempre que dichos requerimientos guarden relación con el servicio ejecutado por el Tercero.

2. PCI.

Cuando el Tercero preste servicios que almacenen, procesen o trasmitan datos de titulares de tarjetas y/o datos confidenciales de autenticación, de acuerdo al estándar PCI DSS, se exige a El Tercero:

A. El cumplimiento o Certificación de los requisitos de la regulación PCI que apliquen.

B. Con una periodicidad mínima anual, envío de evidencia del cumplimiento o certificación de dichos requisitos expedida por un QSA calificado a EL BANCO.

3. Alcance a ley de protección de datos.

El tercero debe declarar en términos contractuales que conoce y acepta que en el evento que se realice tratamiento de datos personales de cualquier titular del dato, el tercero cumplirá con la normatividad vigente en materia de habeas data y de protección de datos personales.

De igual forma, si el tercero suministra la información de personas deberá contar con la autorización de uso y tratamiento de datos correspondiente por los propietarios de la información. También debe comprometerse a tener a disposición de cualquier Autoridad que los requiera toda la información pertinente que soporte el Tratamiento legítimo que le competa.
Cuanto el tercero detenta la calidad de Responsables del Tratamiento, éste debe declarar contractualmente que asumen con total transparencia su rol ante el usuario o cliente y que velará porque en sus procesos internos se cuente con medidas suficientes y apropiadas que permitan salvaguardar la confidencialidad, seguridad y sujeción a la finalidad de prevención de fraude que soporta este contrato.

En el evento en que el tercero sea requerido por una autoridad para el suministro de la información deberá informar inmediatamente al Banco a fin de que ambas partes estén preparadas en lo que corresponda y puedan adoptar las medidas necesarias para atender adecuadamente el requerimiento.

Cuando se presente una ocurrencia en materia de seguridad de la información que pueda constituir un incidente en los términos de ley, esto es que afecte o amenace la integridad, seguridad y/o confidencialidad de la información el tercero debe informar al Banco.

4. Clasificación de activos de información.

El supervisor del contrato y/o dueño del proceso de negocio deberá realizar un inventario de los activos de información de acuerdo a la metodología establecida, con el propósito de establecer los controles necesarios que garanticen la confidencialidad, integridad y disponibilidad de la información.