Banco Davivienda S.A.

NORMA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD PARA TERCEROS

DAVIVIENDA

NORMA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD PARA TERCEROS

Tipo de Manual: Manuales Seguridad de la Información y Ciberseguridad	**Empresa:** Banco Davivienda	**Versión:** 8
Fecha de Publicación: 06/04/2022	**Código:** MAN_159	

Contenido

Tipo de Manual: Manuales Seguridad de la Información y Ciberseguridad	**Empresa:** Banco Davivienda	**Versión:** 8
Fecha de Publicación: 06/04/2022	**Código:** MAN_159	

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 y Filiales. Al mencionar Banco se hace referencia al Banco y sus Filiales

III. RESPONSABILIDADES DE LOS SUPERVISORES DE CONTRATO.

1. Aspectos Legales.

Toda vinculación de terceros con el Banco debe estar formalmente legalizada a través de los documentos idóneos definidos por la Vicepresidencia Jurídica del Banco y su respectivo visto bueno. Al mencionar Terceros en este documento hacemos referencia a cualquier tipo de persona jurídica o natural con quien el Banco establezca relaciones comerciales, de negocio, alianzas o para recibir cualquier tipo de servicio o producto.

2. Supervisor del Contrato.

El supervisor del contrato es responsable de garantizar que el tercero cumpla las políticas, normas y estándares de seguridad de la información definidos para el desarrollo de sus servicios, durante toda la vigencia de la relación contractual. Cuando el servicio que prestará el tercero involucre intercambio periódico de información, el supervisor debe formalizarlo a través de los acuerdos de intercambio o los documentos legales que el área jurídica del Banco diseñe en conjunto con el Departamento de Seguridad de la Información.

Velará por el estricto cumplimiento de las obligaciones contenidas en las cláusulas relativas a la seguridad de la información del contrato, por parte del proveedor. En caso de tener dudas de carácter técnico o de la forma como éstas se deben controlar, deberá consultar con los expertos del Departamento de Seguridad de la Información y Ciberseguridad.

IV. 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 de la información y Ciberseguridad, 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 y/o generada durante la vigencia de la relación contractual es propiedad exclusiva del BANCO DAVIVIENDA S.A. En consecuencia, dicha información no podrá ser utilizada o compartida por el Tercero para fines diferentes al desarrollo del servicio contratado.

3. Confidencialidad de los terceros

El Tercero, 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, se obligan a no revelar a terceras personas cualquier información que reciba del BANCO DAVIVIENDA o que se genere en virtud del servicio contratado y, en consecuencia se obliga a mantenerla de manera confidencial y privada estableciendo procedimientos y mecanismos para protegerla y evitar su divulgación. Así mismo, El Tercero no dará a la información recibida un uso distinto para el cual fue compartida o suministrada, salvo previa autorización por escrito de Banco Davivienda.

El Tercero en virtud del presente contrato deberá cumplir con las siguientes obligaciones:

a. Implementar todos los controles necesarios, incluyendo cláusulas o acuerdos de confidencialidad para garantizar que el personal a su cargo que tenga acceso a la información, cumpla con el deber de confidencialidad.

b. Dar aviso de manera inmediata al Banco Davivienda, a partir del descubrimiento del uso o revelación no autorizada de cualquier tipo de información y retomar la posesión de dicha información así como evitar su uso futuro no autorizado, sin perjuicio de las acciones a que haya lugar.

c. El Tercero deberá devolver la información física o digital de propiedad de EL BANCO DAVIVIENDA, entregada o generada en virtud del servicio contratado, a la terminación del contrato y/o cuando así lo solicite EL BANCO DAVIVIENDA. El Tercero deberá realizar el borrado a bajo nivel de toda la información que se haya intercambiado física o lógicamente y esté almacenada en su infraestructura tecnológica o de sus Contratistas dando cumplimiento a los lineamientos definidos en sus normas de seguridad de la información.

La violación de lo aquí dispuesto le acarreará a El Tercero las sanciones legales a que haya lugar además de la terminación anticipada y unilateral del Contrato por parte de EL BANCO DAVIVIENDA, sin requerimiento previo y sin que dicha terminación dé lugar a indemnización alguna a cargo de EL BANCO DAVIVIENDA.

4. Auditabilidad.

El Tercero deberá entregar a EL BANCO DAVIVIENDA a la firma del Contrato un informe escrito emitido y firmado por un auditor externo independiente, de una compañía que cuente con experiencia certificada y que lo acredite como experto auditor en temas de tecnología, certificado que debe contener el resultado del proceso de evaluación de los controles de tecnología y de procesos relacionados con las actividades desarrolladas por EL CONTRATISTA para el cumplimiento del Contrato.

El anterior certificado deberá ser aceptado de forma escrita por el Supervisor del Contrato.
EL Tercero permitirá a EL BANCO DAVIVIENDA o a terceros autorizados por EL BANCO DAVIVIENDA, llevar a cabo visitas de auditoría, pruebas de seguridad y análisis de vulnerabilidades, con el objetivo de verificar el cumplimiento de controles y procedimientos propios de El Tercero, así como los requisitos incluidos en este contrato, anexos y demás documentos asociados.

EL BANCO DAVIVIENDA podrá comunicar por cualquier medio, la fecha y hora en que se llevará a cabo la (s) respectiva (s) auditoría (s) o realizarlas en el momento que lo considere necesario.

En caso que EL BANCO DAVIVIENDA o su tercero, evidencien incumplimientos en la visita, emitirá el informe respectivo e informará a las áreas correspondientes para que se determinen las sanciones a las que haya lugar.

5. Gestión de Riesgo del Proveedor.

Cuando el servicio del tercero sea para procesos críticos de negocio, el tercero debe implementar una metodología para la evaluación de los riesgos de seguridad de la información y ciberseguridad sobre los activos del servicio contratado en los cuales se almacene o transmita información confidencial del Banco o sus clientes, al igual que la implementación y seguimiento a los planes de tratamiento de riesgo, dejando evidencia de ello.

El tercero debe mantener implementada una metodología de gestión de proyectos para asegurar que se identifican, gestionan y mitigan los riesgos de seguridad de información en los proyectos asociados al servicio contratado por el Banco.

6. Organización de Seguridad de la Información y Ciberseguridad.

Teniendo en cuenta que toda la información que Banco comparta con los terceros es de carácter confidencial, el tercero se sujetará a las siguientes obligaciones:

- Definir, implementar y mantener vigente un sistema de seguridad de la información y ciberseguridad en la organización el cual esté apoyado por la alta dirección de su organización.
- El enfoque de la organización para la gestión de la seguridad de la información y ciberseguridad debe contar con objetivos de control, los controles, las políticas, los procesos los procedimientos e indicadores de gestión se debe revisar mínimo una vez al año o cuando ocurran cambios significativos en la infraestructura o procesos que soporten el servicio contratado por el Banco.
- Tener definidas, asignadas y documentadas las responsabilidades frente a la seguridad de la información y ciberseguridad de sus empleados y contratistas.
- Tener implementada una política de seguridad de la información que incluya las medidas de seguridad necesarias y suficientes para proteger la información confidencial del Banco y sus clientes a la que tiene acceso, para su almacenamiento y/o procesamiento.
- La información de productos de los clientes del Banco (números de tarjetas, cuentas, etc.) que maneje El Tercero debe estar cifrada y/o ofuscada en cualquiera de los estados en que se encuentre la información tránsito o reposo.

- Notificar al supervisor del contrato del Banco sobre cualquier cambio en su infraestructura tecnológica, en los procesos o manejo de la información confidencial que soporte los servicios contratados por el Banco, siempre que los mismos desmejoren las condiciones de seguridad inicialmente pactados
- Tener definida su política de teletrabajo e implementar los controles necesarios para garantizar la integridad, disponibilidad y confidencialidad de la información accedida, almacenada o transmitida bajo este esquema de trabajo (Seguridad dispositivos móviles, Cifrado información, controles acceso, Conexiones (VPN), etc), mitigando los riesgos de fuga o uso indebido o no autorizado de la información.
- Verificar los antecedentes judiciales de todos los candidatos a un empleo, se debe llevar a cabo de acuerdo con la normativa colombiana y el reglamento interno del tercero.
- Los acuerdos contractuales con empleados y contratistas deben establecer claramente las responsabilidades y las de la organización en cuanto al manejo, uso y gestión de la información, durante el desarrollo de sus funciones así como las implicaciones legales en caso de evidenciar un uso indebido.
- Dentro del contrato suscrito con empleados o contratistas, o en un documento anexo al mismo, debe existir un acuerdo y/o cláusula de confidencialidad de la información, el cual debe estar debidamente firmado por el empleado y/o Contratista (si aplica), y debe tener vigencia por un periodo de 5 años posterior a la finalización del vínculo contractual.
- Documentar e implementar un procedimiento de intercambio seguro de información, que proteja esta información de: intercepciones, copias, modificaciones, desvíos y/o destrucción total o parcial. Este procedimiento debe aplicarse para la información que se comparte a través de diferentes canales y medios (Ej.: Correo electrónico, sistemas de información, aplicaciones, información impresa, entre otros), además, la información que debe viajar cifrada y por canales seguros.
- Si para el servicio contratado se requiere realizar intercambio de información entre las partes se deben utilizar los canales seguros definidos por el Banco, así como suscribir el acuerdo de intercambio de información del Banco. Este documento debe ser actualizado cada vez que se presente algún cambio en la información intercambiada o cuando se realice una renovación del contrato u otrosí al mismo.
- Realizar auditorías a sus contratistas catalogados como críticos en la prestación del servicio contratado por el Banco, frente al cumplimiento de los controles de seguridad de la información y ciberseguridad.
- Validar que sus empleados y contratistas aplican y dan cumplimiento a las políticas y procedimientos establecidos por la organización frente a seguridad de la información y ciberseguridad, dejando las evidencias que correspondan.
- Definir un programa de capacitación y sensibilización sobre seguridad de la información y ciberseguridad, el cual debe ser recibido por todos los empleados de la organización y contratistas (cuando aplique), dejando evidencia de la misma y debe ser medible para comprobar la efectividad y/o entendimiento, igualmente debe incluir reentrenamiento a las políticas de seguridad, los riesgos de la información, las amenazas que pueden afectar la información y el procedimiento de gestión de incidentes.
- Tener definido, implementado y comunicado a todos sus funcionarios el procedimiento sancionatorio en caso de evidenciar una violación a las políticas de seguridad de la información definidas en la organización.
- Establecer controles que garanticen la remoción de los privilegios de accesos a todos los sistemas de la información inmediatamente se notifica la desvinculación del empleado o Contratistas.
- Implementar procedimientos para la gestión de medios de almacenamiento removibles, de acuerdo con el esquema de clasificación adoptado por la organización. Estos medios se deben mantener en un lugar en el cual se encuentren protegidos de accesos no autorizados, modificaciones, daño o destrucción total.

- Notificar al Banco en caso de requerir dar de baja un activo de información que almacene datos del Banco.
- Proteger los medios de almacenamiento que contienen información contra accesos no autorizados, uso indebido o adulteración, debe disponer de mecanismos de encripción o cifrado y control de accesos para garantizar la confidencialidad de la información.
- El tercero no podrá utilizar los equipos donde se almacenaba la información del Banco, hasta que éste apruebe formalmente el proceso de eliminación de la información y verifique la evidencia del cumplimiento de esta actividad. El Tercero debe contar con procedimientos para el desecho y reutilización de los equipos de cómputo y en general de la infraestructura tecnológica que almacene información confidencial del Banco.
- Garantizar que los equipos estén ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado a los mismos.
- Asegurar la configuración en los equipos de cómputo para el bloqueo automático de la sesión después de máximo 5 minutos de inactividad
- Adoptar y mantener vigente una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.
- Hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar la prestación del servicio contratado por el Banco.
- Establecer y acordar todos los requisitos de seguridad de la información pertinentes con terceras partes que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
- Exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que se informe cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

V. ASPECTOS OPERACIONALES.

1. Inventario de Tecnología.

El Tercero deberá realizar y mantener actualizado un inventario de los activos de información e infraestructura tecnológica que hacen parte de los servicios contratados por el Banco, definiendo el propietario, las personas que cuentan con acceso, su uso aceptable, la clasificación de cada activo y el etiquetado de información frente a confidencialidad, integridad y disponibilidad, asimismo con los respectivos diagramas de la red de datos, relacionando los controles de seguridad perimetral correspondientes.

Así mismo, el tercero deberá presentar al Banco un inventario de los controles técnicos o lógicos, físicos y administrativos para proteger los activos de información del Banco en desarrollo del servicio a prestar.

Aplicar medidas de seguridad a los activos que almacenan información del Banco y sus clientes (independientemente si están ubicados en las instalaciones del Tercero o no) estableciendo controles de Cifrado, DLP, Antimalware /Antivirus, Bloqueo de puertos y periféricos, Firewall local y garantizar el mantenimiento de los controles y las actualizaciones de seguridad.

Identificar, documentar e implementar controles para garantizar el uso aceptable de la información y de los activos de información a los cuales tienen acceso los empleados o los Contratistas del tercero para el desarrollo de sus funciones.

2. Incidentes de Seguridad.

El Tercero debe tener definido e implementado un procedimiento de reporte, registro, investigación y respuesta ante materialización de eventos, amenazas e incidentes de seguridad y/o ciberseguridad.

El procedimiento debe ser divulgado y sensibilizado a todo el personal que prestará el servicio.

El procedimiento debe establecer los responsables, las definiciones de incidentes y las acciones a tomar por parte de El Tercero; entre ellas las actividades de cooperación en la respuesta, contención e investigación del incidente con EL BANCO DAVIVIENDA una vez se detecten eventos, amenazas, incidentes de seguridad o ciberseguridad. Así mismo debe verificar que se mantenga un registro de los eventos (causa raíz del incidente, los efectos e impactos causados, los detalles sobre el plan de respuesta y cierre, entre otros) y mantener las evidencias digitales, custodia y disponibilidad de las mismas, y los planes de acción para evitar nuevas materializaciones.

En caso que El Tecero identifique una amenaza o la materialización de cualquier tipo de evento de seguridad de la información y/o ciberseguridad que atente o pudiese afectar la reputación, la operación o cualquier tipo de afectación al BANCO DAVIVIENDA en el servicio contratado se debe reportar inmediatamente al correo iris@davivienda.com y al supervisor del contrato para que en conjunto se tomen las acciones pertinentes.

3. Monitoreo de Seguridad.

El tercero debe contar con un procedimiento de Monitoreo de Seguridad documentado, implementado y en ejecución. Éste debe tener como alcance la totalidad de la infraestructura que será utilizada por el Banco para almacenar, transportar 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 pérdida de continuidad en la prestación de servicios por parte de los terceros del Tercero.

5. Acuerdos de Niveles de Servicio.

Para garantizar la correcta ejecución del contrato, el supervisor del contrato deberá establecer acuerdos de niveles de servicio, claramente definidos, medibles, obligatorios.

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 de 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.

El proveedor debe garantizar que el cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información, estén protegidos contra interceptaciones, interferencia o daño.

7. Seguridad de Información en el Ciclo de Desarrollo de Software.

El tercero debe utilizar estándares para desarrollo seguro de software. Éstos 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 para 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
- Cumplimiento con las normas y estándares para desarrollo de software del Banco.
- Restringir el acceso a códigos fuente de programas, teniendo en cuenta que son acciones designadas únicamente al equipo de desarrollo.

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 el 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.

El tercero debe establecer y aplicar reglas para el desarrollo de software seguro y bajo las buenas prácticas dentro de la organización, también debe llevar a cabo pruebas de funcionalidad de la seguridad y ciberseguridad sobre los desarrollos antes de pasar a producción.

El tercero debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.

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. Requerimientos De Seguridad para Aplicaciones WEB de Terceros

Las aplicaciones web de terceros que el Banco utilice para su procesos o servicios o aquellas que utilice para el desarrollo de alianzas o estrategias comerciales que impliquen el uso de la marca de Davivienda, se deberán proteger contra nuevas amenazas y vulnerabilidades mediante la instalación de firewall de aplicación web (WAF) y mediante la evaluación de seguridad e identificación de vulnerabilidades de aplicación a través del uso de herramientas o métodos automáticos o manuales. Estas evaluaciones deberán estar alineadas con metodologías abiertas y mejores prácticas de pruebas de penetración, como lo son entre otras: OSSTMM, OWASP, NIST SP 800-115. Las evaluaciones deberán realizarse por lo menos dos veces al año y después de cada cambio en la aplicación. Las aplicaciones web públicas deben incluir el uso de certificados digitales.

14. Control de Cambios.

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

Establecer un proceso de gestión de cambios donde se encuentren detalladas las restricciones a los cambios de paquetes de software, revisión técnica de las aplicaciones luego de los cambios y garantizar la protección de la información en todo su ciclo de vida.

Gestionar los cambios en el suministro de servicios por parte de terceras partes, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.

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 y probados 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.
- Hacer copias de respaldo de la información, software e imágenes de los sistemas y realizar pruebas periódicamente de acuerdo con una política de copias de respaldo. Si, la información a respaldar contiene información confidencial como datos de productos, pin, datos personales, entre otros sin ser excluyentes, debe ir ofuscada/enmascarada y cifrada.
- Elaborar, conservar y revisar regularmente los registros de eventos (logs) acerca de actividades de usuario excepcionales, fallas y eventos de seguridad de la información, dicha información debe quedar almacenada por lo menos por 5 años luego de la desvinculación contractual.

17. Infraestructura de Seguridad Perimetral e Interna.

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

Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.

Garantizar la identificación de cada uno de los equipos en la red, proteger los puertos de configuración y de diagnóstico remoto, así como separar lógicamente las redes de administración y de producción.

Garantizar que la información involucrada en servicios de aplicaciones que pasan sobre redes públicas se proteja de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas, garantizando el uso de canales seguros, revisión de código y ofuscación del mismo.

Garantizar que la información involucrada en las transacciones de servicios de aplicaciones se proteja para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.

18. Pruebas de Vulnerabilidad.

Los terceros deben obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado, estableciendo escaneos como mínimo dos veces al año a toda la infraestructura o recursos que almacenan información crítica del contrato, para sin determinar tiempos de remediación frente a las vulnerabilidades encontradas (críticas, altas, medias y bajas).

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

A. Deber realizar pruebas de ethical hacking en todos los componentes de la infraestructura que soporta la prestación del servicio contratado por el BANCO DAVIVIENDA, con una periodicidad mínima de dos (2) veces por año, con una diferencia de al menos seis meses entre cada prueba durante la vigencia del contrato, y cada vez que se realicen cambios en la infraestructura tecnológica que soporta el servicio contratado.
B. Debe realizar escaneos de vulnerabilidades trimestrales sobre la infraestructura de las aplicaciones/servicios que soportan el servicio adquirido por el BANCO DAVIVIENDA.

Cuando el tercero preste servicios de desarrollo y/o hosting de sitios web del Banco debe:

A. Para los sitios web informativos ejecutar pruebas de vulnerabilidad y realizar pruebas de ethical hacking en todos los componentes de la infraestructura que soporta la prestación del servicio contratado por el BANCO DAVIVIENDA, con una periodicidad mínima de dos (2) veces por año, con una diferencia de al menos seis meses entre cada prueba durante la vigencia del contrato, y cada vez que se realicen cambios en la infraestructura tecnológica que soporta el servicio contratado.
B. Para los sitios web transaccionales ejecutar pruebas de vulnerabilidad con una periodicidad mínima de cuatro (4) veces por año.
C. 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.

El tercero debe comprometerse a dar cierre a las vulnerabilidades identificadas de acuerdo a su criticidad en un periodo no mayor a: críticas/altas: 30 días, medias/severas: 60 días y moderadas o bajas: 90 días. y que se hagan pruebas trimestrales sobre las aplicaciones.

El Tercero debe reportar al Supervisor del Contrato de EL BANCO DAVIVIENDA cuando presente incumplimiento de frente a los

tiempos de remediación de las vulnerabilidades críticas y altas, así mismo debe incluir las fechas de cierre de las mismas y remitir la certificación correspondiente una vez hayan sido subsanadas.

VI. CONTROL DE ACCESO LÓGICO.

1. Gestión de Usuarios.

Todo servicio prestado por un tercero acceso a la infraestructura del Banco deberá cumplir con los procedimientos de gestión de usuarios y requerimientos de seguridad establecidos en Davivienda.

Es obligación del tercero reportar inmediatamente al supervisor del contrato del Banco, de todo retiro, ingreso o modificación del Rol de sus funcionarios que tengan acceso a aplicaciones o infraestructura del Banco.

Bajo ningún motivo está autorizado el préstamo de usuarios y contraseñas.

El tercero debe asegurar el cambio de contraseñas en un plazo no mayor a un mes y garantizar que no se use la misma contraseña en un periodo de tiempo no mayor a 60 días.

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 doble factor de autenticación (token, certificado digital, QR, Push) 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.

En caso de que el tercero requiera la asignación de usuarios privilegiados y/o de aplicación para el desarrollo del servicio contratado, éste debe justificar la necesidad del acceso y el usuario debe firmar el acuerdo de uso y confidencialidad de la información antes de ser asignado el acceso.

El tercero debe definir e implementar una política y procedimientos de control de acceso, de tal forma que sólo se permita el acceso de los usuarios a los sistemas de información y a los servicios de red para los que hayan sido autorizados, dejando evidencia o trazabilidad de los accesos solicitados y otorgados. Así mismo, debe garantizar que exista segregación de funciones y se cumpla el principio de menor privilegio a la información del Banco y sus clientes.

Garantizar la segregación de funciones y áreas de responsabilidad en conflicto para reducir las posibilidades de modificación no autorizada o no intencional de la información o datos, así como el uso indebido de los activos de la organización.

Implementar un proceso de asignación o cancelación de accesos a todo tipo de usuarios para todos los sistemas y servicios propios, especialmente a aquellos en donde se almacene información del Banco.

Restringir y controlar la asignación y uso de derechos de acceso privilegiados. Debe realizar monitoreo a los usuarios privilegiados.

Garantizar y realizar depuración de los accesos como mínimo una vez al año para asegurar que se cumple el mínimo privilegio y validar que los accesos se encuentren acorde con las funciones de los empleados y/o proveedores.

Implementar y establecer el procedimiento para controlar la instalación de software en sistemas operativos por parte de los usuarios, estableciendo controles donde se incluya la línea base de programas permitidos por la organización y roles específicos para poder gestionar dichas actividades.

Restringir y controlar el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones, manteniendo dentro de la línea base los programas autorizados por la organización.

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.

5. 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.

6. Protocolos Seguros.

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

El Tercero debe garantizar que las conexiones remotas con la red del Banco, se hagan a través de VPN (IPSEC) con doble factor de autenticación 2FA, uso del protocolo IKEv2 para el intercambio de llaves y se utilice AES 256 para el cifrado y SHA 256 o RSA 2048 para autenticación.

Implementar protocolos de comunicación seguros y controles de seguridad para proteger la información de los sistemas y aplicaciones (Canales cifrados). Los controles deberán proteger la red de intrusiones externas a ella por medio de firewalls perimetrales, autenticación de conexiones wireless y otros controles complementarios que se identifiquen como resultado del proceso de análisis y tratamiento de riesgos, realizado por el tercero.

7. 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.

8. 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.

VII. CONTROL DE ACCESO FÍSICO EN INFRAESTRUCTURA DEL TERCERO.

El Tercero deberá contar con protocolos y dispositivos de seguridad electrónica, con grabación de vídeo mínima de seis meses, 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).

Las áreas seguras del tercero se deben proteger mediante controles de ingreso para garantizar que a dichas áreas solamente se permite el acceso a personal autorizado.

Las puertas del centro de cómputo deben tener diseño antifuego, el sistema de video debe estar distribuido en toda la zona interna cubriendo corredores, entrada y salida del centro de cómputo incluida la de emergencia, equipos de procesamiento, áreas de trabajo de operadores.

2. Vigilancia.

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

Garantizar que las instalaciones donde se maneje información confidencial del Banco y sus clientes cuenten con: circuito cerrado de televisión con capacidad de almacenamiento de seis meses, controles de acceso físico, restricción en el uso de dispositivos móviles o wearables (si aplica), contar con elementos de dotación adecuados para evitar el ingreso de elementos (cámaras, libretas, medios removibles,etc) y prohibición del ingreso de personal no autorizado.

3. Visitantes.

Para garantizar una debida gestión de acceso de visitantes debe existir un procedimiento 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 debe 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 y todas las zonas en donde se manipule información del Banco debe contar con un sistema de detección de incendios que incluya alerta por sensores de humo y/o temperatura, así como sistemas de extinción para combatir cualquier conato o incendio que se presente.

VIII. 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 transmitan datos de titulares de tarjetas y/o datos confidenciales de autenticación, de acuerdo con el 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. 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, 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 acuerdo con los términos que exige la ley, de tratamiento de datos de los titulares dueños de los datos. También debe comprometerse a tener a disposición de cualquier autoridad que lo requiera toda la información pertinente que soporte el Tratamiento legítimo que le competa.

Cuando el tercero ostenta la calidad de Responsables del Tratamiento, éste debe declarar contractualmente que asumen con total transparencia su rol ante el usuario o cliente y que aplicará las medidas técnicas, humanas y administrativas necesarias para proteger los datos tratados evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

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 involucre datos personales que pueda constituir un incidente en los términos de ley, el tercero debe informar al Banco.

3.1 Medidas aplicables al tratamiento de datos personales

En los casos en que el Tercero actúe como Encargado del tratamiento de datos personales en nombre de DAVIVIENDA deberá cumplir con las obligaciones establecidas a continuación:

3.1.1 Recolección

Al momento de solicitar al Titular la autorización de tratamiento de datos personales , deberá informarle de manera clara y expresa lo siguiente:

a. El tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
b. El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre datos de las niñas, niños y adolescentes.
c. Los derechos que le asisten como Titular.
d. La identificación, dirección física o electrónica y teléfono del Responsable del tratamiento.

Deberá conservar prueba del cumplimiento de los anteriores ítem y, cuando el Banco lo solicite, entregarle copia de esta.

La autorización puede manifestarse por escrito, de forma oral o mediante conductas inequívocas del Titular que permitan concluir de forma razonable que otorgó la autorización, en ningún caso el silencio podrá asimilarse a una conducta inequívoca.

Deberá implementar y adoptar las acciones tendientes y necesarias para mantener registros o mecanismos técnicos o tecnológicos idóneos, de cuándo y cómo obtuvo autorización por parte de los Titulares de datos personales para el tratamiento de los mismos. Para dar cumplimiento a lo anterior, se podrán establecer archivos físicos o repositorios electrónicos dispuestos de manera directa o a través de terceros contratados para tal fin.

Los textos de autorización de Titulares deberán ser revisados de forma periódica (mínimo una vez al año) y/o ajustados en caso de ser necesario con respecto al cumplimiento de ley o por cambios en los contratos o reglamentos de los productos y servicios ofrecidos por **DAVIVIENDA**.

El registro de las autorizaciones de tratamiento de datos personales debe contener los siguientes campos:

- Fecha en la que se hizo check para otorgar la autorización.
- Hora en la que se hizo check en la casilla de autorización.
- Campo que guarda el check de la autorización.

- Dirección IP desde la que se está accediendo.
- Nombres y apellidos del Titular
- Texto que se muestra al Titular.
- Fuente: formato físico o digital
- Indicar que se validó la identidad del Titular.
- Resultado del proceso de validación del Titular.

3.1.2 Almacenamiento

Los datos personales almacenados por el tercero en calidad de Encargado debe:

- Garantizar que sean veraces, completos, exactos, actualizados, comprobables y comprensibles.
- Aplicar las Normas de Seguridad de la Información de DAVIVIENDA establecidas para evitar la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Almacenar la información de acuerdo a los tiempos establecidos en el contrato con DAVIVIENDA.

3.1.3 Uso

Los datos personales se utilizarán únicamente con los fines establecidos en el contrato de Transmisión o Transferencia de Datos personales firmado entre Davivienda y el encargado.

3.1.4 Circulación

Para la transmisión o transferencia de datos personales con un Encargado , se aplicarán las siguientes reglas:

Las transmisiones y transferencias internacionales de datos personales deberán observar lo previsto en los artículos 24 y 25 del Decreto Reglamentario 1377 de 2013 y el artículo 26 de la ley 1581 de 2012.

Las transmisiones internacionales de datos personales que se efectúen entre **DAVIVIENDA** como Responsable y un tercero como Encargado, no requerirán ser informadas al Titular ni contar con su consentimiento cuando exista un contrato en los términos del artículo 25 del decreto 1377 de 2013.

En los casos que **DAVIVIENDA** en desarrollo de sus procesos de negocio requiera circular (transmitir o transferir) datos personales debe tener en cuenta:

DAVIVIENDA, como Responsable de los datos personales almacenados en sus bases de datos y en desarrollo de las finalidades descritas en la Política de Tratamiento de Datos Personales, podrá realizar transferencia o transmisión nacional o internacional de datos personales.

DAVIVIENDA celebrará con el tercero Encargado un contrato de transmisión o transferencia u otro instrumento jurídico que garantice la protección de los datos personales objeto de transmisión o transferencia y en los casos en que aplique, **DAVIVIENDA** solicitará la declaración de conformidad a la Superintendencia de Industria y Comercio.

El contrato de transmisión o transferencia de datos personales, debe señalar los alcances del tratamiento, las actividades que el tercero Encargado realizará por cuenta del Responsable para el tratamiento de los datos personales, y las obligaciones del tercero Encargado para con el Titular y el Responsable.

Mediante dicho contrato el tercero Encargado se compromete a aplicar las obligaciones que establezca **DAVIVIENDA** bajo la política de tratamiento de datos personales fijada por ésta, y a realizar el tratamiento de datos de acuerdo con la finalidad que los Titulares hayan autorizado y con las leyes aplicables.

Además de las obligaciones que impongan las normas aplicables dentro del citado contrato, deberán incluirse las siguientes obligaciones en cabeza del respectivo tercero Encargado:

- Dar tratamiento, a nombre del Responsable, a los datos personales conforme a los principios que los tutelan.
- Salvaguardar la seguridad de las bases de datos en las que se contengan datos personales.
- Guardar confidencialidad respecto del tratamiento de los datos personales.

Si **DAVIVIENDA** entrega bases de datos que contengan datos personales a algún tercero Encargado del tratamiento, se deberá precisar si son personas naturales o jurídicas; cuál es la forma de entrega o acceso a la información y qué tipo de tratamiento debe realizar el tercero Encargado.

Además se deberá: (i) determinar quién será la persona que al interior de **DAVIVIENDA** realizará las labores de seguimiento, gestión y control a los terceros Encargados del tratamiento; y (ii) definir si permite o no que terceros recolecten información en su nombre, a través de qué documentos, y cuáles serán las exigencias a estos terceros.

3.1.5 Supresión

Los datos personales se suprimirán de acuerdo a lo establecido en el contrato de Transmisión o Transferencia de Datos Personales firmado entre DAVIVIENDA y el tercero Encargado y teniendo en cuenta que:

La supresión de datos personales deberá aplicar las normas de seguridad de la información que impidan su consulta o copia por terceros no autorizados y se deberá generar un registro de su eliminación.

Esta supresión implica la eliminación total o parcial de la información personal en las bases de datos que contengan datos personales en **DAVIVIENDA** y el Encargado**,** de acuerdo con lo solicitado por el Titular.

La supresión de datos personales se genera a partir de los reclamos que realizan los Titulares a través de los canales definidos para este fin. Las reclamaciones son recibidas por el departamento de Operaciones de Reclamos, quien debe solicitar al departamento de Operaciones de Información al Cliente la eliminación del dato y con el apoyo del área de tecnología correspondiente verificar que la novedad se aplique en los sistemas de información del banco.

3.2. Medidas de Seguridad aplicables al tratamiento de datos personales

Todo tercero que reciba información del Banco Davivienda, adicionalmente a todo lo expuesto en esta norma deberán cumplir con las siguientes obligaciones:

1. Tener implementada una política y medidas de seguridad necesarias y suficientes que protejan la información confidencial del Banco.
2. Los datos confidenciales (biométricos, relacionados con salud, fotos, videos, número de tarjeta, número de cuenta, saldo, entre otros), tratados por el Tercero, deben estar cifrados y/o ofuscados mientras que éstos se encuentren en reposo o en tránsito.
3. El tercero debe notificar, con dos semanas de anticipación, al Supervisor del contrato en el Banco Davivienda, cualquier cambio en su infraestructura tecnológica, en los procesos o en el manejo de la información confidencial que soporte los servicios contratados por el Banco Davivienda.
4. El tercero debe tener definida una política para teletrabajo y/o trabajo en casa e implementar los controles necesarios para garantizar la integridad, disponibilidad y confidencialidad de la información accedida, almacenada o transmitida bajo estas modalidades de trabajo mitigando los riesgos de fuga o uso indebido o no autorizado de la información confidencial del Banco Davivienda.
5. Los acuerdos contractuales con empleados y contratistas deben establecer claramente las responsabilidades de la organización en cuanto al manejo, uso y gestión de la información confidencial, durante el desarrollo de sus funciones, así como las implicaciones legales en caso de evidenciar un uso indebido.
6. Dentro del contrato suscrito con empleados y/o contratistas, o como anexo al mismo, debe existir una cláusula y/o acuerdo de confidencialidad de la información que debe estar firmada por el empleado y/o El Tercero, y debe tener vigencia mínimo por el tiempo de duración de la relación contractual y por el tiempo que la Ley o la regulación vigente así lo indique.
7. El tercero debe documentar e implementar un procedimiento de intercambio que incluya cifrado de datos y canales seguros para el envío de información confidencial, que proteja del acceso no autorizado y uso indebido de los datos independiente del canal o medio utilizado.
8. El tercero debe suscribir el acuerdo de intercambio de información definido por el Banco Davivienda, si para el servicio contratado se requiere realizar intercambio de información confidencial entre las partes, es obligatorio realizar actualización del mismo, cada vez que se presente algún cambio en la información intercambiada o cuando se realice renovación del contrato u otro si al mismo.
9. Se debe suscribir un contrato de Transmisión o Transferencia de datos si el intercambio de información incluye datos personales.
10. El tercero debe desarrollar un programa de capacitación y sensibilización sobre seguridad de la información y ciberseguridad, el cual debe ser recibido por todos los empleados de la organización y contratistas (cuando aplique), dejando evidencia de la misma y debe ser medible para comprobar la efectividad y/o entendimiento, igualmente debe incluir reentrenamiento en las políticas de seguridad, los riesgos sobre la información confidencial, las amenazas que pueden afectar la información confidencial y el procedimiento de gestión de incidentes.
11. El tercero al finalizar el contrato debe garantizar la entrega y borrado a bajo nivel de toda la información confidencial del Banco Davivienda que se haya intercambiado y esté almacenada en infraestructura tecnológica propia o de Contratistas. Esta

actividad debe realizarse mediante el uso de procedimientos y herramientas que garanticen el borrado a bajo nivel. El Tercero debe notificar al supervisor del contrato el procedimiento de borrado de información para su revisión y aval; asimismo, una vez realizada la actividad debe remitir al Banco Davivienda la certificación del borrado realizado.

12. El tercero debe realizar y mantener actualizado un inventario de los activos de información que hacen parte de los servicios contratados por el Banco Davivienda, definiendo el propietario, control de acceso, clasificación y el etiquetado de información frente a confidencialidad, integridad y disponibilidad.
13. El tercero debe garantizar que todos los equipos utilizados para el desarrollo del servicio contratado por el Banco Davivienda que maneje información confidencial tengan implementados mecanismos que aseguren su protección contra cualquier tipo de amenazas a la seguridad de punto final (endpoint security).
14. El tercero debe tener un procedimiento para la gestión de incidentes de Seguridad y Ciberseguridad; debe reportar al supervisor de contrato en el Banco Davivienda tan pronto identifique la ocurrencia de un incidente que involucre información confidencial del Banco.

IX. REQUERIMIENTOS PARA FÁBRICAS DE SOFTWARE INTERNAS, EXTERNAS O TERCERIZADAS

Adicionalmente a lo anteriormente expuesto en esta norma, las fábricas de Software deben cumplir con los siguientes requisitos:

1. Almacenamiento de Código Fuente en Nube:

1.1. No se permite la carga, almacenamiento o envío de código fuente, archivos, parámetros o información de las aplicaciones, modelos de analítica, servicios y canales digitales del Banco en forma parcial o total a repositorios de código, correos electrónicos, repositorios y/o redes sociales en internet con cuentas personales, corporativas o en general no autorizadas por el Banco.

1.2. El único repositorio público autorizado para el almacenamiento de código es el disponibilizado por el Banco con cuenta corporativa (para fábrica interna y externa con terceros).

1.3. Las fábricas de software de terceros pueden utilizar repositorios de nube pública pero únicamente con cuentas corporativas y deben acceder únicamente a través del control de acceso a nube suministrado por el Banco para garantizar la gestión de privilegios, monitoreo y supervisión de ciberseguridad desde el Banco.

1.4. El acceso a repositorios corporativos en nube del Banco y sus terceros debe ser restringido únicamente a direcciones IP de la organización y previamente autorizadas por la Dirección de Ciberseguridad TI del Banco.

1.5. Se debe restringir el acceso a correos electrónicos, repositorios en internet y a aplicaciones en nube o shadow IT diferentes a los autorizados por el Banco mediante controles de navegación y prevención de fuga de información de desarrollo, tanto a nivel de red como en computadores de usuario final tanto en oficinas

presenciales como en estaciones de trabajo de tipo VDI (Virtual Desktop Infrastructure), workspaces o similar asignados para teletrabajo o trabajo remoto.

2. **Identidad:**

2.1. El acceso y autenticación en ambientes de laboratorio, desarrollo, pruebas y producción se debe realizar únicamente con usuarios corporativos, aplicación, o administración basados en roles y perfiles estandarizados y configurados en plataformas de gestión de identidad centralizada como IDM..

2.2. La autenticación en los repositorios de código públicos autorizados por el Banco se debe realizar únicamente con usuarios de dominio y restringir la autenticación con cuentas de otros dominios no autorizados.

2.3. La autenticación en repositorios de código en nube autorizados debe utilizar doble factor de autenticación mediante token, certificado digital, QR, Push u OTP.

2.4. No se permiten contraseñas y claves escritas en los códigos de aplicaciones, APIs, scripts, runbooks, playbook, archivos de configuración o similares.

3. **Reducción de la superficie de ataque:**

3.1. Se deben ofuscar o cifrar los códigos con lógica asociada a los canales o aplicaciones críticas para el negocio y firmar los metadatos y versión del código con estampas de tiempo para mitigar riesgos de integridad y confidencialidad del código o información sensible del Banco.

3.2. Los repositorios de código deben cifrar la información tanto en reposo como tránsito (según el estándar del Banco).

4. **Segmentación**

4.1. Los ambientes de desarrollo deben estar completamente separados a nivel de red mediante una segmentación y aislamiento de ambientes con controles de acceso a la información del Banco. No se permite la extracción de información de estos ambientes hacia repositorios públicos o personales de los desarrolladores o administradores de las plataformas.

5. **Llaves y secretos**

5.1. Todas las contraseñas, claves y parámetros de seguridad deben ser revisados y cambiados periódicamente según los lineamientos de las políticas de control de acceso, inclusive en ambientes de desarrollo, pruebas y certificación.

5.2. Se deben utilizar mecanismos seguros como contenedores de llaves, cripto-procesadores como HSM, KMS, Key Vault, o JKS - Java Key Store para el almacenamiento y procesamiento de secretos o parámetros de seguridad como contraseñas, claves, URIs, usuarios, llaves criptográficas y certificados.

6. **Modelamiento de Amenazas**

6.1. Aplicar metodologías de desarrollo seguro de software basados en mejores prácticas como OWASP SAMM, incluyendo como mínimo modelamiento de amenazas, manejo de errores, casos de abuso, casos de uso de seguridad y arquitectura de seguridad.

6.2. Se deben realizar revisiones periódicas de código estático y dinámico y pruebas de vulnerabilidades de aplicación mediante hacking ético. En todos los casos se deben aplicar las remediaciones pertinentes de la siguiente manera: 30 días para remediar vulnerabilidades críticas o severas, 60 días para vulnerabilidades altas y 90 días para las vulnerabilidades medias.

7. **Visibilidad en Ambientes de Desarrollo**

7.1. Todos los activos, dispositivos, componentes, tecnologías (hardware o software), instancias, identidades, proveedores y demás elementos involucrados (Lambdas, workloads, serverless, IaC, Kubernetes, etc) independientemente del modelo de servicio escogido (IaaS, PaaS, SaaS, Híbrido) deben ser auditados. Esto implica que deben generar logs de eventos de seguridad que deben redireccionarse al centro de operaciones de ciberseguridad del Banco llamado IRIS.

8. **Monitoreo de CiberAmenazas y Respuesta a Incidentes.**

8.1. Para fábricas de software de terceros, este debe implementar mecanismos de monitoreo permanente y durante la vigencia del contrato que permita identificar si información del Banco ha sido expuesta en repositorios públicos por parte de sus Empleados y notificarlo de manera inmediata al siguiente correo electrónico iris@davivienda.com y al supervisor del contrato. De igual manera, deberá notificar inmediatamente cualquier incidente de seguridad que afecte a la información del Banco y/o sus clientes directa o indirectamente). De igual

manera, debe tener la capacidad de responder y contener de manera oportuna y coordinada con el equipo de respuesta a incidentes de ciberseguridad del Banco.

8.2. Se debe diseñar casos de uso para el monitoreo en el correlacionador de eventos. Las Alertas generadas a partir de estos serán gestionadas mediante el proceso de Incidentes de ciberseguridad del Banco.

8.3. Ciberseguridad TI realizará monitoreo aleatorio en repositorios públicos para identificar fugas de información.

X. LINEAMIENTOS PARA EL BORRADO SEGURO DE LA INFORMACIÓN

Estos lineamientos son de obligatorio cumplimiento por todos los terceros con los cuales el Banco Davivienda ha determinado finalizar y/o no renovar el contrato, proyecto o relación comercial establecida.

1. El Tercero junto con el área dueña de la información y el Supervisor del contrato, debe de notificar al Departamento de Seguridad de la Información y Ciberseguridad del Banco la finalización comercial y debe haber gestionado el levantamiento de los siguientes requisitos:

    i. Tener el inventario de todos los activos de información que hacen parte del proyecto, servicios administrados o en infraestructura del tercero y que almacenen datos del banco o clientes.
    ii. Tener identificada la información que almacena, procesa o gestiona el tercero.
    iii. Si existe algún requerimiento legal, normativo o de negocio que exija la conservación de la información debe gestionar con el Banco los recursos tecnológicos para la custodia de los mismos.
    iv. En la notificación de borrado de información, debe indicar los datos de contacto del responsable de certificar la ejecución del proceso.