DAVIVIENDA

GUÍA DE BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD PARA LOS TERCEROS

GUÍA DE BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD PARA LOS TERCEROS

Contenido

I. Guía de buenas prácticas para los Terceros

Supervisor de contrato:

Para este documento, el término "supervisor del contrato" se refiere a el Director, Gerente o Líder de área que gestione cualquier tipo de vinculación de un Tercero con el Banco, (un contrato, alianza, contrato de colaboración, etc.).

Al mencionar Terceros en este documento hacemos referencia a cualquier tipo de persona jurídica o natural de quien el Banco reciba cualquier tipo de servicio o producto o con quien el Banco establezca relaciones comerciales, de negocio, alianzas, acuerdos de colaboración, etc.

1. Gestión de Riesgos de Seguridad de la Información y Ciberseguridad por parte del Tercero

Los Terceros deben tener implementada una metodología para la evaluación de los riesgos de seguridad de la información y ciberseguridad sobre los activos (Activos físicos, digitales, *software*, *hardware*) del servicio contratado en los cuales se almacene, procese 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. Asimismo, el tercero de acuerdo con su realidad operativa debe mantener implementada una metodología de gestión de riesgos para asegurar que se identifican, gestionan y mitigan los riesgos de seguridad de información.

2. Aspectos generales de seguridad de la información

- Si el tercero cuenta con esquema de trabajo remoto, debe 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, SASE etc), mitigando los riesgos de fuga o uso indebido o no autorizado de la información.

- El Tercero debe verificar la información de la hoja de vida, las referencias y posibles antecedentes judiciales de todos los candidatos a un empleo, de acuerdo con la normativa colombiana y el reglamento interno del tercero.

- En caso de que el Banco autorice al tercero una subcontratación, el Tercero debe garantizar al Banco que sus contratistas cumplan con controles que garanticen la confidencialidad, integridad y disponibilidad de la información.

- Los acuerdos contractuales del Tercero con sus empleados y contratistas deben establecer claramente sus 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.

- El Tercero debe garantizar que sus empleados y contratistas aplican y dan cumplimiento a las políticas y procedimientos establecidos en seguridad de la información y ciberseguridad, dejando las evidencias que correspondan.

- El Tercero deberá contar con un programa de capacitación y sensibilización sobre seguridad de la información y ciberseguridad, que incluya, sin limitarse, temas asociados a políticas de seguridad, riesgos de la información (fuga, exfiltración, confidencialidad, integridad, entre otros), amenazas que pueden afectar la información y procedimientos de gestión de incidentes. Este programa deberá ser actualizado e impartido periódicamente a todos los empleados de la organización y contratistas que tengan relación directa en el desarrollo del objeto contractual, asimismo el tercero deberá dejar evidencia de su ejecución y comprobar la efectividad y/o entendimiento del mismo.

- El Tercero debe tener definido, implementado y comunicado a todos sus funcionarios un procedimiento sancionatorio en caso de evidenciar una violación a las políticas de seguridad de la información definidas por el Tercero.

- El Tercero debe establecer controles que garanticen la remoción de los privilegios de accesos a todos los sistemas de información inmediatamente se notifica la desvinculación de los empleados o contratistas a su cargo. Cuando se retiren empleados o contratistas a cargo del tercero que hagan parte del proceso contratado por el Banco, el Tercero debe informar al supervisor del contrato del Banco para que los permisos sean retirados en todos los activos de información donde aplique.

- El Tercero debe implementar procedimientos para la gestión de medios de almacenamiento removibles, de acuerdo con el esquema de clasificación adoptado por el Tercero. Estos medios se deben mantener en un lugar en el cual se encuentren protegidos de accesos no autorizados, modificaciones, daño o destrucción total.

- El Tercero debe notificar al Supervisor del Contrato del Banco cuando se requiera dar de baja o eliminar un repositorio que almacene información del Banco.

- El Tercero debe proteger los medios de almacenamiento que contienen información del Banco contra accesos no autorizados, uso indebido o adulteración; debe disponer de mecanismos de cifrado y control de accesos para garantizar la confidencialidad de la información.

- 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.

- El Tercero debe 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.

- El Tercero debe implementar guías de hardening sobre la infraestructura tecnológica sobre la cual transporte, procese o almacene información del Banco.

- El Tercero debe 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.

- El Tercero debe hacer seguimiento al uso, capacidad y disponibilidad de los recursos tecnológicos para asegurar la prestación del servicio derivado del objeto contractual con el Banco.

- El Tercero debe exigir a todos sus empleados y contratistas que usan los servicios y sistemas de información del Banco informar cualquier debilidad, vulnerabilidad o brecha de seguridad de la información observada o sospechada en los sistemas o servicios.

3. Inventario de Tecnología

Los terceros que presten servicios al Banco a través de su infraestructura tecnológica deberán realizar y mantener actualizado un inventario de los activos de información e infraestructura tecnológica que hacen parte de los servicios contratados por el Banco, las personas que cuentan con acceso, los privilegios de acceso de esas personas, la clasificación y etiquetado de cada activo frente a confidencialidad, integridad y disponibilidad, adicionalmente a garantizar la debida generación de logs en los cuales se evidencie la trazabilidad de las acciones realizadas por sus funcionarios, asimismo los respectivos diagramas de la red de datos, relacionando los controles de seguridad perimetral correspondientes.

El Terceros debe aplicar medidas de seguridad para mitigar los riesgos de seguridad de la información y ciberseguridad de los activos que almacenan información del Banco y sus clientes (independientemente si están ubicados en las instalaciones del Tercero o no) estableciendo controles tales como el Cifrado, DLP, Antimalware /Antivirus, Bloqueo de puertos y periféricos, WAF y Firewall, entre otros y garantizar el mantenimiento de los controles y las actualizaciones de seguridad.

4. 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 del Tercero; entre ellas las actividades de cooperación en la respuesta, contención e investigación del incidente con el BANCO DAVIVIENDA una vez se detecten eventos inusuales, 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 Tercero identifique una amenaza o la materialización de cualquier tipo de incidente de seguridad de la información y ciberseguridad que atente o pudiese afectar la reputación, la operación o impactar negativamente al BANCO DAVIVIENDA en el servicio contratado, se debe reportar inmediatamente al correo *incidenteseguridadti@davivienda.com* y al supervisor del contrato para que en conjunto se tomen las acciones pertinentes.

5. Monitoreo de Seguridad

Los terceros que presten servicios al Banco a través de su infraestructura tecnológica deben contar con un procedimiento de Monitoreo de Seguridad documentado, implementado y en ejecución. Éste debe tener como alcance la totalidad de la infra estructura 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.

6. Control de Acceso Físico para Terceros con infraestructura tecnológica

El Tercero deberá contar con protocolos y controles de seguridad física (CCTV, tarjetas aproximación, biométrica, vigilancia entre otros), que permitan proteger las áreas que contienen información y medios de procesamiento de información y su perímetro frente a accesos no autorizados.

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.

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.

Las grabaciones del sistema de cámaras deben retenerse por un periodo mínimo de seis meses.

Garantizar que las instalaciones donde se maneje información confidencial del Banco y sus clientes cuenten con: circuito cerrado de televisión, 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.

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.

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.

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 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.