1.1. Estándar

Todos los terceros que tengan acceso y manejen información confidencial y Confidencial restringida del Banco en sus instalaciones, deben cumplir con los controles y medidas de seguridad referenciadas en esta categoría, con el fin de garantizar que la información suministrada por la Entidad conserve las propiedades de confidencialidad e integridad acorde con los parámetros de seguridad establecidos.

1.2 Objetivo

Establecer los requisitos de seguridad de la información y ciberseguridad a tener en cuenta en la contratación de servicios donde Terceros por tener acceso a o manejar recursos de información del Banco, están comprometidos a aceptarlos y a cumplirlos para minimizar las amenazas internas o externas, deliberadas o accidentales a que pueda estar expuesta la información del Banco.

1.3 Alcance

Este estándar se aplica a todos los servicios tercerizados donde el Proveedor requiere tener acceso a la información confidencial, confidencial restringido, recursos y/o la administración de sistemas de Información del Banco, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información suministrada por el Banco objeto del contrato.

1.4 Obligaciones y Responsabilidades

Los Terceros deben ser conscientes de las responsabilidades y obligaciones en materia de seguridad de la información y ciberseguridad que están involucradas en el proceso contratado. Para ello, debe aplicar el estándar de seguridad de la información y ciberseguridad del Banco AV Villas de cumplimiento obligatorio durante la vigencia del contrato.

1.5 Requerimientos de Seguridad de la Información y Ciberseguridad

Todo acuerdo de servicios donde se maneje información del Banco debe contener como mínimo los siguientes aspectos:

- Niveles de servicio y operación;
- Responsabilidades y obligaciones del proveedor y del Banco;
- Exigencias de confidencialidad sobre la información manejada y sobre las actividades desarrolladas;
- Derechos de propiedad Intelectual de la Información y Acuerdos de no divulgación;
- Derechos de evaluación, seguimiento y monitoreo por parte del Banco;

- Constancia acreditando el cumplimiento del estándar de seguridad de la información y ciberseguridad física y lógica de acuerdo con el servicio a contratar;
- Programas de formalización y concientización sobre responsabilidades y aspectos de seguridad y ciberseguridad a todo el personal asignado a la ejecución del proceso tercerizado;
- Procedimientos para detectar y reportar eventos de alteración, manipulación ó modificación de la información no autorizada;
- Procedimientos y controles para la entrega y destrucción de la Información manejada por parte del Tercero;
- Planes de contingencia y continuidad del Negocio del servicio contratado; y
- Responsabilidades relacionadas con asuntos legales y frente al cumplimiento de los requisitos contractuales.

1.6 Evaluación, Seguimiento y/o Monitoreo del Servicio Contratado

1.6.1 El Banco, a través del área responsable de la administración del servicio contratado, adelantará procesos de evaluación, seguimiento y/o monitoreos periódicos a la prestación y resultados del servicio contratado acorde con los parámetros definidos en el correspondiente acuerdo de servicio en las instalaciones del Tercero cuando así lo considere pertinente.

1.6.2 Los procesos de evaluación, seguimiento y/o monitoreo son ejecutados directamente por el área responsable de la administración del servicio contratado. Sin embargo, lo anterior no exime a que el Banco a través de la Contraloría General pueda ejecutar procesos de auditoría sobre los temas que ésta considere pertinentes. Los resultados de dichas auditorías son comunicados a través del área responsable de la administración del servicio.

1.7 **Requisitos de seguridad de la información y ciberseguridad**

Para garantizar la protección de la información del Banco, el Tercero debe contar con todas las medidas referenciadas en esta categoría para impedir que la información sea copiada, divulgada, revelada o utilizada en forma indebida o no autorizada.

Para ello, el Tercero debe demostrar que sus instalaciones cuentan con los siguientes aspectos de gestión de seguridad de la información y ciberseguridad:

1.7.1 Disponer del Área de Seguridad de la información y ciberseguridad con roles y responsabilidades que permitan gestionar y custodiar el adecuado manejo de la información de Banco.

1.7.2 Mantener estándares, normas y procedimientos de seguridad de la información y ciberseguridad con el fin de preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su manejo: equipos, software, procedimientos; así como de los recursos humanos que utilizan dichos componentes.

1.7.3 Documentar y actualizar los estándares y procedimientos de manejo de seguridad de la información y ciberseguridad en la medida que se implementan acciones de mejora.

1.7.4 Implementar mecanismos de protección y detección ante la consulta, copia y extracción de la información con propósitos distintos a los inicialmente pactados y contratados.

1.7.5 Contar con estándares restrictivas sobre uso y transferencia de información a través de Internet, correo electrónico, fotocopiadoras y fax.

1.7.6 Establecer estándares de restricción que detecten y bloquen la salida de información del Banco a través de control de dispositivos de almacenamiento extraíbles**,** mensajería instantánea, captura de pantallas, unidades de red y carpetas compartidas, entre otros.

1.7.7 Disponer de resultados de Pruebas de penetración y vulnerabilidades, propias o por Terceros que permitan evaluar la eficacia de los controles establecidos para proteger la información del Banco.

1.7.8 Contar con estándares de gestión documental que indiquen el trato a seguir para la custodia, entrega y/o eliminación de información física y/o lógica suministrada por el Banco.

El Tercero que se contrate debe garantizar gestión y monitoreo continuo del servicio en términos de auditoría, como mínimo los siguientes requerimientos:

1.7.9 Disponer de un área de auditoría interna

1.7.10 Contar con un plan anual de auditoría interna de seguridad de la información y ciberseguridad definido y documentado.

1.7.11 Dentro del programa de auditoría deben incluirse como mínimo los requerimientos de seguridad de la información y ciberseguridad, plasmados tanto en el contrato, en el acuerdo de servicio como en el anexo del nivel de seguridad exigido por el Banco para cumplimiento por parte del Tercero.

1.7.12 Realizar evaluaciones periódicas de riesgos de seguridad de la información y ciberseguridad para identificar amenazas en el ambiente técnico, operativo y funcional que puedan comprometer la seguridad de la información y ciberseguridad del Banco.

1.7.13 Emitir recomendaciones y verificar la implementación de acciones correctivas.

1.7.14 Informar al área administradora del contrato las acciones de mejoras implementadas para fortalecer los controles de seguridad de la información y ciberseguridad establecidas por este estándar.

2 Requerimientos de Seguridad del Recurso Humano

Orientados a reducir el riesgo de omisión o error humano, comisión de ilícitos, uso inadecuado o indebido de activos de información, el Tercero debe proporcionar un grado mínimo de confianza con el personal contratado que por sus funciones y responsabilidades accede permanente a las instalaciones y a las plataformas donde reside información del Banco, teniendo en cuenta los siguientes aspectos:

Selección

2.1 Disponer de procesos de selección definidos para la verificación de la idoneidad del personal a contratar (certificaciones personales, laborales, experiencia y verificación de referencias, entre otras).

Términos y condiciones laborales

2.2 Contar con acuerdos de manejo, acceso y confidencialidad de la información los cuales deben hacerse explícitos desde el momento de la contratación.

2.3 Realizar pruebas o inspecciones periódicas tendientes a mitigar el riesgo de infidelidad por parte del personal sobre documentos, imágenes e información objeto del contrato.

Controles durante la vigencia del contrato

2.4 Disponer del sistema de identificación del personal contratado, mediante la expedición del carnet y la dotación de uniformes sin bolsillo al personal encargado del proceso del servicio contratado, los cuales deben ser de uso obligatorio y permanente.

2.5 Contar con procedimientos documentados que indiquen los parámetros de manejo y procesamiento de la información por parte del personal contratado, especificando que su uso es exclusivo para los fines previstos en el contrato.

2.6 Mantener el acuerdo de derecho a la propiedad intelectual y no revelación de los desarrollos, manejo y operación que se den durante el proceso del servicio contratado que es de propiedad exclusiva del Banco.

2.7 Hacer específico en términos laborales que la responsabilidad frente al manejo de la información se extiende más allá del horario y recinto laboral o tiempo de prestación del servicio.

Educación, formación y concientización sobre la seguridad de la información y ciberseguridad

2.8 Garantizar que el personal contratado por el Tercero tenga pleno conocimiento de los riesgos y consecuencias que se pueden presentar en materia de seguridad y confidencialidad de la información. Para ello, el Tercero debe tener implementados de forma periódica modelos de capacitación y actualización en términos de manejo y seguridad de la información y ciberseguridad que incluyan como mínimo:

- Requerimientos seguridad de la información y ciberseguridad (física, lógica)
- Responsabilidades legales
- Controles existentes
- Uso de recursos (Recursos para el acceso y manejo de la información)

Normas disciplinarias establecidas en la contratación laboral

2.1 Debe contar con procesos disciplinarios formalizados que indiquen las acciones a tomar cuando se evidencien irregularidades en el manejo de información por parte del personal del Tercero que perpetren o colaboren en violaciones de seguridad de la información y ciberseguridad.

3 Requerimientos de Seguridad Física y del Entorno

Destinado a impedir accesos no autorizados, daños o pérdida de activos de información del Banco durante su transporte, en las instalaciones, equipos y medios de almacenamiento custodiados por el Tercero.

Para ello, Tercero debe contemplar como mínimo las siguientes medidas de control:

Seguridad física perimetral

3.1 Dotar de un sistema de seguridad perimetral el entorno en el cual se encuentre ubicada geográficamente las instalaciones el Tercero, con apoyo de vigilancia privada y entes de seguridad del estado.

3.2 Contar con un sistema electrónico de alarma para alertar local o remotamente un intento de intrusión o sabotaje y un sistema de Circuito Cerrado de Televisión con el fin de verificar las alarmas que generan los sistemas perimetrales y la grabación de imágenes de incidencias.

Controles de acceso físico

3.3 Deberá contar con un estándar de control de acceso donde se especifique el proceso a seguir para ingresar a la empresa ya sea a través de bitácoras, registro, puertas esclusas, sistemas biométricos, lectoras de proximidad, la autorización de ingreso y acompañamiento de los visitantes por parte de un funcionario del Tercero.

3.4 Mantener mecanismos que permitan identificar de forma adecuada y oportuna al personal que labora en la empresa (carné, uniforme sin bolsillos). Además, debe garantizar un sistema de identificación para los Terceros que ingresan a las instalaciones (Visitantes, Proveedores, etc.)

Protección de Oficinas, Recintos e Instalaciones

3.5 Mantener señalización con delimitación de zonas y accesos restringidos.

3.6 Acceso restringido a las instalaciones o áreas donde se presta el servicio contratado, las cuales deben estar en un espacio delimitado por barreras físicas fuertes (puertas, rejas, cristales y cerraduras), en el que se ejerce control sobre movimiento y permanencia de funcionarios y visitantes.

3.7 Mantener mecanismos de seguridad que impidan el ingreso y utilización de equipos fotográficos, de video, de audio y demás que permitan el registro y almacenamiento de información (celulares, USB, cámaras, ipods, pocket pc, diskettes).

3.8 En las áreas de procesamiento del servicio contratado restringir el porte de cualquier medio de escritura, papel, lapicero, lápiz, celulares, grabadoras, portátiles y cámaras.

3.9 Disponer de estándares y controles para la protección de la información sensible contenida en medios (CD/DVD, medios magnéticos), documentación, títulos valor, entre otros; custodiados en bóvedas, cajas fuertes o archivadores de seguridad bajo llave, para asegurar el resguardo de información crítica entregada por el Banco.

3.10 Implementar controles para restringir el acceso físico a equipos informáticos, fotográficos, de video, de audio o cualquier otro tipo de dispositivo para evitar el

extravío, manipulación y copia de documentos (físicos y electrónicos), de manera que se proteja su integridad y confidencialidad, al menos que hayan sido formalmente autorizados por el responsable de dicha área o el Responsable de seguridad de la información y ciberseguridad.

Protección contra amenazas externas y ambientales

3.11 Disponer de medidas de protección contra fuego, fallas del fluido eléctrico, falta de condiciones ambientes (Humedad, Temperatura, Aire acondicionado) en las áreas protegidas donde se encuentra la documentación/información sensible y los equipos de cómputo que la albergan.

3.12 Contar con equipos de respuesta ante situaciones de peligro como conato de incendio, inundaciones, desastres, etc.

3.13 Contar con dispositivos que garanticen un adecuado suministro de energía (UPS, planta eléctrica). Cuando no se cuente con dichos equipos se debe garantizar la prestación del servicio en otra sede alterna a la de funcionamiento del Tercero contratado.

Seguridad Áreas de carga, despacho y acceso público

3.14 Debe existir un área destinada para el cargue y descargue de materiales, suministros y elementos, aislada de los procesos de operación vigilada con mecanismos de cámaras de seguridad y monitoreo permanente.

3.15 Mantener control de tráfico de personas, paquetes, correspondencia.

3.16 Contar con estándares que indiquen el proceso a seguir para el ingreso y retiro de equipos tanto dentro como fuera de la organización (Tanto para funcionarios como para personal ajeno a la organización).

Ubicación y protección de los equipos

3.17 Disponer de mecanismo de seguridad para restringir el acceso a las instalaciones de procesamiento u otras áreas de servicios críticos.

3.18 Mantener áreas aisladas para los equipos de trabajo que procesan y almacenan información (Cuartos de cableado, centro de cómputo, áreas de digitalización, áreas de bóveda y custodia).

3.19 Ubicar los equipos de impresión como impresoras, fotocopiadoras, máquinas de fax en un sitio que permita la supervisión durante su uso.

Seguridad en la reutilización o eliminación de los equipos

3.21 Los dispositivos que contienen información clasificada como confidencial y confidencial restringida deben ser sometidos a un proceso de borrado seguro mediante el uso de herramientas especializadas que permitan que la información original no se pueda recuperar.

4 Requerimientos de seguridad lógica

Para evitar posible acceso o uso indebido, pérdida o fuga, alteración o divulgación no autorizada de la información del Banco que se alberga en las instalaciones del Tercero.

Gestión de la seguridad de redes

El Tercero debe garantizar control y monitoreo permanente sobre los diferentes canales que se utilicen, por lo anterior, se deben considerar los siguientes aspectos:

4.1 Las conexiones a la red privada del Banco AV Villas y hacia otras redes externas deben realizarse de una manera segura para preservar la confidencialidad, integridad, disponibilidad y privacidad de la información trasmitida sobre la red.

4.2 Toda conexión desde o hacia Internet que envía información sensible y confidencial al Banco debe utilizar mecanismos de cifrado y autenticación.

4.3 Toda la conexión de red externa hacia la entidad el canal debe cifrase y realizarse la transmisión a través del firewall habilitando los servicios y puertos requeridos.

4.4 Mantener control y gestión sobre los equipos de comunicación para asegurar el acceso a la red basado en listas de autenticación de dispositivos por dirección físicas MAC mitigando posibles conexiones de dispositivos de red no corporativos.

4.5 Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que soporta la red, manteniendo independencia del segmento de red de procesamiento de la información de otras áreas administrativas

4.6 Retirar privilegios y restringir comandos de administración sobre los equipos que albergan o procesan información del Banco con el fin de evitar copias o modificaciones no autorizadas sobre los mismos.

4.7 Realizar revisiones periódicas de los logs del sistema y de la red (En lo posible se debe mantener registro de dichas revisiones).

Intercambio de Información

El intercambio de información y de software debe ser protegido contra la interceptación, extracción, alteración, transmisión incompleta, repeticiones, envíos incorrectos y negación del servicio, sin importar el medio o servicio de comunicación que se utilice.

Por lo tanto se deben cumplir con los siguientes aspectos:

4.8 Todo intercambio de información confidencial que se haga entre el Banco y los Terceros debe hacerse cifrando los archivos a transmitir.

4.9 Si el intercambio de información con los Terceros se realiza a través de correo electrónico se debe emplear certificados digitales.

Control de Acceso lógico

Para prevenir accesos no autorizados y uso indebido de la información confidencial y confidencial restringida del Banco, el Tercero debe garantizar que sólo los usuarios autorizados tengan los debidos privilegios sobre la información proporcionada por el Banco, otorgándoles sólo los mínimos permisos posibles.

Gestión de cuentas de usuarios y contraseñas

4.10 Acceso restringido de los usuarios a los sistemas mediante la utilización de cuentas de usuario (únicas, personales e intransferibles) con contraseñas complejas y cambio periódico, estándares que deben estar reglamentadas por directivas locales o por dominio.

4.11 Implementar el uso de cuentas personalizadas en el esquema de autenticación sobre la plataforma operacional (estaciones de trabajo, servidores, aplicaciones) del Tercero donde se maneja la información del Banco.

4.12 Contar con un estándar frente al manejo de usuarios y contraseñas que indique como mínimo los responsables de su asignación, el tiempo de respuesta y los términos de bloqueo y eliminación de estas. Así mismo, dicho estándar debe indicar el tiempo de renovación de la misma por parte de los usuarios.

4.13 Las cuentas de usuario deben ser bloqueadas después de tres intentos fallidos al ingresar una contraseña inválida.

4.14 Mantener registros actualizados que indiquen como mínimo el usuario, fecha, hora, e información consultada sobre los diferentes aplicativos (manejo de logs).

4.15 Restringir el uso compartido de las cuentas de usuarios como de las llaves de desciframiento asignadas por el Banco a los Terceros para el ingreso al sistema y el acceso a los servicios de transferencia segura de la información.

Gestión de Privilegios

4.16 Los privilegios asignados a los usuarios para el manejo de la información del Banco deben estar en concordancia con las funciones y responsabilidades, con el fin de evitar otorgar más atribuciones de las requeridas.

4.17 Aplicar estándares globales o locales restrictivas que mitiguen la elevación de privilegios y accesos.

4.18 Contar con un estándar documentada frente a los derechos de acceso a la información del Banco (Copia, procesamiento, transformación, consulta y eliminación de información)

4.19 Revisar regularmente los perfiles otorgados con el fin de asegurar que no haya derechos de accesos asignados a usuarios no autorizados o privilegios no necesarios para el desarrollo de su función.

4.20 Restringir el acceso a herramientas y archivos de los sistemas operacionales, comando ejecutar, panel de control, consolas de administración de sistemas operativos, unidades de red, unidades locales, usuarios limitados sobre los equipos, editores de texto, entre otros, sólo a las funciones autorizadas a ejecutar.

Controles contra Código Malicioso

Para salvaguardar la confidencialidad e integridad de la información entregada

4.21 El Tercero debe contar con una solución de antivirus, debidamente administrada, actualizada y configurada para sus escaneos, reparación y eliminación de software malicioso sobre los servidores y las estaciones de trabajo donde reside

y opera información y/o servicio contratado, como mecanismo de prevención, detección y corrección de software malicioso.

4.22 Mantener gestión periódica de parches críticos y de seguridad sobre los sistemas operativos con el fin de salvaguardar la plataforma y la red de las posibles vulnerabilidades que puedan afectar información y/o servicio contratado del Banco.

Controles contra Fuga de Información

Debe mantener los siguientes controles sobre cuentas de usuarios, estaciones de trabajo y servidores para restringir la copia y divulgación de información del Banco.

4.23 Restringir acceso a enlaces de Internet desde los cuales pueda presentarse fuga de información a través de correos personales, redes sociales, ftp o lugares de almacenamiento no corporativos, entre otros.

4.24 Restringir acceso a Internet por filtros por listas blancas a través de PROXY o Firewall según el medio utilizado por el Tercero.

4.25 Controlar la información saliente por medio de herramientas de filtro de contenido, o en su defecto con aplicación de mecanismos de restricción de salida de correos en el que se limite el origen y destino de acuerdo con las necesidades del servicio contratado.

4.26 Restringir el uso de dispositivos de almacenamiento USB, SERIAL, WIFI, BLUETOOTH físico y lógico mediante aplicaciones y/o setup del equipo.

4.27 Restringir el uso de dispositivos o conexiones inalámbricas en el área del proceso contratado.

4.28 Restringir el uso y transferencia de información del Banco a través de Internet, correo electrónico, mensajería instantánea, fotocopiadoras y fax.

Gestión de los recursos de Información del Banco almacenada en equipos del Tercero

4.29 Para restringir el acceso a la información guardada en carpetas, se deben limitar los privilegios de ingreso al grupo de usuarios autorizados con los permisos según la necesidad (excepto control total), además del retiro del grupo especial ‘everyone’ sobre cada una de las carpetas compartidas y su contenido.

El Tercero que procesa y almacena en sus bases de datos información de un producto o un servicio del Banco además de garantizar que su manejo es exclusivo para los fines contratados, debe cumplir con los siguientes requisitos:

4.30 Tener una definición de estándares para la gestión de Bases de Datos.

4.31 Contar con la definición estructurada de usuarios y privilegios de gestión sobre las bases de datos (DBA).

4.32 Los datos del Banco por ser información confidencial y confidencial restringida deben mantenerse en instancias independientes y/o unidades almacenamiento no compartido con la data de otras organizaciones.

4.33 Contar con un procedimiento documentado y divulgado de Control de cambios a nivel de las BD y/o aplicaciones.

4.34 Almacenar cifrada la Información confidencial y confidencial restringida del Banco en las Bases de Datos mediante mecanismo algoritmos fuertes de cifrado.

4.35 Tener estándares de backup de aplicaciones.

4.36 Contar con logs de las aplicaciones que tienen acceso a la información confidencial del Banco y realizar revisiones periódicas de los mismos. (En lo posible se debe dejar registro de dichas revisiones)

4.37 Disponer de un plan de contingencia para el funcionamiento y continuidad de la Base de datos

4.38 Contar con procedimientos de seguridad establecidos para la eliminación de los archivos con información del Banco una vez concluido el proceso operativo contratado, dejando constancia de la eliminación realizada.

Los Terceros donde se realicen procesos de realce, estampado, grabado y magnetización de tarjetas, entre otros, así como de la impresión del scrash off, deben garantizar además los siguientes controles:

4.39 Contar con procedimientos, controles y medidas de seguridad orientadas a evitar que la información relacionada pueda ser copiada, modificada o utilizada con fines diferentes a los de la fabricación de la misma.

4.40 Contar con procedimientos y controles que garanticen la destrucción de aquellas tarjetas y scrash off que no superen las pruebas de calidad establecidas para su elaboración, así como la información de los clientes utilizada durante el proceso.

4.41 Disponer de procedimientos y controles que garanticen la eliminación y destrucción automática de la información transmitida del Banco (archivos o cualquier medio de almacenamiento), concluida la ejecución correcta de la orden de personalización del servicio contratado.

Eliminación/Destrucción de Documentos/Información

4.42 Establecer un acuerdo específico de eliminación de datos/información o documentos objeto del servicio contratado, donde se garantice por parte del Tercero la eliminación de los datos transmitidos por el Banco de su plataforma, concluida la ejecución correcta de la orden del servicio contratado, dejando registro de la acción realizada.

4.43 En caso de destrucción de información almacenada en bases de datos se debe establecer un acuerdo indicando la frecuencia y las condiciones para adelantar dicha actividad en presencia del área responsable del contrato y suscribiendo el acta correspondiente.

4.44 Los datos de pruebas entregados a los Terceros serán canalizados únicamente a través del área del Banco que administra el contrato, quien determina la permanencia y eliminación de la plataforma del Tercero.

Respuesta a incidentes y Anomalías en materia de seguridad de la información y ciberseguridad

4.45 Programar pruebas de penetración y de vulnerabilidades sobre la red y servidores, mínimo cuatro veces al año manteniendo los registros de las amenazas detectadas y las acciones de mejora para corregirlas según los reportes obtenidos.

4.46 Identificar y reportar al área administradora del contrato del Banco, los incidentes que se presenten en materia de seguridad física y lógica, con el con el objeto de minimizar sus efectos y reducir su reincidencia.

4.47. Garantizar el uso de mecanismos, herramientas y procedimientos para el monitoreo y recolección de logs en los recursos tecnológicos, que hagan parte de la plataforma que soporta el servicio que se le brinda al BAVV.

4.48. En caso de que sea requerido por necesidad del BAVV, se debe garantizar la posibilidad de compartir Logs, en un formato compatible con las herramientas de seguridad de la entidad.

5. Requerimientos de Seguridad para el Desarrollo de Software

Para los casos donde el Tercero (Proveedor) suministre desarrollos propios o distribuya productos de software, este debe:

5.47. Contar con políticas y procedimientos que garanticen calidad y seguridad a nivel de desarrollo.

5.48. Garantizar el uso de guías y buenas prácticas de seguridad para el desarrollo.

5.49. Garantizar la ejecución y aprobación de pruebas estáticas y dinámicas basadas en OWASP, sobre el producto final.

5.50. Disponer de informes que certifiquen la NO existencia de vulnerabilidades en el código del producto final.

5.51. Garantizar la emisión continua y oportuna de parches o mejoras que se requieran sobre el producto.

5.52. Garantizar el uso e implementación de un flujo o procedimiento para la ejecución de controles de gestión de cambios, instalación de parches de seguridad y las actualizaciones requeridas por el fabricante. Estas deberán ser evaluadas inicialmente en un ambiente de prueba o testing, antes del despliegue en ambientes productivos.

6. Requisitos de Aseguramiento (Hardening)

Para los casos donde el Tercero (Proveedor) que Acceda, almacenen y/o procese información confidencial del banco, este debe

6.47. Contar con políticas y procedimientos que regulen la gestión de aseguramiento (hardening) en la plataforma tecnológica que soporta el servicio.

6.48. Garantizar la implementación y actualización periódica de guías de aseguramiento (hardening) para las máquinas y dispositivos de red relacionadas con el servicio contratado, con base en estándares internacionales, ejemplo CIS.

6.49. Garantizar que todos los sistemas operativos de los equipos relacionados con la operación del servicio contratado cuentan con las últimas actualizaciones de seguridad del fabricante.

6.50. Disponer de un informe de análisis de vulnerabilidades que garantice la aplicación de las guías de aseguramiento implementadas y la no existencia de vulnerabilidades para la plataforma tecnológica que soporte el servicio contratado.

7 Requerimientos del plan de continuidad

Orientado a contrarrestar las interrupciones de las actividades tercerizadas y proteger los procesos críticos contratados de los efectos de fallas significativas o desastres.

El Tercero debe contar con un panorama de riesgos de continuidad del negocio que pueda afectar la prestación del servicio que ofrece al Banco AV Villas; estos deben tener probabilidad, impacto, controles y planes de acción en caso de materializarse, por lo anterior el Tercero deben garantizar:

7.1 Una prestación continúa del servicio manteniendo los requisitos de seguridad y de operación del servicio acordado, suministrándolo en un tiempo de respuesta óptimo frente a los requerimientos del Banco.

7.2 Desarrollar, probar e implementar en los planes de continuidad los requisitos de seguridad de la información y ciberseguridad necesarios para proteger la información para la continuidad del servicio.

7.3 Tener máquinas de respaldo tanto para los servidores como para las estaciones de trabajo cuando así se requiera y tener procedimientos de respaldo de los archivos vitales y documentos físicos importantes en el proceso. Con las mismas restricciones de seguridad aplicadas en la sede principal.

7.4 Contar con procesos de capacitación para las personas que tienen algún rol en el proceso de Continuidad del Negocio y para todos los funcionarios en general, a través de los cuales se definan claramente las responsabilidades y el proceso a ejecutar para la recuperación ante eventos fortuitos dependiendo del rol establecido.

7.5 Desarrollar y revisar periódicamente pruebas al plan de contingencia y continuidad para asegurar su actualización y eficacia con el fin de verificar si estos planes presentados funcionan en las condiciones de seguridad acordadas y aceptadas por el Tercero.

7.6 Operar semestralmente por lo menos un día con el centro de contingencia para garantizar su correcto funcionamiento.

7.7 Mantener los resultados de las pruebas de continuidad y los planes de acción formulados de acuerdo con las fallas registradas.

7.8 Contar con sedes, oficinas o ubicaciones alternas de trabajo que permitan dar continuidad en la prestación del servicio contratado. (En calidad de préstamo y no necesariamente de propiedad del Tercero).

8. Requerimientos para el uso de Dispositivos Móviles.

Los terceros que por necesidades del servicio ofrecido al Banco AV Villas utilice dispositivos móviles personales y/o corporativos para acceder a los recursos de la organización deben garantizar:

8.1. Garantizar que en los dispositivos móviles:

- Estén instaladas las versiones de sistemas operativos que tengan soporte de seguridad por el fabricante.
- No este rooteado (Android) o con Jailbreak (iOS).

8.2. Los colaboradores de los terceros asociados con el alcance del servicio contratado que requiera el uso de aplicaciones corporativas en su dispositivo móvil y tenga sistema operativo Android deben instalar la herramienta (MAM) usada por el Banco AV Villas y se deben vincular en los grupos del Directorio Activo al colaborador autorizado para usar aplicaciones corporativas en dispositivos móviles, así como tener una licencia asignada del MAM usada por el Banco AV Villas.

8.3. Los colaboradores de los terceros asociados con el alcance del servicio contratado deben garantizar que:

- La confidencialidad de la información del Banco a la que tiene alcance, usando los controles de seguridad dispuestos para tal fin.
- Apliquen y validen regularmente las actualizaciones de seguridad y los parches de software proporcionados por el fabricante para mantener sus dispositivos móviles protegidos.
- Reportar en caso de perdida, robo, novedad o anomalía que se presente con el dispositivo móvil a la mesa de ayuda (avvillas-mds@bancoavvillas.com.co), así como a los equipos de seguridad informática (seguridadinformatica@bancoavvillas.com.co) y seguridad de la información (seguridaddelainformación@bancoavvillas.com.co). Esto permitirá llevar a cabo los procedimientos adecuados para salvaguardar la confidencialidad, integridad, disponibilidad y privacidad de la información sensible del Banco y de datos personales.
- Hacer un uso responsable y seguro de sus dispositivos móviles para evitar que se pueda llegar a comprometer la seguridad de la información y/o la reputación del Banco con el uso y acceso a las aplicaciones autorizadas.
- Cumplir con las capacitaciones y concientizaciones remitidas por seguridad de la información y aplicar los controles para el uso de herramientas en los dispositivos móviles.
- Configurar mecanismos seguros de bloqueo de pantalla de cada dispositivo móvil, mediante el uso de contraseña y/o autenticación biométrica como huella digital o Face ID.
- Configurar el bloqueo del dispositivo debe configurarse de manera automática con un tiempo no mayor a 1 minuto de inactividad.

9. Responsabilidades por incumplimiento de requisitos legales, reglamentarios y contractuales

El incumplimiento de este estándar constituirá infracción a las normas de seguridad de la información y ciberseguridad exigidas por el Banco AV Villas y a la normatividad exigida por los entes regulatorios y en consecuencia hace acreedor al Tercero de la totalidad de los perjuicios y de sanciones legales que se causen al Banco.

.