Anexo A
Seguridad de la información

TABLA DE CONTENIDO

1 CRITERIOS

1.1 CRITERIOS DE SEGURIDAD DE LA INFORMACIÓN

a) **Confidencialidad**: Hace referencia a la protección de información cuya divulgación no está autorizada.

b) **Integridad**: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

c) **Disponibilidad**: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

1.2 CRITERIOS DE CALIDAD DE LA INFORMACIÓN

a) **Efectividad**: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.

b) **Eficiencia**: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.

c) **Confiabilidad**: La información debe ser la apropiada para la administración de la Entidad y el cumplimiento de sus obligaciones.

2 DEFINICIONES

1. **Vulnerabilidad informática**: Ausencia o deficiencia que permite violar las medidas de seguridad informáticas para poder acceder a un canal de distribución o a un sistema específico de forma no autorizada y emplearlo en beneficio propio o como origen u objetivo de ataques por parte de terceros.

2. **Cifrado fuerte**: Técnicas de codificación para protección de la información que utilizan algoritmos de robustez reconocidos internacionalmente, brindando al menos los niveles de seguridad ofrecidos por 3DES y/o AES.

3 CONDICIONES GENERALES DE SEGURIDAD

El Oferente certifica que cumple con las condiciones aquí expuestas o que estarán disponibles en el momento del inicio de prestación de servicios al Banco:

1. Política de Seguridad: Contar con un documento de políticas de seguridad aprobado por la Alta Dirección del Oferente y publicado formalmente.

2. Organización de la Seguridad de la Información: Tener formalizada y en operación una estructura organizacional que defina los roles y responsabilidades frente a la seguridad de la información.

3. Gestión de los Activos: Todos los activos que conforman la infraestructura informática que soporta la operación del Oferente y los servicios ofrecidos estarán configurados con base en un estándar aprobado de seguridad, definido con base en las mejores prácticas de seguridad de la industria.

4. Seguridad del Recurso Humano: Garantizar que los procesos de administración de personal ponen en práctica los aspectos relacionados con la seguridad de la información para que los empleados y terceros con acceso a los recursos de información del Oferente y de sus clientes, se administren y usen de acuerdo con la política de seguridad definida.

5. Seguridad Física y del Entorno: Tener implantados controles de acceso físico y mecanismos de identificación y autenticación que protejan contra acceso físico no autorizado a las áreas que almacenan los recursos de información o informáticos usados para la prestación de los servicios y dichos controles son monitoreados de forma continua, manteniendo el registro de los accesos y resguardando los registros de CCTV generados por acceso a los centros de datos.

6. Gestión de Comunicaciones y Operaciones: tener implantadas medidas de prevención y protección de la infraestructura así como prácticas seguras en los procesos de actualización o cambio de la infraestructura informática que soporta los servicios para reducir y prevenir posibles cambios no controlados que pudieran generar riesgos o vulnerabilidades que afecten la seguridad de la infraestructura o los servicios.

7. Control de Acceso: Garantizar que sólo las personas y los dispositivos autorizados (por ejemplo dispositivos gestionados por protocolo SNMP) pueden realizar actividades de gestión o administración en los dispositivos de red o el enlace de comunicaciones, o tener acceso a la información procesada o transmitida por la infraestructura usada para la prestación de los servicios. Los accesos a dichos dispositivos son asignados bajo el principio del menor privilegio.

8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información: garantizar que para la infraestructura y para las aplicaciones - sean adquiridas o desarrolladas internamente - se aplica un proceso seguro en su ciclo de vida, acorde con estándares y regulaciones de la industria (PCI, SOX, ISO 27000).

9. Gestión de Incidentes de la Seguridad de la Información: contar con un procedimiento de reporte y gestión de incidentes que incluya la identificación, respuesta, recuperación y revisión post-implementación de los incidentes de seguridad de la información. Este procedimiento considera la interacción con las áreas y responsables del manejo de estos incidentes en el Banco cuando puedan comprometer la seguridad en la prestación de los servicios.

10. Gestión de la Continuidad del Negocio: Tener implantados procesos de gestión de continuidad del negocio que propendan, entre otros aspectos, por la seguridad de la información en los posibles eventos que requieran su activación.

11. Cumplimiento: Definir y ejecutar periódicamente, al menos una vez al año, un programa de verificación, tanto a nivel administrativo como técnico, del cumplimiento de las definiciones de seguridad y de las normas legales e institucionales que rigen la prestación de los servicios.

12. Autenticación: Verificar la identidad de la persona o el dispositivo que realiza la actividad de gestión administrativa, que observa o modifica información de control en el dispositivo de red o el enlace de comunicaciones, o que tiene acceso a los recursos o datos que transitan o se almacenan en cualquier elemento, conectado o no, usado para la prestación de los servicios ofrecidos. La autenticación debe ser fuerte, generar registros y forzar los cambios de contraseñas. Los controles implementados facilitan el monitoreo y la revisión de las actividades de los usuarios privilegiados (ej.: súper usuarios, administradores, DBAs, o personas con acceso a información sensible o crítica).

13. No repudio: Crear y mantener un registro de las personas o dispositivos que realizan cada actividad de gestión y de las personas que han observado, modificado o tenido acceso a la información en los dispositivos de red o en el enlace de comunicaciones, así como de las acciones realizadas.

14. Confidencialidad de los datos: Proteger la información de configuración y gestión de los servicios y dispositivos de red, los enlaces de comunicaciones y cualquier información de sus clientes contra el acceso o la consulta no autorizados. Esta protección se aplica a la información de configuración que reside en los dispositivos de red y/o en los enlaces de comunicaciones, la información de configuración y/o de los clientes que se transmite por los dispositivos de red o por los enlaces de comunicaciones, y a la información de configuración duplicada para seguridad y almacenada en sistemas no conectados.

15. Seguridad de la comunicación: En el caso de la gestión remota de un dispositivo de red o un enlace de comunicaciones, garantizar que la información de gestión sólo circula entre las estaciones de gestión remotas y los dispositivos o enlaces de comunicaciones gestionados. La información de gestión no debe ser

desviada ni interceptada entre estos puntos extremos. Esta protección incluye la información administrativa de autenticación. Los datos de los usuarios que transitan por un elemento de red o por un enlace de comunicación no pueden ser desviados ni interceptados entre estos puntos extremos sin una autorización de acceso (por ejemplo, interceptación legal).

16. Integridad de los datos: Proteger la información de configuración de dispositivos de red o enlaces de comunicaciones contra creación, modificación, eliminación y retransmisión sin autorización. Esta protección se aplica a la información de configuración que reside en el dispositivo de red o de enlace de comunicaciones, y también a la información de configuración que está en tránsito o almacenada en sistemas no conectados. Proteger contra modificación, supresión, creación y regeneración sin autorización, la información de control y los datos de los usuarios que residen en los dispositivos de red, que están en tránsito por la red o que son almacenados fuera de línea.

17. Privacidad: Garantizar que la información que permite identificar el dispositivo de red, el enlace de comunicaciones o los sistemas para administración de la aplicación de red no está disponible para personas y dispositivos no autorizados. Garantizar que los elementos de red no proporcionan información sobre las actividades de los usuarios (por ejemplo, la posición geográfica del usuario o los sitios web visitados, parte de llamadas en un servicio VoIP, etc.) a personas o dispositivos no autorizados.

4 CONDICIONES PARTICULARES DE SEGURIDAD

El Oferente se responsabiliza de cumplir los siguientes requerimientos y de hacer validaciones periódicas con el fin de comprobar su funcionamiento:

1. Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información del Banco y de sus clientes en condiciones de seguridad y calidad.

2. Velar porque los niveles de seguridad de los elementos usados en los canales no se vean disminuidos durante toda su vida útil.

3. Establecer los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo sólo los pueda realizar personal debidamente autorizado.

4. Realizar una adecuada segregación de funciones del personal que administre, opere, mantenga y, en general, tenga la posibilidad de acceder a los dispositivos y sistemas usados en los distintos canales y medios. En desarrollo de lo anterior,

establecerlos y aplicar los procedimientos y controles para el alistamiento, transporte, instalación y mantenimiento de los dispositivos usados en los canales de distribución de servicios.

5. Sincronizar todos los relojes de los sistemas de información involucrados en los canales de distribución, teniendo como referencia la hora oficial suministrada por la Superintendencia de Industria y Comercio de Colombia.

6. Configurar los equipos utilizados para la prestación de los servicios contratados con los estándares técnicos de seguridad y tener en operación sólo los protocolos, servicios, aplicaciones, usuarios, equipos, entre otros, necesarios para la prestación de los servicios.

7. Contar con controles y alarmas que informen sobre el estado de los canales, y además permitan identificar y corregir las fallas oportunamente.

8. A solicitud del Banco, presentar los informes acerca de los siguientes aspectos:

    a. Restricciones sobre el software empleado.
    b. Normas de seguridad informática y física a ser aplicadas.
    c. Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de equipos o información.
    d. Procedimientos y controles para la entrega de la información manejada y la devolución o destrucción de la misma por parte del Oferente una vez finalizado el servicio.

9. Llevar el registro de las actividades adelantadas sobre los dispositivos finales usados en los canales de distribución de servicios, cuando se realice su alistamiento, transporte, mantenimiento, instalación y activación.

10. Contar con soporte por parte del fabricante o proveedor para los sistemas informáticos empleados para la prestación de servicios.

11. El Oferente garantiza que cumplirá con las normas expedidas por la Superintendencia Financiera para la encripción de los canales de comunicación utilizados para la prestación de los servicios. El Oferente evaluará con regularidad la efectividad y vigencia de los mecanismos de cifrado adoptados.

12. En caso de que se requiera de encripción, los dispositivos utilizados soportarán el intercambio dinámico de llaves. Adicionalmente se implementará el intercambio dinámico de llaves entre los sistemas de cifrado, con la frecuencia necesaria para dotar de seguridad a las operaciones realizadas; si el intercambio de llaves es automático no se deberá requerir intervención del Oferente.

13. Garantizar que los procesos, procedimientos e infraestructura que soportan la prestación de los servicios ofrecidos y que a su vez soportan la operación del Banco, facilitan el cumplimiento de las regulaciones locales e internacionales actuales (Circulares de la Superintendencia Financiera de Colombia, SOX, PCI) y que se aplicarán los ajustes pertinentes que se requieran para poder dar cumplimiento a las regulaciones futuras.

14. Contratar con un proveedor externo idóneo, como mínimo dos veces al año, una prueba de vulnerabilidad y penetración sobre un mínimo del 10% de la infraestructura, el software base y las aplicaciones utilizados por el Oferente para la prestación de los servicios. Cuando se realizan cambios en dicha infraestructura que puedan afectar la seguridad, se contratará la ejecución de una prueba adicional. Los informes generados producto de esta validación serán enviados a los responsables de los servicios en el Banco. Los planes de acción que surjan de este análisis se aplicarán al 100 % de la infraestructura utilizada por el Oferente para la prestación de los servicios.

15. Mantener documentada y actualizada, al menos, la siguiente información: parámetros de los equipos utilizados para la prestación de los servicios, incluido el ambiente de comunicaciones; versión del software en uso; soportes de las pruebas realizadas a los sistemas en operación; y procedimientos de instalación del software. Si durante la prestación de los servicios esta información es requerida para alguna Entidad, el Proponente está en capacidad de entregar un informe actualizado a la fecha de la solicitud o, como máximo, al mes anterior.

16. Generar de manera automática, por lo menos dos veces al año, un informe consolidado de las vulnerabilidades encontradas en la plataforma informática que soporta los servicios ofrecidos. Los informes generados producto de esta verificación son enviados a los responsables de los servicios en el cliente.

17. Aplicar las medidas necesarias para remediar las vulnerabilidades detectadas. Los correctivos a implementar serán presentados inmediatamente después de detectar la vulnerabilidad y serán aplicados después de ser autorizados por el Banco o de inmediato si el riesgo para la operación es crítico. Las revisiones y los informes sobre los análisis de vulnerabilidad tomarán como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org).

18. Tener implementadas las defensas contra malware en toda la infraestructura que soporta la prestación de los servicios.

19. Contar con las medidas y mecanismos automáticos de control de dispositivos en las redes inalámbricas.

20. El personal encargado del Sistema de Gestión de Seguridad del Oferente debe contar con las habilidades y el apropiado entrenamiento en seguridad.

21. Contar con procesos, procedimientos, respaldo, estándares y requerimientos legales, asociados a la generación, administración, mantenimiento, monitoreo y análisis de los logs de auditoría y seguridad. Los controles de acceso estarán basados en la necesidad de conocer y se tendrán implementados mecanismos o procesos de control y monitoreo de cuentas de usuarios.

22. Implementar herramientas o controles que eviten la pérdida o la fuga de información y de datos.

23. Llevar a cabo una gestión de riesgos de información para los aspectos claves del servicio, de forma regular y consistente, utilizando una metodología estructurada.

24. Aplicar un método para identificar, mantener y proteger la información privada, de propiedad intelectual, transaccional o información personal.

25. Suministrar redes robustas y resistentes que puedan soportar los niveles de tráfico requeridos por el Banco, incorporando los dispositivos y medidas de seguridad que garanticen el control de acceso y la protección ante posibles ataques informáticos.

26. Separar las bases de datos de un cliente de los otros, tanto física como lógicamente.

27. Restringir el uso de dispositivos no aprobados y deshabilitar la función de copia de datos sin autorización.

28. Llevar a cabo un monitoreo continuo de los sistemas y redes utilizados para la prestación de los servicios, empleando sistemas de detección de intrusos (IDS, IPS) y registro y gestión de los eventos de seguridad.

29. Tener implementado un proceso de gestión de cambios para la información y los sistemas, que incluya pruebas y aceptación de los cambios y evaluación de las implicaciones de seguridad.

30. Llevar a cabo regularmente auditorias de seguridad independientes y, en caso de requerirse, facilitar al Banco el acceso a los resultados.

31. Ofrecer la facilidad para que, en cualquier momento, el Banco realice procesos de auditoría sobre la infraestructura y los procesos directamente relacionados con la prestación de los servicios ofrecidos.

32. Tener implementadas las defensas contra ataques de negación de servicio (DoS - por las siglas en ingles de Denial of Service) y contra ataques distribuidos de negación de servicio (DDOS - por las siglas en ingles de Distributed Denial of Service) en toda la infraestructura que soporta la prestación de los servicios. Esta protección debe evitar la inundación por tráfico de los canales de conexión a internet del Banco.

33. Garantizar que los servicios de encripción o cifrado de redes se ofrece con protocolos y estándares reconocidos y avalados por las regulaciones y estándares locales e internacionales.