Manual general

MG1145 Políticas y normas de seguridad de la información para proveedores

Manual general

Introducción

La información administrada, procesada y trasmitida por los proveedores del Banco Itaú Colombia y Filiales (en adelante Banco) es considerada como un activo de alto valor, por tanto, es esencial que se establezcan controles de seguridad de la información y ciberseguridad para que a través de la gestión de los terceros esta se proteja.

Este documento establece las políticas de seguridad de la información y ciberseguridad que deben cumplir todos los proveedores del banco. La elaboración de este se basa en estándares internacionales y buenas prácticas tales como: legislación local vigente (Circular Básica Jurídica de la Superintendencia Financiera de Colombia), estándares internacionales ISO/IEC 27001:2022 e ISO/IEC 27032, NIST Cybersecurity Framework, PCI-DSS, normativa emitida por la Gerencia de Seguridad de la información y gobierno de ciberseguridad y políticas emitidas por casa matriz.

La seguridad de la información es una prioridad para el Banco, por tanto, es responsabilidad del proveedor velar por la adecuada gestión y aplicación en su interior, por lo cual se deben comprometer con:

- **La protección de la información** asegurando la confidencialidad, integridad, disponibilidad, auditabilidad, efectividad, eficiencia y confiabilidad, en la manipulación, custodia y correcto uso de la información utilizada por los usuarios internos y externos.

- **El cumplimiento de las normas y marcos legales** a través del conocimiento, acatamiento y alineación de nuestra actuación, conforme a las disposiciones legales emitidas por entes de control nacional e internacional y los acuerdos contractuales establecidos con terceras partes.

- **La protección de los recursos tecnológicos** implementando medidas para asegurar los componentes de la infraestructura tecnológica empleados para la prestación de servicios de T.I.

- **La continuidad del negocio** gestionando los riesgos asociados a los activos de información, velando por la continuidad de los procesos críticos ante incidentes.

1. Descripción general

1.1 Objeto general

Dar a conocer los requisitos mínimos y parámetros de seguridad de la información y ciberseguridad, para establecer controles efectivos sobre las actividades de los terceros involucrados en la operación y empresas que prestan servicios al Banco, garantizando el correcto uso de los sistemas, herramientas, recursos e información en cualquier medio magnético y físico, ya sea generada, procesada o almacenada de manera local o en el ciberespacio por los proveedores del banco.

1.2 Principios

Los principios sobre los cuales los proveedores deben establecer la seguridad de la información y ciberseguridad son:

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

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

- **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.

1.3 Alcance

Las políticas de seguridad de la información y ciberseguridad cubren aspectos administrativos y de control que deben ser cumplidos por todos los proveedores que sostengan cualquier relación contractual con el Banco.

1.4 Audiencia objetivo

Las presentes políticas están dirigidas a todos los terceros (proveedores, contratistas y empresas con las que se intercambie información) del Banco. Quienes las deben conocer y tener en cuenta para la realización de sus actividades diarias, en procura de salvaguardar la seguridad y calidad de la información utilizada.

1.5 Propiedad y actualización de este documento

La Vicepresidencia de Riesgos del Banco ha delegado la propiedad de este documento a la Gerencia de Seguridad de la Información y Gobierno de Ciberseguridad quien es responsable de mantenerlo actualizado realizando la revisión de este documento mínimo una vez al año y en caso de realizar ajustes de fondo, deberá presentarlo ante la comisión superior de seguridad digital y prevención de fraudes y debe ser publicado en un lugar accesible y comunicado a todos los empleados relevantes y partes externas.

2. Contenido

A continuación, se detalla la compilación de las directrices generales dispuestas para guiar las gestiones que los proveedores del Banco deben aplicar para mantener un adecuado nivel de seguridad de la información y ciberseguridad, así mismo, se presentan los lineamientos y políticas de seguridad de la información y ciberseguridad definidas por el Banco para que sean aplicadas por los proveedores.

Los proveedores y los terceros deben, implementar medidas diseñadas para cumplir con los requerimientos del programa de seguridad de la información y el plan de gestión de riesgos en ciberseguridad del Banco, el cual debe ser divulgado por las áreas responsables de proveedores y/o servicios prestados por terceros.

2.1 Seguridad de los recursos humanos

El proveedor debe contar con un proceso de selección que incluya como mínimo aspectos como: Verificación de la información personal, académica, laboral y legal de sus candidatos, definición de procesos disciplinarios para los casos de incumplimientos a políticas internas y reglas para el proceso de desvinculación de sus colaboradores.

2.2 Acuerdo de confidencialidad y no divulgación

Los proveedores que por justificación de negocio tendrán acceso a la información del banco, deben firmar una cláusula de confidencialidad, donde se exprese la autorización del banco. Si un funcionario de los terceros contratados viola las disposiciones de las políticas de seguridad, por negligencia o intencionalmente, el banco se reserva el derecho de tomar las acciones legales, reclamo de compensación por daños, u otras.

El proveedor se compromete a mantener toda la información que reciba bajo la más estricta confidencialidad en todo momento; comprometiéndose a cumplir con los Deberes de Reserva Legal a que está sujeta la información, y obligándose a no compartirla con ningún tercero sin autorización previa por parte del banco.

Para evitar la divulgación no autorizada de la información se debe contar con acuerdos de confidencialidad y No divulgación de sus empleados y terceros, donde se describa las responsabilidades y acciones, manteniendo la confidencialidad de toda la información a la que se acceda.

2.3 Programa de concientización y educación en seguridad de la información

Deben contar con un programa formal establecido con el objetivo de sensibilizar a los empleados y terceros sobre temas de seguridad de la información, el valor de la información y su papel en la protección de este activo.

2.4 Control de acceso lógico

Se deben contar con una política de control de accesos físico y lógico, documentada y basada en requerimientos de información y seguridad empresarial, asegurar que los activos de información se mantengan protegidos de una manera consistente con su valor para el negocio y evitar la pérdida de confidencialidad, integridad y disponibilidad de la información.

El acceso lógico y uso de los sistemas de información y recursos tecnológicos del proveedor debe ser restringido, limitado o controlado mediante la implementación de mecanismos de identificación, autenticación y autorización, definiendo lineamientos de accesos, con el fin de evitar que personas no autorizadas tengan acceso a información y/o recursos, siempre teniendo en cuenta el principio del menor privilegio, se deben implementar técnicas y controles de acceso que cuenten con múltiples factores de autenticación a las consolas de administración del servicio y de la información.

2.5 Control de acceso físico

Debe contar con un proceso donde se definan directrices para el control de acceso físico, asegurando las áreas críticas mediante controles de entrada apropiados para garantizar que solo las personas autorizadas tengan acceso permitido, con el objetivo de controlar y evitar accesos no autorizados, daños por eventos provocados que puedan llegar a interrumpir la prestación del servicio entregado al Banco.

En el caso que los proveedores deban ingresar a las sedes del banco, deben portar la identificación física con la cual se pueda identificar, de manera inequívoca, a los colaboradores de los terceros contratados.

2.6 Segregación de funciones

Debe contar con un método de segregación de funciones de roles y áreas para reducir las oportunidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.

2.7 Escritorio limpio

Debe contar con una política de escritorio limpio teniendo en cuenta la clasificación de la información, los requisitos contractuales y legales, y los correspondientes aspectos de riesgo y culturales de la organización, para reducir el riesgo de acceso no autorizado a la información impresa o electrónica para evitar la pérdida y el daño de la información durante y fuera de las horas normales de trabajo.

2.8 Gestión de contraseñas

Deben contar con políticas de seguridad que garantice una adecuada gestión de contraseñas, promoviendo contraseñas de calidad que cuenten con parámetros aceptables de seguridad como longitud mínima, tiempo determinado de caducidad y uso de mecanismos de autenticación segura con el fin de evitar el acceso indebido a la información.

2.9 Gestión de la seguridad de la red

Debe contar con mecanismos de seguridad, niveles de servicio y requisitos de administración para todos los servicios de red, asegurando la protección de la información en redes y recursos de procesamiento de información.

2.10 Clasificación de la información

Deben contar con procesos debidamente formalizada bajo políticas de gestión de activos de información donde definan el proceso de identificación de estos, tanto en el ciberespacio como en el interior de la organización.

La información debe clasificarse en términos de su valor, requisitos legales, sensibilidad y criticidad para evitar modificaciones o divulgaciones no autorizadas. Esta clasificación debe basarse en requisitos de cumplimiento contractual o legal, tales como: LGPD, PCI, ISO 27001, SOX, etc., asegurando que la información reciba un nivel adecuado de protección, de acuerdo con su importancia para la organización.

2.11 Procedimiento de tratamiento de la información

Los proveedores del banco deben garantizar que la información del banco lo largo del ciclo de vida (recepción, procesamiento, almacenamiento y salida esté cifrada y/o con control de acceso restringido y monitoreado. Con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de la información enviada o accedida por la empresa en la ejecución del servicio para el que fue contratada.

2.12 Borrado Seguro

Los proveedores del banco deben contar con políticas y procedimientos de borrado seguro de la información y se compromete a borrar de forma segura todos los datos que hayan sido entregados por el banco en ejecución de los servicios ofrecidos cuando así sea solicitado o cuando el banco elimine o reemplace por cualquier causa los medios de almacenamiento previamente utilizados para la conservación de los datos.

2.13 Gestión de incidentes de seguridad de la información

Los proveedores del banco deben cumplir los siguientes lineamientos referentes a la gestión de incidentes de seguridad de la información:

- Deben contar con una metodología que contenga procedimiento y flujos de respuestas de gestión de incidentes de Seguridad de la Información y ciberseguridad que permita asegurar respuestas rápidas y ordenadas que se puedan presentar, incluyendo actividades de inteligencia de amenazas.

- En el caso de presentarse algún incidente asociado a seguridad de la información y ciberseguridad del lado del proveedor que involucre información o servicios prestados al banco, estos **deberán ser reportados de forma inmediata** al correo de **cibersegridad@itau.co**, siguiendo el procedimiento descrito en el **FT11382 - Formato Documentación incidentes de seguridad de la información y ciberseguridad**, para tomar las acciones requeridas que se consideren relevantes y dar cumplimiento a la Circular Externa 033 de 2020 (CE033) de la Superintendencia Financiera de Colombia.

- El proveedor deberá generar un informe periódico cada 3 meses al buzón de **ciberseguridad@itau.co** con la cantidad total de incidentes de seguridad de la información y ciberseguridad presentados en los servicios que prestan al banco con el objetivo de dar cumplimiento al Formato 403 asociado a la Circular Externa 033 de 2020 impartida por la Superintendencia Financiera de Colombia; de igual manera se debe reportar si no se presentaron incidentes.

2.14 Seguridad de la aplicación

En los servicios prestados por el proveedor que involucre autenticación en aplicaciones de usuario se debe contar con los mecanismos administrativos y tecnológicos para garantizar el correcto funcionamiento de los servicios prestados al banco, definiendo una política de seguridad de aplicaciones; con el fin de tener control y restricción de acceso a la información, funciones de los sistemas de la aplicación.

2.15 Navegación por internet

Contar con mecanismos de control en la navegación por internet, para evitar el acceso a sitios web maliciosos o inseguros, indisponibilidad en el entorno, fuga de información y riesgo de imagen.

2.16 Mensajes electrónicos (e-mail)

La información que viaja en los mensajes electrónicos debe protegerse adecuadamente para evitar la fuga de información, para ello los proveedores del banco deben contar con la capacidad de integrase a los métodos usados por el banco para el intercambio seguro de información, protección de mensajes de correo electrónico, entre otros.

2.17 Sincronización horaria

Contar con un procedimiento que garantice la sincronización de los relojes en los sistemas con un estándar de tiempo confiable o un estándar de hora local garantizando la precisión de los registros de auditoría, de ser necesarios para investigaciones o como evidencia en casos legales o disciplinarios.

2.18 Gestión de Infraestructura tecnológica segura

Deben existir lineamientos documentados sobre el correcto aprovisionamiento y mantenimiento de infraestructura tecnológica segura incluyendo actividades como hardening y validación de vulnerabilidades previo a la salida a ambientes productivos.

Si dentro de los servicios que el proveedor brinda al banco, existen sitios web expuestos a internet, estos deben contar con certificados digitales vigentes y sus renovaciones no pueden exceder la fecha de vigencia de los mismos.

2.19 Registros y monitoreo (logs/audit trail)

A través del registro de eventos, se deben mantener y analizar críticamente a intervalos regulares todos los eventos de actividad del usuario, excepciones, errores y eventos de seguridad, garantizando la trazabilidad del entorno de red y sistemas, para posibles investigaciones por el uso indebido de los sistemas.

2.20 Desarrollo Seguro

En caso de que el servicio a prestar esté relacionado con desarrollo de software, se debe contar por parte del proveedor, de preferencia, con certificaciones de desarrollo seguro o en su defecto contar con manuales, procedimientos y/o guías que permitan realizar prácticas seguras de desarrollo de software. Así mismo, todo desarrollo que se entregue al Banco debe estar certificado como seguro.

2.21 Criptografía

Contar con una política de controles criptográficos para la protección de la información almacenada y transportada, asegurando el uso adecuado del cifrado (almacenamiento y tráfico) para proteger la confidencialidad, autenticidad e integridad de la información:

- La información trasmitida a través de canales públicos como internet deberá estar cifrada usando hardware o software de propósito específico, o una combinación de los anteriores, empleando cifrado fuerte.
- La trasmisión de archivos debe ser realizada utilizando protocolos de comunicación seguros.
- El uso de certificados digitales seguros emitidos por un Certificate Authority (CA) externo autorizado es obligatorio para servicios web.
- El uso de certificados digitales seguros emitidos por un CA externo autorizado es obligatorio para la firma de transacciones entre aplicaciones.
- Para los sitios web expuestos a internet, que usen imagen del banco se deben implementar mecanismos que permitan verificar constantemente que no sea alterado su contenido (defacement), que no sean suplantados, no estén vencidos los certificados digitales y que no sea alterada la resolución de los DNS.

2.22 Backups

Los proveedores deben contar con una política de generación de backups definida donde se especifique la estrategia de recuperación que permita el restablecimiento de copias de seguridad de información, software e imágenes del sistema, de los servicios prestados al banco en un tiempo optimo, con el objetivo de evitar impactos negativos prolongados y los efectos de fallas significativas y/o desastres, se debe tener en cuenta también que los planes de contingencia del proveedor deben contar con pruebas de ejecución realizadas y probadas anualmente, garantizando la disponibilidad de la información.

Se debe garantizar el resguardo de backups, esto teniendo en cuenta en los casos que aplique, las consideraciones de las regulaciones emitidas por la superintendencia financiera de Colombia y las normas o leyes que lleguen a regir al tipo de servicio brindado por el proveedor, así mismo la entrega de estos respaldos, en los casos que apliquen por términos contractuales deben hacerse bajo los parámetros que se hayan establecido entre el banco y el proveedor.

2.23 Separación de entornos de desarrollo, pruebas y producción

Los proveedores del banco deben garantizar que los entornos de desarrollo, pruebas y producción estén separados para reducir el riesgo de acceso no autorizado o modificación del entorno de producción evitando modificaciones inesperadas del entorno de archivos o sistemas o errores del sistema.

2.24 Protección contra Malware

Contar con mecanismos de control de detección, prevención y recuperación para proteger contra malware, combinado con un programa de concientización del usuario adecuado, asegurando que la información y las capacidades de procesamiento de información estén protegidas contra el malware.

2.25 Gestión de vulnerabilidades

Los proveedores del banco deben cumplir los siguientes lineamientos referentes a vulnerabilidades:

- Deben contar con procedimientos para la identificación de vulnerabilidades en configuraciones de red y servidores mediante el análisis de hosts, puertos, versiones y configuraciones de servicio, evitando la explotación de vulnerabilidades en el entorno que puedan provocar ataques (APT, DDOS, etc.) y provocar indisponibilidad del entorno.
- Deben contar con procedimientos de gestión de vulnerabilidades.
- Los proveedores deben generar de manera automática, semestralmente, un informe consolidado de las vulnerabilidades encontradas en los sistemas tecnológicos que soportan los servicios prestados al banco y el cual estará en todo momento a disposición del banco.
- Los informes generados por el proveedor de los últimos dos años deberán estar a disposición del banco permitiendo el análisis de vulnerabilidades sobre estos sistemas tecnológicos cuando así lo requiera.
- Para efectos de la generación de los informes solicitados se deberá tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org).
- Los proveedores deberán tomar las medidas necesarias para remediar las vulnerabilidades detectadas en sus análisis o en los reportados por el banco, los ANS de remediación de vulnerabilidades no pueden ser superiores a los del banco.
- Las herramientas usadas en el análisis de vulnerabilidades deberán estar homologadas por el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización.

2.26 Gestión de Ethical Hacking y pruebas de seguridad

Los proveedores del banco deben cumplir los siguientes lineamientos referentes a la ejecución de ethical hacking garantizando la protección de los recursos informáticos del banco.

- Deben contar con procedimientos donde se refleje la ejecución regular de pruebas de seguridad y la adecuada gestión en la remediación de las vulnerabilidades, las cuales deben estar alineadas a los tiempos establecidos por el banco.
- Deben contar con procedimientos donde se especifique la ejecución periódica de las pruebas de penetración y hacking éticos a sus sistemas y redes.
- Si dentro de los servicios que el proveedor brinda al banco, existen sitios web expuestos a internet que utilicen la imagen del banco y/o procesen o transmitan información confidencial, se debe permitir la ejecución de pruebas de seguridad ejecutadas por el banco.
- Si dentro de los servicios que el proveedor brinda al banco existen servicios que se expongan a internet, se deben alinear a las herramientas de balanceo y enmascaramiento de URL dispuestos por el banco.
- Todo proveedor que ofrezca servicios web para el banco debe alinearse a las normas, requerimientos y/o requisitos de la Superintendencia financiera de Colombia en todo lo que compete a servicios web.

2.27 Servicios Cloud

Los proveedores que presten servicios cloud (Servicios en la Nube “Cloud Computing”) deberán contar y mantener vigente la certificación ISO/IEC 27001, y de observancia a los estándares o buenas prácticas, tales como ISO/IEC 27017 y 27018. El proveedor puede certificarse con estándares o mejores prácticas que reemplacen, sustituyan o modifiquen las anteriores y debe disponer de informes de controles de organización de servicios (SOC1, SOC2, SOC3).

Adicional deberán cumplir con lo establecido en el formato **FT11385 - Formato Evaluación para proveedores cloud** el cual contienen los criterios específicos para este tipo de servicios.

2.28 Gestión del cambio

Los proveedores deben garantizar la administración de los cambios a la provisión de servicios, manteniendo y mejorando las políticas de seguridad de la información y los procedimientos específicos.

Para ello debe contar con una política de gestión del cambio donde se establezcan lineamientos que garanticen que los cambios en la organización, los procesos de negocio, los recursos de procesamiento de información y los sistemas que afectan la seguridad de la información tienen el control adecuado para las modificaciones, sin causar fallas de seguridad o indisponibilidad de la información.

2.29 Gestión del Riesgo

Deben contar con una metodología para la adecuada gestión de riesgos con la cual identifiquen, midan, controlen y mitiguen los riesgos referentes a seguridad de la información y ciberseguridad.

2.30 Cumplimiento y normativa

Los proveedores del banco deben cumplir los siguientes lineamientos:

- Los proveedores que tengan empleados con accesos al banco deben conocer y cumplir las Políticas Generales de Seguridad de la Información del banco. En caso de presentarse algún cambio a las mencionadas políticas, el banco enviará una comunicación al proveedor informando las modificaciones efectuadas.
- Debe asegurar el cumplimiento de la normativa local y la implementación de niveles adecuados de protección y control y el cumplimiento de los compromisos contractuales establecidos con el banco.
- Todos los requisitos legales, normativos y contractuales nacionales o internacionales, referentes a la seguridad de los sistemas y activos de información, que sean aplicables al negocio financiero del Banco, deben ser identificados, documentados e informados al Banco como garantía de su cumplimiento.
- Deben contar con un proceso documentado de revisión y auditoría periódico, que asegure el cumplimiento de los requerimientos normativos para la prestación del servicio ofrecido, incluyendo, pero sin limitarse a la circular externa 005 de 2019 expedida por la Superintendencia Financiera o cualquier otra norma que la modifique, derogue o que sea aplicable.
- El proveedor se compromete a mantener actualizados los contactos para tratar temas relacionados a seguridad de la información y ciberseguridad, enviando de manera mensual al buzón de **ciberseguridad@itau.co,** actualizaciones y/o novedades con (contactos, celulares y/o correos electrónicos) según corresponda.

3. Glosario

Los siguientes términos son útiles como referencia en el uso del presente documento:

Activo de información: Es cualquier información o sistema relacionado con el tratamiento de esta, que tenga valor para la organización.

Administración de usuarios: creación, modificación, consulta, inactivación, activación y eliminación de la cuenta de un usuario.

Amenaza: Circunstancia desfavorable que al ser explotada puede tener consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.

Análisis de riesgos: proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de estas, a fin de determinar los controles adecuados para tratar el riesgo.

Ataque cibernético: Intento malicioso de acceder o causar daños en un sistema de información o la red, por medio de la explotación de vulnerabilidades.

Autenticación fuerte: esquema de autenticación mediante el cual el usuario se está identificando ante un sistema y demuestra que es realmente quien dice ser.

Ciberespacio: Entorno complejo resultante de la interacción de personas, software y servicios en internet, mediante dispositivos tecnológicos, que no existe en ninguna forma física.

Ciberseguridad: Conjunto de políticas, recursos, controles, directrices y buenas prácticas para la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

Cifrado fuerte: Procedimiento utilizado para la protección de la información, que utilizan algoritmos aprobados por los estándares internacionales y buenas prácticas.

Continuidad: es la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

Evaluación de riesgos de seguridad de la información: proceso que contempla la medición, evaluación, continuidad, amenazas, impacto y vulnerabilidades sobre los activos de información, para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

Evento de seguridad de la información: se considera un evento de seguridad de la información a cualquier situación que indique una posible brecha en las políticas de seguridad, falla en los controles y/o protecciones establecidas.

Gestión de activos: busca gestionar todo el ciclo de vida de los activos físicos y digitales de una organización con el fin de maximizar su valor, cubre procesos como el diseño, construcción, explotación, mantenimiento y reemplazo de activos e infraestructuras.

Gestión de incidentes: tiene como objetivo resolver cualquier incidente que atente contra los servicios que presta el Banco.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Gestión de vulnerabilidades: proceso sistemático y medible que permite identificar, priorizar y dar tratamiento en forma proactiva a las vulnerabilidades de carácter tecnológico.

Incidente de seguridad de la información: Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la Organización, como el incumplimiento o amenaza inminente a las políticas de seguridad de la información del Banco, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Política: directriz de una organización tal como lo expresa formalmente su alta dirección.

Recursos tecnológicos: elementos de tecnología que pueden ser hardware y/o software, tales como equipos de cómputo, servidores, impresoras, teléfonos, faxes, programas y/o aplicativos de software, dispositivos, USB, entre otros.

Riesgos: es el estudio de las causas de las posibles amenazas, eventos no deseados, daños y consecuencias que éstos puedan producir.

Sistema de información: aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información.

Sistema de gestión de seguridad de la información (SGSI): comprende todo el sistema de gestión, basado en un enfoque de riesgo del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye organigrama, políticas, planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

Terceros: se entiende por tercero a toda persona, jurídica o natural, como proveedores, temporales, contratistas o consultores, que provean servicios o productos a la compañía.

Vulnerabilidad informática: ausencia o deficiencia de los controles informáticos que permiten el acceso no autorizado a los canales de distribución o a los sistemas informáticos de la entidad.