Capítulo VI

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

En este capitulo se elaboraran las políticas de seguridad con el propósito de proteger la información de la empresa, estas servirán de guía para la implementación de medidas de seguridad que contribuirán a mantener la integridad, confidencialidad y disponibilidad de los datos dentro de los sistemas de aplicación, redes, instalaciones de cómputo y procedimientos manuales.
El documento de políticas de seguridad ha sido elaborado tomando como base la siguiente documentación:

- Estándar de seguridad de la información ISO 17799
- Requerimientos de la Circular N° G-105-2002 de la Superintendencia de Banca y Seguros (SBS) sobre Riesgos de Tecnología de Información.
- Normas internas del Banco referidas a seguridad de información.

6.1 Definición

Una Política de seguridad de información es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.

Propósito

El propósito de las políticas de seguridad de la información es proteger la información y los activos de datos del Banco. Las políticas son guías para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación, redes, instalaciones de cómputo y procedimientos manuales.

6.2 CUMPLIMIENTO OBLIGATORIO

El cumplimiento de las políticas y estándares de seguridad de la información es obligatorio y debe ser considerado como una condición en los contratos del personal.

El Banco puede obviar algunas de las políticas de seguridad definidas en este documento, únicamente cuando se ha demostrado claramente que el cumplimiento de dichas políticas tendría un impacto significativo e inaceptable para el negocio. Toda excepción a las políticas debe ser documentada y aprobada por el área de seguridad informática y el área de auditoria interna, detallando el motivo que justifica el no-cumplimiento de la política.

6.3 ORGANIZACIÓN DE LA SEGURIDAD

En esta política se definen los roles y responsabilidades a lo largo de la organización con respecto a la protección de recursos de información. Esta política se aplica a todos los empleados y otros asociados con el Banco, cada uno de los cuales cumple un rol en la administración de la seguridad de la información. Todos los empleados son responsables de mantener un ambiente seguro, en tanto que el área de seguridad informática debe monitorear el cumplimiento de la política de seguridad definida y realizar las actualizaciones que sean necesarias, producto de los cambios en el entorno informático y las necesidades del negocio.

6.3.1 Estructura Organizacional

En la administración de la seguridad de la información participan todos los empleados siguiendo uno o más de los siguientes roles:

- Área de Seguridad Informática
- Usuario
- Custodio de información
- Propietario de información
- Auditor interno

Los roles y funciones de administración de la seguridad de la información de cada uno de estas personas están detalladas en el Capitulo IV.

6.3.2 Acceso por parte de terceros

El Banco debe establecer para terceros al menos las mismas restricciones de acceso a la información que a un usuario interno. Además, el acceso a la información debe limitarse a lo mínimo indispensable para cumplir con el trabajo asignado. Las excepciones deben ser analizadas y aprobadas por el área de seguridad informática. Esto incluye tanto acceso físico como lógico a los recursos de información del Banco.

Todo acceso por parte de personal externo debe ser autorizado por un responsable interno, quien asume la responsabilidad por las acciones que pueda realizar el mismo. El personal externo debe firmar un acuerdo de no-divulgación antes de obtener acceso a información del Banco. Proveedores que requieran acceso a los sistemas de información del Banco deben tener acceso únicamente cuando sea necesario.

Todas las conexiones que se originan desde redes o equipos externos al Banco, deben limitarse únicamente a los servidores y aplicaciones necesarios. Si es posible, estos servidores destino de las conexiones deben estar físicamente o lógicamente separados de la red interna del Banco.

Los contratos relacionados a servicios de tecnologías de información deben ser aprobados por el área legal del Banco, y en el caso de que afecten la seguridad o las redes de la organización deben ser aprobados adicionalmente por el área de seguridad informática. Bajo determinadas condiciones, como en la ejecución de servicios críticos para el negocio, el Banco debe considerar efectuar una revisión independiente de la estructura de control interno del proveedor.

En los contratos de procesamiento de datos externos se debe especificar los requerimientos de seguridad y acciones a tomar en caso de violación de los contratos. Todos los contratos deben incluir una cláusula donde se establezca el derecho del Banco de nombrar a un representante autorizado para evaluar la estructura de control interna del proveedor.

6.3.3 Outsourcing

Todos los contratos de Outsourcing deben incluir lo siguiente:

- Acuerdos sobre políticas y controles de seguridad.
- Determinación de niveles de disponibilidad aceptable.
- El derecho del Banco de auditar los controles de seguridad de información del proveedor.
- Determinación de los requerimientos legales del Banco.
- Metodología del proveedor para mantener y probar cíclicamente la seguridad del sistema.
- Que el servicio de procesamiento y la información del Banco objeto de la subcontratación estén aislados, en todo momento y bajo cualquier circunstancia.

El proveedor es responsable de inmediatamente informar al responsable del contrato de cualquier brecha de seguridad que pueda comprometer información del Banco. Cualquier empleado del Banco debe informar de violaciones a la seguridad de la información por parte de proveedores al área de seguridad informática.

6.4 EVALUACION DE RIESGO

El costo de las medidas y controles de seguridad no debe exceder la pérdida que se espera evitar. Para la evaluación del riesgo se deben de seguir los siguientes pasos:

- Clasificación del acceso de la información

- Ejecución del análisis del riesgo identificando áreas vulnerables, pérdida potencial y selección de controles y objetivos de control para mitigar los riesgos, de acuerdo a los siguientes estándares.

6.4.1 Inventario de activos

Los inventarios de activos ayudan a garantizar la vigencia de una protección eficaz de los recursos, y también pueden ser necesarios para otros propósitos de la empresa, como los relacionados con sanidad y seguridad, seguros o finanzas (administración de recursos). El proceso de compilación de un inventario de activos es un aspecto importante de la administración de riesgos. Una organización debe contar con la capacidad de identificar sus activos y el valor relativo e importancia de los mismos. Sobre la base de esta información, la organización puede entonces, asignar niveles de protección proporcionales al valor e importancia de los activos. Se debe elaborar y mantener un inventario de los activos importantes asociados a cada sistema de información. Cada activo debe ser claramente identificado y su propietario y clasificación en cuanto a seguridad deben ser acordados y documentados, junto con la ubicación vigente del mismo (importante cuando se emprende una recuperación posterior a una pérdida o daño). Ejemplos de activos asociados a sistemas de información son los siguientes:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información perdida (“fallback”), información archivada;
- Recursos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios;
- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones

(routers, PBXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas y discos), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento;

- Servicios: servicios informáticos y de comunicaciones, utilitarios generales, por Ej. calefacción, iluminación, energía eléctrica, aire acondicionado.

6.4.2 Clasificación del acceso de la información

Toda la información debe de ser clasificada como Restringida, Confidencial, Uso Interno o General de acuerdo a lo definido en el capitulo 4.2.1. La clasificación de información debe de ser documentada por el Propietario, aprobada por la gerencia responsable y distribuida a los Custodios durante el proceso de desarrollo de sistemas o antes de la distribución de los documentos o datos.

La clasificación asignada a un tipo de información, solo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación.

La información que existe en más de un medio (por ejemplo, documento fuente, registro electrónico, reporte o red) debe de tener la misma clasificación sin importar el formato.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, verbigracia, cuando la información se ha hecho pública. Este aspecto debe ser tomado en cuenta por el propietario de la información, para realizar una reclasificación de la misma, puesto que la clasificación por exceso (“over- classification”) puede traducirse en gastos adicionales innecesarios para la organización.

La información debe de ser examinada para determinar el impacto en el Banco si fuera divulgada o alterada por medios no autorizados. A continuación detallamos algunos ejemplos de información sensible:

- Datos de interés para la competencia:
  - Estrategias de marketing
  - Listas de clientes
  - Fechas de renovación de créditos
  - Tarifaciones
  - Datos usados en decisiones de inversión
- Datos que proveen acceso a información o servicios:
  - Llaves de encripción o autenticación
  - Contraseñas
- Datos protegidos por legislación de privacidad vigente
  - Registros del personal
  - Montos de los pasivos de clientes
  - Datos históricos con 10 años de antigüedad
- Datos que tienen un alto riesgo de ser blanco de fraude u otra actividad ilícita:
  - Datos contables utilizados en sistemas
  - Sistemas que controlan desembolsos de fondos

6.4.3 Definiciones

Restringida: Información con mayor grado de sensibilidad; el acceso a esta información debe de ser autorizado caso por caso.

Confidencial: Información sensible que solo debe ser divulgada a aquellas personas que la necesiten para el cumplimiento de sus funciones.

Uso Interno: Datos generados para facilitar las operaciones diarias; deben de ser manejados de una manera discreta, pero no requiere de medidas elaboradas de seguridad.

General: Información que es generada específicamente para su divulgación a la población general de usuarios.

6.4.4 Aplicación de controles para la información clasificada

Las medidas de seguridad a ser aplicadas a los activos de información clasificados, incluyen pero no se limitan a las siguientes:

6.4.4.1 Información de la Compañía almacenada en formato digital

- Todo contenedor de información en medio digital (CD´s, cintas de backup, diskettes, etc.) debe presentar una etiqueta con la clasificación correspondiente.
- La información en formato digital clasificada como de acceso “General”, puede ser almacenada en cualquier sistema de la Compañía. Sin embargo se deben tomar las medidas necesarias para no mezclar información “General” con información correspondiente a otra clasificación.
- Todo usuario, antes de transmitir información clasificada como “Restringida” o “Confidencial”, debe asegurarse que el destinatario de la información esté autorizado a recibir dicha información.
- Todo usuario que requiere acceso a información clasificada como “Restringida” o “Confidencial”, debe ser autorizado por el propietario de la misma. Las autorizaciones de acceso a este tipo de información deben ser documentadas.
- La clasificación asignada a un tipo de información, solo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación.
- Información en formato digital, clasificada como “Restringida”, debe ser encriptada con un método aprobado por los encargados de la administración de seguridad de la información, cuando es almacenada en cualquier medio (disco duro, disquetes, cintas, CDs, etc.).

- Es recomendable el uso de técnicas de encripción para la información clasificada como “Restringida” o “Confidencial”, transmitida a través de la red de datos del Banco.
- Toda transmisión de Información clasificada como “Restringida”, “Confidencial” o de “Uso Interno” realizada hacia o a través de redes externas a la Compañía debe realizarse utilizando un medio de transmisión seguro o utilizando técnicas de encripción aprobadas.
- Todo documento en formato digital, debe presentar la clasificación correspondiente en la parte superior (cabecera) e inferior (pié de página) de cada página del documento.
- Los medios de almacenamiento, incluyendo discos duros de computadoras, que albergan información clasificada como “Restringida”, deben ser ubicados en ambientes cerrados diseñados para el almacenamiento de dicho tipo de información. En lugar de protección física, la información clasificada como “Restringida”, podría ser protegida con técnicas de encripción aprobadas por la Compañía.

6.4.4.2 Información de la Compañía almacenada en formato no digital

- Todo documento o contenedor de información debe ser etiquetado como “Restringida”, “Confidencial”, de “Uso interno” o de Acceso “General”, dependiendo de la clasificación asignada.
- Todo documento que presente información clasificada como “Confidencial” o “Restringida”, debe ser etiquetado en la parte superior e inferior de cada página con la clasificación correspondiente.
- Todo documento clasificado como “Confidencial” o “Restringido” debe contar con una carátula en la cual se muestre la clasificación de la información que contiene.

- Los activos de información correspondiente a distintos niveles de clasificación, deben ser almacenados en distintos contenedores, de no ser posible dicha distinción, se asignará el nivel más critico de la información identificada a todo el contenedor de información.
- El ambiente donde se almacena la información clasificada como "Restringida", debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia. El acceso debe ser permitido solo al personal formalmente autorizado. Personal de limpieza debe ingresar al ambiente acompañado por personal autorizado.
- Solo el personal formalmente autorizado debe tener acceso a información clasificada como "Restringida" o "Confidencial"
- Los usuarios que utilizan documentos con información "Confidencial" o "Restringida" deben asegurarse de:
  - Almacenarlos en lugares adecuados
  - Evitar que usuarios no autorizados accedan a dichos documentos
  - Destruir los documentos si luego de su utilización dejan de ser necesarios

6.4.5 Análisis de riesgo

Los Propietarios de la información y custodios son conjuntamente responsables del desarrollo de análisis de riesgos anual de los sistemas a su cargo. Como parte del análisis se debe identificar las aplicaciones de alta criticidad como críticas para la recuperación ante desastres. Es importante identificar:

- Áreas vulnerables
- Pérdida potencial
- Selección de controles y objetivos de control para mitigar los riesgos, indicando las razones para su inclusión o exclusión (Seguridad de

datos, Plan de respaldo/recuperación, Procedimientos estándar de operación)

Adicionalmente, un análisis de riesgo debe de ser conducido luego de cualquier cambio significativo en los sistemas, en concordancia con el clima cambiante de las operaciones en el negocio del Banco.

El análisis de riesgo debe tener un propósito claramente definido y delimitado, existiendo dos posibilidades: cumplimiento con los controles y/o medidas de protección o la aceptación del riesgo.

6.4.6 Cumplimiento

El cumplimiento satisfactorio del proceso de evaluación del riesgo se caracteriza por:

- Identificación y clasificación correcta de los activos a ser protegidos.
- Aplicación consistente y continua de los controles y/o medidas para mitigar el riesgo (seguridad efectiva de datos, recuperación ante desastres adecuado)
- Detección temprana de los riesgos, reporte adecuado de pérdidas, así como una respuesta oportuna y efectiva ante las perdidas ya materializadas.

6.4.7 Aceptación de riesgo

La gerencia responsable puede obviar algún control o requerimiento de protección y aceptar el riesgo identificado solo cuando ha sido claramente demostrado que las opciones disponibles para lograr el cumplimiento han sido identificadas y evaluadas, y que éstas tendrían un impacto significativo y no aceptable para el negocio.

La aceptación de riesgo por falta de cumplimiento de los controles y/o medidas de protección debe ser documentada, revisada por las partes

involucradas, comunicada por escrito y aceptada por las áreas responsables de la administración de la seguridad.

6.5 SEGURIDAD DEL PERSONAL

Los estándares relacionados al personal deben ser aplicados para asegurarse que los empleados sean seleccionados adecuadamente antes de ser contratados, puedan ser fácilmente identificados mientras formen parte del Banco y que el acceso sea revocado oportunamente cuando un empleado es despedido o transferido. Deben desarrollarse estándares adicionales para asegurar que el personal sea consciente de todas sus responsabilidades y acciones apropiadas en el reporte de incidentes.

Esta política se aplica a todos los empleados, personal contratado y proveedores.

Los empleados son los activos más valiosos del Banco. Sin embargo, un gran número de problemas de seguridad de cómputo pueden ser causados por descuido o desinformación. Se deben de implementar procedimientos para manejar estos riesgos y ayudar al personal del Banco a crear un ambiente de trabajo seguro.

Medidas de precaución deben de ser tomadas cuando se contrata, transfiere y despide a los empleados. Deben de establecerse controles para comunicar los cambios del personal y los requerimientos de recursos de cómputo a los responsables de la administración de la seguridad de la información. Es crucial que estos cambios sean atendidos a tiempo.

6.5.1 Seguridad en la definición de puestos de trabajo y recursos

El departamento de Recursos Humanos debe de notificar al área de seguridad informática, la renuncia o despido de los empleados así como el inicio y fin de los periodos de vacaciones de los mismos. Cuando se notifique un despido o transferencia, el Custodio de información debe de asegurarse que el identificador de usuario sea revocado. Cuando se

notifique una transferencia o despido, el área de seguridad debe de asegurarse que las fichas o placas sean devueltas al Banco. Cualquier ítem entregado al empleado o proveedor como computadoras portátiles, llaves, tarjetas de identificación, software, datos, documentación, manuales, etc. deben de ser entregados a su gerente o al área de Recursos Humanos.

La seguridad es responsabilidad de todos los empleados y personas involucradas con el Banco. Por ende, todos los empleados, contratistas, proveedores y personas con acceso a las instalaciones e información del Banco deben de acatar los estándares documentados en la política de seguridad del Banco e incluir la seguridad como una de sus responsabilidades principales.

Todos los dispositivos personales de información, como por ejemplo computadoras de propiedad de los empleados o asistentes digitales personales (PDA – Personal Digital Assistant), que interactúen con los sistemas del Banco, deben ser aprobados y autorizados por la gerencia del Banco.

6.5.2 Capacitación de usuarios

Es responsabilidad del área de seguridad informática promover constantemente la importancia de la seguridad a todos los usuarios de los sistemas de información. El programa de concientización en seguridad debe de contener continuas capacitaciones y charlas, adicionalmente se puede emplear diversos métodos como afiches, llaveros, mensajes de log-in, etc., los cuales recuerden permanentemente al usuario el papel importante que cumplen en el mantenimiento de la seguridad de la información.

Orientación para los empleados y/o servicios de terceros nuevos

Cuando se contrate a un empleado nuevo y/o el servicio de algún tercero, se debe de entregar la política de seguridad así como las normas y procedimientos para el uso de las aplicaciones y los sistemas de información del Banco. Asimismo se debe entregar un resumen escrito de las medidas básicas de seguridad de la información.

El personal de terceros debe recibir una copia del acuerdo de no divulgación firmado por el Banco y por el proveedor de servicios de terceros así como orientación con respecto a su responsabilidad en la confidencialidad de la información del Banco.

Entre otros aspectos se debe considerar:

- El personal debe de ser comunicado de las implicancias de seguridad en relación a las responsabilidades de su trabajo
- Una copia firmada de la política de seguridad de información debe de ser guardada en el archivo del empleado

Concientización periódica

Estudios muestran que la retención y el conocimiento aplicable se incrementa considerablemente cuando el tema es sujeto a revisión. Los usuarios deben de ser informados anualmente sobre la importancia de la seguridad de la información. Un resumen escrito de la información básica debe de ser entregada nuevamente a cada empleado y una copia firmada debe de ser guardada en sus archivos.

La capacitación en seguridad debe de incluir, pero no estar limitado, a los siguientes aspectos:

- Requerimientos de identificador de usuario y contraseña
- Seguridad de PC, incluyendo protección de virus
- Responsabilidades de la organización de seguridad de información
- Concientización de las técnicas utilizadas por “hackers”
- Programas de cumplimiento

- Guías de acceso a Internet
- Guías de uso del correo electrónico
- Procesos de monitoreo de seguridad de la información utilizados
- Persona de contacto para información adicional

6.5.3 Procedimientos de respuesta ante incidentes de seguridad

El personal encargado de la administración de seguridad debe ser plenamente identificado por todos los empleados del Banco.

Si un empleado del Banco detecta o sospecha la ocurrencia de un incidente de seguridad, tiene la obligación de notificarlo al personal de seguridad informática. Si se sospecha la presencia de un virus en un sistema, el usuario debe desconectar el equipo de la red de datos, notificar al área de seguridad informática quien trabajará en coordinación con el área de soporte técnico, para la eliminación del virus antes de restablecer la conexión a la red de datos. Es responsabilidad del usuario (con la apropiada asistencia técnica) asegurarse que el virus haya sido eliminado por completo del sistema antes de conectar nuevamente el equipo a la red de datos.

Si un empleado detecta una vulnerabilidad en la seguridad de la información debe notificarlo al personal encargado de la administración de la seguridad, asimismo, está prohibido para el empleado realizar pruebas de dicha vulnerabilidad o aprovechar ésta para propósito alguno.

El área de seguridad informática debe documentar todos los reportes de incidentes de seguridad.

Cualquier error o falla en los sistemas debe ser notificado a soporte técnico, quién determinará si el error es indicativo de una vulnerabilidad en la seguridad.

Las acciones disciplinarias tomadas contra socios de negocio o proveedores por la ocurrencia de una violación de seguridad, deben ser

consistentes con la magnitud de la falta, ellas deben ser coordinadas con el área de Recursos Humanos.

6.5.3.1 Registro de fallas

El personal encargado de operar los sistemas de información debe registrar todos lo errores y fallas que ocurren en el procesamiento de información o en los sistemas de comunicaciones. Estos registros deben incluir lo siguiente:

- Nombre de la persona que reporta la falla
- Hora y fecha de ocurrencia de la falla
- Descripción del error o problema
- Responsable de solucionar el problema
- Descripción de la respuesta inicial ante el problema
- Descripción de la solución al problema
- Hora y fecha en la que se solucionó el problema

Los registros de fallas deben ser revisados semanalmente. Los registros de errores no solucionados deben permanecer abiertos hasta que se encuentre una solución al problema. Además, estos registros deben ser almacenados para una posterior verificación independiente.

6.5.3.2 Intercambios de información y correo electrónico

Los mensajes de correo electrónico deben ser considerados de igual manera que un memorándum formal, son considerados como parte de los registros del Banco y están sujetos a monitoreo y auditoria. Los sistemas de correo electrónico no deben ser utilizados para lo siguiente:

- Enviar cadenas de mensajes
- Enviar mensajes relacionados a seguridad, exceptuando al personal encargado de la administración de la seguridad de la información
- Enviar propaganda de candidatos políticos

- Actividades ilegales, no éticas o impropias
- Actividades no relacionadas con el negocio del Banco
- Diseminar direcciones de correo electrónico a listas públicas

No deben utilizarse reglas de reenvío automático a direcciones que no pertenecen a la organización. No existe control sobre los mensajes de correo electrónico una vez que estos se encuentran fuera de la red del Banco.

Deben establecerse controles sobre el intercambio de información del Banco con terceros para asegurar la confidencialidad e integridad de la información, y que se respete la propiedad intelectual de la misma. Debe tomarse en consideración:

- Acuerdos para el intercambio de software
- Seguridad de media en tránsito
- Controles sobre la transmisión mediante redes

Debe establecerse un proceso formal para aprobar la publicación de información del Banco. El desarrollo de páginas Web programables o inteligentes (utilizando tecnologías como CGI o ASP) debe considerarse como desarrollo de software y debe estar sujeto a los mismos controles.

La información contenida en sistemas públicos no debe contener información restringida, confidencial o de uso interno. De igual manera, los equipos que brindan servicios Web, correo electrónico, comercio electrónico u otros servicios públicos no deben almacenar información restringida, confidencial o de uso interno. Antes que un empleado del Banco libere información que no sea de uso general debe verificarse la identidad del individuo u organización recipiente utilizando firmas digitales, referencias de terceros, conversaciones telefónicas u otros mecanismos similares.

Debe establecerse controles sobre equipos de oficina como teléfonos, faxes e impresoras que procesan información sensible del Banco.

Información restringida o confidencial solo debe imprimirse en equipos específicamente designados para esta tarea.

6.5.3.3 Seguridad para media en tránsito

La información a ser transferida en media digital o impresa debe ser etiquetada con la clasificación de información respectiva y detallando claramente el remitente y recipiente del mismo. La información enviada por servicios postales debe ser protegida de accesos no autorizados mediante la utilización de:

- Paquetes sellados o lacrados
- Entrega en persona
- Firmado y sellado de un cargo

6.6 SEGURIDAD FÍSICA DE LAS INSTALACIONES DE PROCESAMIENTO DE DATOS

Se deben implementar medidas de seguridad física para asegurar la integridad de las instalaciones y centros de cómputo. Las medidas de protección deben ser consistentes con el nivel de clasificación de los activos y el valor de la información procesada y almacenada en las instalaciones.

6.6.1 Protección de las instalaciones de los centros de datos

Un centro de procesamiento de datos o de cómputo es definido como cualquier edificio o ambiente dentro de un edificio que contenga equipos de almacenamiento, proceso o transmisión de información. Estos incluyen pero no se limitan a los siguientes:

- Mainframe, servidores, computadoras personales y periféricos
- Consolas de administración
- Librerías de cassettes o DASD
- Equipos de telecomunicaciones

- Centrales telefónicas, PBX
- Armarios de alambrado eléctrico o cables

Los controles deben de ser evaluados anualmente para compensar cualquier cambio con relación a los riesgos físicos.

Los gerentes que estén planeando o revisando cualquier ambiente automatizado, incluyendo el uso de las computadoras personales, deben contactarse con el personal encargado de la administración de la seguridad de la información para asistencia en el diseño de los controles físicos de seguridad.

6.6.2 Control de acceso a las instalaciones de cómputo

El acceso a cualquier instalación de cómputo debe estar restringido únicamente al personal autorizado.

Todas las visitas deben ser identificadas y se debe mantener un registro escrito de las mismas. Estas visitas deben ser en compañía de un empleado durante la permanencia en las instalaciones de computo.

Si bien es recomendable que los proveedores de mantenimiento, a quienes se les otorga acceso continuo a las áreas sensibles, estén siempre acompañados por un empleado autorizado de la empresa, puede resultar poco práctico en algunos casos.

Todo el personal en las instalaciones de cómputo deben de portar un carné, placa o ficha de identificación. Sistemas automatizados de seguridad para acceso físico deben de ser instalados en centros de cómputo principales. Centros pequeños pueden controlar el acceso físico mediante el uso de candados de combinación o llaves.

Medidas apropiadas como guardias o puertas con alarmas, deben de ser utilizadas para proteger las instalaciones durante las horas no laborables.

El retiro de cualquier equipo o medio electrónico de las instalaciones de cómputo debe de ser aprobado por escrito por personal autorizado.

6.6.3 Acuerdo con regulaciones y leyes

Los controles de seguridad física deben de estar en acuerdo con las regulaciones existentes de fuego y seguridad, así como con los requerimientos contractuales de los seguros contratados.

6.7 ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIONES

La administración de las comunicaciones y operaciones del Banco, son esenciales para mantener un adecuado nivel de servicio a los clientes. Los requerimientos de seguridad deben ser desarrollados e implementados para mantener el control sobre las comunicaciones y las operaciones.

Los procedimientos operacionales y las responsabilidades para mantener accesos adecuados a los sistemas, así como el control y la disponibilidad de los mismos, deben ser incluidas en las funciones operativas del Banco. Todas las comunicaciones e intercambios de información, tanto dentro de las instalaciones y sistemas del Banco como externas a ella, deben ser aseguradas, de acuerdo al valor de la información protegida.

6.7.1 Procedimientos y Responsabilidades Operacionales

6.7.1.1 Procedimientos operativos documentados

Todos los procedimientos de operación de los sistemas deben ser documentados y los cambios realizados a dichos procedimientos deben ser autorizados por la gerencia respectiva.

Todos los procedimientos de encendido y apagado de los equipos deben ser documentados; dichos procedimientos deben incluir el detalle de personal clave a ser contactado en caso de fallas no contempladas en el procedimiento regular documentado.

Todas las tareas programadas en los sistemas para su realización periódica, deben ser documentadas. Este documento debe incluir tiempo

de inicio, tiempo de duración de la tarea, procedimientos en caso de falla, entre otros.

Los procedimientos para resolución de errores deben ser documentados, entre ellos se debe incluir:

- Errores en la ejecución de procesos por lotes
- Fallas o apagado de los sistemas
- Códigos de error en la ejecución de procesos por lotes
- Información de los contactos que podrían colaborar con la resolución de errores.

6.7.1.2 Administración de operaciones realizadas por terceros

Todos los procesos de operación realizados por terceros deben ser sujetos a una evaluación de riesgos de seguridad y se debe desarrollar procedimientos para administrar estos riesgos.

- Asignación de responsables para la supervisión de dichas actividades
- Determinar si se procesará información crítica.
- Determinar los controles de seguridad a implementar
- Evaluar el cumplimiento de los estándares de seguridad del Banco.
- Evaluar la implicancia de dichas tareas en los planes de contingencia del negocio
- Procedimientos de respuesta ante incidentes de seguridad
- Evaluar el cumplimiento de los estándares del Banco referentes a contratos con terceros.

6.7.1.3 Control de cambios operacionales

Todos los cambios realizados en los sistemas del Banco, a excepción de los cambios de emergencia, deben seguir los procedimientos de cambios establecidos.

Solo el personal encargado de la administración de la seguridad puede realizar o aprobar un cambio de emergencia. Dicho cambio debe ser documentado y aprobado en un periodo máximo de 24 horas luego de haberse producido el cambio.

Los roles del personal involucrado en la ejecución de los cambios en los sistemas deben encontrarse debidamente especificados.

Los cambios deben ser aprobados por la gerencia del área usuaria, el personal encargado de la administración de la seguridad de la información y el encargado del área de sistemas. Todos los requerimientos de cambios deben ser debidamente documentados, siguiendo los procedimientos para cambios existentes en el Banco. Antes de la realización de cualquier cambio a los sistemas se debe generar copias de respaldo de dichos sistemas.

6.7.1.4 Administración de incidentes de seguridad

Luego de reportado el incidente de seguridad, éste debe ser investigado por el área de seguridad informática. Se debe identificar la severidad del incidente para la toma de medidas correctivas.

El personal encargado de la administración de la seguridad debe realizar la investigación de los incidentes de forma rápida y confidencial.

Se debe mantener una documentación de todos los incidentes de seguridad ocurridos en el Banco.

Se debe mantener intacta la evidencia que prueba la ocurrencia de una violación de seguridad producida tanto por entes internos o externos, para su posterior utilización en procesos legales en caso de ser necesario.

6.7.1.5 Separación de funciones de operaciones y desarrollo

El ambiente de prueba debe de mantenerse siempre separado del ambiente de producción, debiendo existir controles de acceso adecuados para cada uno de ellos.

El ambiente de producción es aquel en el cual residen los programas ejecutables de producción y los datos necesarios para el funcionamiento de los mismos. Solo el personal autorizado a efectuar los cambios en los sistemas debe contar con privilegios de escritura en los mismos.

Los programas compiladores no deben ser instalados en los sistemas en producción, todo el código debe ser compilado antes de ser transferido al ambiente de producción.

Las pruebas deben de realizarse utilizando datos de prueba. Sin embargo, copias de datos de producción pueden ser usadas para las pruebas, siempre y cuando los datos sean autorizados por el propietario y manejados de manera confidencial.

El personal de desarrollo puede tener acceso de solo lectura a los datos de producción. La actualización de los permisos de acceso a los datos de producción debe de ser autorizada por el propietario de información y otorgada por un periodo limitado.

Se deben utilizar estándares de nombres para distinguir el conjunto de nombres de las tareas y de los datos, del modelo y de los ambientes de producción.

Un procedimiento de control de cambio debe de asegurar que todos los cambios del modelo y ambientes de producción hayan sido revisados y aprobados por el (los) gerente(s) apropiados.

6.7.2 Protección contra virus

El área de seguridad informática debe realizar esfuerzos para determinar el origen de la infección por virus informático, para evitar la reinfección de los equipos del Banco.

La posesión de virus o cualquier programa malicioso está prohibida a todos los usuarios. Se tomarán medidas disciplinarias en caso se encuentren dichos programas en computadoras personales de usuarios.

Todos los archivos adjuntos recibidos a través del correo electrónico desde Internet deben ser revisados por un antivirus antes de ejecutarlos.

Asimismo está prohibido el uso de diskettes y discos compactos provenientes de otra fuente que no sea la del mismo BANCO ABC, a excepción de los provenientes de las interfaces con organismos reguladores, proveedores y clientes, los cuales necesariamente deben pasar por un proceso de verificación y control en el área de Sistemas (Help Desk), antes de ser leídos.

El programa antivirus debe encontrarse habilitado en todos las computadoras del Banco y debe ser actualizado periódicamente. En caso de detectar fallas en el funcionamiento de dichos programas éstas deben ser comunicadas al área de soporte técnico. El programa antivirus debe ser configurado para realizar revisiones periódicas para la detección de virus en los medios de almacenamiento de las computadoras del Banco.

Debe contarse con un procedimiento para la actualización periódica de los programas antivirus y el monitoreo de los virus detectados.

Es obligación del personal del Banco, emplear sólo los programas cuyas licencias han sido obtenidas por el Banco y forman parte de su plataforma estándar. Asimismo, se debe evitar compartir directorios o archivos con otros usuarios; en caso de ser absolutamente necesario, coordinar con la Gerencia respectiva y habilitar el acceso sólo a nivel de lectura, informando al Departamento de Producción y Soporte Técnico.

Todo el personal del Banco debe utilizar los protectores de pantalla y/o papel tapiz autorizados por la Institución; el estándar es:

Papel Tapiz: BANCO ABC

Protector de Pantalla: BANCO ABC.

6.7.3 Copias de respaldo

Los Custodios de información deben definir un cronograma para la retención y rotación de las copias de respaldo, basado en los requerimientos establecidos por los Propietarios de información, incluyendo el almacenamiento en uno o más ubicaciones distintos a las del centro de cómputo. Los Custodios de información son también responsables de asegurar que se generen copias de respaldo del software de los servidores del Banco, y que las políticas de manipulación de información se ejercen para las copias de respaldo trasladadas o almacenadas fuera de los locales del Banco. Debe formalmente definirse procedimientos para la creación y recuperación de copias de respaldo.

Trimestralmente deben efectuarse pruebas para probar la capacidad de restaurar información en caso sea necesario. Estas pruebas deben efectuarse en un ambiente distinto al ambiente de producción.
Los usuarios deben generar copias de respaldo de información crítica transfiriendo o duplicando archivos a la carpeta personal establecida para dicho fin por la Gerencia de Sistemas, la cual se encuentra ubicada en uno de los servidores del Banco. Deben generarse copias de respaldo de estos servidores según un cronograma definido por los Custodios de información.

Las cintas con copias de respaldo deben ser enviadas a un local remoto periódicamente, basándose en un cronograma determinado por la gerencia del Banco.
Los mensajes electrónicos, así como cualquier información considerada importante, deben ser guardados en copias de respaldo y retenidos por dispositivos automáticos.

6.8 CONTROL DE ACCESO DE DATOS

La información manejada por los sistemas de información y las redes asociadas debe estar adecuadamente protegida contra modificaciones no autorizadas, divulgación o destrucción. El uso inteligente de controles de acceso previene errores o negligencias del personal, así como reduce la posibilidad del acceso no autorizado.

6.8.1 Identificación de Usuarios

Cada usuario de un sistema automatizado debe de ser identificado de manera única, y el acceso del usuario así como su actividad en los sistemas debe de ser controlado, monitoreado y revisado.

Cada usuario de un sistema debe tener un código de identificación que no sea compartido con otro usuario. Para lograr el acceso a los sistemas automatizados, se requiere que el usuario provea una clave que solo sea conocida por él.

Debe establecerse un procedimiento para asegurar que el código de identificación de un usuario sea retirado de todos los sistemas cuando un empleado es despedido o transferido.

Los terminales y computadoras personales deben bloquearse luego de quince (15) minutos de inactividad. El usuario tendrá que autenticarse antes de reanudar su actividad.

El usuario debe ser instruido en el uso correcto de las características de seguridad del terminal y funciones de todas las plataformas, estaciones de trabajo, terminales, computadoras personales, etc., y debe cerrar la sesión o bloquear la estación de trabajo cuando se encuentre desatendida.

Todos los consultores, contratistas, proveedores y personal temporal deben tener los derechos de acceso cuidadosamente controlados. El acceso solo debe ser válido hasta el final del trimestre o incluso antes, dependiendo de la terminación del contrato.

Todos los sistemas deben proveer pistas de auditoria del ingreso a los sistemas y violaciones de los mismos. A partir de estos datos, los custodios de los sistemas deben elaborar reportes periódicos los cuales deben ser revisados por el área de seguridad informática. Estos reportes también deben incluir la identidad del usuario, y la fecha y hora del evento. Si es apropiado, las violaciones deben ser reportadas al gerente del individuo. Violaciones repetitivas o significantes o atentados de accesos deben ser reportados al gerente a cargo de la persona y al área de seguridad de la información.

6.8.2 Seguridad de contraseñas

6.8.2.1 Estructura

Todas las contraseñas deben tener una longitud mínima de ocho (8) caracteres y no deben contener espacios en blanco.

Las contraseñas deben ser difíciles de adivinar. Palabras de diccionario, identificadores de usuario y secuencias comunes de caracteres, como por ejemplo “12345678” o “QWERTY”, no deben ser empleadas. Así mismo, detalles personales como los nombres de familiares, número de documento de identidad, número de teléfono o fechas de cumpleaños no deben ser usadas salvo acompañados con otros caracteres adicionales que no tengan relación directa. Las contraseñas deben incluir al menos un carácter no alfanumérico. Las contraseñas deben contener al menos un carácter alfabético en mayúscula y uno en minúscula.

6.8.2.2 Vigencia

Todas las contraseñas deben expirar dentro de un periodo que no exceda los noventa (90) días. Cada gerente debe determinar un máximo periodo de vigencia de las contraseñas, el cual es recomendable no sea menos de (30) días.

6.8.2.3 Reutilización de contraseñas

No debe permitirse la reutilización de ninguna de las 5 últimas contraseñas. Esto asegura que los usuarios no utilicen las mismas contraseñas en intervalos regulares. Los usuarios no deben poder cambiar sus contraseñas más de una vez al día.

A los usuarios con privilegios administrativos, no se les debe permitir la reutilización de las últimas 13 contraseñas.

6.8.2.4 Intentos fallidos de ingreso

Todos los sistemas deben estar configurados para deshabilitar los identificadores de los usuarios en caso de ocurrir (3) intentos fallidos de autenticación.

En los casos que los sistemas utilizados no soporten controles para las características establecidas para la estructura, vigencia, reutilización e intentos fallidos de ingreso, se debe documentar la excepción a la política, detallando la viabilidad de modificar la aplicación para soportar las características establecidas para las contraseñas.

6.8.2.5 Seguridad de contraseñas

Es importante que todos los empleados protejan sus contraseñas, debiéndose seguir las siguientes regulaciones:

- Bajo ninguna circunstancia, se debe escribir las contraseñas en papel, o almacenarlas en medios digitales no encriptados.
- Las contraseñas no deben ser divulgadas a ningún otro usuario salvo bajo el pedido de un gerente, con autorización del área de seguridad informática y auditoria interna. Si se divulga la contraseña, esta debe ser cambiada durante el próximo ingreso.
- El usuario autorizado es responsable de todas las acciones realizadas por alguna persona a quién se le ha comunicado la contraseña o identificador de usuario.

- Los sistemas no deben mostrar la contraseña en pantalla o en impresiones, para prevenir que éstas sean observadas o recuperadas.
- Las contraseñas deben estar siempre encriptadas cuando se encuentren almacenadas o cuando sean transmitidas a través de redes.
- El control de acceso a archivos, bases de datos, computadoras y otros sistemas de recursos mediante contraseñas compartidas está prohibido.

6.8.3 Control de transacciones

Los empleados deben tener acceso únicamente al conjunto de transacciones en línea requeridas para ejecutar sus tareas asignadas. Este conjunto de transacciones debe estar claramente definido para prevenir alguna ocurrencia de fraude y malversación.

El conjunto de transacciones debe ser definido durante el proceso de desarrollo de sistemas, revisado periódicamente y mantenido por la gerencia Propietaria.

El acceso para la ejecución de transacciones sensibles debe ser controlado mediante una adecuada segregación de tareas. Por ejemplo, los usuarios que tengan permiso para registrar instrucciones de pago no deben poder verificar o aprobar su propio trabajo.

Toda operación realizada en los sistemas que afecten información sensible como saldos operativos contables, deben contar con controles duales de aprobación, dichos controles de aprobación deben ser asignados con una adecuada segregación de funciones.

Reportes de auditoria de transacciones sensibles o de alto valor deben ser revisadas por la gerencia usuaria responsable en intervalos regulares apropiados. Los reportes deben incluir la identidad del usuario, la fecha y la hora del evento.

6.8.4 Control de producción y prueba

El ambiente de prueba debe mantenerse siempre separado del ambiente de producción, se deben implementar controles de acceso adecuados en ambos ambientes.

Las pruebas deben realizarse utilizando datos de prueba. Sin embargo, copias de datos de producción pueden ser usadas para las pruebas, siempre y cuando los datos sean autorizados por el Propietario y manejados de manera confidencial.

El personal de desarrollo puede tener acceso de sólo lectura a los datos de producción. La actualización de los permisos de acceso a los datos de producción debe ser autorizada por el propietario y otorgada por un periodo limitado.

Estándares de nombres deben ser utilizados para distinguir los datos y programas de desarrollo y producción.

Un procedimiento de control de cambios debe asegurar que todos los cambios del modelo y ambientes de producción hayan sido revisados y aprobados por el (los) gerente(s) apropiados, y el personal encargado de la administración de la seguridad de la información.

Los programas de producción, sistemas operativos y librerías de documentación deben ser considerados datos confidenciales y ser protegidos.

Debe realizarse una adecuada segregación de tareas dentro del área de procesamiento de datos o sistemas. Las tareas del personal de soporte de aplicación, soporte técnico, y operadores del centro de datos deben estar claramente definidas y sus permisos de acceso a los datos deben basarse en los requerimientos específicos de su trabajo.

6.8.5 Controles de acceso de programas

Los controles de acceso de programas deben asegurar que los usuarios no puedan acceder a la información sin autorización.

Los programas deben poder generar una pista de auditoria de todos los accesos y violaciones.

Las violaciones de los controles de acceso deben ser registradas y revisadas por el propietario o por el personal del área de sistemas custodio de los datos. Las violaciones de seguridad deben ser reportadas al gerente del empleado y al área responsable de la administración de la seguridad de la información.

Se debe tener cuidado particular en todos los ambientes para asegurar que ninguna persona tenga control absoluto. Los operadores de sistemas, por ejemplo, no deben tener acceso ilimitado a los identificadores de superusuario. Dichos identificadores de usuario, son solo necesarios durante una emergencia y deben ser cuidadosamente controlados por la gerencia usuaria, quien debe realizar un monitoreo periódico de su utilización.

6.8.6 Administración de acceso de usuarios

La asignación de identificadores de usuario especiales o privilegiados (como cuentas administrativas y supervisores) debe ser revisada cada 3 meses.

Los propietarios de la información son responsables de revisar los privilegios de los sistemas periódicamente y de retirar todos aquellos que ya no sean requeridos por los usuarios. Es recomendable realizar revisiones trimestralmente debido al continuo cambio de los ambientes de trabajo y la importancia de los datos.

Es responsabilidad del propietario de la información y de los administradores de sistemas ver que los privilegios de acceso estén alineados con las necesidades del negocio, sean asignados basándose en requerimientos y que se comunique la lista correcta de accesos al área de sistemas de información.

En las situaciones donde los usuarios con accesos a información altamente sensible sean despedidos, los supervisores deben coordinar directamente con el área de seguridad informática para eliminar el acceso de ese usuario.

Se debe buscar el desarrollo de soluciones técnicas para evitar el uso de accesos privilegiados innecesarios.

Luego del despido o renuncia de algún empleado, es responsabilidad del jefe del empleado revisar cualquier archivo físico o digital elaborado o modificado por el usuario. El gerente debe también asignar la propiedad de dicha información a la persona relevante así como determinar la destrucción de los archivos innecesarios.

Todos los usuarios que tienen acceso a las cuentas privilegiadas deben tener sus propias cuentas personales para uso del negocio. Por ende, los administradores de sistemas y empleados con acceso a cuentas privilegiadas deben usar sus cuentas personales para realizar actividades de tipo no privilegiadas.

Cuentas de usuario que no son utilizadas por noventa (90) días deben ser automáticamente deshabilitadas. Las cuentas que no han sido utilizadas por un periodo largo demuestran que el acceso de información de ese sistema no es necesario. Los custodios de la información deben informar al propietario de la información la existencia de las cuentas inactivas.

Todos los accesos a los sistemas de información deben estar controlados mediante un método de autenticación incluyendo una combinación mínima de identificador de usuario/contraseña. Dicha combinación debe proveer la verificación de la identidad del usuario.

Para los usuarios con tareas similares, se debe utilizar grupos o controles de acceso relacionados a roles para asignar permisos y accesos a las cuentas del individuo.

Todos los usuarios de los sistemas de información deben de tener un identificador de usuario único que sea válido durante el período laboral del

usuario. Los identificadores de usuarios no deben de ser utilizados por otros individuos incluso luego de que el usuario original haya renunciado o haya sido despedido.

Los sistemas no deben permitir que los usuarios puedan tener sesiones múltiples para un mismo sistema, salvo bajo autorización específica del propietario de la información.

6.8.7 Responsabilidades del usuario

Todo equipo de cómputo, alquilado o de propiedad del Banco, así como los servicios compartidos facturados a cada unidad de negocio serán usados solo para actividades relacionadas al negocio del Banco.

Los sistemas del Banco no pueden ser usados para desarrollar software para negocios personales o externos al Banco.

Los equipos no deben ser usados para preparar documentos para uso externo, salvo bajo la aprobación escrita del gerente del área usuaria.

Se debe implementar protectores de pantallas en todas las computadoras personales y servidores, activándose luego de cinco (5) minutos de inactividad.

Toda la actividad realizada utilizando un identificador de usuario determinado, es de responsabilidad del empleado a quién le fue asignado. Por consiguiente, los usuarios no deben compartir la información de su identificador con otros o permitir que otros empleados utilicen su identificador de usuario para realizar cualquier acción. También, los usuarios están prohibidos de realizar cualquier acción utilizando un identificador que no sea el propio.

6.8.8 Seguridad de computadoras

Se debe mantener un inventario actualizado de todo el software y hardware existente en el Banco, la responsabilidad del mantenimiento del

inventario es del jefe de producción de la gerencia de sistemas. Todo traslado o asignación de equipos debe ser requerida por el gerente del área usuaria, es de responsabilidad del jefe de producción de la gerencia de sistemas, la verificación y realización del requerimiento.

Es de responsabilidad del usuario, efectuar un correcto uso del equipo de cómputo que le fue asignado, así como de los programas en él instalados; cualquier cambio y/o traslado deberá ser solicitado con anticipación por su respectiva Gerencia. Asimismo el usuario debe verificar que cualquier cambio y/o traslado del Equipo de Cómputo que le fue asignado, se realice por personal de Soporte Técnico, así como también la instalación o retiro de software.

Cualquier microcomputador, computadora personal o portátil / notebook perteneciente al Banco debe ser únicamente utilizada para propósitos de negocios. Estas computadoras pueden ser utilizadas de las siguientes maneras:

- Como un terminal comunicándose con otra computadora
- Como una computadora aislada que realice su propio procesamiento sin comunicación con ninguna otra computadora

Medidas apropiadas de seguridad de computadoras personales, como los programas de seguridad de computadoras personales o los candados físicos, deben ser utilizados en relación con los datos y aplicaciones en ejecución.

Sin importar su uso, las medidas de seguridad deben ser implementadas en todas las microcomputadoras y computadoras personales:

- Una vez habilitada la computadora, ésta no debe dejarse desatendida, incluso por un periodo corto.
- Todo los disquetes, cintas, CD´s y otros dispositivos de almacenamiento de información incluyendo información impresa, que contengan datos sensibles deben ser guardados en un ambiente seguro cuando no sean utilizados.

- El acceso a los datos almacenados en un microcomputador debe ser limitado a los usuarios apropiados.

Los discos duros no deben contener datos sensibles salvo en las computadoras cuyo acceso físico sea restringido o que tengan instalados un programa de seguridad y que los accesos a la computadora y a sus archivos sean controlados adecuadamente.

Los disquetes no deben ser expuestos a temperaturas altas o a elementos altamente magnéticos.

Deben generarse copias de respaldo de documentos y datos de manera periódica, asimismo, deben desarrollarse procedimientos para su adecuada restauración en el caso de pérdida.

Todos los programas instalados en las computadoras deben ser legales, aprobados y periódicamente inventariados.

Solo los programas adquiridos o aprobados por el Banco, serán instalados en las computadoras del Banco.

El uso de programas de juegos, de distribución gratuita (freeware o shareware) o de propiedad personal está prohibido, salvo que éste sea aprobado por la gerencia y se haya revisado la ausencia de virus en el mismo.

6.8.9 Control de acceso a redes

6.8.9.1 Conexiones con redes externas

Los sistemas de red son vulnerables y presentan riesgos inherentes a su naturaleza y complejidad. Los accesos remotos (*dial-in*) y conexiones con redes externas, exponen a los sistemas del Banco a niveles mayores de riesgo. Asegurando que todos los enlaces de una red cuenten con adecuados niveles de seguridad, se logra que los activos más valiosos de las unidades de negocio estén protegidos de un ataque directo o indirecto.

Todas las conexiones realizadas entre la red interna del Banco e Internet, deben ser controladas por un firewall para prevenir accesos no autorizados. El área de seguridad de información debe aprobar todas las conexiones con redes o dispositivos externos.

El acceso desde Internet hacia la red interna del Banco no debe ser permitido sin un dispositivo de fuerte autenticación o certificado basado en utilización de contraseñas dinámicas.

El esquema de direccionamiento interno de la red no debe ser visible desde redes o equipos externos. Esto evita que “hackers” u otras personas pueden obtener fácilmente información sobre la estructura de red del Banco y computadoras internas.

Para eliminar las vulnerabilidades inherentes al protocolo TCP/IP, ruteadores y firewalls deben rechazar conexiones externas que parecieran originarias de direcciones internas (ip spoofing).

6.8.9.2 Estándares generales

Los accesos a los recursos de información deben solicitar como mínimo uno de los tres factores de autenticación:

- Factor de conocimiento: algo que solo el usuario conoce. Por ejemplo: contraseña o PIN.
- Factor de posesión: algo que solo el usuario posee. Por ejemplo: smartcard o token.
- Factor biométrico: algo propio de las características biológicas del usuario. Por ejemplo: lectores de retina o identificadores de voz.

La posibilidad de efectuar encaminamiento y re-direccionamiento de paquetes, debe ser configurada estrictamente en los equipos que necesiten realizar dicha función.

Todos los componentes de la red deben mostrar el siguiente mensaje de alerta en el acceso inicial.

"Aviso de alerta: Estos sistemas son de uso exclusivo del personal y agentes autorizados del Banco. El uso no autorizado está prohibido y sujeto a penalidades legales".

Todos los componentes de la red de datos deben ser identificados de manera única y su uso restringido. Esto incluye la protección física de todos los puntos vulnerables de una red.

Las estaciones de trabajo y computadoras personales deben ser bloqueadas mediante la facilidad del sistema operativo, mientras se encuentren desatendidas.

Todos los dispositivos de red, así como el cableado deben ser ubicado de manera segura.

Cualquier unidad de control, concentrador, multiplexor o procesador de comunicación ubicado fuera de una área con seguridad física, debe estar protegido de un acceso no autorizado.

6.8.9.3 Política del uso de servicio de redes

Todas las conexiones de red internas y externas deben cumplir con las políticas del Banco sobre servicios de red y control de acceso. Es responsabilidad del área de sistemas de información y seguridad de información determinar lo siguiente:

- Elementos de la red que pueden ser accedidos
- El procedimiento de autorización para la obtención de acceso
- Controles para la protección de la red.

Todos los servicios habilitados en los sistemas deben contar con una justificación coherente con las necesidades del negocio. Los riesgos asociados a los servicios de red deben determinarse y ser resueltos antes de la implementación del servicio. Algunos servicios estrictamente prohibidos incluyen TFTP e IRC/Chat.

6.8.9.4 Segmentación de redes

La arquitectura de red del Banco debe considerar la separación de redes que requieran distintos niveles de seguridad. Esta separación debe realizarse de acuerdo a la clase de información albergada en los sistemas que constituyen dichas redes. Esto debe incluir equipos de acceso público.

6.8.9.5 Análisis de riesgo de red

Cualquier nodo de la red de datos, debe asumir el nivel de sensibilidad de la información o actividad de procesamiento de datos más sensible al que tenga acceso. Se deben implementar controles que compensen los riesgos más altos.

6.8.9.6 Acceso remoto(*dial-in*)

Los usuarios que ingresen a los sistemas del Banco mediante acceso remoto (*dial-in*) deben ser identificados antes de obtener acceso a los sistemas. Por lo tanto, dicho acceso debe ser controlado por un equipo que permita la autenticación de los usuarios al conectarse a la red de datos.

Técnicas y productos apropiadas para el control de los accesos remotos (*dial-in*) incluyen:

- Técnicas de identificación de usuarios: Técnicas que permitan identificar de manera unívoca al usuario que inicia la conexión, es recomendable que la técnica elegida utilice por lo menos 2 de los factores de autenticación definidos anteriormente. Ejemplo: tokens (dispositivos generadores de contraseñas dinámicas).
- Técnicas de identificación de terminales: Técnicas que permiten identificar unívocamente al terminal remoto que realiza la conexión. Ejemplo: callback (técnica que permite asegurar que el número telefónico fuente de la conexión sea autorizado)

6.8.9.7 Encripción de los datos

Los algoritmos de encripción DES, 3DES y RSA son técnicas de encripción aceptables para las necesidades de los negocios de hoy. Estas pueden ser empleadas para satisfacer los requerimientos de encripción de datos del Banco.

Las contraseñas, los códigos o números de identificación personal y los identificadores de terminales de acceso remoto deben encontrarse encriptados durante la transmisión y en su medio de almacenamiento. La encripción de datos ofrece protección ante accesos no autorizados a la misma; debe ser utilizada si luego de una evaluación de riesgo se concluye que es necesaria.

6.8.10 Control de acceso al sistema operativo

6.8.10.1 Estándares generales

Los usuarios que posean privilegios de superusuario, deben utilizar el mismo identificador con el que se autentican normalmente en los sistemas. Los administradores deben otorgarle los privilegios especiales a los identificadores de los usuarios que lo necesiten.

Todos los usuarios deben poseer un único identificador. El uso de identificadores de usuario compartidos debe estar sujeto a autorización. Cada cuenta de usuario debe poseer una contraseña asociada, la cual solo debe ser conocida por el dueño del identificador de usuario. Seguridad adicional puede ser añadida al proceso, como identificadores biométricos o generadores de contraseñas dinámicas.

6.8.10.2 Limitaciones de horario

Las aplicaciones críticas deben estar sujetas a periodos de acceso restringidos, el acceso a los sistemas en un horario distinto debe ser deshabilitado o suspendido.

6.8.10.3 Administración de contraseñas

Los administradores de seguridad deben realizar pruebas mensuales sobre la calidad de las contraseñas que son empleadas por los usuarios, esta actividad puede involucrar el uso de herramientas para obtención de contraseñas.

Todas las bases de datos o aplicaciones que almacenen contraseñas deben ser aseguradas, de tal manera, que solo los administradores de los sistemas tengan acceso a ellas.

6.8.10.4 Inactividad del sistema

Las sesiones en los sistemas que no se encuentren activas por mas de 30 minutos deben ser concluidas de manera automática.

Las computadoras personales, laptops y servidores, deben ser configurados con un protector de pantalla con contraseña, cuando sea aplicable. El periodo de inactividad para la activación del protector de pantalla debe ser de 5 minutos.

Los sistemas deben forzar la reautenticación de los usuarios luego de 2 horas de inactividad.

6.8.10.5 Estándares de autenticación en los sistemas

Los sistemas, durante el proceso de autenticación, deben mostrar avisos preventivos sobre los accesos no autorizados a los sistemas.

Los identificadores de los usuarios deben ser bloqueados luego de 3 intentos fallidos de autenticación en los sistemas, el desbloqueo de la cuenta debe ser realizado manualmente por el administrador del sistema.

Los sistemas deben ser configurados para no mostrar ninguna información que pueda facilitar el acceso a los mismos, luego de intentos fallidos de autenticación.

6.8.11 Control de acceso de aplicación

6.8.11.1 Restricciones de acceso a información

Para la generación de cuentas de usuario en los sistemas así como para la asignación de perfiles, el gerente del área usuaria es el responsable de presentar la 'Solicitud de Usuarios y/o Perfiles de Acceso a los Sistemas de Cómputo', al área de Seguridad Informática, quien generará los Usuarios y Contraseñas correspondientes, para luego remitirlas al Departamento de Recursos Humanos, para que éste a su vez los entregue al Usuario Final, con la confidencialidad requerida.

Se debe otorgar a los usuarios acceso solamente a la información mínima necesaria para la realización de sus labores.

Esta tarea puede ser realizada utilizando una combinación de:

- Seguridad lógica de la aplicación.
- Ocultar opciones no autorizadas en los sistemas
- Restringir el acceso a línea de comando
- Limitar los permisos a los archivos de los sistemas (solo lectura)
- Controles sobre la información de salida de los sistemas (reportes, consultas en línea, etc.)

6.8.11.2 Aislamiento de sistemas críticos

Basados en el tipo de información, las redes pueden requerir separación. Los sistemas que procesan información muy crítica deben ser aislados físicamente de sistemas que procesan información menos crítica.

6.8.12 Monitoreo del acceso y uso de los sistemas

6.8.12.1 Sincronización del reloj

Los relojes de todos los sistemas deben ser sincronizados para asegurar la consistencia de todos los registros de auditoria. Debe desarrollarse un

procedimiento para el ajuste de cualquier desvío en la sincronización de los sistemas.

6.8.12.2 Responsabilidades generales

Los administradores de los sistemas deben realizar monitoreo periódico de los sistemas como parte de su rutina diaria de trabajo, este monitoreo no debe estar limitado solamente a la utilización y performance del sistema sino debe incluir el monitoreo del acceso de los usuarios a los sistemas.

6.8.12.3 Registro de eventos del sistema

La actividad de los usuarios vinculada al acceso a información clasificada como “confidencial” o “restringida” debe ser registrada para su posterior inspección. El propietario de la información debe revisar dicho registro mensualmente.

Todos los eventos de seguridad relevantes de una computadora que alberga información confidencial, deben ser registrados en un log de eventos de seguridad. Esto incluye errores en autenticación, modificaciones de datos, utilización de cuentas privilegiadas, cambios en la configuración de acceso a archivos, modificación a los programas o sistema operativo instalados, cambios en los privilegios o permisos de los usuarios o el uso de cualquier función privilegiada del sistema.

Los “logs” (bitácoras) de seguridad deben ser almacenados por un periodo mínimo de 3 meses. Acceso a dichos logs debe ser permitido solo a personal autorizado. En la medida de lo posible, los logs deben ser almacenados en medios de “solo lectura”.

6.8.13 Computación móvil y teletrabajo

6.8.13.1 Responsabilidades generales

Los usuarios que realizan trabajo en casa con información del Banco, pueden tener el concepto errado de que la seguridad de información solo es aplicable en el trabajo en oficina, sin tomar en cuenta que algunas amenazas de seguridad son comunes en ambos entornos de trabajo y que incluso existen algunas nuevas amenazas en el trabajo en casa. El personal que realiza trabajo en casa debe tener en cuenta las amenazas de seguridad que existen en dicho entorno laboral y tomar las medidas apropiadas para mantener la seguridad de información.

La utilización de programas para el control remoto de equipos como PC-Anywhere está prohibida a menos que se cuente con el consentimiento formal del administrador de seguridad. La utilización inapropiada de este tipo de programas puede facilitar el acceso de un intruso a los sistemas de información del Banco.

6.8.13.2 Acceso remoto

Medidas de seguridad adicionales deben ser implementadas para proteger la información almacenada en dispositivos móviles. Entre las medidas a tomarse se deben incluir:

- Encripción de los datos
- Contraseñas de encendido
- Concientización de usuarios
- Protección de la data transmitida hacia y desde dispositivos móviles. Ej. VPN, SSL o PGP.
- Medidas de autenticación adicionales para obtener acceso a la red de datos. Ej. SecureID tokens.

Con el propósito de evitar los problemas relacionados a virus informáticos y propiedad de los datos existentes en computadoras externas, solamente equipos del Banco deben ser utilizados para ser conectados a su red de datos. La única excepción a este punto es la conexión hacia el servidor de correo electrónico para recepción y envío del correo electrónico.

Todos los accesos dial-in/dial-out deben contar con autorización del área de seguridad informática y deben contar con la autorización respectiva que justifique su necesidad para el desenvolvimiento del negocio.

6.9 DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

El diseño de la infraestructura del Banco, las aplicaciones de negocio y las aplicaciones del usuario final deben soportar los requerimientos generales de seguridad documentados en la política de seguridad del Banco. Estos requerimientos deben ser incorporados en cada paso del ciclo de desarrollo de los sistemas, incluyendo todas las fases de diseño, desarrollo, mantenimiento y producción.

Los requerimientos de seguridad y control deben estar:

- determinados durante cualquier diseño de sistemas,
- desarrollados dentro de la arquitectura del sistema
- implementados en la instalación final del sistema.

Adicionalmente, todo los procesos de desarrollo y soporte a estos sistemas deben seguir los requerimientos de seguridad incluidos en esta política de seguridad.

6.9.1 Requerimientos de seguridad de sistemas

6.9.1.1 Control de cambios

El área responsable de la administración de cambios debe retener todos los formularios de solicitud de cambio, planes de cambio de programa y

resultados de pruebas de acuerdo con los estándares de retención de registros del Banco. Los gerentes técnicos de las áreas son responsables de retener una copia de la documentación de solicitud de cambio pertinente a su respectiva área.

Los procedimientos de prueba deben estar documentados en los formularios de solicitud de cambio. Si se notara problemas durante el proceso de prueba, el proveedor debe documentar el problema, realizar las modificaciones apropiadas en el ambiente de desarrollo y entregarlo para que se vuelva a probar.

6.9.1.2 Análisis y especificación de los requerimientos de seguridad

Para todos los sistemas desarrollados por o para el Banco, se debe determinar los requerimientos de seguridad antes de comenzar la fase de desarrollo de la aplicación. Durante la fase de diseño del sistema, los propietarios de la información, el área de sistemas y el área de seguridad de la información deben determinar un control adecuado para el ambiente de la aplicación. Estos requerimientos deben incluir, pero no están limitadas a:

- Control de acceso
- Autorización
- Criticidad del sistema
- Clasificación de la información
- Niveles de disponibilidad requeridos
- Confidencialidad e integridad de la información

6.9.2 Seguridad en sistemas de aplicación

6.9.2.1 Desarrollo y prueba de aplicaciones

Los procedimientos de prueba deben estar adecuadamente documentados en los formularios de solicitud de cambio. El gerente del desarrollador debe efectuar una revisión independiente de los resultados de la unidad de prueba. Como resultado, se debe evidenciar una aprobación formal por parte del gerente del desarrollador en el formulario de solicitud de cambio.

Durante la prueba de integración, restricciones de acceso lógico deben asegurar que los desarrolladores no tengan accesos de actualización y que el código siendo probado no sea modificado sin consentimiento del usuario. Copias de los datos de producción o conjuntos prediseñados de datos de prueba deben ser usados para propósitos de prueba.

Todas las modificaciones significativas, mejoras grandes y sistemas nuevos deben ser probados por los usuarios del sistema antes de la instalación del software en el ambiente de producción. El plan de aceptación del usuario debe incluir pruebas de todas las funciones principales, procesos y sistemas de interfaces. Los procedimientos de prueba deben ser adecuadamente documentados en los formularios de solicitud de cambio.

Durante las pruebas de aceptación, restricciones lógicas de acceso deben asegurar que los desarrolladores no tengan acceso de actualización y que el código fuente siendo probado no pueda ser modificado sin consentimiento escrito por el usuario. Si se notara problemas, el usuario debe documentar el problema, el desarrollador debe realizar las modificaciones apropiadas en el ambiente de desarrollo y lo entregará para volver a probarlo.

6.10 CUMPLIMIENTO NORMATIVO

Toda ley, norma, regulación o acuerdo contractual debe ser documentado y revisado por el área legal del Banco. Requerimientos específicos para controles y otras actividades relacionadas a estas regulaciones legales deben ser delegados al área organizacional respectiva, la cual es responsable por el cumplimiento de la norma en cuestión.

Los recursos informáticos del Banco deben ser empleados exclusivamente para tareas vinculadas al negocio.

6.10.1 Registros

Deben desarrollarse estándares de retención, almacenamiento, manejo y eliminación de registros que son requeridos por normas legales u otras regulaciones. Debe definirse un cronograma de retención para estos registros que debe incluir:

- Tipo de información
- Regulaciones o leyes aplicables
- Fuentes de este tipo de información
- Tiempos de retención requeridos
- Requerimientos de traslado y almacenamiento
- Procedimientos de eliminación
- Requerimientos de control específicos estipulados en la norma relacionada

6.10.2 Revisión de la política de seguridad y cumplimiento técnico

Los gerentes y jefes deben asegurarse que las responsabilidades de seguridad sean cumplidas y las funciones relacionadas se ejecuten apropiadamente.

Es responsabilidad del personal encargado de la administración de la seguridad y de auditoria interna verificar el cumplimiento de las políticas

de seguridad. Las excepciones deben ser reportadas a la gerencia apropiada.

6.10.3 Propiedad de los programas

Cualquier programa escrito por algún empleado del Banco dentro del alcance de su trabajo así como aquellos adquiridos por el Banco son de propiedad del Banco.

Los contratos para desarrollo externo deben acordarse por escrito y deben señalar claramente el propietario de los derechos del programa. En la mayoría de circunstancias, el Banco debería ser propietaria de todos los programas de cómputo desarrollados, debiendo pagar los costos de desarrollo.

Cada programa elaborado por desarrolladores propios del Banco o por desarrolladores externos contratados por el Banco, debe contener la información de derecho de autor correspondiente. Generalmente, el aviso debe aparecer en cuando el usuario inicie la aplicación. Un aviso legible también debe estar anexado a las copias de los programas almacenados en dispositivos como cartuchos, cassettes, discos o disquetes.

6.10.4 Copiado de software adquirido y alquilado

Los contratos con proveedores y paquetes propietarios de software deben definir claramente los límites de su uso. Los empleados están prohibidos de copiar o utilizar dicho software de manera contraria a la provisión del contrato. Toda infracción de los derechos de autor del software constituye robo.

Los productos adquiridos o alquilados para ejecutarse en una unidad de procesamiento o en un sitio particular no deben ser copiados y ejecutados en procesadores adicionales sin algún acuerdo por parte del proveedor.

Los programas no pueden ser copiados salvo dentro del límite acordado con el proveedor (por ejemplo, copias de respaldo para protección). Los empleados o contratistas que realicen copias adicionales para evitar el costo de adquisición de otro paquete serán hechos responsables de sus acciones.

6.11 CONSIDERACIONES DE AUDITORIA DE SISTEMAS

6.11.1 Protección de las herramientas de auditoria

Todas las herramientas, incluyendo programas, aplicaciones, documentación y papeles de trabajo, requeridos para la auditoria de sistemas deben protegerse de amenazas posibles como se indica en esta política de seguridad.

6.11.2 Controles de auditoria de sistemas

Todas las actividades de auditoria deben ser revisadas para el planeamiento y la ejecución correcta de la auditoria. Esto incluye, pero no se limita a lo siguiente:

- minimizar cualquier interrupción de las operaciones del negocio
- acuerdo de todas las actividades y objetivos de auditoria con la gerencia
- límite del alcance de la evaluación de un ambiente controlado, asegurando que no se brinde accesos impropios para la realización de las tareas de auditoria
- identificación de los recursos y habilidades necesarias para cualquier tarea técnica
- registro de todas las actividades y desarrollo de la documentación de las tareas realizadas, procedimientos de auditoria, hallazgos y recomendaciones.

6.12 POLÍTICA DE COMERCIO ELECTRÓNICO

El propósito de esta política es presentar un esquema para el comportamiento aceptable cuando se realizan actividades de comercio electrónico (e-commerce). Los controles definidos, tienen el propósito de proteger el comercio electrónico de numerosas amenazas de red que puedan resultar en actividad fraudulenta y divulgación o modificación de la información.

Esta política se aplica a todos los empleados del Banco involucrados con comercio electrónico y a los socios de comercio electrónico del Banco. Los socios de comercio electrónico del Banco incluyen las unidades de negocio de la organización, los clientes, socios comerciales y otros terceros.

El Banco debe asegurar la claridad de toda la información documentada y divulgar la información necesaria para asegurar el uso apropiado del comercio electrónico. El Banco y los socios de comercio electrónico deben de someterse a la legislación nacional sobre el uso de la información de clientes y las estadísticas derivadas.

Los documentos y transacciones electrónicas usadas en el comercio electrónico deben ser legalmente admisibles. Las unidades de negocio afiliadas del Banco deben demostrar que sus sistemas de cómputo funcionan adecuadamente para establecer la autenticación de los documentos y transacciones legales. Los sistemas de información usados deben estar de acuerdo con los estándares de seguridad corporativos antes de estar disponibles en producción.

Los sistemas de comercio electrónico deben publicar sus términos de negocios a los clientes. El uso de autoridades de certificación y archivos

confiables de terceros deben estar documentados, de acuerdo con la política de seguridad de información del Banco.

Actividades de roles y responsabilidades entre el Banco y los socios de comercio electrónico deben de establecerse, documentarse y ser soportadas por un acuerdo documentado que comprometa a ambos al acuerdo de los términos de transacciones.

6.12.1 Términos e información de comercio electrónico

6.12.1.1 Recolección de información y privacidad

El Banco debe utilizar niveles apropiados de seguridad según el tipo de información recolectada, mantenida y transferida a terceros debiendo asegurarse de:

- Aplicar estándares corporativos de encripción y autenticación para la transferencia de información sensible.
- Aplicar controles corporativos técnicos de seguridad para proteger los datos mantenidos por computadoras; y
- Considerar la necesidad de que los terceros involucrados en las transacciones de clientes, también mantengan niveles apropiados de seguridad.

El Banco debe adoptar prácticas de información que manejen cuidadosamente la información personal de los clientes. Todos los sistemas de comercio electrónico del Banco deben seguir una política de privacidad basada en principios de información, deben tomar medidas apropiadas para proveer seguridad adecuada y respetar las preferencias de los clientes con respecto al envío de mensajes de correo electrónico no solicitados.

6.12.1.2 Divulgación

El Banco debe proveer suficiente información sobre la propia transacción en línea, para permitir que los clientes tomen una decisión informada sobre si ejecutar las transacciones en línea.

Información divulgada debe incluir, pero no estar limitada a:

- Términos de transacción;
- Disponibilidad de producto e información de envío; y
- Precios y costos.

El Banco debe también brindar al cliente las opciones de:

- Revisión y aprobación de la transacción; y
- Recepción de una confirmación.

6.12.2 Transferencia electrónica de fondos

Transacciones de valor, sobre redes de telecomunicación, que resulten de movimientos de fondos, deben estar protegidas con medidas que sean proporcionales a la pérdida potencial debido a error o fraude. En sistemas donde el valor promedio de transacción excede los $50,000 o en los cuales transacciones sobre los $100,000 sean frecuentes, se debe verificar el origen de la transacción así como el contenido de la misma de acuerdo a los estándares definidos por el Banco.

Para todos los casos en que un mensaje de transferencia electrónica de fondos sea enviado sobre un circuito por lo menos se debe verificar el origen del mensaje mediante un método apropiado considerando el riesgo involucrado.

Algunas circunstancias requieren de la verificación de la ubicación física del terminal que origina la transacción, mientras que en otras una adecuada técnica usada para identificar el usuario del terminal es suficiente.

Los sistemas que utilicen soluciones de encripción o autenticación deben usar los estándares de ANSI aceptados.
La encripción de la información transmitida es necesaria cuando el origen y el destino se encuentran conectados por un enlace físico de comunicación que pueda ser accedido por un tercero. Las soluciones de punto a punto son preferibles para redes multi-nodos.

Los datos de identificación personal como PIN's, PIC's y contraseñas no deben ser transmitidas o almacenadas sin protección en cualquier medio.
Los sistemas nuevos que involucren el movimiento de fondos o transacciones de valor sobre redes de telecomunicaciones debe incorporar estos controles en su diseño.

Cualquier cambio en los sistemas o redes existentes, deben respetar dichos controles.

6.13 INFORMACIÓN ALMACENADA EN MEDIOS DIGITALES Y FÍSICOS

Toda información almacenada en cualquier dispositivo o medio del Banco, incluyendo disquetes, reportes, códigos fuentes de programas de computadora, correo electrónico y datos confidenciales de los clientes, es propiedad del Banco.
Las prácticas de seguridad de datos deben ser consistentes para ser efectivas. Los datos sensibles deben ser protegidos, sin importar la forma en que sean almacenados.

6.13.1 Etiquetado de la información

Toda información impresa o almacenada en medios físicos transportables (cintas de backup, cd´s, etc.) que sean confidenciales o restringidas,

deben estar claramente etiquetadas como tal, con letras grandes que sean legibles sin la necesidad de un lector especial.

Todo documento o contenedor de información debe ser etiquetado como "Restringida", "Confidencial", de "Uso interno" o de Acceso "General", dependiendo de la clasificación asignada.

Todo documento en formato digital o impreso, debe presentar una etiqueta en la parte superior e inferior de cada página, con la clasificación correspondiente.

Todo documento clasificado como "Confidencial" o "Restringido" debe contar con una carátula en la cual se muestre la clasificación de la información que contiene.

6.13.2 Copiado de la información

Reportes confidenciales y restringidos no deben ser copiados sin la autorización del propietario de la información.

Reportes confidenciales pueden ser copiados sólo para los individuos autorizados a conocer su contenido. Los gerentes son los responsables de determinar dicha necesidad, para cada persona a la cual le sea distribuido dicho reporte.

Los reportes restringidos deben ser controlados por un solo custodio, quién es responsable de registrar los individuos autorizados que soliciten el documento.

El copiado de cualquier dato restringido o confidencial almacenado en un medio magnético debe ser aprobado por el propietario y clasificado al igual que el original.

6.13.3 Distribución de la información

La información confidencial y restringida debe ser controlada cuando es trasmitida por correo electrónico interno, externo o por courier. Si el

servicio de courier o correo externo es usado, se debe solicitar una confirmación de entrega al receptor.

Los reportes confidenciales y otros documentos sensibles deben usarse en conjunto con sobres confidenciales y estos últimos también ser sellados. Materiales restringidos de alta sensibilidad deben enviarse con un sobre etiquetado 'Solo a ser abierto por el destinatario'. La entrega personal es requisito para la información extremadamente sensible.

Los datos sensibles de la empresa que sean transportados a otra instalación deben ser transportados en contenedores apropiados.

Todo usuario, antes de transmitir información clasificada como "Restringida" o "Confidencial", debe asegurarse que el destinatario de la información esté autorizado a recibir dicha información.

La transmisión de información clasificada como "Restringida" o "Confidencial", transmitida desde o hacia el Banco a través de redes externas, debe realizarse utilizando un medio de transmisión seguro, es recomendable el uso de técnicas de encripción para la información transmitida.

6.13.4 Almacenamiento de la información

Los activos de información correspondiente a distintos niveles de clasificación, deben ser almacenados en distintos contenedores.

La información etiquetada como "de uso interno" debe ser guardada de manera que sea inaccesible a personas ajenas a la empresa. La información "Confidencial o "Restringida" debe ser asegurada para que esté sólo disponible a los individuos específicamente autorizados para acceder a ella.

El ambiente donde se almacena la información clasificada como "Restringida", debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia. El acceso debe ser

permitido solo al personal formalmente autorizado. Personal de limpieza debe ingresar al ambiente acompañado por personal autorizado.

La información en formato digital clasificada como de acceso “General”, puede ser almacenada en cualquier sistema del Banco. Sin embargo se deben tomar las medidas necesarias para no mezclar información “General” con información correspondiente a otra clasificación.

Información en Formato digital, clasificada como “Restringida”, debe ser encriptada con un método aprobado por el área de seguridad informática, cuando es almacenada en cualquier medio (disco duro, disquetes, cintas, CD´s, etc.).

Los medios de almacenamiento, incluyendo discos duros de computadoras, que albergan información clasificada como “Restringida”, deben ser ubicados en ambientes cerrados diseñados para el almacenamiento de dicho tipo de información.
Cuando información clasificada como “de uso Interno”, Confidencial o Restringida se guarde fuera del Banco, debe ser almacenada en instalaciones que cuenten con adecuados controles de acceso.
El envío y recepción de medios magnéticos para ser almacenados en instalaciones alternas debe ser autorizado por el personal responsable de los mismos y registrado en bitácoras apropiadas.

6.13.5 Eliminación de la información

La eliminación de documentos y otras formas de información deben asegurar la confidencialidad de la información de las unidades de negocio.

Se debe borrar los datos de los medios magnéticos, como cassettes, disquetes, discos duros, DASD, que se dejen de usar en el Banco debido a daño u obsolencia, antes de que estos sean eliminados.

En el caso de los equipos dañados, la empresa de reparación o destrucción del equipo debe certificar que los datos hayan sido destruidos o borrados.