Capítulo IV

SEGURIDAD DE LA INFORMACIÓN – ROLES Y ESTRUCTURA ORGANIZACIONAL

4.1 Situación actual

La administración de seguridad de información se encuentra distribuida principalmente entre las áreas de sistemas y el área de seguridad informática.
En algunos casos, la administración de accesos es realizada por la jefatura o gerencia del área que utiliza la aplicación.

Las labores de seguridad realizadas actualmente por el área de seguridad informática son las siguientes:

- Creación y eliminación de usuarios
- Verificación y asignación de perfiles en las aplicaciones

Las labores de seguridad realizadas por el área de sistemas son las siguientes:

- Control de red
- Administración del firewall
- Administración de accesos a bases de datos

Las funciones de desarrollo y mantenimiento de políticas y estándares de seguridad no están definidas dentro de los roles de la organización.
Cabe mencionar que el acceso con privilegio administrativo al computador central es restringido, el área de seguridad informática define una contraseña, la cual es enviada a la oficina de seguridad (Gerencia de Administración) en un sobre cerrado, en caso de necesitarse acceso con dicho privilegio, la contraseña puede ser obtenida por el gerente de sistemas o el jefe de soporte

técnico y producción, solicitando el sobre a la oficina de seguridad. Luego deben realizar un informe sobre la actividad realizada en el computador central.

4.2 ROLES Y RESPONSABILIDADES DE LA ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE INFORMACIÓN

El área organizacional encargada de la administración de seguridad de información debe soportar los objetivos de seguridad de información del Banco. Dentro de sus responsabilidades se encuentran la gestión del plan de seguridad de información así como la coordinación de esfuerzos entre el personal de sistemas y los empleados de las áreas de negocios, siendo éstos últimos los responsables de la información que utilizan. Asimismo, es responsable de promover la seguridad de información a lo largo de la organización con el fin de incluirla en el planeamiento y ejecución de los objetivos del negocio.

Es importante mencionar que las responsabilidades referentes a la seguridad de información son distribuidas dentro de toda la organización y no son de entera responsabilidad del área de seguridad informática, en ese sentido existen roles adicionales que recaen en los propietarios de la información, los custodios de información y el área de auditoria interna.
Los propietarios de la información deben verificar la integridad de su información y velar por que se mantenga la disponibilidad y confidencialidad de la misma.

Los custodios de información tienen la responsabilidad de monitorear el cumplimiento de las actividades encargadas y el área de auditoria interna debe monitorear el cumplimiento de la política de seguridad y el cumplimiento adecuado de los procesos definidos para mantener la seguridad de información.

A continuación presentamos los roles y responsabilidades relacionadas a la administración de seguridad de información:

Área de Seguridad Informática.

El área organizacional encargada de la administración de seguridad de información tiene como responsabilidades:

- Establecer y documentar las responsabilidades de la organización en cuanto a seguridad de información.
- Mantener la política y estándares de seguridad de información de la organización.
- Identificar objetivos de seguridad y estándares del Banco (prevención de virus, uso de herramientas de monitoreo, etc.)
- Definir metodologías y procesos relacionados a la seguridad de información.
- Comunicar aspectos básicos de seguridad de información a los empleados del Banco. Esto incluye un programa de concientización para comunicar aspectos básicos de seguridad de información y de las políticas del Banco.
- Desarrollar controles para las tecnologías que utiliza la organización. Esto incluye el monitoreo de vulnerabilidades documentadas por los proveedores.
- Monitorear el cumplimiento de la política de seguridad del Banco.
- Controlar e investigar incidentes de seguridad o violaciones de seguridad.
- Realizar una evaluación periódica de vulnerabilidades de los sistemas que conforman la red de datos del Banco.
- Evaluar aspectos de seguridad de productos de tecnología, sistemas o aplicaciones utilizados en el Banco.
- Asistir a las gerencias de división en la evaluación de seguridad de las iniciativas del negocio.
- Verificar que cada activo de información del Banco haya sido asignado a un “propietario” el cual debe definir los requerimientos de seguridad como

políticas de protección, perfiles de acceso, respuesta ante incidentes y sea responsable final del mismo.

- Administrar un programa de clasificación de activos de información, incluyendo la identificación de los propietarios de las aplicaciones y datos.
- Coordinación de todas las funciones relacionadas a seguridad, como seguridad física, seguridad de personal y seguridad de información almacenada en medios no electrónicos.
- Desarrollar y administrar el presupuesto de seguridad de información.
- Reportar periódicamente a la gerencia de Administración y Operaciones.
- Administración de accesos a las principales aplicaciones del Banco.
- Elaborar y mantener un registro con la relación de los accesos de los usuarios sobre los sistemas y aplicaciones del Banco y realizar revisiones periódicas de la configuración de dichos accesos en los sistemas.
- Controlar aspectos de seguridad en el intercambio de información con entidades externas.
- Monitorear la aplicación de los controles de seguridad física de los principales activos de información.

Custodio de Información:

Es el responsable de la administración diaria de la seguridad en los sistemas de información y el monitoreo del cumplimiento de las políticas de seguridad en los sistemas que se encuentran bajo su administración. Sus responsabilidades son:

- Administrar accesos a nivel de red (sistema operativo).
- Administrar accesos a nivel de bases de datos.
- Administrar los accesos a archivos físicos de información almacenada en medios magnéticos (diskettes, cintas), ópticos (cd´s) o impresa.
- Implementar controles definidos para los sistemas de información, incluyendo investigación e implementación de actualizaciones de seguridad

de los sistemas (service packs, fixes, etc.) en coordinación con el área de seguridad informática.
- Desarrollar procedimientos de autorización y autenticación.
- Monitorear el cumplimiento de la política y procedimientos de seguridad en los activos de información que custodia.
- Investigar brechas e incidentes de seguridad.
- Entrenar a los empleados en aspectos de seguridad de información en nuevas tecnologías o sistemas implantados bajo su custodia.
- Asistir y administrar los procedimientos de backup, recuperación y plan de continuidad de sistemas.

Usuario:

Las responsabilidades de los usuarios finales, es decir, aquellas personas que utilizan información del Banco como parte de su trabajo diario están definidas a continuación:
- Mantener la confidencialidad de las contraseñas de aplicaciones y sistemas.
- Reportar supuestas violaciones de la seguridad de información.
- Asegurarse de ingresar información adecuada a los sistemas.
- Adecuarse a las políticas de seguridad del Banco.
- Utilizar la información del Banco únicamente para los propósitos autorizados.

Propietario de Información:

Los propietarios de información son los gerentes y jefes de las unidades de negocio, los cuales, son responsables de la información que se genera y se utiliza en las operaciones de su unidad. Las áreas de negocios deben ser conscientes de los riesgos de tal forma que sea posible tomar decisiones para disminuir los mismos.

Entre las responsabilidades de los propietarios de información se tienen:
- Asignar los niveles iniciales de clasificación de información.

- Revisión periódica de la clasificación de la información con el propósito de verificar que cumpla con los requerimientos del negocio.
- Asegurar que los controles de seguridad aplicados sean consistentes con la clasificación realizada.
- Determinar los criterios y niveles de acceso a la información.
- Revisar periódicamente los niveles de acceso a los sistemas a su cargo.
- Determinar los requerimientos de copias de respaldo para la información que les pertenece.
- Tomar las acciones adecuadas en caso de violaciones de seguridad.
- Verificar periódicamente la integridad y coherencia de la información producto de los procesos de su área.

Auditoria Interna:

El personal de auditoria interna es responsable de monitorear el cumplimiento de los estándares y guías definidas en las políticas internas. Una estrecha relación del área de auditoria interna con el área de seguridad informática es crítica para la protección de los activos de información. Por lo tanto dentro del plan anual de evaluación del área de auditoria interna se debe incluir la evaluación periódica de los controles de seguridad de información definidos por el Banco.

Auditoria interna debe colaborar con el área de seguridad informática en la identificación de amenazas y vulnerabilidades referentes a la seguridad de información del Banco.

4.3 ORGANIZACIÓN DEL AREA DE SEGURIDAD INFORMÁTICA PROPUESTA

Dado el volumen de operaciones y la criticidad que presenta la información para el negocio del Banco y tomando en cuenta las mejores prácticas de la industria, es necesaria la existencia de un área organizacional que administre la seguridad informática. Como requisito indispensable, esta área debe ser

independiente de la Gerencia de Sistemas, la cual en muchos casos es la ejecutora de las normas y medidas de seguridad elaboradas.

Este proceso de independización de la administración de la seguridad del área de sistemas ya fue iniciado por el Banco al crear el área de seguridad informática, la cual, reporta a la Gerencia de división de Administración y Operaciones.

Considerando la falta de recursos con el perfil requerido que puedan ser rápidamente reasignados, el proceso de entendimiento y asimilación de las responsabilidades, los roles definidos correspondientes al área de seguridad informática, y la necesidad de implementar un esquema adecuado de seguridad, proponemos definir una estructura organizacional de seguridad transitoria en la cual se creará un comité de coordinación de seguridad de la información para la definición de los objetivos del área y el monitoreo de las actividades de la misma.

El comité de coordinación de seguridad de la información, estará conformado por las siguientes personas:

- Gerente de división de Administración y Operaciones (presidente del comité).
- Jefe del área de seguridad informática (responsable del comité).
- Gerente de Sistemas.
- Auditor de Sistemas.
- Jefe del departamento de Riesgo Operativo y Tecnológico**.**

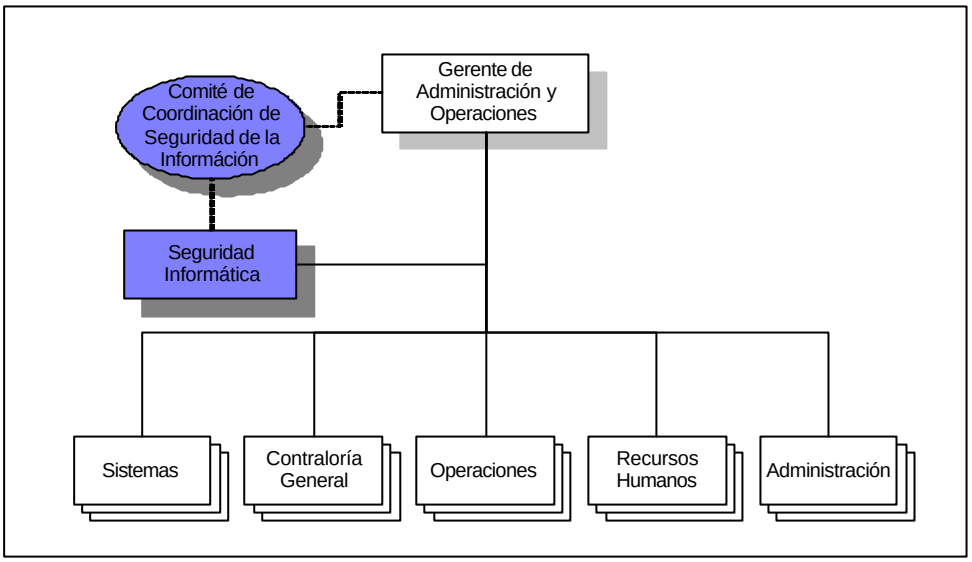

Fig. 1: Estructura organizacional transitoria propuesta para la administración de la seguridad de información.

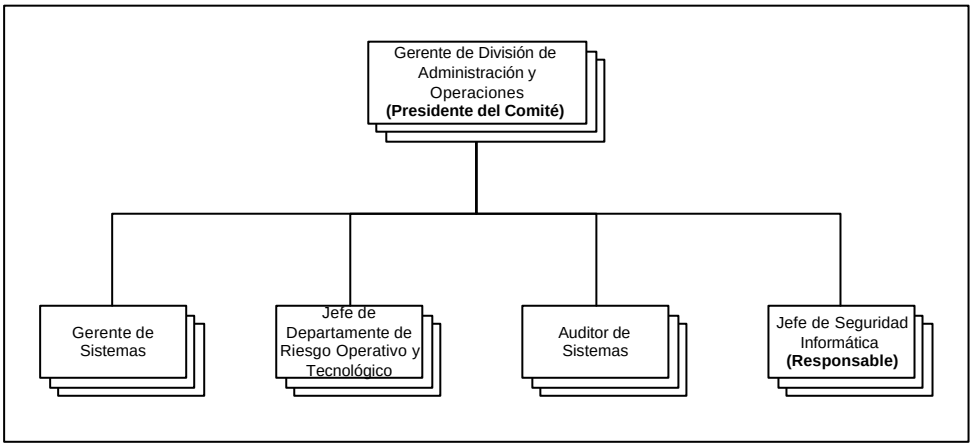

Fig. 2: Organización del Comité de coordinación de Seguridad de la Información.

Este comité, determinará el gradual traslado de las responsabilidades de seguridad al área de seguridad informática, monitoreará las labores realizadas por el área, colaborando a su vez con el entendimiento de la plataforma tecnológica, los procesos del negocio del Banco y la planificación inicial de actividades que desarrollará el área a corto plazo.

El comité de coordinación deberá reunirse con una frecuencia quincenal, con la posibilidad de convocar reuniones de emergencia en caso de existir alguna necesidad que lo amerite.

Es importante resaltar que luego que el área de seguridad informática haya logrado una asimilación de sus funciones, un entendimiento de los procesos del negocio del Banco y una adecuada interrelación con las gerencias de las distintas divisiones del Banco, el jefe de área de seguridad informática debe reportar directamente al Gerente de división de Administración y Operaciones, convirtiéndose el comité de coordinación de seguridad informática, en un ente consultivo, dejando la labor de monitoreo a la gerencia de división.