UNIVERSIDAD NACIONAL DE INGENIERÍA

Facultad de Ingeniería Industrial y de Sistemas

IMPLANTACIÓN DE LA FUNCIÓN DE SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN EN UNA ENTIDAD BANCARIA

INFORME DE SUFICIENCIA

Para optar el Título Profesional de:

INGENIERO DE SISTEMAS

MARTÍN FELIPE BLAS RIVERA

LIMA – PERÚ
2003

Con cariño para mi esposa Alejandra
y mis hijas Paola y Olenka,
por su tolerancia y comprensión
en estas largas horas recorridas,
y a mis padres quienes me
brindaron todo su apoyo.

INDICE

Descriptores Temáticos

1. *Seguridad*
2. *Seguridad de Información*
3. *Riesgos*
4. *Administración de Riesgos*
5. *Tecnología de Información*
6. *Plan de Continuidad de Negocios*
7. *Plan de Seguridad*
8. *Recuperación de Desastres*
9. *Plan de Contingencia*
10. *Políticas de Seguridad*

RESUMEN EJECUTIVO

El BANCO, es una de las instituciones financieras que actualmente se mantiene consolidado en el sistema financiero, empresa sólida y dinámica con presencia activa en los mercados que atiende, conformando grupo económico relevante con empresas peruanas importantes, siendo el principal accionista el Grupo F, y que viene operando en el Perú por más de once años manteniéndose a la vanguardia tecnológica. Las bases fundamentales de su misión son brindar a sus clientes un servicio de elevado nivel de personalización mediante servicios y productos de alta calidad y valor agregado, maximizar la rentabilidad de los accionistas y contribuir al desarrollo del personal que lo conforma.

Con el fin de cumplir con la misión comprometida el BANCO ha realizado esfuerzos para optimizar el servicio eficiente a los clientes que lo caracteriza mediante: la renovación tecnológica; mejora de los tiempos de atención y la calidad de servicio; confidencialidad, disponibilidad e integridad de la información, entre otros.

En ese contexto, en estos últimos años, se observa el tema de Seguridad de Tecnología de Información como una ventaja competitiva para proporcionar mayor confiabilidad a los clientes a través del cual sería posible centrarnos incuestionablemente en ellos: atender sus necesidades, analizar sus comportamientos, conocer su evolución, maximizar satisfacción y rentabilidad para el BANCO.

El presente informe plantea la necesidad de implementar la función de Seguridad de Tecnología de Información cuyo propósito es garantizar la protección de la información y los activos relacionados con su captación, almacenamiento, transmisión, proceso, distribución y uso, proporcionando consecuentemente confianza a los clientes, toda vez que actualmente las actividades relacionadas con la Seguridad de Tecnología de Información se vienen llevando en el BANCO en forma aislada o simplemente se desarrollan en forma deficiente.

Los objetivos de la función de Seguridad de Tecnología de Información son: 1) Maximizar los beneficios y valor agregado al negocio, cumpliendo con los requerimientos de seguridad, auditoría y control, manteniendo la disponibilidad, oportunidad e integridad de la información; 2) Minimizar los riesgos del negocio.

En el presente informe se describe la importancia de implementar la función de Seguridad de Tecnología de Información en la institución, así como sus objetivos, los problemas de seguridad y tipos de riesgos que impactan en el costo, los obstáculos claves para su implementación, las políticas de protección, las responsabilidades que se deben tener al respecto y las metodologías de evaluación de riesgo que se debe adoptar.

La identificación preliminar de los aspectos de seguridad existentes permitió lograr un adecuado respaldo por parte de la Alta Gerencia, logrando comprender en gran dimensión el rol de esta función y la importancia que ella tiene para el logro de los objetivos de la empresa, toda vez que ésta es realmente un “problema de negocios”.

Considerando que los problemas de seguridad tienen un gran impacto en el costo, dando como resultado pérdidas financieras; que el personal de tecnología y los directivos vienen tomando conciencia cada vez sobre las consecuencias; y que es importante contar con una unidad que vele por la

administración de la información que maneja el BANCO con una visión integral del negocio, se inició un proyecto para la implementación de la función de Seguridad de Tecnología de información.

Actualmente, el BANCO cuenta con una importante infraestructura tecnológica y viene implementando una arquitectura de Seguridad de Tecnología de Información que le permitirá diferenciarse competitivamente de sus similares, permitiendo brindar los servicios con valor agregado y gran confiabilidad para los clientes.

La implementación de la función de Seguridad de Tecnología de Información, permitirá mantener a esta institución en un lugar de vanguardia tecnológica en el sector financiero. Por lo cual es importante desarrollar una estrategia de actualización del modelo de arquitectura de Seguridad de Tecnología de información a fin de facilitar el proceso de desarrollo e incorporación de la política, estándares, procesos y servicios de seguridad adecuadas a las necesidades específicas de la organización.

El BANCO al igual que otras entidades financieras deberá enfrentar además del desarrollo tecnológico y de la diversidad de las plataformas tecnológicas, de la complejidad de las operaciones que hoy en día se realizan, de las amenazas latentes en un medio ambiente regido por la intensa competencia, el reto de los errores y el creciente crimen informático en una economía que cada día está más informatizada, haciendo necesario la aplicación de un enfoque estructurado de protección de los recursos informáticos.

INTRODUCCIÓN

La Seguridad de Tecnología de Información está orientada a disminuir, de manera importante, los riesgos específicos de tecnología de información de todo negocio posibilitando brindar servicios al cliente en forma más eficiente y confiable.

Asimismo, las diversas plataformas tecnológicas, la complejidad de las operaciones que hoy en día se realizan y las amenazas latentes en un medio ambiente regido por la intensa competencia, los errores y el creciente crimen informático, hacen necesaria la aplicación de un enfoque estructurado de protección de los recursos de tecnología de información.

El objetivo del presente trabajo es ***evaluar la problemática de seguridad de información y tecnologías relacionadas*** existente en una entidad bancaria de nuestro medio (BANCO en adelante) y formular una alternativa de solución integral que contribuya a garantizar la protección de los recursos informáticos mediante la ***implementación de la función de Seguridad de Tecnología de Información, bajo una Arquitectura de Seguridad*** (políticas, metodología de administración de riesgos, planes y estrategias que definen los servicios, mecanismos y objetos de seguridad, así como los estándares, estructuras organizacionales y procesos).

El proyecto de Seguridad de Tecnología de Información en el BANCO fue iniciado formalmente en el mes de febrero del año en curso y resume las experiencias del suscrito en las actividades de diagnóstico, planeamiento,

desarrollo e implementación de esta unidad funcional, así como el desarrollo de la Arquitectura de Seguridad de Tecnología de Información.

La Seguridad de Tecnología de Información significa un preciso control de la integridad, disponibilidad y confidencialidad de la información; su implementación en el BANCO con un enfoque moderno y adecuada administración, permitirá disminuir de manera importante los riesgos específicos del negocio.

Por tal razón surge la necesidad de implementar una unidad funcional con el objetivo de administrar en forma eficiente los aspectos inherentes a la Seguridad de Tecnología de Información existentes en la organización, siendo necesario contar con la percepción objetiva de la Alta Dirección que permita su implementación bajo un enfoque estratégico y como un elemento de decisión.

Este proyecto tuvo como logros más importantes: el reconocimiento y respaldo de la Alta Dirección, percibiendo a la administración de la Seguridad de Tecnología de Información como un componente fundamental para lograr los objetivos del negocio; el establecimiento de las bases tecnológicas para el desarrollo del programa y arquitectura de Seguridad de Tecnología de Información; la formalización, optimización e integración de la administración de la Seguridad de Tecnología de información a nivel corporativo, contribuyendo en el cambio de la cultura de protección y seguridad en la Institución; la adopción e incorporación de una metodología para la evaluación de riesgos, el desarrollo del Plan de Seguridad de Información y el desarrollo del Plan de Continuidad de Negocios, como parte del diseño de una arquitectura de seguridad corporativa; y la implementación de un centro de procesamiento de respaldo, que por mucho tiempo había quedado relegado por diversas razones.

Es importante mencionar que desde hace unos dos años se contaba con un computador alternativo (espejo), el cual fue producto de la adquisición de un

nuevo computador central por razones de mejora de capacidad y no por razones de un plan de seguridad; asimismo, esta solución parcial tenía la limitación de que el computador alternativo residía físicamente en el mismo centro de procesamiento principal.

La creación de una unidad organizativa encargada de las mismas.

Se consideró conveniente recomendar que la unidad propuesta se ubique como una Gerencia de Apoyo a la Gerencia Central de Medios Técnicos; y que esté a cargo de un profesional que cumpla con el perfil en sistemas de información y tecnologías relacionadas, con experiencia en gestión de riesgos e implementación de controles.

Si bien se estima que tal unidad requerirá estar integrada por un mínimo de 2 funcionarios, su exacta cantidad y perfil profesional deberá definirse por quien asuma su jefatura, a base de la organización interna y distribución de funciones que contemple para la misma.

Las limitaciones presentadas en este proyecto se encontraron inicialmente a nivel presupuestal, debido a que no estuvo considerado en el plan institucional, por lo cual no se contaron con fondos para asesorías y/o consultorías, personal y adquisición de equipamiento o software. Sin embargo, el éxito del proyecto abrió tecnologías relacionadas a la seguridad de tecnología de información, como es el caso de la reciente adquisición del Software de Monitoreo Monitor Byte (Anexo 4) y las capacitaciones vertidas en torno a la evaluación de riesgos y administración de seguridad de información.

CAPÍTULO I
ANTECEDENTES

1.1 DIAGNÓSTICO ESTRATÉGICO

La misión del BANCO, como institución financiera, es la siguiente

"Brindar a sus clientes un servicio de elevado nivel de personalización mediante servicios y productos de alta calidad y valor agregado, maximizar la rentabilidad de los accionistas y contribuir al desarrollo del personal que lo conforma. "

A continuación se presentan las principales conclusiones del proceso de Planificación Estratégica del BANCO realizado a inicios del 2001:

1.1.1. Fortalezas y Debilidades

Fortalezas

- Existe un alto grado de profesionalismo del personal, lo cual genera capacidad institucional para responder a los retos, calidad técnica de los trabajos y disposición para entrar en el proceso de desarrollo institucional.
- Se cuenta con recursos materiales suficientes y de adecuada calidad (infraestructura, equipo, mobiliarios, etc.)
- Disponibilidad tecnológica y adecuada cultura informática
- Eficiente calidad de servicio al cliente.
- Cultura empresarial (Anexo 1)

- Capacitación técnica y ética permanente. Esto es posibilidad de capacitar al personal interna y externamente, como resultado de los recursos disponibles y la importancia que se le da al tema.
- Buena formación académica.
- Personal comprometido y honesto.
- Remuneraciones promedio al mercado.
- El BANCO pertenece a un Grupo de Empresas importante y consolidada

Debilidades

- Descoordinación institucional. Uno de los principales problemas detectados a nivel interno es la descoordinación de recursos, la comunicación ineficiente y la individualidad que caracterizan la relación entre las unidades, lo que hace lento el trabajo.
- Inexperiencia para gerenciar en algunas jefaturas
- Falta de perfil de liderazgo en algunas jefaturas
- Retroalimentación inadecuada entre área operativa y normativa.
- Uso limitado de la información disponible.

1.1.2. Oportunidades y amenazas

Oportunidades

- Existencia adecuada de estabilidad política y legal.
- Crecimiento de la economía.
- Mejora en la gestión del Estado.
- Inversión extranjera adecuada.
- El desarrollo tecnológico en el ámbito de sistemas de información y comunicaciones ofrece nuevas oportunidades para lograr una mayor eficiencia.

Amenazas

- Alta competencia en el sector bancario
- Disposiciones reguladoras periódicas de los órganos de control

De acuerdo a lo anterior se trazaron los objetivos estratégicos externos e internos hacia el 2002:

Objetivos Estratégicos Externos

1. Ampliación de la masa crítica de clientes.
2. Cuota de mercado: mayor captación de depósitos.
3. Banco de clientes, banco de calidad
4. Implantación de nuevas oficinas, mayor cobertura de servicio, presencia del BANCO cerca del cliente

Objetivos Estratégicos Internos

5. Optimización de estructura de costos.
6. Eficiente comunicación interna.
7. Cultura de servicio al Cliente.
8. Difusión de la cultura empresarial
9. Óptima planificación y control de gestión.
10. Eficiente tecnología como elemento diferenciador en la relación con los clientes.
11. Banco sin papeles
12. Información como vector de soporte a la toma de decisiones
13. Implementación de la seguridad de tecnología de información.

Podemos concluir en este punto que la implementación de la Seguridad de Tecnología de Información, que motivó el presente informe, contribuyen al cumplimiento de los objetivos estratégicos, en particular de los objetivos 3, 7, 10, 11, 12 y 13.

1.2. DIAGNÓSTICO FUNCIONAL

1.2.1. ***Productos.*** El BANCO ofrece una serie de productos y servicios bancarios a sus clientes, como son:

- DEPÓSITOS Y OBLIGACIONES
  - CUENTAS CORRIENTES
  - CUENTA INTERAMERICANA
  - CUENTAS DE AHORROS
  - CUENTAS DE AHORRO EMPRESARIAL
  - CREDIAHORRO
  - CUENTAS A PLAZO
  - DEPÓSITOS C.T.S.
    CERTIFICADOS BANCARIOS EN M.E.
  - CERTIFICADO DE DEPÓSITO NEGOCIABLE
  - BONOS DE ARRENDAMIENTO FINANCIERO
  - BONOS SUBORDINADOS
  - LETRAS HIPOTECARIAS
- CRÉDITOS DIRECTOS
  - SOBREGIRO
  - CRÉDITO EN CUENTA CORRIENTE
  - AVANCE EN CUENTA CORRIENTE
  - AVANCE INMOBILIARIO - CONSTRUCCIÓN DE VIVIENDAS
  - AVANCE INMOBILIARIO - CONSTRUCCIÓN DE LOCALES
  - DESCUENTO DE LETRAS COMERCIALES
  - PRÉSTAMOS EMPRESARIALES
  - PRÉSTAMOS COMERCIALES HIPOTECARIOS
  - PRÉSTAMOS VEHICULARES
  - PRÉSTAMOS PERSONALES DE LIBRE DISPONIBILIDAD
  - PRÉSTAMOS CON LETRAS HIPOTECARIAS
  - PRÉSTAMOS PERSONALES HIPOTECARIOS
  - PRÉSTAMOS PERSONALES - MIVIVIENDA
  - PRÉSTAMOS PERSONALES - SUPERTECHO
  - PRÉSTAMOS CREDIAHORRO
  - ARRENDAMIENTO FINANCIERO
  - ARRENDAMIENTO FINANCIERO INMOBILIARIO
  - TARJETA DE CRÉDITO VISA INTERAMERICANA
  - MAESTRÍAS
- CRÉDITOS INDIRECTOS
  - AVALES

- CARTAS FIANZA
- CARTAS DE CRÉDITO DE IMPORTACIÓN
- CARTAS DE CRÉDITO DE EXPORTACIÓN CONFIRMADAS
- FINANCIAMIENTO DE IMPORTACIONES
- FINANCIAMIENTO DE EXPORTACIONES

• SERVICIOS DE CARTERA

- CARTAS DE CRÉDITO DE EXPORTACIÓN AVISADA
- COBRANZAS DE IMPORTACIÓN
- COBRANZAS DE EXPORTACIÓN
- CARTAS DE CRÉDITO STAND BY
- COBRANZAS LOCALES

• OTROS SERVICIOS

- COMPRA-VENTA DE MONEDA EXTRANJERA
- NEGOCIACIÓN DE CHEQUES
- TRANSPORTE DE CAUDALES
- CUSTODIA DE VALORES
- CAJAS DE SEGURIDAD
  CERTIFICACIÓN DE CHEQUES
- CHEQUES DE GERENCIA
- CHEQUES DE VIAJERO (TRAVELERS CHECK)
- GIROS AL EXTERIOR
- TRANSFERENCIAS
- TARJETA DE DÉBITO ELECTRÓN
- RECAUDACIÓN DE IMPUESTOS
- PAGOS
- HABERES
- TELEBANCA
- PAGO DE PENSIONES

Una de las características fundamentales de los productos y servicios brindados por el Banco es que éstos son diferenciados a los existentes en el mercado financiero.

1.2.2. ***Clientes***. El BANCO tiene 22,977 clientes aproximadamente, los cuales son captados mediante evaluaciones rigurosas y pertenecen fundamentalmente al sector económico A y B. Se encuentran distribuidos a través de las 17 agencias que tiene,

tanto en Lima como en Trujillo. Según el tipo de cliente se tiene:

- Personas naturales. 20,910 clientes que representan el 91% de los clientes.
- Personas jurídicas. 2,067 empresas que representan el 9% de los clientes.

1.2.3. *Proveedores*. Los proveedores pueden clasificarse de la siguiente manera:

- *De Recursos Operacionales*, como útiles de oficina, muebles y equipos de cómputo.
- *De infraestructura tecnológica*, hardware, software de base, manejador de base de datos, telecomunicaciones, telefonía, etc. Aquí destacan : IBM, Microsoft, Telefónica Perú, Proveedor del software integral Integral IBS, proveedor de software de monitoreo Monitor Byte (Anexo 4), entre otros.
- *De Servicios de Vigilancia y Seguridad,* como los proporcionados por el personal que controla el acceso al BANCO y seguimiento a las actividades efectuadas en las instalaciones de la institución.
- *De servicios de capacitación,* la administración bancaria, soportada con herramientas tecnológicas de avanzada, desarrolla una actividad eminentemente técnica donde el insumo principal es el conocimiento profesional por lo que este rubro es muy importante. Se contratan servicios a través de cursos pre-diseñados por la propia institución y también se contratan cursos a medida. Asimismo, en algunos casos la capacitación se recibe a través de las charlas y seminarios proporcionados por el personal con experiencia y conocimientos de las diversas áreas de la institución.

1.2.4. ***Procesos.*** Se pueden identificar 2 grandes procesos: Procesos de Atención a los Clientes (Front End, vinculados a la interacción con el cliente), Procesos Administrativos (Back End, apoyo a la labor técnica y administrativa).

Procesos de atención a los clientes (Front End). Los más importantes son:

- Captación de clientes y apertura de cuentas. Mediante las promotoras y ejecutivos de negocio (plataforma de atención al cliente).
- Operaciones transaccionales. Atención a los clientes en las ventanillas por los Representantes de Servicio a Clientes.

Procesos Administrativos (Back End). Los más importantes son:

- Administración, abastecimiento y servicios. Se encarga de la adquisición y provisión de bienes y servicios a las áreas solicitantes.
- Remuneraciones y Capacitación.
- Presupuesto. Determina, considerando los planes y proyectos establecidos, los recursos económicos y financieros requeridos para un ejercicio y controla su ejecución.
- Contabilidad. Realiza la contabilidad interna así como el cumplimiento de las obligaciones tributarias.
- Tesorería. Autoriza y supervisa los desembolsos de los clientes y define las tasas activas y pasivas.
- Tecnología de Información. Proporciona el soporte tecnológico y de procesamiento de la información.

- Auditoría. Verifica el cumplimiento de las normativas y políticas establecidas y evalúa los controles internos en los procesos operativos.
- Calidad de Servicio al cliente. Constantemente verifica el uso del protocolo para la contestación telefónica a los clientes internos y externos.

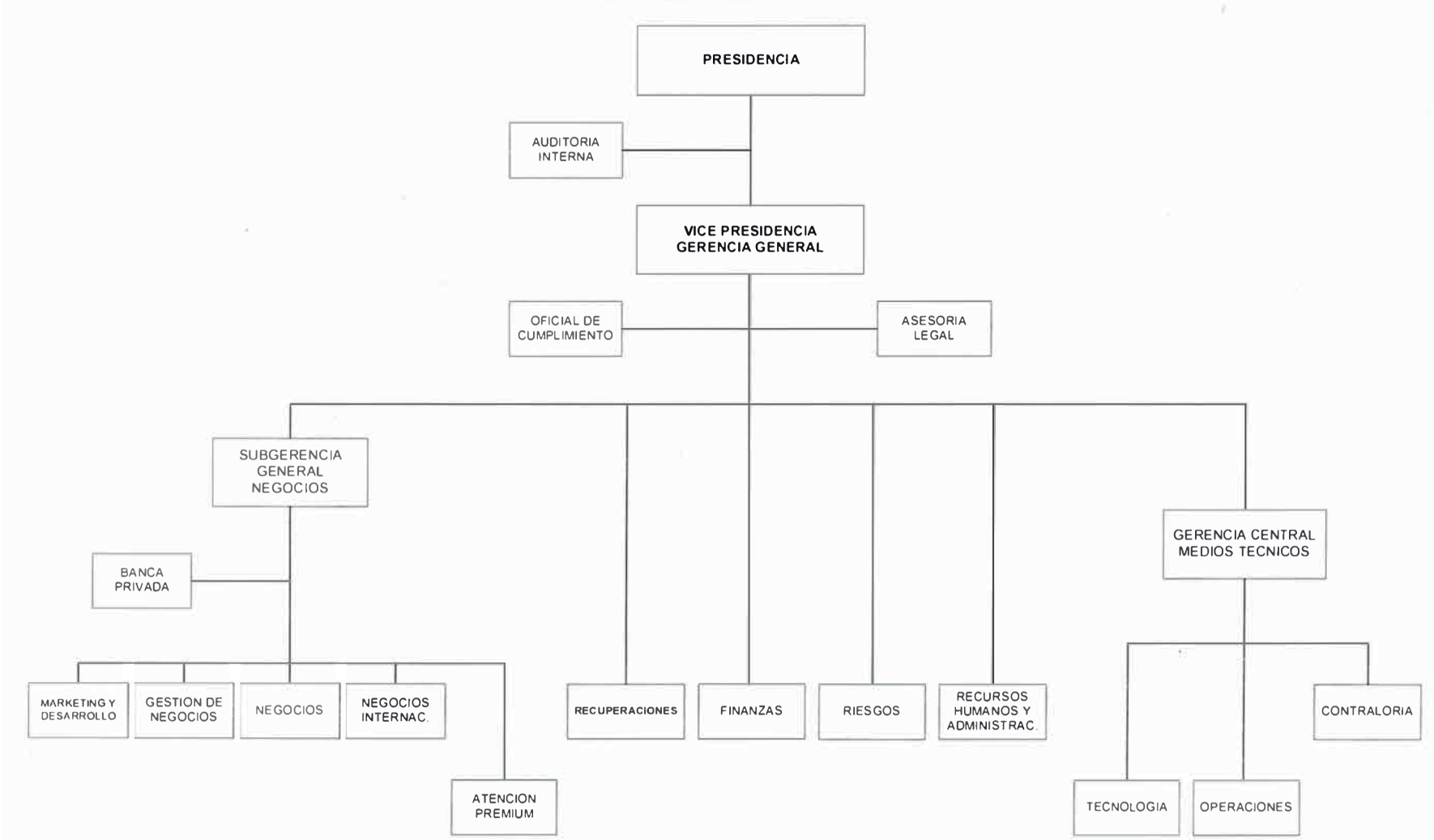
1.2.5. *Organización de la empresa.*

El BANCO cuenta con la siguiente estructura organizativa:

- Presidencia.
- Vicepresidencia Gerencia General. Encargada de administrar el BANCO con las funciones inherentes a la Alta Gerencia.
- Auditoría Interna. Reporta directamente al Directorio. Es el responsable de verificar que los diferentes procesos operativos y administrativos del BANCO, sean efectuados de acuerdo a la normatividad y control interno existentes, y de ser necesario, plantear recomendaciones de optimización, así como realizar las investigaciones correspondientes cuando se presuma que han ocurrido irregularidades en dichos procesos.
- Órgano de Apoyo. Conformado por :
  - Asesoría Legal. Es la encargada de prestar asesoría a la Vicepresidencia Gerencia General y a las diferentes áreas del BANCO. Se ocupa asimismo, de representar al BANCO en los procesos judiciales que ésta decida iniciar y de defender sus intereses en los procesos que en su contra se abran. Elabora los contratos, de modo que se asegure la protección de los intereses del BANCO.

- Sub-Gerencias Generales y Gerencias Centrales. Son las funciones de línea que a su vez están conformadas por Divisiones. Éstas son:
  - Sub-Gerencia General de Negocios. Encargada de administrar la red de agencias y responsable de que las agencias bajo su responsabilidad sean el medio más eficiente para brindar los diversos productos y servicios del BANCO.
  - Gerencia Central de Medios Técnicos. Asegura el funcionamiento de las áreas operativas evaluando y controlando su gestión. Brinda el soporte vinculado a Logística, Tesorería y Tecnología, proporcionando los sistemas, procedimientos e infraestructura tecnológica.
- Otras Divisiones. También son funciones de línea y que por ahora no reportan a una Sub-Gerencia General. Éstas son: Recuperaciones, Contraloría, Riesgos y Recursos Humanos.

ORGANIGRAMA GENERAL



CAPÍTULO II
MARCO TEÓRICO

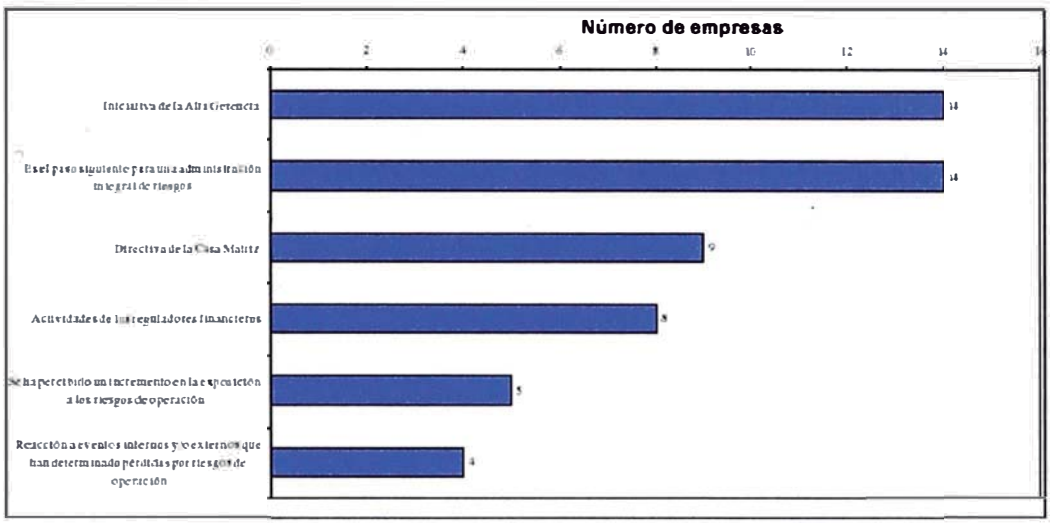
El objetivo del presente trabajo es evaluar la problemática de la seguridad de tecnología de información y formular una propuesta de solución integral en el BANCO. Es importante mencionar que las entidades financieras en nuestro medio no cuentan, en su gran mayoría, con una infraestructura de seguridad de tecnología de información, lo que implicó que tanto las tecnologías y herramientas, como las políticas y procedimientos relacionadas al tema se encontraban de manera informal y/o en evolución y no podría identificarse una experiencia exitosa que sirviera de guía a implantaciones futuras.

El reto, por lo tanto, para desarrollar una arquitectura de seguridad de tecnología de información era conjugar múltiples herramientas, departamentos, habilidades, tecnologías y metodologías en un ambiente de cambio rápido y permanente.

2.1. SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN

Diversas publicaciones muestran el crecimiento explosivo que viene experimentando en los últimos años la administración de la Seguridad de Tecnología de Información por parte de empresas de los más diversos sectores, quienes la definen como un "problema de negocio" y la utilizan como una herramienta estratégica para lograr los objetivos del negocio. Según algunas encuestas esta percepción es cada vez más notoria en las empresas, tal como se muestra en el cuadro adjunto.

Por qué ha iniciado o iniciaría actividades en torno a ROP?



Debido que el mercado es cada vez más competitivo y cambiante, a las empresas se les hace más difícil retener a sus clientes y captar nuevos, por lo que se ven en la necesidad de mejorar permanentemente la calidad de los productos y servicios que ofrecen. En consecuencia, demandan a sus áreas de tecnologías de la información la construcción de aplicaciones que brinden la funcionalidad y soporte respectivo para propósitos específicos buscando no sólo agilizar los procesos sino también brindar la seguridad en términos de integridad, disponibilidad y confiabilidad de la información tanto a la institución como a los clientes.

2.1.1. Definición de Seguridad de Tecnología de Información

Seguridad

Es la protección de los activos:

Personas

- Instalaciones
- Información
- Equipo
- Software

- Accesorios
- Medios de comunicación
- Capacidades de Cómputo
- Dinero

Seguridad de Tecnología de Información

Es la protección de la información y los activos relacionados con su captación, almacenamiento, transmisión, proceso, distribución y uso.

Su propósito es reducir la probabilidad de pérdida, a un nivel mínimo aceptable, a un costo razonable y asegurar la adecuada y pronta recuperación.

2.1.2. Riesgos de Seguridad de Tecnología de Información

La seguridad de tecnología de información está directamente relacionada al riesgo y al valor de la información que se debe proteger. La seguridad de tecnología de información se ha convertido en un aspecto crítico para todas las empresas debido a factores tales como:

- El incremento de la información de clientes correspondiente a sus datos individuales y actividad comercial.
- El incremento de la complejidad de las operaciones de la empresa y su dependencia en sistemas de información.
- Las consecuencias debidas a la pérdida de información crítica, por acciones maliciosas internas, externas o negligencia.
- El riesgo o la vulnerabilidad de la seguridad de tecnología de información de la empresa la cual puede ser explotada por agentes internos y externos.

2.1.3. Componentes de la Seguridad de Tecnología de Información

La seguridad de Tecnología de Información se establece a partir de un componente de gestión y un componente técnico:

- La gestión de seguridad está relacionada a la creación de la estructura organizacional responsable por la seguridad de tecnología de información, el desarrollo de políticas, estándares, guías y procedimientos.
- El componente técnico de seguridad tiene que ver con la evaluación de los entornos operativos y el uso de herramientas informáticas.

En conjunto ambos componentes establecen la arquitectura de seguridad de tecnología de información en la empresa cuyos objetivos son mantener la:

- *Confidencialidad*. Se refiere a que la información debe ser utilizada únicamente por las personas que por su función deben tener acceso a dicha información.
- *Integridad*. Comprende dos aspectos en seguridad de tecnología de información, el primero es que la información se crea a partir de datos que son correctos, y segundo que están completos, es decir que son datos confiables y verificables.
- *Disponibilidad*. La información debe estar disponible para los propósitos para los que fue creada y debe ser protegida mediante controles de acceso. La disponibilidad de información es un factor que afecta el resultado de la operación de la empresa.

Los entornos de seguridad que forman parte de la evaluación y formulación de la seguridad de información son cuatro:

1. El entorno del sistema operativo el cual alberga los sistemas y herramientas;
2. El entorno de bases de datos que almacena y custodia los datos operativos e informativos;
3. El entorno de aplicaciones el cual provee soporte operativo y de control a los procesos de la empresa;
4. El entorno de redes de datos el cual permite la interconexión de los usuarios y los entornos operativos internos (dominios de ambientes operativos) y externos (extranet, internet); y

5. Finalmente el entorno normativo que articula los aspectos de gestión y técnicos de la seguridad de tecnología de información.

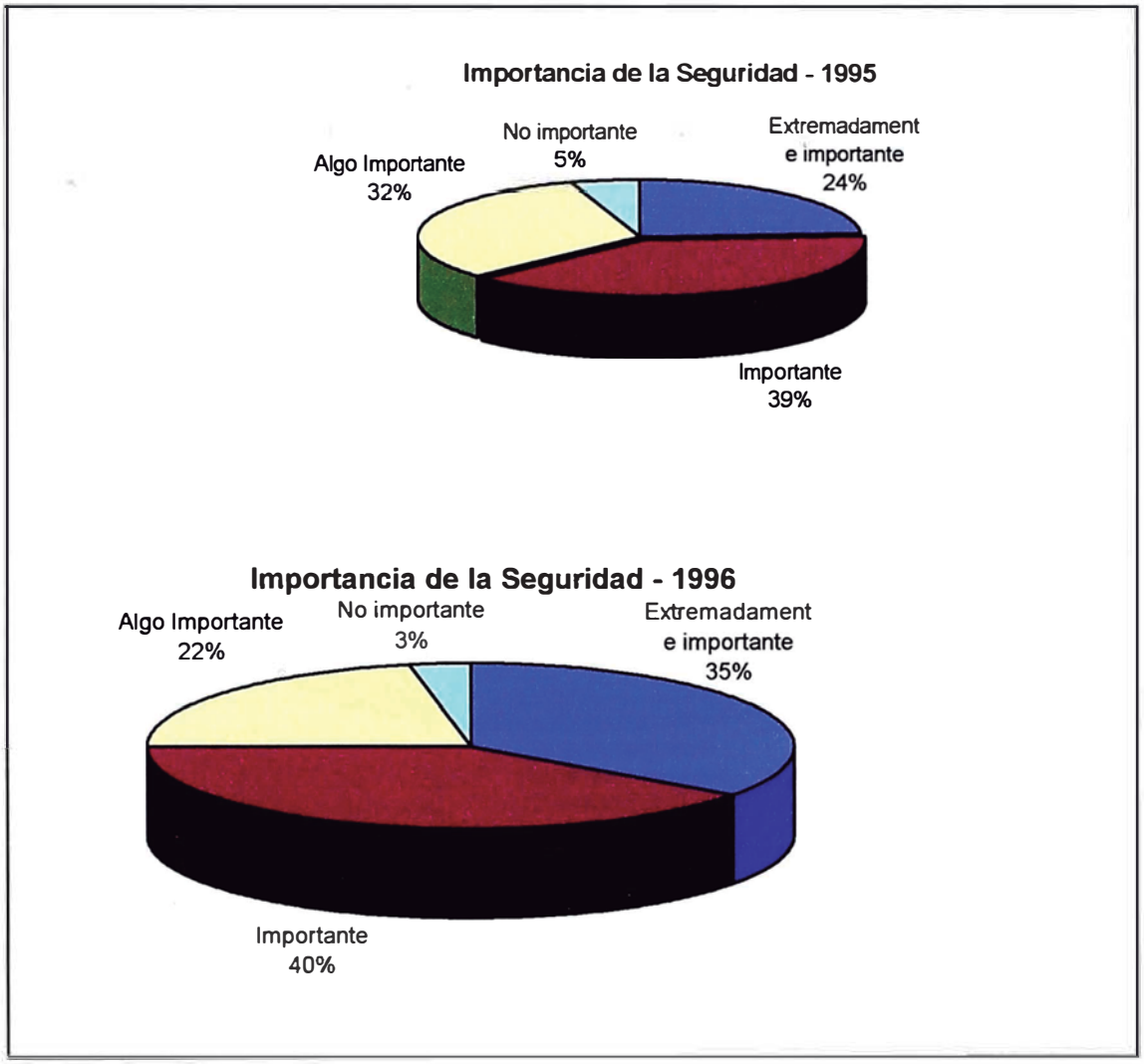
2.1.4. Funciones la Seguridad Tecnología de Información

1. Evitar o minimizar oportunidades de violación a sistemas informáticos
2. Evitar posibles daños o usos fraudulentos de recursos informáticos
3. Rutinas de controles periódicos al ambiente, normas y procedimientos
4. Identificar las violaciones o fraudes
5. Asegurar la continuidad del negocio

2.1.5. Importancia de la Seguridad Tecnología de Información

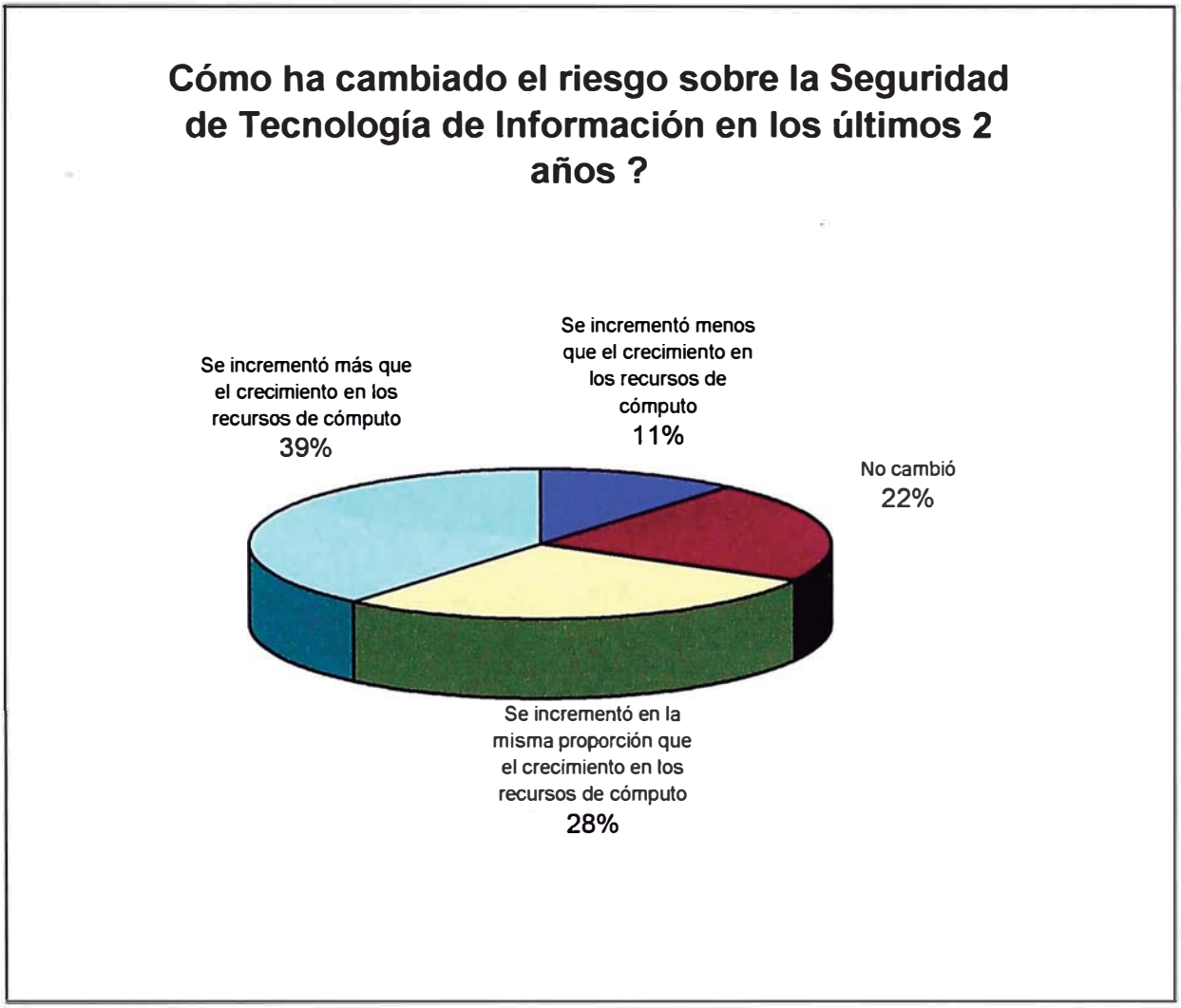
Hoy en día es importante la seguridad de tecnología de información porque:

- Las empresas enfrentan mayores riesgos por agentes más inteligentes, motivados y con mayores recursos
- La inversión tiempo / recursos en soluciones a problemas de seguridad pueden generar nuevas o mayores vulnerabilidades en interoperabilidad y administración
- Los riesgos sobre la información están cambiando de internos a combinación de internos-externos basados en conocimiento



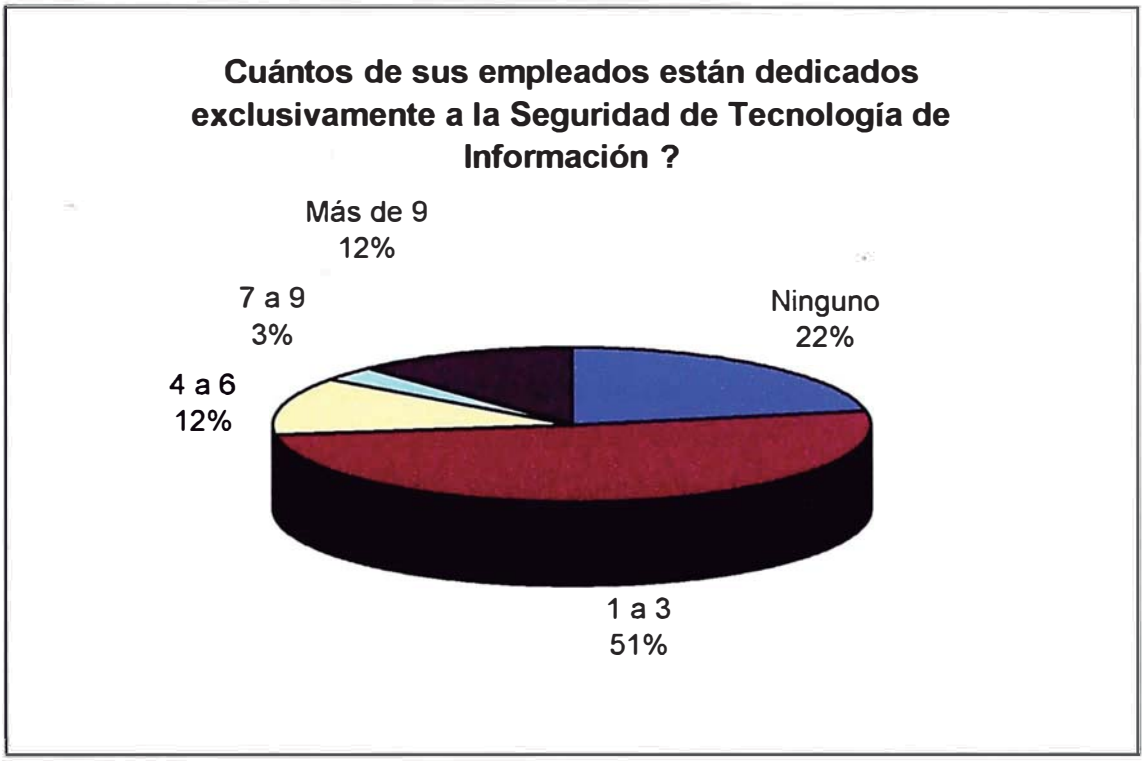
Fuente: Information weeks/Ernst & Young survey of 1320 IT managers and professionals

CAMBIOS EN LA SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN



Fuente: Information weeks/Ernst & Young survey of 1320 IT managers and professionals

NUMERO DE EMPLEADOS ASIGNADOS A SEGURIDAD DE T.I.



Fuente: Information weeks/Ernst & Young survey of 1320 IT managers and professionals

2.1.6. Aspectos estratégicos para desarrollar la Seguridad Tecnología de Información

- Materializar una política en la empresa en la materia.
- Invertir en el tema por lo menos a nivel del mínimo internacional en la materia: 5% de la inversión total en tecnología de información.
- Determinar una metodología de trabajo que dinamice su aplicabilidad diaria. Como los métodos para el análisis y la administración de los riesgos.
- Definir la función de seguridad de tecnología de información asignando por lo menos a una persona el mayor tiempo posible para el tema.
- Lograr que todos participen en el esfuerzo

- Capacitar a tres niveles: Dirección y/o asesoría (Jerarquía de línea, Asesores, Jefes de Auditorias Internas), Mandos Medios, Oficiales de Seguridad / Auditores Internos
- Desarrollar un plan de recuperación de desastres que asegure la continuidad del negocio, que sea probado y actualizado

2.2. ARQUITECTURA DE SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN

2.2.1. Por qué definir una arquitectura de seguridad

- Maximizar los beneficios y valor agregado al negocio
  - Cumpliendo con los requerimientos de seguridad, auditoría u control
  - Manteniendo la disponibilidad, oportunidad e integridad de la información
- Minimizar los riesgos del negocio.

2.2.2. Relación de la Arquitectura de Seguridad de Tecnología de Información con el negocio

- El proceso de arquitectura empieza con el entendimiento de la empresa y de los datos que constituyen su infraestructura de información.

2.2.3. Qué demanda la organización en la función de sistemas de información

- Acceso oportuno a los datos y cuando sea necesario.
- Formateo útil de los mismos, fácil interpretación.
- Datos precisos y consistentes a través de cada departamento.
- Respuestas oportunas a las rápidas condiciones cambiantes del negocio.
- Compartir datos a lo largo de empresa o empresas de la corporación.

2.2.4. Pero cuál es realmente el problema

- Se ha incrementado el uso de usuarios y los usos de las computadoras.
- Demasiado número de logon´s, passwords e identificadores
- Demasiados puntos de autenticación
- Los dominios de confianza no se quedan exclusivamente en la Empresa

2.2.5. Considerando lo anterior, cuál es la misión de la organización de T.I.

- Proveer datos de calidad a aquellos que los necesitan
- Sin embargo:
  - No es un proceso espontáneo
  - No resulta de focalizar en la productividad
  - Debe ser un proceso planeado

2.2.6. Cuál es la misión de la organización de seguridad de T.I.

- Acceso a los datos en un formato útil, cuando y donde sean necesarios: DISPONIBILIDAD / Acceso oportuno a los datos
- Habilidad para adaptarse a las necesidades cambiantes del negocio: ADMINISTRACIÓN / Procesos flexibles, sistemas seguros, fáciles de mantener
- Datos precisos y consistentes: ESTÁNDARES E INTEGRIDAD de datos y sistemas
- Compartir datos a lo largo de la organización: CONFIDENCIALIDAD E INTEGRACIÓN de sistemas y datos
- Conteniendo los costos: COSTO / BENEFICIO fácil de usar versus seguridad

2.2.7. En otras palabras, el propósito de la seguridad de tecnología de información es:

- Asegurar la continuidad del negocio y minimizar los damos al mismo, mediante la prevención y reducción al mínimo de los impactos por incidentes de seguridad.

- La administración de la seguridad de tecnología de información permite que sea compartida mientras se asegura la protección de los activos de cómputo e información.

2.2.8. Por lo tanto, qué debemos esperar de la arquitectura de seguridad

- Permita que los servicios de seguridad:
  - Sean visibles para el usuario
  - Continuamente invocados
  - Altamente integrada a la arquitectura de T.I.
  - Actividades, roles y responsabilidades claramente definidos

2.2.9. Entonces, qué es una Arquitectura de Seguridad de TI

- Son los modelos, bosquejos detallados y planes o estrategias que definen los servicios, mecanismos y objetos de seguridad, así como los estándares, estructuras organizacionales y procesos necesarios para soportar la función segura del negocio.
- Otra definición: Un conjunto específico de modelos con medidas de seguridad técnicas, procedurales y operacionales complementarias, seleccionados y organizados en forma lógica y efectiva para proteger la confidencialidad, integridad y disponibilidad de los activos de sistemas a un nivel determinado, a través de la evaluación de riesgos y aceptados por los usuarios responsables y recomendado por las autoridades de seguridad.

2.2.10. Objetivos de la Arquitectura de Seguridad de T.I.

- Soportar los requerimientos del negocio en términos de seguridad en T.I. en los próximos años.
- Crear una infraestructura efectiva para administrar la seguridad en la T.I.

- Simplificar el desarrollo, soporte y operaciones de la seguridad en T.I.
- Ofrecer componentes estratégicos de seguridad a través de todos los sistemas y servicios
- Ofrecer un soporte efectivo, en todos los servicios que el negocio lleve al mundo exterior de la organización
- Habilitar y facilitar las actualizaciones tecnológicas

2.2.11. Por lo tanto, la Arquitectura de Seguridad de T.I. permitirá:

- Desarrollar una estrategia coherente en la organización para la seguridad de sus sistemas y aplicaciones
- Incorporar las metodologías necesarias para soportar las necesidades de seguridad del negocio en medio de T.I., heterogéneo y rápidamente cambiante.
- Considerando y/o partiendo de:
  - Amenazas
  - Políticas de Seguridad
  - Aspectos regulatorios y legales
  - Auditabilidad
  - Requerimientos de usuarios
  - Ventajas competitivas

2.2.12. Enfoque antiguo VS Enfoque actual

El enfoque antiguo:

- Falta de alineación con el negocio
- Tradicionalmente impulsada por el área de sistemas
- Estrategia a corto plazo, soluciones puntuales a problemas tácticos
- Falta de estandarización real
- Los marcos de referencia no consideran nuevos requerimientos

El enfoque actual:

- Análisis de Riesgos

- Vulnerabilidades
- Amenazas

2.2.13. Consideraciones durante el plan de implantación de la Arquitectura de Seguridad de Tecnología de Información

- El programa de seguridad no es proyecto
- La implantación es un cambio de cultura en la organización
- El cambio debe iniciar en el más alto nivel
- La implantación requiere de inversión de tiempo y dinero
- El cambio es continuo y progresivo
- Toda la organización debe estar involucrada en el proceso
- Se requiere conocer en forma detallada los procesos y estrategias actuales y futuras de negocio y tecnológicas
- El cambio no permanecerá sin un esfuerzo consciente, y el reforzamiento y entrenamiento continuo
- La capacidad de los procesos de la organización puede madurar únicamente a través de pasos de mejora incrementales
- Los productos de seguridad deber ser integrados de manera consciente y estrecha
- Utilizar los productos comercialmente disponibles de diferentes y múltiples vendors

2.2.14. Factores críticos de éxito en la implantación de la Arquitectura de Seguridad de Tecnología de Información

Para diseñar e implementar adecuadamente la estructura de Seguridad de Tecnología de Información deben tenerse en cuenta los siguientes factores de éxito en el orden que se presentan:

- Plan de negocio
- Infraestructura estratégica informática
- Evaluación del riesgo informático

- Evaluación del riesgo de seguridad
- Objetivos de seguridad
- Plan Estratégico de Seguridad de Tecnología de Información
- Plan Táctico de Seguridad de Tecnología de Información
- Feedback y evaluación

Es decir, los objetivos y actividades de seguridad estén basados en los requerimientos y objetivos del negocio; compromiso y Soporte visible a niveles altos de la Organización; entender los riesgos de seguridad (amenazas y vulnerabilidades) de los activos de la organización, basados en su valor e importancia; mercadeo efectivo de la seguridad a todos los niveles; publicar y distribuir las guías y políticas y estándares a los empleados y proveedores.

2.2.15. Metodología para el desarrollo de la Arquitectura de Seguridad de Tecnología de Información

Todos están de acuerdo en que la Seguridad de Tecnología de Información es importante, pero pocos están de acuerdo sobre el nivel de seguridad que una empresa necesita. Por ello es necesario contar con una metodología probada para desarrollar una Arquitectura de Seguridad de Tecnología de Información.

Modelo de Seguridad

Objetivo

La solución concentra todos los conocimientos relacionados con la gestión de riesgos en tecnología de información:

- Orientado al negocio
- Fácil de entender
- Integral
- Flexible
- Aplicable a otros modelos de riesgo
- Independiente de la tecnología

Principios Básicos

- Las estrategias de seguridad deben basarse en Riesgos de Negocio y no sólo en riesgos técnicos
- Una administración efectiva de los riesgos de seguridad involucra una combinación de estrategia, organización, procesos y tecnología
- Un proceso integral de administración del riesgo debe aplicarse a componentes, diferenciados pero interrelacionados, de los procesos de negocio y a la informática vinculada a ellos.

Procesos Clave

Los siguientes elementos de control concentran todas las categorías de controles. El tipo y nivel de control aplicado dependerá de los resultados de la Evaluación de los Riesgos de Seguridad.

- Estrategia y Políticas.

  Las políticas gerenciales determinan el grado de la eficacia de todo el programa de seguridad. Las políticas deben:

  - Fijar la visión de la gerencia sobre la aceptación del riesgo
  - Ser concisas, comprensibles y posibles de aplicar
  - Adaptarse a la unidad de negocios a la cual se aplican

- Cubrir los sistemas y los ambientes de procesamiento críticos
- Establecer lineamientos y ejemplos para lograr consistencia

– Manejo de Cambios
  - Administrar la arquitectura técnica incluso las redes
  - Establecer la función de Administración de Seguridad para hacer cumplir las políticas y procedimientos vigentes (Anexo 6)
  - Diseñar la seguridad en aplicaciones nuevas y modificadas
  - Definir estrategias de Usuarios, Recursos y Grupos
  - Altas, bajas y modificaciones de usuarios
  - Tratar los cambios organizacionales
  - Capacitación y conscientización en seguridad
– Monitoreo de Eventos

  El Monitoreo de Eventos es una serie de procesos que comprende:
  - Evaluar el impacto que tiene la seguridad sobre los usuarios y la arquitectura técnica
  - Identificar los riesgos de seguridad de las nuevas tecnologías y aplicaciones
  - Definir y evaluar anormalidades a través de reportes de violaciones, pistas de auditoría, etc.
  - Cambios en la dinámica de la organización
  - Cumplimiento de las políticas
  - Revisión periódica de los usuarios y sus derechos / privilegios
  - Detectar violaciones
– Arquitectura Tecnológica

  La Arquitectura Técnica de la Seguridad comprende:
  - Aplicaciones
    - Acceso
    - Autorización
    - Segregación de funciones
    - Monitoreo
  - Bases de datos

- Acceso
- Recuperación
- Administración
- Monitoreo
- Servidores de Datos

- Usuarios Finales
  - Acceso
  - Administración
  - Monitoreo
  - Desarrollo
- Redes
  - Acceso / autenticación
  - Detección de intrusos
  - Firewalls
  - Monitoreo
  - Dial-up
  - Encripción
- Server/Host
  - Acceso a los datos
  - Firewalls
  - Monitoreo
  - Control de cambios
- Puestos de trabajo
  - Control de virus
  - Acceso Físico
  - Acceso Lógico
  - Encripción

2.3. ADMINISTRACIÓN DE RIESGOS

2.3.1. Definición de Riesgo.

Es la incertidumbre de que ocurra un evento que podría tener un impacto en el logro de los objetivos.

El riesgo es medido en términos de consecuencias y probabilidades.

2.3.1. Riesgos de Tecnología de Información que las empresas deben enfrentar.

- *Problemas vinculados a los desarrollos de los sistemas*
  - Utilización inapropiada de los recursos tecnológicos
  - Incorrecto análisis de los requerimientos
  - Equívocos en el diseño de los sistemas
  - Fallas en la implementación del hardware y el software
  - Pobres recursos de soporte técnico
  - Mala apreciación del mundo físico, el ambiente operativo y el comportamiento humano
  - Inapropiada verificación de post implantación
  - Evolución errática por problemas de mantenimiento
  - Falta de oportunidad y prolijidad en la suplantación de los sistemas
- *Problemas vinculados al uso y a la operación de los sistemas*
  - Factores ambientales naturales (incendios, inundaciones, rayos, etc.)
  - Factores infraestructurales (falta de energía eléctrica o aire acondicionado)
  - Alteraciones del funcionamiento del hardware
  - Defectos en el comportamiento del software
  - Fallas en los medios de comunicación
  - Influencias humanas en el uso del sistema
    - Problemas de instalación
    - Uso inapropiado
      - Involuntario: Por errores, distracciones, omisiones, etc.
      - Intencional: Por problemas financieros o personales; débil contextura moral; mal pago, mal atendido, mal conscientizado; interpretación robinhoodiana de ir contra el sistema pero contra nadie en particular; aspectos de oportunidad; revancha de personas despedidas.

2.3.2. Administración de los Riesgos de Tecnología de Información

- La teoría de análisis de riesgos en las organizaciones es nueva y está en proceso de cambios.
- El impacto sobre las organizaciones de los riesgos actuales es tan grande, que tiene que ver con eficacia y eficiencia de las mismas.
- Su impacto compromete particularmente a la dirección superior y niveles gerenciales.
- Cambio de controles o medidas "Reactivas" a "Proactivas".
- Necesidad de existencia de un sistema de administración de riesgos, distinto de auditoría y control.
- Necesidad de contar con "Objetivos de control" claramente definidos (por ejemplo COBIT).
- Regulación a través de estándares

2.3.3. Proceso de Evaluación de Riesgos

Metodología para el Análisis de Riesgo.

Etapas:

1. Identificar las mayores amenazas a los puntos de control claves.
   Esta etapa determina, lo que puede suceder y en qué punto de control.
2. Estimar el riesgo
   Esta etapa determina, cuán a menudo ocurre el riesgo
3. Cuantificar la exposición
   En esta etapa se determina cuánto se pierde al ocurrir el riesgo
4. Definir los objetivos de control específicos (requerimientos)
   En esta etapa se determina cuáles son los objetivos de control a satisfacer.
5. Seleccionar los estándares para satisfacer los objetivos
   En esta etapa se determinan los estándares que satisfacen el objetivo de control.
6. Justificar los estándares
   En esta etapa se determina si los estándares son costo-efectivos.

7. Revisar si todo es adecuado. De serlo implementar y documentar, de lo contrario revisar desde la etapa 5.

En el Anexo 5, presentamos una visión general de la administración de riesgos, así como el proceso de administración de riesgos.

2.4. PLAN INTEGRAL DE SEGURIDAD DE INFORMACIÓN

Las políticas de seguridad de la información, forman parte del plan, las cuales son estrategias frente a los riesgos que pueden atentar contra la confidencialidad, la integridad y la disponibilidad de los recursos informáticos; son elaboradas en base a la identificación de los riesgos tanto internos como externos de toda la infraestructura informática de la institución.

Un Plan de Seguridad de Información presenta las políticas de seguridad de la información, que deben ser tomadas como la base para el desarrollo de normas, procedimientos y controles, con el objetivo de tener y mantener las fuentes de información funcionando y lograr la continuidad en los servicios informáticos de las unidades organizativas del Banco.

2.4.1. Objetivos

a. Resumir las políticas, procedimientos y estándares relacionados con la seguridad de información, que deben cumplir todos los niveles de la administración de la organización, que intervienen en los diversos procesos de negocio.
b. Definir los procedimientos y estándares de seguridad de información para lograr un adecuado aseguramiento de la información en términos de confidencialidad, integridad y disponibilidad.

2.4.2. Debe incluir por lo menos los siguientes aspectos:

a. Roles y Responsabilidades

b. Metodología para la Administración de Riesgos de Seguridad de Información
c. Clasificación de los activos de información
d. Objetivos de control
e. Controles
f. Políticas de Seguridad de Información
g. Plan de Implementación de Controles
h. Mantenimiento y revisiones del Plan

2.5. POLÍTICAS DE SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN

Para una organización es esencial contar con una política de seguridad actualizada y de aplicación obligatoria. La defensa más segura es una política de seguridad bien desarrollada, y complementada por herramientas de seguridad bien seleccionadas.

Las políticas deben enfocar todo el comportamiento esperado, aún el más obvio. Los usuarios deberían realizar el "log out" cuando abandonan sus escritorios, utilizar fuertes passwords, y no compartir sus passwords con otros. La información sensible no debería dejarse sin protección. Las cuentas inactivas deberían ser dadas de baja. El resumir los puntos clave en memos, proveyendo las razones del por qué de cada regla, puede ayudar a mejorar la toma de conciencia sobre seguridad en la organización. Se deben incluir las penalidades por incumplimiento. Reforzar el mensaje con seminarios que expliquen por qué la seguridad es importante para la salud de la compañía - aún si es algo inconveniente para los usuarios. Los seminarios son una forma efectiva para educar a los usuarios acerca de los riesgos de responder a pedidos de información de gente externa a la empresa - el método más elemental que los hackers utilizan para obtener la información necesaria para lograr el acceso.

El personal de seguridad debería recorrer las áreas periódicamente tratando de detectar las violaciones, tales como passwords visibles, estaciones de trabajo conectadas y desatendidas, materiales sensibles dejados en lugares accesibles y a la vista. Informar las violaciones detectadas a los gerentes a

cargo de obligar el cumplimiento en el nivel local. Si la responsabilidad por la seguridad es a nivel departamental, pocos podrán ignorar esta problemática. El hacer leer y firmar la política de seguridad periódicamente, como parte del proceso de revisión de los empleados, asegura que el personal debe leer la política de seguridad como mínimo una vez al año.

Una Política típica de Seguridad de Tecnología de Información debe incluir los siguientes puntos:

La protección de la información relativa al negocio es una responsabilidad básica de la gerencia.

- Los gerentes son responsables de identificar y proteger todos los activos de información dentro de su área asignada de control gerencial.

  Los gerentes son responsables de certificar que todos sus empleados entienden su obligación de proteger los activos de información de la empresa.
- Los gerentes son responsables de implantar procedimientos de seguridad y recuperación en caso de desastre que sean consistentes con la política de la empresa y el valor de los activos.
- Los gerentes son responsables de vigilar las desviaciones de lo establecido en las prácticas de seguridad y de iniciar las acciones correctivas.

2.6. PLANEACIÓN DE LA CONTINUIDAD DE NEGOCIOS

La interrupción de los procesos críticos de un negocio suele traducirse en pérdidas espectaculares de dinero y en efectos devastadores para la organización. Paradójicamente, la planeación anticipada de las tareas requeridas para prevenir y/o minimizar los impactos de estas interrupciones representa una labor que ha sido frecuentemente relegada al último lugar de las prioridades organizacionales. La experiencia acumulada en los últimos años, así como las interrupciones enfrentadas por diversas corporaciones e instituciones han revelado la existencia de ciertos principios básicos

(prácticas) que deben regir las tareas asociadas a la planeación de la continuidad del negocio.

2.6.1. Definición del Plan de Continuidad de Negocios (BCP)

Es la identificación de los procesos críticos del negocio y de los recursos necesarios para mantener un nivel aceptable de operaciones, la protección de éstos y la preparación de procedimientos para asegurar la sobrevivencia de la organización ante cualquier interrupción.

Plan de Contingencias Informático

Es el elemento del sistema de control interno establecido para asegurar la disponibilidad de la información y los recursos informáticos durante la interrupción de procesamiento.

2.6.2. Objetivos de un Plan de Continuidad de Negocios

El principal objetivo es brindar a la organización la habilidad para continuar las operaciones críticas administrando la disponibilidad de los recursos y datos de los sistemas de información en la eventualidad de una interrupción del procesamiento.

Los planes de continuidad de negocio requieren un cuidadoso y detallado desarrollo de procedimientos de back-up y recupero de desastres. Igualmente importante, un plan de continuidad de negocios debe estar mantenido en forma continuada, ser actualizado y testeado. Un plan que no es mantenido y comprobado periódicamente, puede volverse obsoleto, no tener utilidad alguna y podría llegar a exacerbar los problemas en caso de producirse la interrupción del procesamiento.

Así la clave para un planeamiento efectivo es la amplia comprensión de los requerimientos y prioridades de procesamiento de la organización.

Podemos resumir los objetivos del Plan de Continuidad de Negocios en lo siguiente:

General

- Asegurar la continuidad de las operaciones de la organización.

Particulares

- Minimizar el número de interrupciones del negocio.
- Limitar la interrupción y el daño
- Establecer medios alternos de operación antes de ser requeridos
- Entrenar y familiarizar al personal con procedimientos de emergencia
- Minimizar el tiempo de recuperación
- Minimizar el impacto económico de la interrupción
- Satisfacer obligaciones legales

2.6.3. Importancia de contar con un Plan de Continuidad de Negocios

- La empresa moderna tiene una total dependencia sobre los sistemas computarizados de información.
- Planificar la continuidad de la empresa forma parte integral del "oficio" empresarial.
- Si Ud. es una persona positiva que planifica para el éxito y no para el fracaso, recuerde, no obstante, que el "optimismo a ultranza" es negativo a la hora de enfrentar problemas inevitables.
- Si hasta hoy Murphy ha sido su amigo, lo que es buena cosa, ello no lo inmuniza del riguroso cumplimiento de su ley.
- Una reciente encuesta en los E.U.A. constató que el 90% de las empresas siniestradas que no tenían un plan de recuperación se veían obligadas a salir del mercado dentro de los 18 meses de producido el siniestro.
- Las leyes de probabilidad tienen vigencia universal, por lo que la experiencia de otros países debe ser tomada en cuenta. Ejemplo: los índices de siniestralidad en Gran Bretaña indican que una de cada 750 empresas puede tener un desastre informático en el correr de cada año.

A modo informativo, en los siguientes cuadros, mostramos información estadística de por qué necesitamos servicios de recuperación:

POR QUÉ NECESITAMOS SERVICIOS DE RECUPERACIÓN	
EVENTO	**OCURRENCIA (%)**
Falla Eléctrica	15.1
Incendio	13.2
Terremoto	12.8
Error humano	12.8
Fraude	10.7
Virus	7.3
Inundación	7.1
Error de Hardware	4.8
Huracán	3.8
Terrorismo	3.4
Paro de la Red	3.4
Error de Software	3.3
Otros	2.3

Fuente: Contingency Planning Research Inc.
Causas de más de 300 desastres registrados

POR QUÉ NECESITAMOS SERVICIOS DE RECUPERACIÓN			
FECHA	**EVENTO**	**UBICACIÓN**	**IMPACTO US $**
15/02/94	Terremoto	Los Ángeles	50 Billones
13/04/92	Inundación	Chicago	30 Billones
24/08/92	Huracán Andrew	Florida	20 Billones
17/10/89	Terremoto	Loma Prieta	5.6 Billones
10/04/92	Bomba	Londres	1.7 Billones
26/02/93	Bomba	WTC	590 Millones
26/08/86	Incendio	Montreal	110 Millones

¿ QUIÉN UTILIZA SERVICIOS DE RECUPERACIÓN ?	
INDUSTRIA	**% DE LA BASE TOTAL DE CLIENTES**
Bancos	35
Manufactura / Energía	20
Finanzas / Seguros	12
Servicios	9
Menudeo / Mayoreo	6
Transportación	6
Médica / Educación	5
Otros	7

Fuente: BANK Disaster Contingency Planner VN6, Julio 1998
Basado en un estudio de uno de los más importantes proveedores de servicios de recuperación de desastres, con más de 1,200 clientes en los EE.UU.

¿ QUIÉN UTILIZA SERVICIOS DE RECUPERACIÓN ?	
Asignación del presupuesto de TI para recuperación de desastres	
Compañías con menos de 200 millones	1.53 %
Compañías entre 200 y 500 millones	0.75 %
Compañías sobre 500 millones	0.94 %
Industria de Servicios	0.78 %
Financieras	2.44 %
Manufactureras	1.21 %
Gobierno, Educación, Medicina	0.21 %

Fuente: DP Budget, Volumen 11 Número 3, marzo 1998

2.6.4. Consecuencias de un Plan de Continuidad de Negocios inadecuado

- Pérdida de ventas o flujo de caja que podría resultar si la interrupción en el procesamiento causa una interrupción en las actividades de generación de ingresos.
- La pérdida de ventaja competitiva es un riesgo para cualquier organización que utilice sistemas de información para lograr dicha ventaja competitiva.
- La imposibilidad de entregar productos o servicios a los clientes podría resultar en efectos a largo plazo más allá de las pérdidas inmediatas en ventas e ingresos, si los clientes se llevan sus operaciones a otra parte.
- Podrán verificarse multas y sanciones, debido a problemas legales, violaciones contractuales, litigios y otras penalidades

2.6.5. Contenido de un Plan de Continuidad de Negocios

1. Definir teams de respuesta ante una emergencia:
    - Detección
    - Operación de Emergencia
    - Desarrollo
    - Recuperación
    - Transporte

- Comunicaciones
- Alta Conducción
- Usuarios
- Reubicación y Reconstrucción
- Administración del Plan
- Evaluación de daños

2. Escribir un plan de acción dividido en fases operativas
   - Fase de Preparación: Distribución, testeo, mantenimiento
   - Fase de Ocurrencia
   - Fase de Activación
   - Fase en Régimen
   - Fase de Reconstrucción
   - Fase de Retorno
3. Incorporar anexos de información vital
   - Funciones críticas del negocio.
   - Estrategias de recuperación de sistemas y comunicaciones.
   - Procedimiento de evacuación del edificio.
   - Procedimiento para la administración de la bóveda externa.
   - Detalle de proveedores del centro de computación.
   - Otros

CAPÍTULO III
PROCESO DE TOMA DE DECISIONES

El presente trabajo involucra una serie de actividades planificadas y coordinadas para llegar a un objetivo final.

Cabe mencionar que un aspecto muy importante que fue evaluado previamente a la implementación de la función de Seguridad de Tecnología de Información fue decidir su ubicación como unidad organizacional en la estructura orgánica de la empresa.

3.1. PLANTEAMIENTO DEL PROBLEMA

Antes de plantear el problema, efectuaré una breve descripción de la situación actual, presentando los riesgos y ventajas de la situación actual.

Situación actual

Las funciones relacionadas con la seguridad de tecnología de información se vienen llevando en forma aislada, o simplemente no se desarrollan.

Es decir, no se encuentra centralizada la función de seguridad de tecnología de información. Esta se encuentra compartida entre los Departamentos de Organización y Métodos en lo que respecta al mantenimiento de los perfiles de usuario al AS/400; de Redes en lo que respecta al mantenimiento de los usuarios de red; y de Auditoría Interna en lo que respecta al seguimiento de los "logs" de ocurrencias. Se puede apreciar que la mayor parte de las funciones

de seguridad de TI se encuentran bajo la responsabilidad de la División de Tecnología.

La unidad que atienden éstas en mayor proporción, pero sólo en los aspectos relacionados a la información mantenida en las computadoras (central y servidores de red), es la unidad de Organización y Métodos, que depende de la División de Tecnología, y las autorizaciones para los pases a producción así como del otorgamiento de accesos al Sistema Integrado de Administración Financiera (SIAF) son realizados por la unidad de Auditoría Interna.

Las principales labores que se desarrollan en este aspecto están referidas a la definición de usuarios y sus perfiles de acceso, pases a producción, y generación de copias de respaldo de información; cuya cobertura señalamos sucintamente en los párrafos siguientes.

- Referente a la definición de usuarios

  Existen dos tipos de usuarios, según el ambiente al que deben acceder.

  - Usuarios del ambiente del computador central

    Las solicitudes de asignación se canalizan por intermedio de las jefaturas de la unidad solicitante y son evaluados por la unidad de Auditoría Interna.

    Una vez que la solicitud satisface el proceso de verificación, se transfiere al Dpto. de Organización y Métodos donde el funcionario responsable, luego de evaluar los requerimientos del usuario y efectuar las coordinaciones que fueren pertinentes, procede a inscribir los niveles de accesos otorgados y a comunicar al usuario la atención de su pedido.

  - Usuarios del ambiente de redes

    El BANCO cuenta actualmente con el sistema operativo para redes Windows NT, el cual permite, según como se definan los recursos, que cada usuario pueda acceder hasta el disco duro de las demás estaciones de trabajo conectadas a la red, así

como puntos de conexión al computador central mediante software de emulación.

Los requerimientos de acceso se envían al Dpto. de Redes. Éstos deben ser utilizados por la jefatura de la unidad a la que pertenece el usuario.

Según el Departamento al que pertenezca el usuario, el Administrador de la Red inscribirá al usuario como miembro de los grupos cuyos privilegios satisfagan sus necesidades de acceso.

- Referente a la definición de perfiles de usuarios

  - Procedimiento para el computador central.

  El Dpto. de Organización y Métodos crea perfiles para grupos de usuarios, en función al área organizativa a que pertenecen y a las funciones inherentes al cargo que desempeñen. Esto con la finalidad de facilitar y lograr un mejor control de accesos.

  - Procedimiento para las redes

  La autorización de acceso se otorga inscribiendo a cada usuario como miembro de uno o más de grupos definidos, con lo cual obtiene acceso a los directorios públicos disponibles para los grupos en cuestión, labor que es efectuado por el Dpto. de Redes. Sin embargo el mantenimiento de los usuarios (baja, bloqueo) es efectuado por el Dpto. de Organización y Métodos.

  Se puede definir además, según las necesidades, directorios privados para los usuarios que así lo requieran.

  No se cuenta, sin embargo, con perfiles por puestos de trabajo.

- Referente a la clasificación de la información según su sensibilidad

  Actualmente la información no se clasifica a solicitud del usuario, es más no existe el concepto de propietario de la información.

- Referente a los procedimientos de destrucción

Actualmente no están difundidas las instrucciones sobre cómo, quién, cuál ni cuándo destruir información.

Si bien se conocen los reportes y archivos a retener en las Oficinas, y el período luego del cual deben enviarse al Archivo Central, no existen similares directivas para su destrucción, independientemente del medio (papeles, archivos, manuales, disquetes, etc.) en que la información esté contenida o almacenada.

- Referente al soporte para contingencias
  - Equipos de Cómputo
    - Computador central

      El procesador de menor capacidad ha sido liberado de las labores de producción y desarrollo, para que mantenga réplicas en línea de la información, pero no necesariamente es un computador alterno, y está ubicado físicamente en el mismo centro principal de procesamiento.
    - Estaciones de trabajo

      No se cuenta con un grupo de equipos destinados al respaldo de las estaciones de trabajo y periféricos. Cualquier necesidad específica no podría ser atendida inmediatamente, limitándose a lo que pueda existir en el almacén o a las transferencias de equipos de otros usuarios, o pedidos de emergencia al proveedor.
  - Respaldo de Información (Backup)
    - En el computador central

      Se obtiene copias de respaldo de información con periodicidad diaria, semanal, mensual, semestral y anual.

      Los respaldos diarios comprenden tanto los archivos de datos de las aplicaciones como de las bibliotecas de programas, más no los del sistema operativo.

      Los respaldos semanales son completos (full backups), ya que comprende tanto los archivos de las aplicaciones, como

los del sistema operativo y bibliotecas de programas. Se utilizan durante cuatro semanas, al cabo de las cuales se reutiliza el medio magnético.

Los respaldos mensuales están referidos a los archivos de cada aplicación o sistema de información, y se conservan durante 12 meses, luego de los cuales se reutiliza el medio magnético.

Debe mencionarse que todas las cintas de respaldo se mantiene custodiado en la Bóveda del BANCO y un duplicado de las mismas se encuentran en la Bóveda de la Agencia de Miraflores.

Para los backups de los procesos batch se obtienen dos backups: el primero antes de iniciar el proceso diario (pre-proceso) y el segundo, a la finalización del mismo (post-proceso). Esto para respaldar la información existente antes y después de los procesos diarios.

- En el ambiente de Red

  Actualmente, en la Red de Windows NT sólo se obtiene copias de respaldo de los archivos SQL.

- Referente al fluido eléctrico

  Se cuenta con respaldo para los equipos ubicados en el centro de procesamiento principal, mediante un UPS que brinda una autonomía de 15 minutos.

  Los servidores de red al estar ubicados en el centro de procesamiento principal, reciben el mismo respaldo de suministro eléctrico que los demás equipos instalados en dicho ambiente.

  El respaldo eléctrico para las diferentes estaciones de trabajo, son respaldados también por el mismo UPS.

Riesgos y ventajas de la situación actual

En lo que se refiere al ambiente del Computador Central, existe la posibilidad que se otorgue acceso a la información excediendo las

necesidades del personal y poniendo en riesgo la confidencialidad de la misma. Esto debido a que no se tienen definidos los perfiles de usuarios para cada puesto de trabajo, y a que no existe un ente que fiscalice la pertinencia de cada solicitud bajo la perspectiva del puesto del solicitante y la sensibilidad de la información a la que éste desee tener acceso.

Inadecuada o "inexistencia" de la administración de seguridad de TI, ocasionando riesgo de accesos indebidos a los sistemas críticos y dificultando la coordinación entre las diferentes funciones de seguridad.

También constituye un riesgo la falta de información respecto al movimiento o cambio de funciones de los usuarios.

En los ambientes de las PC's de redes, no está definido el responsable de fijar y velar por los criterios de seguridad, función que ha sido asumida indirectamente por el administrador de la red.

El Plan de Contingencias que se tiene actualmente requiere ser actualizado optimizado y probado y tampoco contempla a plenitud los sistemas de PC's y redes, lo que no permite asegurar la disponibilidad de la información mantenida en tales ambientes en una situación de contingencia.

Tampoco se cuenta con un ente que intervenga, durante el desarrollo de nuevos proyectos, proponiendo y evaluando métodos o técnicas de control de información que deban ser adoptadas según las alternativas que se esté considerando para la atención del proyecto.

Similarmente, no existe un responsable que tenga como función permanente indicar los riesgos que –relación con la seguridad de tecnología de información- existen en los procedimientos que se aplican en la empresa, ni investigar nuevas técnicas o tecnologías que pudieran aplicarse para disminuirlos.

Estas situaciones ocasionan que la seguridad de tecnología de información se administre de modo desordenado y sin un criterio directriz que oriente su uso y manejo.

En términos generales se puede concluir que, a nivel general, no existe un política ni doctrina de seguridad de tecnología de información en el BANCO, y menos aún una unidad que haya asumido cabalmente las funciones que serían inherentes a la misma. Las unidades que en la actualidad desarrollan algunas de las funciones relacionadas, lo hacen con una visión restringida del negocio, en un ámbito muy limitado, distraídas por otras tareas y funciones que les son propias, y sin las facultades para lograr el salto cualitativo necesario para enfrentar el problema

Finalmente podemos resumir, los problemas en los siguientes puntos:

- No existe una función formal de seguridad de tecnología de información en el BANCO
- Las debilidades en la seguridad de tecnología de información se ven como problemas técnicos y no como riesgos del negocio
- Las actividades de seguridad de tecnología de información están dispersas en diversas áreas sin contar con una política al respecto
- El aspecto de seguridad de tecnología de información es considerada un requerimiento de menor prioridad en comparación con los requerimientos financieros y operacionales
- El personal no está consciente de las políticas, procedimientos, guías, estándares y riesgos relacionados con la seguridad de tecnología de información
- No existe un entrenamiento periódico del personal en buenas prácticas de seguridad de tecnología de información
- La propiedad y responsabilidad sobre los datos y/o aplicaciones no está establecida claramente

- La seguridad, auditabilidad, control, mantenibilidad y facilidad de uso, no son consideradas con la importancia debida, durante el desarrollo y mantenimiento de las aplicaciones

En tal sentido, podemos definir el problema en los siguientes términos: *En qué parte de la estructura organizacional del BANCO se ubicará la Unidad de Seguridad de Tecnología de Información y cómo se administrará la Seguridad de Tecnología de Información.*

3.2. ALTERNATIVAS DE SOLUCIÓN

Es importante resaltar la necesidad de contar con una unidad funcional que vele por la administración de la seguridad de tecnología de información en el BANCO, con una visión integral del negocio, y que tenga una dependencia funcional que le permita desarrollar cabalmente el cometido propuesto.

Para tal efecto, se plantea las siguientes alternativas de solución viables:

3.2.1. Alternativa 1: *Un Departamento de Seguridad de Tecnología de Información dependiente del Departamento Central de Tecnología y efectuar la implementación mediante Outsourcing.*

Ventajas

El ser una unidad dependiente del Dpto. Central de Tecnología, tendría:

- Una alta injerencia en la definición de las normas y procedimientos internos del BANCO, por su cercanía al Departamento de Organización y Métodos, el cual depende del Dpto. Central de Tecnología.

- Facilidades para tener una visión actualizada de los sistemas y recursos de tecnología de información, por depender del Dpto. Central de Tecnología.
- Facilidades para atender rápidamente las necesidades de definición de accesos y perfiles de usuario, por su proximidad al Departamento de Redes y Producción.
- Facilidades para coordinar con el Departamento Central de Operaciones (que es el área usuaria y generadora de mayor movimiento de información del BANCO), ya que ambas unidades estarían bajo el ámbito de una misma jefatura, Gerencia Central de Medios Técnicos
- Muchas de las funciones consideradas por la unidad, no requerirían integrar nuevos conceptos a la visión actual del Dpto. Central de Tecnología, por tener un perfil tecnológico existente en la misma.

Al ser implementado a través de terceros, se tendría:

- La posibilidad que la unidad de seguridad de tecnología de información se concentre en sus actividades del día a día (otorgamiento de accesos, definición de perfiles de usuario, creación de usuarios, cambio de contraseñas, aprobación de pases a producción, monitoreo de actividades inusuales, entre otros), mientras es desarrollado e implementado la arquitectura de seguridad de tecnología de información.
- El soporte profesional o empresarial, que se entiende debe ser especializado y el "Know How" respectivo.
- Una capacitación superior para producir soportes y servicios más fiables a la organización, lo que significaría una opción muy oportuna.

Desventajas

- Al ser una unidad dependiente del Dpto. Central de Tecnología, el cual tiene a su cargo el desarrollo de proyectos informáticos y la emisión de normas y procedimientos, no estaría en posición de vetar aquellos aspectos considerados en los mismos y que, no obstante contar con el aval de su Gerencia, pudieran no estar acorde con la Política de Seguridad de Información que se hubiera aprobado por el BANCO. Asimismo, existe el riesgo de que ésta pueda ignorar o desactivar ciertos controles críticos con el fin de "resolver" ciertos problemas de información. Por ejemplo, dar acceso al personal de desarrollo al ambiente de producción, con el fin de agilizar la capacidad de respuesta del área de sistemas.
- Su nivel departamental podría ser insuficiente para hacer respetar o implantar criterios de seguridad de tecnología de información que pudieran entrar en conflicto con intereses o prácticas consentidas o avaladas por gerentes de otras áreas.
- Su nivel departamental podría restarle rapidez de respuesta, al estar supeditada cualquier decisión a la aprobación del Jefe del Dpto. Central de Tecnología.
- Su nivel departamental le impediría manejar autónomamente un presupuesto de capacitación, no obstante que la capacitación es un factor básico para poder mantenerse actualizado en las nuevas tecnologías y metodologías emergentes.
- Al ser desarrollados por terceros se perdería confidencialidad en los aspectos de seguridad del BANCO, toda vez que personas externas al BANCO conocerían las

prácticas y los esquemas de seguridad a ser implantadas en el BANCO.

- Por ser considerado por la institución, la seguridad de tecnología de información, de carácter estratégico, es contraproducente efectuar el desarrollo e implantación mediante servicios de terceros.

3.2.2. **Alternativa 2:** ***Un Dpto. de Seguridad de Tecnología de Información dependiente del Dpto. Central de Tecnología, y hacer el desarrollo e implantación con recursos propios.***

A diferencia de la alternativa anterior, significa contar con un equipo de trabajo con recursos del BANCO para el desarrollo e implantación de la seguridad de tecnología de información.

En adición a las ventajas y desventajas mencionadas en la alternativa 1 con respecto a la dependencia del Dpto. Central de Tecnología, se menciona las ventajas y desventajas referidas al desarrollo e implantación con recursos propios:

Ventajas

- Mantener protegido los aspectos de seguridad de tecnología de información, concebidos como recursos estratégicos, ante terceros.
- Involucrarse con mayor profundidad en el desarrollo e implantación de la arquitectura de seguridad de tecnología de información.
- Desarrollar la infraestructura de seguridad haciendo participar directamente a las áreas del BANCO (operaciones, tecnología, entre otros).

- Desarrollo de la infraestructura de seguridad de tecnología de información más acorde a las necesidades del BANCO.

Desventajas

- Inversión económica y de tiempo en capacitación continua de las empresas consultoras especializadas.
- Inversión de tiempo de curva de aprendizaje

3.2.3. **Alternativa 3:** ***Una Gerencia de Apoyo de Seguridad de Tecnología de Información dependiente de la Gerencia Central de Medios Técnicos, y hacer el desarrollo e implantación mediante Outsourcing.***

Ventajas

El ser un área dependiente de la Gerencia Central de Medios Técnicos, tendría:

- El nivel necesario para hacer respetar e implantar criterios de seguridad de tecnología de información, aún ante otras Divisiones o Sub-Gerencias Generales.
- Autonomía para la toma de decisiones y para el manejo de su presupuesto de capacitación.
- Su carácter de función exclusiva le permitiría dedicarse a tiempo completo a administrar la seguridad de tecnología de información.
- Por su dependencia directa a la Gerencia Central de Medios Técnicos, podrá obtener fácilmente la colaboración del Dpto. Central de Tecnología (que incluye al Departamento de Organización y Métodos) y del Departamento de Operaciones, unidades de las que deberá recopilar información, así como interactuar y coordinar constantemente, para el logro de su cometido.

- Su ubicación dentro del organigrama le permitirá lograr y mantener una visión integral y actualizada de negocio.
- Contaría con el apoyo de su jefe de línea inmediato, ya que aparte de la organización en su conjunto, sería la Gerencia Central de Medios Técnicos el área que más beneficio obtendría del valor agregado por la unidad propuesta.
- Respecto a desarrollar e implantar mediante terceros, son las mismas ventajas mencionadas en la alternativa 1.

Desventajas

- La carga de trabajo y responsabilidades inherentes a la Gerencia Central de Medios Técnicos podrían impedir o dificultar la atención o apoyo de la misma hacia la unidad propuesta, en los casos en que ello fuera requerido.
- Por su nivel de gerencia de apoyo, implica destinar un mayor presupuesto en los diversos rubros que se requieren para su constitución.
- Respecto a desarrollar e implantar mediante terceros, son las mismas desventajas mencionadas en la alternativa 1.

3.2.4. Alternativa 4: *Una Gerencia de Apoyo de Seguridad de Tecnología de Información dependiente de la Gerencia Central de Medios Técnicos, y hacer el desarrollo e implantación con recursos propios.*

Ventajas

- Respecto a su ubicación en la estructura organizacional del BANCO, las ventajas son las mismas citadas en la alternativa 3.

- Respecto a desarrollar e implantar mediante recursos propios, las ventajas son las mismas que se mencionaron en la alternativa 2.

Desventajas

- Respecto a su ubicación en la estructura organizacional del BANCO, las desventajas son las mismas a las citadas en la alternativa 3.
- Respecto a desarrollar e implantar mediante recursos propios, las desventajas son las mismas que se mencionaron en la alternativa 2.

3.3. METODOLOGÍA DE SOLUCIÓN

Para decidir la alternativa más conveniente se establecieron criterios de evaluación con el fin de determinar la alternativa más conveniente. Estos criterios fueron determinados en el Comité de Riesgo Operativo.

Los factores de evaluación fueron los siguientes:

1. Independencia de la Unidad de Seguridad de TI del Dpto. Central de Tecnología. En qué medida se garantiza a través de la ubicación del área de seguridad la independencia respecto al Dpto. Central Tecnología.
2. Confidencialidad de la información y del esquema de seguridad del negocio.
3. Personal con conocimiento de los riesgos en tecnología de información del BANCO.
4. Costos de implementación del área.
5. Personal con experiencia en tecnología.

Para cada factor existen valores discretos que serán asignados según cada alternativa. Asimismo, se han establecido ponderaciones que identifican la importancia relativa de cada factor.

El cuadro adjunto resume lo anterior:

	Factores de Evaluación	Peso	Valores / Rango	Puntuación
1	Independencia Funcional de la Unidad de Seguridad de la División de Tecnología	5	Alto Bajo	4 1
2	Confidencialidad de la información en los aspectos de seguridad	4	Riesgo Mínimo Riesgo Medio Riesgo Alto	5 2 0
3	Personal con conocimiento de riesgos en TI del BANCO	4	Alta Media Baja	5 3 1
4	Costo de implementación de la unidad de Seguridad de TI	3	Menor a $25,000 Entre $25,000 y $50,000 Mayor a $50,000	5 3 1

Luego de analizar cada alternativa se han establecido los valores de cada factor, los mismos que se resumen en el cuadro siguiente :

Factor		Alternativa			
		1	2	3	4
1	Independencia Funcional de la Unidad de Seguridad de Información del área de Tecnología	1	1	4	4
2	Confidencialidad de la información en los aspectos de seguridad	0	5	0	5
3	Personal con conocimiento de riesgos en TI del BANCO	1	5	1	5
4	Costo anual de la unidad de Seguridad de TI	1	3	1	3

3.4. TOMA DE DECISIONES

Luego de ponderar los factores se determinó el cuadro final de evaluación:

Factor		Alternativa			
		1	2	3	4
1	Independencia Funcional de la Unidad de Seguridad de Información del área de Tecnología	5	5	20	20
2	Confidencialidad de la información en los aspectos de seguridad	0	20	0	20
3	Personal con conocimiento de riesgos en TI del BANCO	4	20	4	20
4	Costo anual de la unidad de Seguridad de TI	3	9	3	9
Total		12	54	27	69

Esta evaluación determinó que la alternativa 4 era la más conveniente.

Esto es, se adopta la decisión de **implantar una Gerencia de Apoyo de Seguridad de Tecnología de Información dependiente de la Gerencia Central de Medios Técnicos, y efectuar el desarrollo e implantación con recursos propios.**

3.5. ESTRATEGIAS ADOPTADAS

Las estrategias adoptadas están vinculadas a:

- La estructuración de la Gerencia de Apoyo de Seguridad de Tecnología de Información. Anexo 6
- El desarrollo de la funciones del personal del área de Seguridad de TI. Anexo 7

- Identificación e integración de las funciones de seguridad de TI actualmente dispersas entre los departamentos de Organización y Métodos, de Redes y Auditoría Interna, en el área de Seguridad de TI.
- El diseño e implementación de una arquitectura de seguridad de información en el que se incluya:
    - El desarrollo del Plan de Seguridad. Anexo 8
    - El desarrollo de las políticas de seguridad. Anexo 8
    - La definición de la metodología a adoptar (enfoque de administración de riesgos). Anexo 9
    - Optimización del actual Plan de Continuidad de Negocios. Anexo 3
    - Plan de Implementación de Controles de Seguridad de Información. Anexo 10
    - Evaluación de recursos tecnológicos de soporte.

CAPÍTULO IV
EVALUACIÓN DE RESULTADOS

La Gerencia de Apoyo de Seguridad de Tecnología de Información se encuentra en proceso de implementación. La Gerencia General aún está evaluando si esta área finalmente va a ser a nivel gerencial o a nivel departamental, pero siempre independiente de la División de Tecnología. Ya se ha previsto que inicialmente estará conformado por un jefe y un asistente.

Actualmente, se ha centralizado las funciones de seguridad de tecnología de información en el Dpto. de Organización y Métodos, quien posteriormente delegará dichas funciones y responsabilidades al área de Seguridad de TI cuando ésta se constituya formalmente. El desarrollo de las funciones de seguridad bajo este esquema de transición se vienen llevando de manera satisfactoria, lo cual se refleja en el ágil atención en el otorgamiento de accesos a los usuarios, así como en los pases a producción. Asimismo se ha concluido con la implementación del Centro de Cómputo de Contingencia, quedando pendiente la actualización del Plan de Continuidad de Negocios.

El Dpto. de Organización y Métodos viene realizando el desarrollo de las funciones de cada integrante del área de seguridad de TI, el cual deberá ser aprobado por las instancias respectivas y luego oficializado mediante su publicación en la Intranet del BANCO.

Se ha evaluado y designado la persona, dentro del BANCO, que asumirá la jefatura del área de Seguridad de TI, quien viene efectuando, paralelamente, el desarrollo del plan de trabajo anual; y evaluando la metodología a optar para la administración de la seguridad de TI.

CAPÍTULO V
CONCLUSIONES Y RECOMENDADIONES

6.1. CONCLUSIONES

1. La Administración de Tecnología de Información, no sólo es una cuestión técnica, es más que tecnología, es una Decisión Estratégica de Negocios.
2. La Seguridad de Tecnología de Información es responsabilidad de todo el personal del BANCO y en todos los niveles.
3. Contar con una unidad de seguridad de tecnología de información posiciona al BANCO en un lugar de vanguardia tecnológica frente a la competencia; lo que permite mantener una imagen de confiabilidad y seguridad a los clientes.
4. La implementación de la unidad de seguridad de tecnología de información es parte del proceso de mejora continua que viene realizando el BANCO en su afán de seguir creciendo y consolidarse en el sistema financiero.
5. Es importante mantenerse actualizado con las metodologías y herramientas relacionados a la seguridad de tecnología de información a fin de seguir optimizando su administración.

6.2. RECOMENDACIONES

1. Que se cree la unidad encargada exclusivamente de administrar la Seguridad de Tecnología de Información, según las funciones específicas a ser desarrolladas para el cumplimiento de sus objetivos.
2. Que la unidad encargada de administrar la Seguridad de Tecnología de Información, sea una área independiente al área Tecnología.
3. La Administración de Seguridad de Tecnología de Información debe tener un enfoque de riesgos y debe desarrollarse sobre la base de metodologías probadas en proyectos pilotos y los principios generales de seguridad aceptados internacionalmente

GLOSARIO

1. **Procesos Críticos**: *Procesos que impactan significativamente los ingresos y rentabilidad, tienen consecuencias de tipo legal, repercuten negativamente en el servicio al cliente y amenazan la sobrevivencia de la organización*
2. **Activos a proteger.** *Recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos*
3. **Tecnología.** *Software y hardware; sistemas operativos; sistemas de gestión de base de datos; sistemas de red*
4. **Instalaciones.** *Lugar donde se ubican y se mantienen los sistemas de información*
5. **Confidencialidad.** *Protección de la información sensible contra la divulgación no autorizada*
6. **Integridad.** *Seguridad que la información o los datos están protegidos contra modificación y/o destrucción no autorizada, y certidumbre de que la información o los datos no han cambiado sin una razón del negocio*
7. **Disponibilidad.** *Certeza que la información pueda ser utilizada en el momento que se le requiera*
8. **Amenazas.** *Eventos de tipo persona, proceso, tecnológico o externo, que impiden y/o perjudican la confidencialidad, integridad y disponibilidad de la información*
9. **Vulnerabilidad.** *Ocurrencia real de materialización de una amenaza sobre activos*
10. **Impacto.** *Daño producido a la organización por un posible incidente*
11. **Riesgo.** *Posibilidad de que se produzca un impacto*
12. **Función o servicio de salvaguarda.** *Reducción del riesgo*
13. **Mecanismos de Salvaguarda o salvaguarda**. *Dispositivo físico o lógico, capaz de reducir el riesgo*
14. **Sistemas de Información**. *Conjunto de archivos de datos, base de datos, programas, soporte y equipos*
15. **Accesos autorizados**. *Autorizaciones concedidas a un usuario para la utilización de los diversos recursos*
16. **Identificación**. *Procedimiento de reconocimiento de la identidad de un usuario*

17. **Autenticación.** *Procedimiento de comprobación de la identidad de un usuario*
18. **Control de acceso**. *Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos*
19. **Riesgos de operación.** *Posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos*
20. **Administración de riesgos.** *Proceso que consiste en identificar, medir, controlar y reportar adecuadamente los riesgos que la organización enfrenta*
21. **Información.** *Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada. También datos con valor de uso cuyas propiedades de efectividad, eficiencia, integridad, confidencialidad, disponibilidad, cumplimiento y confiabilidad coadyuvan al logro de los objetivos de la organización*
22. **Proceso.** *Conjunto de actividades, tareas y procedimientos organizados y repetibles*
23. **"Líder de Proceso".** *Funcionario de la organización que tiene a cargo o es responsable de un procesos específico considerado crítico*
24. **Servicios críticos provistos por terceros.** *Servicios relacionados a procesos críticos provistos por terceros y cuya falta o ejecución deficiente puede tener un impacto financiero significativo para la organización*
25. **Objetivo de control.** *Una declaración del propósito o resultado deseado mediante la implementación de acciones y controles apropiados en un proceso crítico y / o una actividad de tecnología de información particular considerada esencial para el negocio*
26. **Tecnología de información.** *Incluye los sistemas informáticos y la tecnología asociada a dichos sistemas*
27. **Recursos de Tecnología de Información.** *Incluye datos, tecnología, instalaciones, sistemas de aplicación y recursos humanos destinados a dar soporte a la información*
28. **Riesgos de tecnología de información.** *Riesgos de operación asociados a los sistemas informáticos y a la tecnología relacionada a dichos sistemas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la empresa al atentar contra la confidencialidad, integridad y disponibilidad de la información, entre otros criterios.*
29. **Seguridad de la información.** *Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad.*

BIBLIOGRAFÍA

Feature Security Standard – "ISF Standard of Good Practice"

The Information Security Forum – (formerly known as the European Security Forum).
http://www.securityforum.org/menu.htm

Feature Web Site

The Center for Internet Security
http://www.cisecurity.org/

Information Security Management and Assurance A Call to Action for Corporate Governance

http://www.theiia.org/ecm/guide-ia.cfm?doc_id=1309

Building, Managing, and Auditing Information Security

http://www.theiia.org/iia/bookstore.cfm?fuseaction=product_detail&order_num=435

Info_ec - The Information System Security Professionals Portal

www.infosyssec.com

Leading Disaster Recovery and Business Continuity -- Web Sites

Disaster Recovery Information Exchange (DRIE)
www.drie.org
Disaster Recovery Journal (DRJ) Magazine
www.drj.com
Contingency Planning & Management Magazine
www.contingencyplanning.com/
Disaster Recovery Institute International
www.dr.org
Continuity Planning World
www.business-continuity-world.com
The Business Continuity Plan Generator
www.securityauditor.net/bcp-generator
Disaster Recovery World
- www.disasterrecoveryworld.com

The Business Continuity Toolkit
- www.businesscontinuityworld.com

ANEXOS

ANEXO 1

Cultura Empresarial

CULTURA DEL BANCO

La cultura de una organización marca la manera de actuar, la cual se ve proyectada como una lógica consecuencia, en una Imagen Institucional.

Nuestra Cultura, se edifica sobre sólidos pilares, principios y valores, que están presentes en la convivencia diaria, en nuestras acciones individuales y en equipo que hace que nuestro servicio al cliente sea un servicio Oportuno, Libre de Errores, con Aptitud y Actitud Personal.

Asimismo, nuestra Cultura tiene un trasfondo de desarrollo del empleado a la vez que busca reforzar el negocio logrando la fidelidad, la satisfacción y superación de las expectativas de nuestros clientes a través de un servicio de Alta Calidad, que nos permita diferenciarnos y obtener una ventaja competitiva frente a los otros bancos.

Esta manera de actuar que nos identifica es nuestra cultura, la Cultura BANCO.

NUESTRA MISION

Brindar a nuestros clientes un servicio de elevado nivel de personalización mediante servicios y productos de alta calidad y valor agregado. Maximizar la rentabilidad de los accionistas, y Contribuir al desarrollo integral del personal que lo conforma.

NUESTRA VISION

Institución financiera sólida y rentable, reconocida por una gestión confiable, ética y por la calidad de servicio que brinda.

NUESTROS VALORES

Dirección

Tenemos una clara identificación con la Misión, Visión y Objetivos del BANCO.

Profesionalismo

Asesoramos a nuestros clientes y le brindamos soluciones a sus problemas demostrando nuestra eficiencia. Para ello desarrollamos nuestros conocimientos habilidades y actitudes necesarios para desarrollar nuestro trabajo y alcanzar nuestros objetivos personales y de nuestro Banco. El BANCO provee de programas de capacitación a todo el personal que muestre un gran interés por realizar lo mejor posible su trabajo.

Calidad de Servicio

Todos estamos comprometidos con nuestra Calidad de Servicio. Tenemos una actitud proactiva orientada a satisfacer al cliente y exceder sus expectativas a través de un servicio oportuno, con precisión, con actitud y aptitud personal.

Confidencialidad de la Información

Mantenemos un gran respeto por la confidencialidad de la información de nuestros clientes. Todos velamos para que la discreción sea parte de nuestra atención.

Transparencia

Brindamos toda la información necesaria a nuestros clientes de forma paciente y transparente.

Trabajo en Equipo

Todos debemos trabajar en total unidad. Nos debemos caracterizar por la confianza muta, compromiso, colaboración, solidaridad y respeto por los demás teniendo en cuento que el trabajo de cada uno forma parte de un gran objetivo, el objetivo del BANCO.

Compromiso con el Negocio

Todos nos sentimos comprometidos, a través de nuestro trabajo, con el negocio del BANCO. Mostramos una actitud vendedora, proyectando positivamente la imagen del BANCO y promoviendo la vinculación de nuestros clientes.

Innovación

Con iniciativa personal y creatividad estamos innovando productos y servicios que atienden a las necesidades de nuestro público objetivo y hacen frente a la competencia.

Modernidad

Estamos atentos a los avances tecnológicos que estén orientado a nuestra eficiencia, productividad y a la satisfacción de nuestros clientes.

Compromiso Social

Somos una organización que vive inmersa en la realidad de nuestro País, es por eso que tanto el BANCO como sus empleados asumimos el compromiso de realizar acciones concretas para ayudar al desarrollo social del Perú.

NUESTRA HISTORIA

El BANCO inició sus operaciones en febrero de 1991 como una muestra de la confianza en el desarrollo futuro del país de su principal accionista, el Grupo F, que cuenta con una sólida presencia en el Perú, destacando en la fabricación de tabacos, fósforos, licores, agroindustria y construcción.

Nuestro BANCO empezó con 29 personas, en un pequeño local ubicado en San Isidro hasta Septiembre de 1997 fecha en que se inaugura el moderno edificio donde actualmente funciona la Sede Principal.

En 1996, cuando se vislumbraba estabilidad económica, política y social en el País, empieza la expansión geográfica con la primera agencia Santa Anita a la vez que se iniciaba un crecimiento en los negocios. Posteriormente se inaugura la agencia Colonial, abriendo paso así a nuevos proyectos como es el de *Credi Ahorro* que se ofreció en las agencias de Villa El Salvador, Villa María del Triunfo y San Juan con promociones de accesos a créditos de canje de artefactos etc. por abrir cuentas de ahorro, esta constituyó la primera promoción del BANCO dirigida a personas naturales.

En la actualidad el BANCO ha conformado una organización dinámica, con metas ambiciosas, que participa activamente en un mercado cada vez más competitivo, ofreciendo una opción en productos y servicios que aporta valor a clientes cada vez más exigentes. Para ello se han destinado recursos humanos y materiales suficientes dotándolos de la infraestructura y tecnología más moderna para brindar la mejor atención bancaria.

La imagen institucional del BANCO es reconocida en el sistema financiero nacional e internacional, lo que se ha traducido en la gran aceptación como emisor de papeles en el mercado de inversionistas locales y en el

otorgamiento de importantes líneas de Bancos corresponsales extranjeros. El manejo prudente de las operaciones activas y el adecuado financiamiento han permitido la expansión de las facilidades crediticias de comercio exterior a nuestros clientes, con el apoyo de una eficiente red de corresponsales en más de cincuenta países de todos los continentes y de los cinco Bancos del Grupo en Curaçao, Ecuador, Estados Unidos, Guatemala y Venezuela.

El BANCO brinda *Confidencialidad y Respaldo* a sus clientes, lo cual nos hace un Banco Competitivo y de gran Solidez, por ello buscamos la eficiencia, competitividad y profesionalismo de nuestro personal, ya que esta es una muestra clara de nuestra imagen.

II. RED DE OFICINAS

- Santa Anita
- Colonial
- San Juan de Miraflores
- Fiori
- Dos de Mayo
- Sede central
- Jr. De la Union
- Mercado de Productores
- Jockey Plaza
- Miraflores
- San Borja
- La Molina
- Chacarilla
- Risso
- Dasso
- San Miguel
- Trujillo

EL GRUPO F

- **Origen del Grupo**

En los años 40, un conocido hombre de negocios español con una exitosa trayectoria empresarial y con una clara visión del potencial y oportunidades que ofrecía el continente americano, decidió realizar un importante esfuerzo

inversor en esta región. Es en este momento cuando se produce el nacimiento del Grupo F.

Si bien en sus orígenes el Grupo F creció fundamentalmente en torno a la industria del fósforo, el carácter emprendedor de sus gestores motivó una significativa diversificación del Grupo en diferentes sectores, y a lo largo de toda la geografía latinoamericana.
Hoy en día, las empresas del Grupo F desarrollan sus actividades productivas y comerciales en la casi totalidad de los mercados latinoamericanos, habiéndose convertido en uno de los mayores y más profesionalizados grupo financiero industrial de esta región.

- **Composición del Grupo**

Actualmente el Grupo F se encuentra altamente diversificado, con más de 10.000 profesionales repartidos en 20 sectores económicos, entre los que cabe destacar los siguientes:

División Industrial	División Financiera
➢ Fósforo y derivados ➢ Tabaco y cigarrillos ➢ Explotaciones forestales ➢ Explotaciones energéticas ➢ Alcohol y licores ➢ Construcción ➢ Negocio inmobiliario ➢ Distribución	➢ Bancos ➢ Compañía de Seguros ➢ Sociedades de Valores ➢ Sociedades de Financiación ➢ Almacenadoras Fiscales ➢ Gestoras de Fondos de Inversión

- **Expansión Geográfica del Grupo**

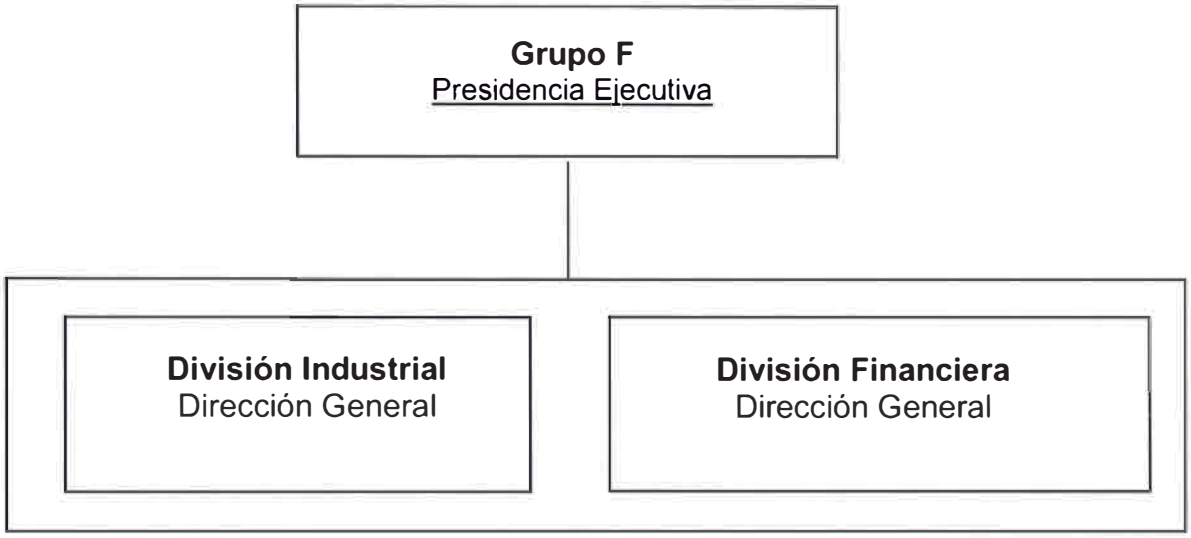
El Grupo F lleva mas de 50 años invirtiendo y desarrollando actividades empresariales en el continente americano, y muy especialmente en Latinoamérica. Esta ininterrumpida trayectoria remarca la confianza del Grupo en esta región y su elevado potencial.

Actualmente, el Grupo F mantiene vínculos comerciales con la totalidad de los mercados latinoamericanos, contando con los centros productivos en los siguientes países:

- Argentina
- Brasil
- Colombia
- Costa Rica
- Ecuador
- España
- Estados Unidos
- Guatemala
- Honduras
- Perú
- El salvador
- Venezuela

- **Estructura Organizativa del Grupo**

A efectos operativos de la Dirección General Corporativa del Grupo F esta segmentada en dos Divisiones, la industrial y la Financiera, a cargo de las cuales se encuentra la tutela y dirección estratégica de las diferentes compañías que lo componen:



- **División Financiera del Grupo**

La división Financiera del Grupo F a través de su Dirección General Corporativa, a cuyo frente se encuentra D. F. R., tiene encomendado el desarrollo de la siguiente misión:

Misión Prioritaria:

Establecer y coordinar la Política, Estrategia y Modelo Básico de Gestión de los bancos que conforman el **Grupo F.**

La Dirección General Corporativa ha definido para cada uno de los bancos que componen la División Financiera el siguiente objetivo:

> *Objetivo Corporativo:*
>
> *Cada banco del **Grupo F** ha de potenciar su crecimiento con rentabilidad y eficiencia, reforzar su posición competitiva en sus respectivos mercados y generar valor para los accionistas, clientes y empleados, de forma sostenida.*

ANEXO 2

LA ADMINISTRACION DE LA SEGURIDAD

1. DEFINICION

El Oficial de Seguridad es la persona encargada exclusivamente de la administración de la seguridad en la organización.

2. BENEFICIOS DE CONTAR CON UN OFICIAL DE SEGURIDAD :

- Permite establecer una adecuada segregación de funciones en la organización, debido que el Departamento Central de Informática se abocará exclusivamente a la Gestión de la tecnología informática y Auditoría Interna controlará tanto el desarrollo de la gestión informática como el cumplimiento de los controles establecidos por el Oficial de Seguridad.
- Permite que el tema de la seguridad, en organizaciones altamente dependientes de la tecnología, tome relevancia dentro de las organizaciones.
- Permite un efectivo control hacia la unidad de mayor riesgo informático: el Departamento Central de Informática.
- Permite eliminar la dependencia de personal de informática.
- Ayuda al orden de las actividades propias de la gestión informática.
- El análisis de la seguridad se hace de una perspectiva del negocio, no sólo técnicamente.

3. FACTORES CRÍTICOS DE ÉXITO PARA LA SEGURIDAD DE DATOS :

- La ubicación jerárquica del Oficial debe ser de alto nivel.
- Debe ser independiente a la Jefatura de Informática.

- Debe ser independiente a Auditoría
- Debe tener el apoyo de la Gerencia General.

4. CARACTERÍSTICAS DE UN OFICIAL DE SEGURIDAD :

Conocimientos de Informática	**35%**
Conocimientos de Seguridad	35%
Habilidad para trabajar en equipo	10%
Instinto Auditor	10%
Conocimiento de la Organización	10%

5. SEGURIDAD DE DATOS

La administración de seguridad debe comenzar con el compromiso de la gerencia por la tarea. La gerencia debe comprender y evaluar los riesgos de seguridad. La gerencia debe desarrollar e imponer una política por escrito que fije en forma clara las normas y procedimientos que se han de llevar a cabo. La tarea del Oficial de Seguridad debe estar definida en esa política. Esa persona debe ser un empleado dedicado en tiempo completo que reporte directamente a la Gerencia y que provea de la adecuada segregación de tareas.

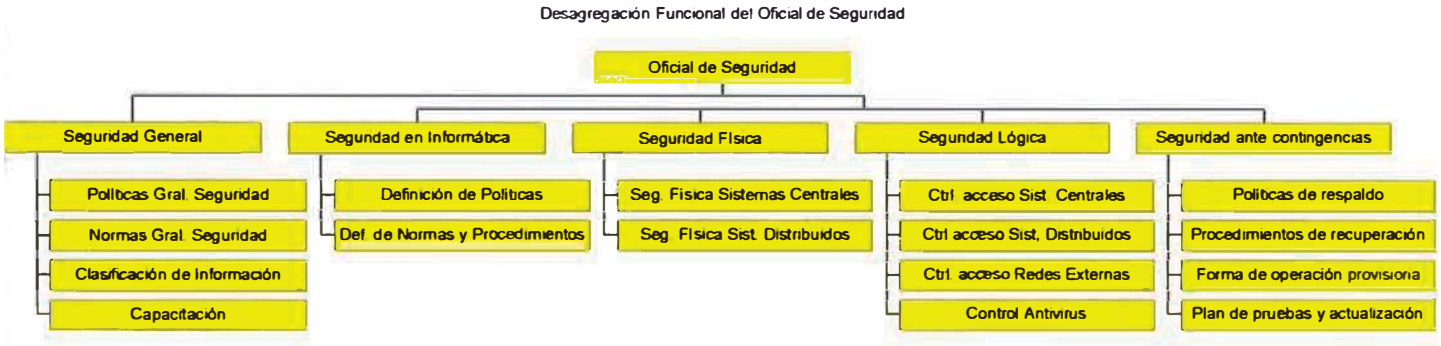
El Oficial de Seguridad debe garantizar que la política de seguridad de la empresa es cumplida por los diversos usuarios y que los controles son adecuados para evitar el acceso no autorizado a los bienes de la empresa (incluyendo datos, programas y recursos de cómputo).

6. LAS FUNCIONES DEL OFICIAL DE SEGURIDAD SON :

- Determinar las reglas de acceso a archivos y recursos.
- Determinar la seguridad y confidencialidad respecto de la emisión y el correcto mantenimiento de los perfiles y contraseñas de los usuarios autorizados.
- Monitorear las violaciones a la seguridad y emprender acción correctiva para garantizar que se brinda la seguridad adecuada.

- Revisar en forma periódica y evaluar la política de seguridad y sugerir a la Gerencia cualquier cambio necesario.
- Debe promover la percepción de la seguridad en los empleados, a través de entrenamientos formales.

El Oficial de Seguridad, tiene a su cargo la responsabilidad de implantar, monitorear y hacer cumplir las normas de seguridad establecidas y autorizadas por la Gerencia. Para lograr una mejor segregación de funciones, no debe estar a cargo de actualizar los datos de las aplicaciones, o ser el usuario final, programador de aplicaciones, operador del computador o encargado del ingreso de datos.



SEGURIDAD GENERAL

Políticas de Seguridad

Establece el alcance, responsabilidades y objetivos que se plantea la organización en términos de la Seguridad de Tecnologías.

Normas Gral. De Seguridad

Establece normas generales sobre seguridad : Manejo de User y password, controles sobre password, controles sobre conexiones y usos de software, procedimientos de solicitud de acceso, sanciones a infractores a políticas y normas.

Clasificación de Información

Permite orientar controles en los elementos de información más críticos. Regula el manejo de información impresa y en medios magnéticos, así como su almacenamiento, transmisión, copiado, distribución y destrucción.

Capacitación

Establece campañas de capacitación y conscientización a todos los usuarios con respecto al tema de seguridad de tecnologías.

SEGURIDAD EN INFORMÁTICA

Definición de Políticas

Establece el alcance y responsabilidades de las unidades del Departamento de Sistemas en cuanto al manejo de la información en producción, así como el alcance y responsabilidades de seguridad de datos con respecto a la gestión informática.

Definición de Normas y Procedimientos

Define normas sobre el manejo de información en los distintos ambientes computacionales de producción. Se definen mecanismos de control a usuarios privilegiados, mecanismos de control a archivos y bibliotecas críticos tanto a nivel de los sistemas básicos como de utilitarios.

SEGURIDAD LÓGICA

Control de acceso a sistemas centrales

Administra los mecanismos de creación, mantención y eliminación de usuarios, así como los perfiles de acceso a todos los recursos computacionales de los sistemas centrales (tanto a nivel sistema operativo como de aplicaciones).

Control de Acceso a sistemas distribuidos

Administra los mecanismos de creación, mantención y eliminación de usuarios, así como los perfiles de acceso a todos los recursos computacionales de los servidores distribuidos en departamentos (tanto a nivel de sistema operativo como de aplicaciones).

Control de acceso a redes externas

Administra, controla y monitorea los mecanismos de acceso a los servidores desde redes externas (internet o conexiones especiales).

Control antivirus

Administra, controla y monitorea los mecanismos de control antivirus, tanto a nivel de servidores como de estaciones.

SEGURIDAD FÍSICA

Seguridad Física a Sistemas Centrales

Establece los mecanismos preventivos y detectivos que permitan proteger los dispositivos computacionales centrales ya sea de siniestros o sabotajes.

Seguridad Física a Sistemas Distribuidos

Establece los mecanismos preventivos y detectivos que permitan proteger los servidores y sus componentes, localizados en departamentos, ya sea de siniestros o sabotajes.

SEGURIDAD ANTE CONTINGENCIAS

Políticas de respaldo

Establece los mecanismos, periodicidades y procedimientos de respaldo para los distintos servidores y/o aplicaciones

Procedimientos de recuperación

Establece los procedimientos de recuperación de servidores y/o aplicaciones ante fallas o contingencias que las afecten.

Forma de Operación Provisoria

Establece mecanismos de operación alternativos para las aplicaciones, en el lapso en que no se disponga de recursos computacionales.

Plan de pruebas y actualización

Establece los programas de pruebas a los planes de contingencia, así como las actualizaciones derivadas de efectos de las pruebas, cambios de equipamiento, personal u otros.

ANEXO 3

PLAN DE CONTINUIDAD DE NEGOCIOS DEL BANCO

INDICE

Extracto del PCN:

1. GENERALIDADES

1.1. INTRODUCCIÓN

*El **Plan de Continuidad de Negocios (PCN),** se define como un proceso continuo de planeación, desarrollo, prueba e implantación de procesos y procedimientos de continuidad y recuperación de las funciones críticas de negocio, ante los casos de emergencia y/o interrupciones que puedan suscitarse en la organización.*

*Debido al alto grado de dependencia que el **Banco**, tiene en las tecnologías de información, que dan soporte a los procesos esenciales, al crecimiento y a los cambios en la Organización, es que se requiere disponer de un PCN, para asegurar la continuidad efectiva y eficiente de las funciones vitales del Banco, en el evento de una contingencia, minimizando el impacto en el desenvolvimiento de las actividades normales del Banco.*

En tal sentido, el presente documento ha sido desarrollado, en concordancia con las políticas de seguridad de información del Banco, con el objetivo de detallar las responsabilidades y procedimientos operativos de las unidades del Banco y, asegurar y mantener la continuidad de las operaciones, ante la presentación de severas interrupciones en los procesos críticos.

*Es importante mencionar que el presente documento es considerado como un '*documento vivo*', por lo que deberá ser revisado y actualizado periódicamente.*

1.2. OBJETIVOS

Los objetivos del PCN del Banco son:

a. *Identificar las actividades, procedimientos y tareas necesarias para soportar la continuidad de los procesos críticos en forma eficiente y efectiva.*
b. *Definir las responsabilidades y roles de las personas que están involucradas en el PCN.*
c. *Asegurar en el evento de una contingencia, la continuidad, recuperación y reanudación de las operaciones del Banco en un tiempo prudencial.*
d. *Organizar y movilizar a los equipos responsables por el proceso de recuperación y reanudación de las operaciones del Banco inmediatamente después de declarada la Contingencia.*
e. *Mantener el control de las operaciones en modalidad de contingencia, permitiendo el flujo de información durante el estado de las actividades de recuperación.*
f. *Permitir el retorno de las operaciones del CC del Banco, una vez que la situación de contingencia haya sido superada.*

g. *Tener un esquema de pruebas del PCN, en lo referente a la alta disponibilidad, comunicaciones y contingencia.*

h. *Tener los lineamientos para la actualización del PCN del Banco.*

1.3. ALCANCES

Al contar el Banco con la identificación de sus procesos y recursos críticos, es posible cumplir con su misión de mantener la continuidad operativa de sus funciones de negocio ante las contingencias que pudieran presentarse.

Este plan proporciona una descripción de las responsabilidades individuales y los procedimientos necesarios para ejecutar los planes de contingencia, así como para poner en marcha el equipo de cómputo alterno del Banco AS/400, Red de Comunicaciones.

2. ORGANIZACIÓN DE LOS EQUIPOS DE TRABAJO

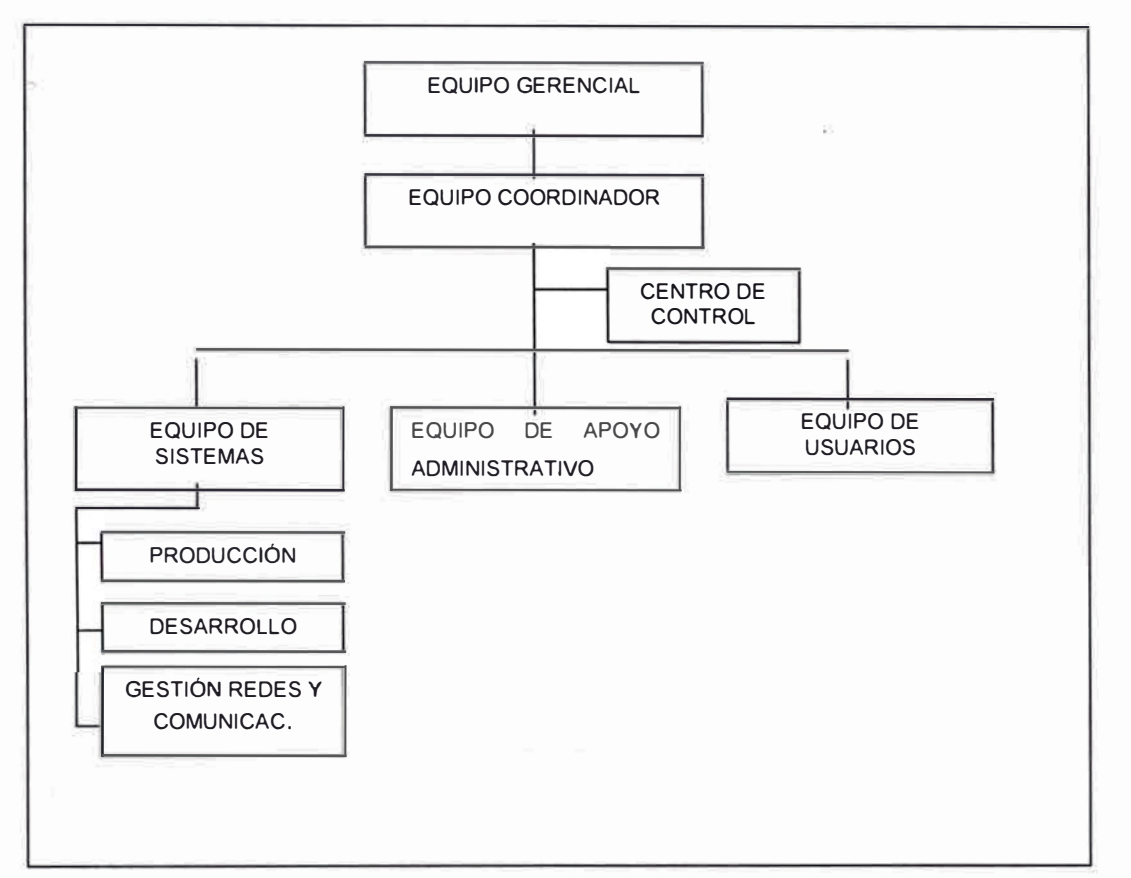
En este capítulo se define la organización y los roles de los diferentes equipos de trabajo definidos para el proceso de recuperación de las operaciones en caso de una contingencia, así como de sus responsabilidades asociadas.

A fin que las actividades estén claramente especificadas, éstas han sido divididas en tres categorías de acuerdo al momento en que deben ser ejecutadas: antes, durante y después de una situación de contingencia.

Asimismo, ha sido necesario considerar las siguientes premisas para la conformación de los equipos:

- *Cada líder de equipo debe tener un alterno*
- *Cada equipo debe estar conformado por lo menos de dos personas, pudiendo ser el alterno uno de ellos*
- *Los equipos deben estar conformados con personal que dispone el Banco, no con personal que se contratará o capacitará.*
- *Ningún integrante debe participar en más de un equipo cuyas tareas durante una contingencia sean concurrentes*
- *Toda persona identificada en el PCN debe conocer las responsabilidades que tiene que asumir. Esto minimizará las posibilidades de inoperatividad de los equipos ante la ausencia de sus integrantes y/o desconocimiento de sus responsabilidades*

2.1. ESTRUCTURA ORGANIZACIONAL



3. PROCESOS CRÍTICOS DE NEGOCIO

El propósito de este numeral es detallar los procesos de negocio considerados como necesarios para la continuidad de las operaciones del Banco, los cuales ante una contingencia ocasionarían la interrupción parcial o total de los servicios del Banco.

4. ESCENARIOS DE CONTINGENCIA

Debemos entender como situación de contingencia al evento o sucesión de eventos no previstos, que superan un período de tiempo determinado, cuyo impacto no permite el desenvolvimiento de las actividades del Banco.

Para propósitos de activación de plan de contingencia, se ha tomado en cuenta aspectos internos como fallas de aplicativos críticos, y también aspectos externos, que comprometen los servicios de suministro de energía eléctrica y transmisión de datos y voz por los operadores telefónicos.

A continuación mostramos los escenarios de contingencia considerados:

	ESCENARIOS DE CONTINGENCIA
1	*INTERRUPCIÓN DE SUMINISTRO ELECTRICO EN LA OFICINA PRINCIPAL*
2	*INTERRUPCIÓN DE SUMINISTRO ELECTRICO EN LAS AGENCIAS QUE CUENTAN CON GRUPO ELECTRÓGENO*
3	*INTERRUPCIÓN DE SUMINISTRO ELECTRICO EN LAS AGENCIAS QUE NO CUENTAN CON GRUPO ELECTRÓGENO*
4	*PARALIZACIÓN DEL CENTRO DE CÓMPUTO PRINCIPAL*
5	*INTERRUPCIÓN CORE CENTRAL EN HORARIO DE ATENCIÓN AL PÚBLICO*
6	*INTERRUPCIÓN EN LOS SERVICIOS DE COMUNICACIÓN / TRANSMISIÓN DE DATOS Y VOZ CON LAS AGENCIAS POR CAÍDA DE ENLACE PRINCIPAL DE COMUNICACIÓN IP-VPN DE 256 Kbps*
7	*INTERRUPCIÓN EN LOS SERVICIOS DE COMUNICACIÓN / TRANSMISIÓN DE DATOS Y VOZ CON LAS AGENCIAS POR FALLA DE EQUIPOS DE COMUNICACIÓN*
8	*FALLA DEL SERVIDOR SWIFT*
9	*INTERRUPCIÓN DEL SISTEMA CORVU POR FALLA DEL SERVIDOR*

ANEXO 4

MONITOR BYTE

Considerando la necesidad actual que tienen las empresas Bancarias y Financieras en contar con sistemas que les permita obtener información confiable y oportuna, a fin de minimizar el riesgo implícito que involucran las transacciones diarias propias del giro del negocio por un lado y por otro lograr un nivel de control en todas las áreas críticas de cualquier institución, es que nos permitimos alcanzarles una propuesta integral de un sistema que calza justo a la medida de la actual circunstancia cuyo nombre es **MONITOR BYTE**.

El Sistema **MONITOR BYTE**, es el resultado de años de experiencia en la Industria Bancaria y Financiera, así como la aplicación de Software de Comunicaciones, que Byte ha implementado en diversos países de Latinoamérica.

Monitor es un sistema que brinda a las instituciones financieras una mayor seguridad permitiéndoles minimizar, en forma eficaz y oportuna, posibles fraudes, riesgos crediticios, descalce de tasas y/o plazos, control de tesorería entre otros.

Monitor es el resultado de la combinación de nuestra gran experiencia en los sectores financieros y de telecomunicaciones ya que, en su concepción y diseño, hemos utilizado componentes de tecnología de punta, propios de ambos sectores.

Lo anterior se aprecia por el alto nivel de sofisticación y el gran rendimiento que se puede alcanzar en el monitoreo de todas las operaciones que pueden considerarse de alto riesgo o con posibilidad de fraude.

Monitor brinda una ágil administración de los eventos a monitorear, gracias a la gran flexibilidad en su parametrización. Lo anterior permite una rápida incorporación de nuevos tipos de control.

Aunada a la versatilidad para administrar e incorporar diferentes tipos de control, Monitor tiene una gran capacidad de envíos de alertas. Los mensajes de alertas pueden ser enviados simultáneamente a uno o a varios miembros de la institución financiera, a sus teléfonos celulares, teléfonos particulares, anexos, busca personas, fax, correo electrónico, entre otros.
Para realizar su labor, monitor se conecta a las plataformas mas difundidas en el mercado: IBM S/390, IBM AS/400, UNIX, WINDOWS NT y LINUX.

Si Consideramos el costo-beneficio que el Monitor puede lograr en una empresa, desde ya se trata de un producto cuya recuperación de la inversión está asegurada.

En base a nuestra experiencia contamos con una lista de eventos que pueden servir de base para fijar los criterios de aceptación dentro de los requerimientos de cada Institución, los cuales describimos a continuación.

- **Transacciones Administrativas:**
  - Autorización de sobregiros.
  - Liberación de fondos en cuentas de ahorros, Cta. Cte. entre otros.
  - Consulta a cuentas de funcionarios, accionistas, empleados o clientes VIP.

- **Transacciones de Plataforma:**

- Emisión de cheques de Gerencia.
- Cambio de datos en archivo de clientes.

- **Transacciones de Caja Monetarios:**

  Pago de cheques sin V.B. del Funcionario(montos mayores)
  - Notas de abono y débito por montos no establecidos.

  Depósitos importantes inusuales
  - Giros y transferencias por montos importantes

- **Transacciones de Caja Ahorros:**
  - Retiros mayores al monto máximo establecido.

  Créditos no autorizados.
  - Abono de intereses por encima del rango.

- **Transacciones de operaciones de Cartera Extranjera o Comercio Exterior:**
  - Compra - venta de moneda extranjera(probable lavado de dinero)
  - Transferencias internacionales dudosas.

- **Transacciones de Tarjeta de Débito:**
  - Retiro de fondos por un monto mayor al establecido.
  - Control de retiros en centros considerados como de alto riesgo.
  - Control de retiros sospechosos en el mismo día.

- **Transacciones de Tarjeta de Crédito:**
  - Transacciones efectuadas en diferente país con poco intervalo de tiempo.
  - Transacciones internacionales por monto mayor al máximo establecido.
  - Monitoreo en establecimientos considerados de alto riesgo.

- Monitoreo de transacciones en tiempo mayor al establecido.(2 horas por ejem.)
- Monitoreo de operaciones en número mayor a las permitidas en un mismo día.

  Monitoreo de modificaciones en las líneas de crédito de los empleados.
- Monitoreo de consumos con tarjetas morosas, sobregiradas o con orden de bloqueo.

Descripción Funcional

Monitor consta de las siguientes funciones

1) Administración y Parametrización
2) Captación y Análisis
3) Generador de Alertas
4) Generador de Reportes

Administración y Parametrización :

A través de esta función se definen: Los eventos a monitorear, las alertas que se utilizaran en cada caso, los usuarios del sistema (tanto a aquellos que son sujetos de monitoreo, como aquellos a los que se les envían las alertas) y otros parámetros que determinan la forma como Monitor va a trabajar la detección de eventos y el envío de alertas.

Captación y Análisis :

Esta es la parte operativa del Monitor . En base a los parámetros definidos en el paso anterior se realiza el monitoreo de eventos. Monitor captura las transacciones que ocurren en el sistema de la institución financiera y se los pasa a diferentes **analizadores**, que son programas que se encargan de determinar si tiene lugar alguno de los eventos que se han definido en la

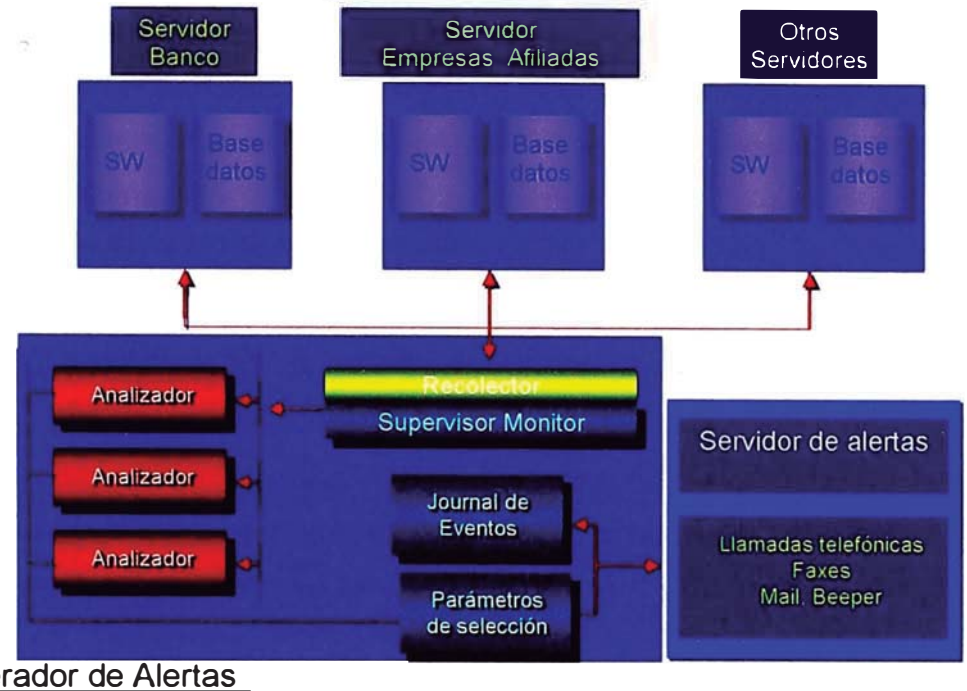
parametrización. De ocurrir esto, el analizador que ha detectado el evento se encarga de avisar al Generador de Alertas.

Existen diversas formas en que Monitor puede capturar la información de las transacciones de la institución. Dependiendo de las características de los sistemas, la captura se puede realizar:

- Del log de transacciones
- Modificando aplicativos de la institución
- Incorporando programas de captura
- Simulando sesiones en terminal

Con estas cuatro alternativas cubrimos todo el aspecto de posibilidades de captura de información por parte del Monitor, para su posterior análisis.

Gráfica de Conectividad



Generador de Alertas

Los eventos a controlar cuya ocurrencia haya sido detectada, son informados inmediatamente al Generador de Alertas. Este, en función de la parametrización definida, se encarga de invocar los mensajes respectivos a los usuarios asociados a dicho evento y a los diferentes medios definidos para tal caso(teléfono, fax, beeper, correo electrónico, etc.).

Generador de Reportes y Consultas en Línea :

Se guarda un Journal de los eventos monitoreados, de las alertas generadas y los mensajes enviados. Esta información permite obtener reportes y consultas en línea con información estadística, útil para análisis de comportamiento en periodos de corto o mediano plazo y, en general, para aplicar correctivos cuando sea necesario.

Componentes de Monitor:

El sistema Monitor es una solución integrada de Hardware, Software y Servicios de Implementación, y que consta de los siguientes componentes:

i) Equipo PC con tarjeta IVR incorporada, con capacidad de realizar 4 llamadas telefónicas simultáneas, acceso a Internet y envío de Fax. (Se tiene la opción de crecer hasta 16 llamadas telefónicas simultáneas)

ii) Software que incluye el Sistema Operativo, Base de Datos y el Aplicativo.
La base de datos es SQL Server, pudiendo utilizar otros como Oracle o DB2 por ejemplo.

iii) Implementación que incluye: asesoría en parametrización, capacitación, soporte puesta en marcha y adecuaciones para interfaces con el host del BANCO.

Requerimientos de equipo complementarios a Monitor:

El BANCO deberá proveer las líneas telefónicas directas o anexos para realizar las llamadas telefónicas y el envío de fax. Adicionalmente se requiere de una conexión con Internet para enviar los mensajes de correo.

ANEXO 5

LA ADMINISTRACIÓN DE RIESGOS

1. REQUERIMIENTOS PARA LA ADMINISTRACIÓN DE RIESGOS

1.1 Propósito

El propósito de esta Sección es describir un proceso formal para establecer un programa sistemático de administración de riesgos.

Se necesita el desarrollo de una política organizacional de administración de riesgos y un mecanismo de soporte con objeto de proveer una estructura para llevar a cabo un programa de administración de riesgos más detallado a nivel sub-organizacional o de proyecto.

1.2 Política de administración de riesgos

El ejecutivo de la organización debe definir y documentar su política para administración de riesgos, incluyendo objetivos para, y su compromiso con, la administración de riesgos. La política de administración de riesgos debe ser relevante para el contexto estratégico de la organización y para sus metas, objetivos y la naturaleza de su negocio. La gerencia asegurará que esta política sea comprendida, implementada y mantenida en todos los niveles de la organización.

1.3 Planeamiento y recursos

1.3.1 Compromiso gerencial

La organización debería asegurar que:

a) se ha establecido, implementado y mantenido un sistema de administración de riesgos, de acuerdo con este Estándar; y

b) se reporta el desempeño del sistema de administración de riesgos a la gerencia de la organización para revisión y como base para su mejora.

1.3.2 Responsabilidad y autoridad

Deberá definirse y documentarse la responsabilidad, autoridad e interrelaciones del personal que realiza y verifica el trabajo que afecta la administración de riesgos, particularmente para la gente que necesita la libertad y autoridad organizacional para realizar una o más de las siguientes acciones:

a) iniciar acciones para prevenir o reducir los efectos adversos de los riesgos;

b) controlar el tratamiento posterior de los riesgos hasta que el nivel de riesgo se haga aceptable;

c) identificar y registrar cualquier problema relativo a la administración de riesgos;

d) iniciar, recomendar o proveer soluciones a través de los canales asignados;

e) verificar la implementación de soluciones; y

f) comunicar y consultar interna y externamente según corresponda.

1.3.3 Recursos

La organización debe identificar los requerimientos de recursos y proveer recursos adecuados,

incluyendo la asignación de personal entrenado para las actividades de administración, desempeño del trabajo, y verificación incluyendo la revisión interna.

1.4 Programa de implementación

Se requiere seguir una cantidad de pasos para implementar un sistema efectivo de administración de riesgos dentro de una organización. En el Apéndice B se proveen ejemplos. Dependiendo de la filosofía, cultura y estructura general de administración de riesgos de la organización, debería ser posible combinar u omitir ciertos pasos. Sin embargo, deberían considerarse todos los pasos.

1.5 Revisión gerencial

El ejecutivo de la organización debe asegurar que se lleve a cabo una revisión del sistema de

administración de riesgos a intervalos especificados, suficiente para asegurar su continua conformidad y efectividad para satisfacer los requerimientos de este Estándar, y las políticas y objetivos de administración de riesgos establecidos en la organización (ver Cláusula 2.2). Deberá llevarse un registro de tales revisiones.

2. VISTA GENERAL DE LA ADMINISTRACIÓN DE RIESGOS

2.1 General

La administración de riesgos es una parte integral del proceso de administración. La administración de riesgos es un proceso multifacético, aspectos apropiados del cual son a menudo llevados a cabo mejor por un equipo multidisciplinario. Es un proceso iterativo de mejora continua.

2.2 Elementos principales

Los elementos principales del proceso de administración de riesgos, como se muestra en la figura Figura 3.1, son los siguientes:

a) Establecer el contexto

Establecer el contexto estratégico, organizacional y de administración de riesgos en el cual tendrá lugar el resto del proceso. Deberían establecerse criterios contra los cuales se evaluarán los riesgos y definirse la estructura del análisis.

b) Identificar riesgos

Identificar qué, por qué y cómo pueden surgir las cosas como base para análisis posterior.

c) Analizar riesgos

Determinar los controles existentes y analizar riesgos en términos de consecuencias y probabilidades en el contexto de esos controles. El análisis debería considerar el rango de consecuencias potenciales y cuán probable es que ocurran esas consecuencias.

Consecuencias y probabilidades pueden ser combinadas para producir un nivel estimado de riesgo.

d) Evaluar riesgos

Comparar niveles estimados de riesgos contra los criterios preestablecidos.
Esto posibilita que los riesgos sean ordenados como para identificar las prioridades de administración. Si los niveles de riesgo establecidos son bajos, los riesgos podrían caer en una categoría aceptable y no se requeriría un tratamiento.

e) Tratar riesgos

Aceptar y monitorear los riesgos de baja prioridad. Para otros riesgos, desarrollar e implementar un plan de administración específico que incluya consideraciones de fondeo.

f) Monitorear y revisar

Monitorear y revisar el desempeño del sistema de administración de riesgos y los cambios que podrían afectarlo.

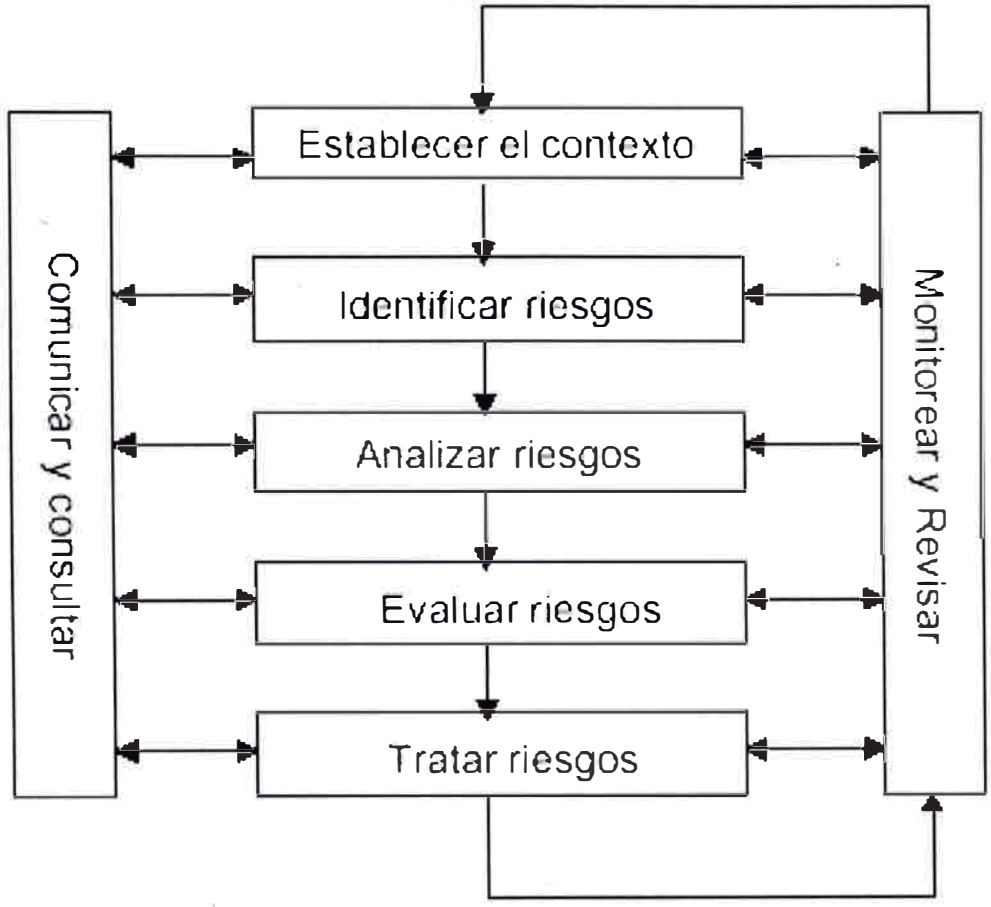
g) Comunicar y consultar

Comunicar y consultar con interesados internos y externos según corresponda en cada etapa del proceso de administración de riesgos y concerniendo al proceso como un todo.

La administración de riesgos se puede aplicar en una organización a muchos niveles. Se lo puede aplicar a nivel estratégico y a niveles operativos. Se lo puede aplicar a proyectos específicos, para asistir con decisiones específicas o para administrar áreas específicas
reconocidas de riesgo.

La administración de riesgos es un proceso iterativo que puede contribuir a la mejora organizacional. Con cada ciclo, los criterios de riesgos se pueden fortalecer para alcanzar progresivamente mejores niveles de administración de riesgos.

Para cada etapa del proceso deberían llevarse registros adecuados, suficientes como para satisfacer a una auditoria independiente.



3.1 Vista General de la Administración de Riesgos

3. PROCESO DE ADMINISTRACIÓN DE RIESGOS

3.1 Establecer el contexto

3.1.1 General

En la Figura 4.1 se muestran los detalles del proceso de administración de riesgos. El proceso ocurre dentro de la estructura del contexto estratégico, organizacional y de administración de riesgos de una organización. Esto necesita ser establecido para definir los parámetros básicos dentro de los cuales deben administrarse los riesgos y para proveer una guía para las decisiones dentro de estudios de administración de riesgos más detallados. Esto establece el alcance para el resto del proceso de administración de riesgos.

3.1.2 Establecer el contexto estratégico

Definir la relación entre la organización y su entorno, identificando las fortalezas, debilidades, oportunidades y amenazas de la organización. El contexto incluye los aspectos financieros, operativos, competitivos, políticos (percepciones públicas / imagen), sociales, de clientes, culturales y legales de las funciones de la organización.

Identificar los interesados internos y externos, y considerar sus objetivos, tomar en cuenta sus percepciones, y establecer políticas de comunicación con estas partes.

nota: Este paso está focalizado en el entorno en el cual opera la organización. La organización debería buscar determinar los elementos cruciales que podrían sustentar o dificultar su habilidad para administrar los riesgos que enfrenta.

Puede llevarse a cabo un análisis estratégico. El mismo debería ser endosado al nivel ejecutivo, para que establezca los parámetros básicos y provea una guía en los procesos más detallados de administración de riesgos. Debería existir una estrecha relación entre la misión u objetivos

estratégicos de una organización y la administración de todos los riesgos a los cuales está expuesta.

3.1.3 Establecer el contexto organizacional

Antes de comenzar un estudio de administración de riesgos, es necesario comprender la organización y sus capacidades, así como sus metas y objetivos y las estrategias que están vigentes para lograrlos.

Esto es importante por las siguientes razones:

a) La administración de riesgos tiene lugar en el contexto de las amplias metas, objetivos y estrategias de la organización;

b) La falla en lograr los objetivos de la organización, o de una actividad específica, o proyecto en consideración, es un conjunto de riesgos que debería ser administrado;

c) La política y metas de la organización ayudan a definir los criterios mediante los cuales se decide si un riesgo es aceptable o no, y constituye la base para las opciones de tratamientos.

3.1.4 Establecer el contexto de administración de riesgos

Deberían establecerse las metas, objetivos, estrategias, alcance y parámetros de la actividad, o parte de la organización a la cual se está aplicando el proceso de administración de riesgos. El proceso debería ser llevado a cabo con plena consideración de la necesidad de balancear costos, beneficios y oportunidades.

También deberían especificarse los recursos requeridos y los registros que se van a llevar.

Establecer el alcance y los límites de una aplicación del proceso de administración de riesgos involucra:

a) Definir el proyecto o actividad y establecer sus metas y objetivos;

b) Definir la extensión del proyecto en tiempo y ubicación;

c) Identificar cualquier estudio necesario y su alcance, objetivos y recursos requeridos. Pueden proveer una guía para esto las fuentes genéricas de riesgo y las áreas de impacto.
d) Definir el alcance y amplitud de las actividades de administración de riesgos a llevar a cabo.
Los aspectos específicos que también podrían ser discutidos incluyen lo siguiente:
i. Los roles y responsabilidades de las distintas partes de la organización que participan en la administración de riesgos;
ii. Las relaciones entre el proyecto y otros proyectos o partes de la organización.

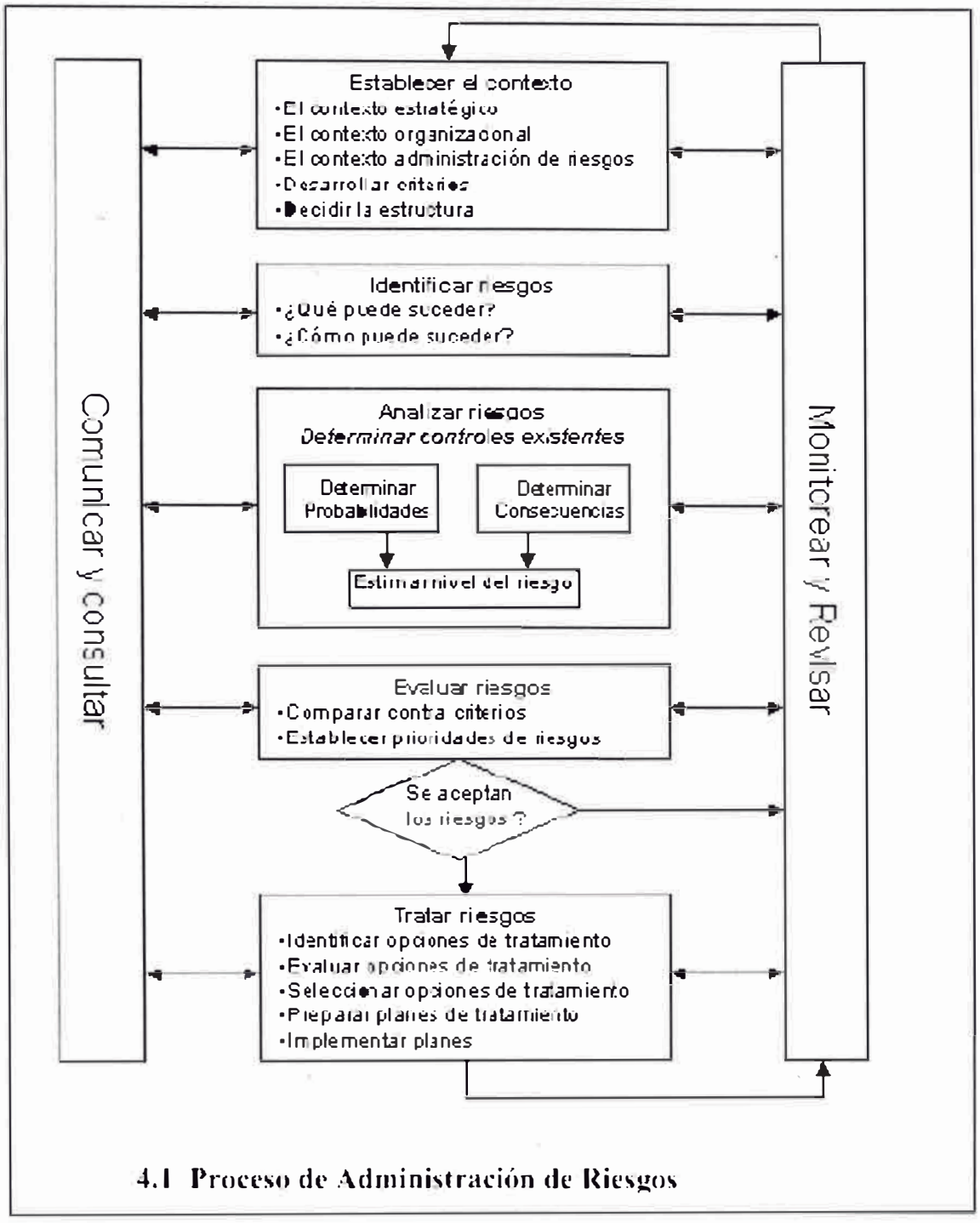
3.1.5 Desarrollar criterios de evaluación de riesgos

Decidir los criterios contra los cuales se va a evaluar el riesgo. Las decisiones concernientes a aceptabilidad de riesgos y tratamiento de riesgos pueden basarse en criterios operativos, técnicos, financieros, legales, sociales, humanitarios u otros. Esto a menudo depende de las políticas, metas y objetivos internos de la organización y de los intereses de las demás partes interesadas.
Los criterios pueden estar afectados por percepciones internas y externas y por requerimientos legales. Es importante que los criterios apropiados sean determinados al comienzo.
Aunque los criterios de riesgo son inicialmente desarrollados como parte del establecimiento del contexto de administración de riesgos, los mismos pueden ser posteriormente desarrollados y refinados a medida que se identifican riesgos particulares y se seleccionan técnicas de análisis de riesgos, ejm: los criterios de riesgo deben corresponder al tipo de riesgos y a la forma en que se expresan los niveles de riesgo.

3.1.6 Definir la estructura

Esto involucra separar la actividad o proyecto en un conjunto de elementos.

Estos elementos proveen una estructura lógica para identificación y análisis lo cual ayuda a asegurar que no se pasen por alto riesgos significativos. La estructura seleccionada depende de la naturaleza de los riesgos y del alcance del proyecto o actividad.



4.1 Proceso de Administración de Riesgos

3.2 Identificación de riesgos

3.2.1 General

Este paso busca identificar los riesgos a administrar. Es crítica una identificación amplia utilizando un proceso sistemático bien estructurado, porque los riesgos potenciales que no se identifican en esta etapa son excluidos de un análisis posterior. La identificación debería incluir todos los riesgos, estén o no bajo control de la organización.

3.2.2 Qué puede suceder

La intención es generar una lista amplia de eventos que podrían afectar a cada elemento de la estructura referida en la Cláusula 4.1.6. Estos son luego considerados en mayor detalle para identificar lo que puede suceder.

3.2.3 Cómo y por qué pueden suceder

Habiendo identificado una lista de eventos, es necesario considerar causas y escenarios posibles.

Hay muchas formas en que se puede iniciar un evento. Es importante que no se omitan las causas significativas.

3.2.4 Herramientas y técnicas

Los enfoques utilizados para identificar riesgos incluyen *"checklist*s", juicios basados en la experiencia y en los registros, diagramas de flujo, *"brainstormin*g", análisis de sistemas, análisis de escenarios y técnicas de ingeniería de sistemas.

El enfoque utilizado dependerá de la naturaleza de las actividades bajo revisión y los tipos de riesgos.

3.3 Análisis de riesgos

3.3.1 General

Los objetivos de análisis son separar los riesgos menores aceptables de los riesgos mayores, y proveer datos para asistir en la evaluación y tratamiento

de los riesgos. El análisis de riesgos involucra prestar consideración a las fuentes de riesgos, sus consecuencias y las probabilidades
de que puedan ocurrir esas consecuencias. Pueden identificarse los factores que afectan a las consecuencias y probabilidades. Se analiza el riesgo combinando estimaciones de consecuencias y probabilidades en el contexto de las medidas de control existentes.
Se puede llevar a cabo un análisis preliminar para excluir del estudio detallado los riesgos similares o de bajo impacto. De ser posible los riesgos excluidos deberían listarse para demostrar que se realizó un análisis de riesgos completo.

3.3.2 Determinar los controles existentes

Identificar la administración, sistemas técnicos y procedimientos existentes para controlar los riesgos y evaluar sus fortalezas y debilidades. Pueden ser apropiadas las herramientas utilizadas en 3.2.4, como asimismo los enfoques tales como inspecciones y técnicas de auto-evaluación de controles ('CSA').

3.3.3 Consecuencias y probabilidades

La magnitud de las consecuencias de un evento, si el mismo ocurriera, y la probabilidad del evento y sus consecuencias asociadas, se evalúan en el contexto de los controles existentes. Las consecuencias y probabilidades se combinan para producir un nivel de riesgo. Se pueden determinar las consecuencias y probabilidades utilizando análisis y cálculos estadísticos.
Alternativamente cuando no se dispone de datos anteriores, se pueden realizar estimaciones subjetivas que reflejan el grado de convicción de un individuo o grupo de que podrá ocurrir un evento o resultado particular.
Para evitar prejuicios subjetivos cuando se analizan consecuencias y probabilidades, deberían utilizarse las mejores técnicas y fuentes de información disponibles.
Se pueden incluir las siguientes fuentes de información:
a) Registros anteriores;

b) Experiencia relevante;
c) Prácticas y experiencia de la industria;
d) Literatura relevante publicada;
e) Comprobaciones de *marketing* e investigaciones de mercado;
f) Experimentos y prototipos;
g) Modelos económicos, de ingeniería u otros;
h) Opiniones y juicios de especialistas y expertos.

Las técnicas incluyen:
i) entrevistas estructuradas con expertos en el área de interés;
ii) utilización de grupos multidisciplinarios de expertos;
iii) evaluaciones individuales utilizando cuestionarios;
iv) uso de modelos de computador u otros; y
v) uso de árboles de fallas y árboles de eventos.
Siempre que sea posible, debería incluirse el nivel de confianza asignado a las estimaciones de los niveles de riesgo.

3.3.4 Tipos de análisis

El análisis de riesgos pueden ser llevado con distintos grados de refinamiento dependiendo de la información de riesgos y datos disponibles. Dependiendo de las circunstancias, el análisis puede ser cualitativo, semi-cuantitativo o cuantitativo o una combinación de estos. El orden de complejidad y costos de estos análisis en orden ascendente, es cualitativo, semi-cuantitativo y cuantitativo. En la práctica, a menudo se utiliza primero el análisis cualitativo para obtener una indicación general del nivel de riesgo. Luego puede ser necesario llevar a cabo un análisis cuantitativo más específico. El detalle de los tipos de análisis es el siguiente:

a) Análisis cualitativo

El análisis cualitativo utiliza formatos de palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la probabilidad de que esas consecuencias ocurran. Estas escalas se pueden modificar o

ajustar para adaptarlas a las circunstancias, y se pueden utilizar distintas descripciones para riesgos diferentes.

El análisis cualitativo se utiliza:

i. como una actividad inicial de tamiz, para identificar los riesgos que requieren un análisis más detallado;

ii. cuando el nivel de riesgo no justifica el tiempo y esfuerzo requerido para un análisis más completo; o

iii. cuando los datos numéricos son inadecuados para un análisis cuantitativo.

b) Análisis semi-cuantitativo

En el análisis semi-cuantitativo, a las escalas cualitativas, tales como las descriptas arriba, se les asignan valores. El número asignado a cada descripción no tiene que guardar una relación precisa con la magnitud real de las consecuencias o probabilidades. Los números pueden ser combinados en cualquier rango de fórmula dado que el sistema utilizado para priorizar confronta el sistema seleccionado para asignar números y combinarlos. El objetivo es producir un ordenamiento de prioridades más detallado que el que se logra normalmente en el análisis cualitativo, y no sugerir valores realistas para los riesgos tales como los que se procuran en el análisis cuantitativo.

Se debe tener cuidado con el uso del análisis semi-cuantitativo porque los números seleccionados podrían no reflejar apropiadamente las relatividades, lo que podría conducir a resultados inconsistentes. El análisis semi-cuantitativo puede no diferenciar apropiadamente entre distintos riesgos, particularmente cuando las consecuencias o las probabilidades son extremas.

A veces es apropiado considerar la probabilidad compuesta de dos elementos, a los que se refiere generalmente como frecuencia de la exposición y probabilidad.

Frecuencia de la exposición es la extensión a la cual una fuente de riesgo existe, y probabilidad es la chance de que, cuando existe esa fuente de

riesgo, le seguirán las consecuencias. Deberá ejercerse precaución en las situaciones en que las relaciones entre
los dos elementos no es completamente independiente, ejm. Cuando hay una fuerte relación entre frecuencia de la exposición y la probabilidad.
Este enfoque se puede aplicar en el análisis semi-cuantitativo y cuantitativo.
c) Análisis cuantitativo
El análisis cuantitativo utiliza valores numéricos para las consecuencias y probabilidades (en lugar de las escalas descriptivas utilizadas en los análisis cualitativos y semi-cuantitativos) utilizando datos de distintas fuentes (tales como las mencionadas en los sub-párrafos (a) a (h) de la Cláusula 3.3.3). La calidad del análisis depende de la precisión e integridad de los valores numéricos utilizados.
Las consecuencias pueden ser estimadas modelando los resultados de un evento o conjunto de eventos, o extrapolando a partir de estudios experimentales o datos del pasado. Las consecuencias pueden ser expresadas en términos de criterios monetarios,
técnicos o humanos, o cualquier otro criterio referido en la Cláusula 3.1.5. En algunos casos se requiere más de un valor numérico para especificar las consecuencias para distintos momentos, lugares, grupos o situaciones.
La probabilidad es expresada generalmente como una probabilidad, una frecuencia, o una combinación de exposición y probabilidad.
La forma en que se expresan las probabilidades y las consecuencias y las formas en que las mismas son combinadas para proveer un nivel de riesgo variarán de acuerdo con el tipo de riesgo y el contexto en el cual se va a utilizar el nivel de riesgo.

3.3.5 Análisis de sensibilidad

Dado que algunas de las estimaciones realizadas en el análisis cuantitativo son imprecisas, deberá llevarse a cabo un análisis de sensibilidad para comprobar el efecto de los cambios en los supuestos y en los datos.

3.4 Evaluación de riesgos

La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente.

El análisis de riesgo y los criterios contra los cuales se comparan los riesgos en la evaluación de riesgos deberían considerarse sobre la misma base. En consecuencia, la evaluación cualitativa involucra la comparación de un nivel cualitativo de riesgo contra criterios cualitativos, y la evaluación cuantitativa involucra la comparación de un nivel numérico de riesgo contra criterios que pueden ser expresados como un número específico, tal como, un valor de fatalidad, frecuencia o monetario.

El producto de una evaluación de riesgo es una lista de riesgos con prioridades para una acción posterior.

Deberían considerarse los objetivos de la organización y el grado de oportunidad que podrían resultar de tomar el riesgo.

Las decisiones deben tener en cuenta el amplio contexto del riesgo e incluir consideración de la tolerabilidad de los riesgos sostenidos por las partes fuera de la organización que se benefician de ellos.

Si los riesgos resultantes caen dentro de las categorías de riesgos bajos o aceptables, pueden ser aceptados con un tratamiento futuro mínimo. Los riesgos bajos y aceptados deberían ser monitoreados y revisados periódicamente para asegurar que se mantienen aceptables.

Si los riesgos no caen dentro de la categoría de riesgos bajos o aceptables, deberían ser tratados utilizando una o más de las opciones consideradas en la Cláusula 3.5.

3.5 Tratamiento de los riesgos

El tratamiento de los riesgos involucra identificar el rango de opciones para tratar los riesgos, evaluar esas opciones, preparar planes para tratamiento de los riesgos e implementarlos.

3.5.1 Identificar opciones para tratamiento de los riesgos

La Figura 4.2 ilustra el proceso de tratamiento de los riesgos. Las opciones, que no son necesariamente mutuamente exclusivas y apropiadas en todas las circunstancias, incluyen lo siguiente:

a) Evitar el riesgo decidiendo no proceder con la actividad que probablemente generaría el riesgo (cuando esto es practicable).

Evitar riesgos puede ocurrir inadecuadamente por una actitud de aversión al riesgo, que es una tendencia en mucha gente (a menudo influenciada por el sistema interno de una organización). Evitar inadecuadamente algunos riesgos puede aumentar la significación de otros.

La aversión a riesgos tiene como resultado:

i) decisiones de evitar o ignorar riesgos independientemente de la información disponible y de los costos incurridos en el tratamiento de esos riesgos.

ii) fallas en tratar los riesgos;

iii) dejar las opciones críticas y/o decisiones en otras partes;

iv) diferir las decisiones que la organización no puede evitar; o

v) seleccionar una opción porque representa un riesgo potencial más bajo independientemente de los beneficios.

b) Reducir la probabilidad de la ocurrencia

c) Reducir las consecuencias

d) Transferir los riesgos

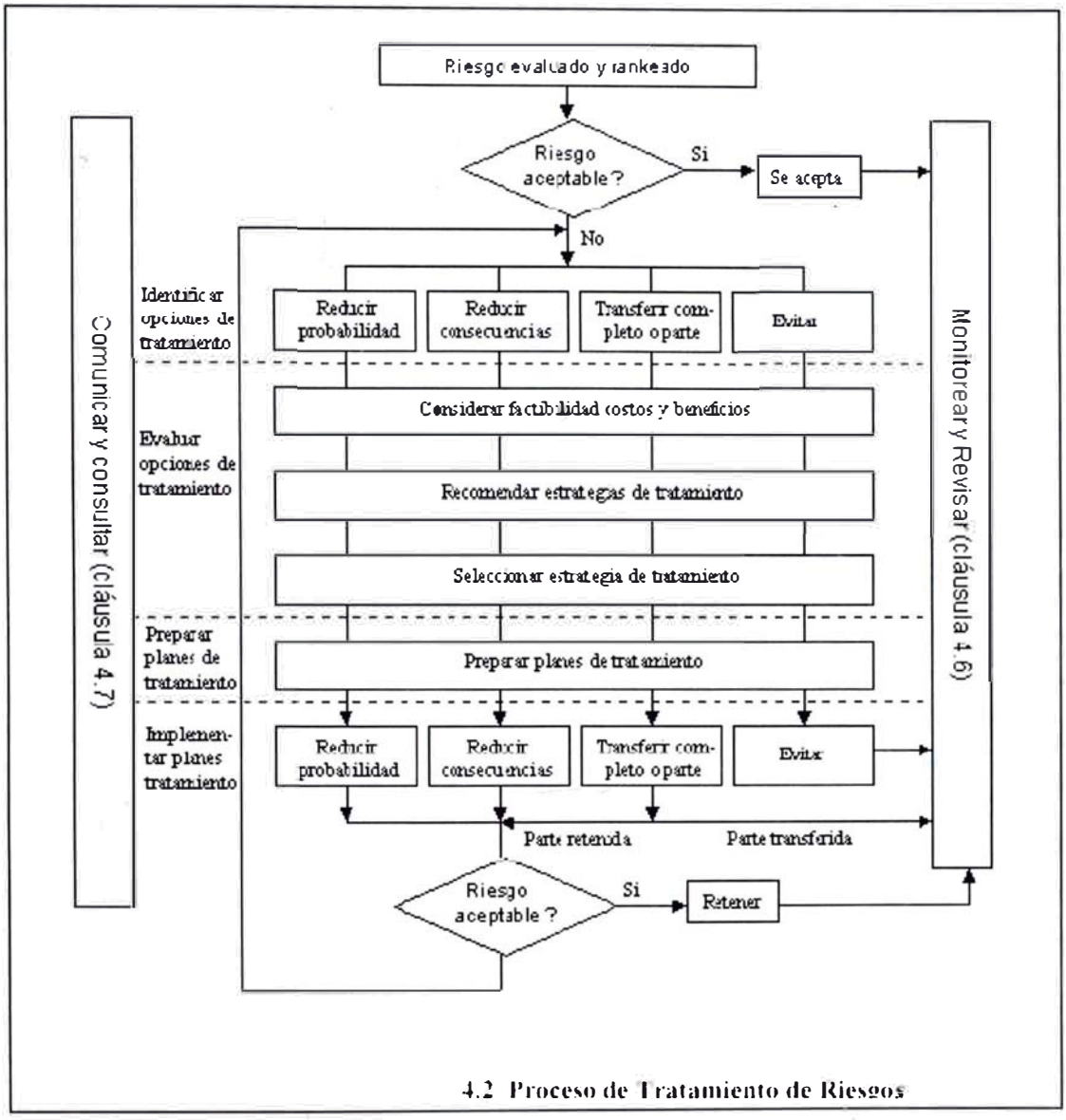
Esto involucra que otra parte soporte o comparta parte del riesgo. Los mecanismos incluyen el uso de contratos, arreglos de seguros y estructuras organizacionales tales como sociedades y *"joint ventures*".

La transferencia de un riesgo a otras partes, o la transferencia física a otros lugares, reducirá el riesgo para la organización original, pero puede no disminuir el nivel general del riesgo para la sociedad.

Cuando los riesgos son total o parcialmente transferidos, la organización que transfiere los riesgos ha adquirido un nuevo riesgo, que la organización a la cual ha transferido el riesgo no pueda administrarlo efectivamente.

e) Retener los riesgos

Luego de que los riesgos hayan sido reducidos o transferidos, podría haber riesgos residuales que sean retenidos. Deberían ponerse en práctica planes para administrar las consecuencias de esos riesgos si los mismos ocurrieran, incluyendo identificar medios de financiar dichos riesgos. Los riesgos también pueden ser retenidos en forma predeterminada, ejm. cuando hay una falla para identificar y/o transferir apropiadamente o de otro modo tratar los riesgos.



4.2 Proceso de Tratamiento de Riesgos

A la reducción de las consecuencias y probabilidades se las puede referir como control de riesgos.

El control de riesgos involucra determinar el beneficio relativo de nuevos controles a la luz de la efectividad de los controles existentes. Los controles pueden involucrar políticas de efectividad, procedimientos o cambios físicos.

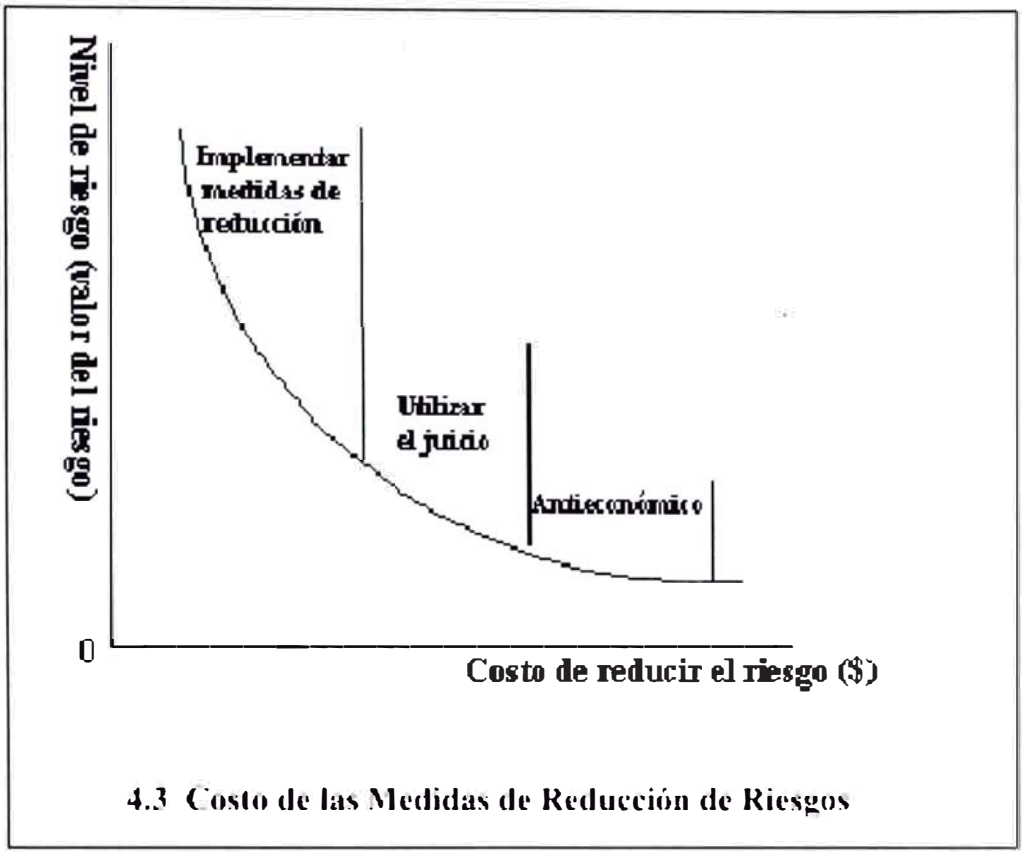
3.5.2 Evaluar opciones de tratamiento de los riesgos

Las opciones deberían ser evaluadas sobre la base del alcance de la reducción del riesgo, y el alcance de cualquier beneficio u oportunidad adicional creadas, tomando en cuenta los criterios
desarrollados en la Cláusula 3.1.5. Pueden considerarse y aplicarse una cantidad de opciones ya sea individualmente o combinadas.

La selección de la opción más apropiada involucra balancear el costo de implementar cada opción contra los beneficios derivados de la misma. En general, el costo de administrar los riesgos necesita ser conmensurada con los beneficios obtenidos.

Cuando se pueden obtener grandes reducciones en el riesgo con un gasto relativamente bajo, tales opciones deberían implementarse. Otras opciones de mejoras pueden ser no económicas y necesita ejercerse el juicio para establecer si son justificables. Esto se ilustra en la Figura 4.3.

Las decisiones deberían tener en cuenta la necesidad de considerar cuidadosamente los riesgos raros pero severos, que podrían justificar medidas de seguridad que no son justificables por fundamentos estrictamente económicos.



4.3 Costo de las Medidas de Reducción de Riesgos

En general el impacto adverso de los riesgos debería hacerse tan bajo como sea razonablemente practicable, independientemente de cualquier criterio absoluto.

Si el nivel de riesgo es alto, pero podrían resultar oportunidades considerables si se lo asume, tal como el uso de una nueva tecnología, entonces la aceptación del riesgo necesita estar basada en una evaluación de los costos de tratamiento y los costos de rectificar las consecuencias potenciales versus las oportunidades que podrían depararse de tomar el riesgo.

En muchos casos, es improbable que cualquier opción de tratamiento del riesgo sea una solución completa para un problema particular. A menudo la organización se beneficiará sustancialmente mediante una combinación de opciones tales como reducir la probabilidad de los riesgos, reducir sus consecuencias, y transferir o retener algunos riesgos residuales. Un ejemplo es el uso efectivo de contratos y la financiación de riesgos sustentados por un programa de reducción de riesgos.

Cuando el costo acumulado de implementación de todos los tratamientos de riesgos excede el presupuesto disponible, el plan debería identificar claramente el orden de prioridad bajo el cual deberían implementarse los tratamientos individuales de los riesgos. El ordenamiento de prioridad puede establecerse utilizando distintas técnicas, incluyendo análisis de *"ranking"* de riesgos y de costo-beneficio. Los tratamientos de riesgos que no puedan ser implementados dentro de los límites del presupuesto disponible deben esperar la disponibilidad de recursos de financiamiento adicionales, o, si por cualquier razón todos o algunos de los tratamientos restantes son considerados importantes, debe plantearse el problema para conseguir el financiamiento adicional.

Las opciones de tratamiento de los riesgos deberían considerar cómo es percibido el riesgo por las partes afectadas y las formas más apropiadas de comunicárselo a dichas partes.

3.5.3 Preparar planes de tratamiento

Los planes deberían documentar cómo deben ser implementadas las opciones seleccionadas.

El plan de tratamiento debería identificar las responsabilidades, el programa, los resultados esperados de los tratamientos, el presupuesto, las medidas de desempeño y el proceso de revisión a establecer.

El plan también debería incluir un mecanismo para evaluar la implementación de las opciones contra criterios de desempeño, las responsabilidades individuales y otros objetivos, y para monitorear los mojones críticos de implementación.

3.5.4 Implementar planes de tratamiento

Idealmente, la responsabilidad por el tratamiento del riesgo debería ser llevada a cabo por aquellos con mejor posibilidad de controlar el riesgo. Las responsabilidades deberían ser acordadas entre las partes en el momento más temprano posible.

La implementación exitosa del plan de tratamiento del riesgo requiere un sistema efectivo de administración que especifique los métodos seleccionados, asigne responsabilidades y compromisos individuales por las acciones, y los monitoree respecto de criterios especificados.

Si luego del tratamiento hay un riesgo residual, debería tomarse la decisión de si retener este riesgo o repetir el proceso de tratamiento.

3.6 Monitoreo y revisión

Es necesario monitorear los riesgos, la efectividad del plan de tratamiento de los riesgos, las estrategias y el sistema de administración que se establece para controlar la implementación. Los riesgos y la efectividad de las medidas de control necesitan ser monitoreadas para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos. Pocos riesgos permanecen estáticos.

Es esencial una revisión sobre la marcha para asegurar que el plan de administración se mantiene relevante. Pueden cambiar los factores que

podrían afectar las probabilidades y consecuencias de un resultado, como también los factores que afectan la conveniencia o costos de las distintas opciones de tratamiento. En consecuencia, es necesario repetir regularmente el ciclo de administración de riesgos. La revisión es una parte integral del plan de tratamiento de la administración de riesgos.

3.7 Comunicación y consulta

La comunicación y consulta son una consideración importante en cada paso del proceso de administración de riesgos. Es importante desarrollar un plan de comunicación para los interesados internos y externos en la etapa más temprana del proceso. Este plan debería encarar aspectos relativos al riesgo en si mismo y al proceso para administrarlo.

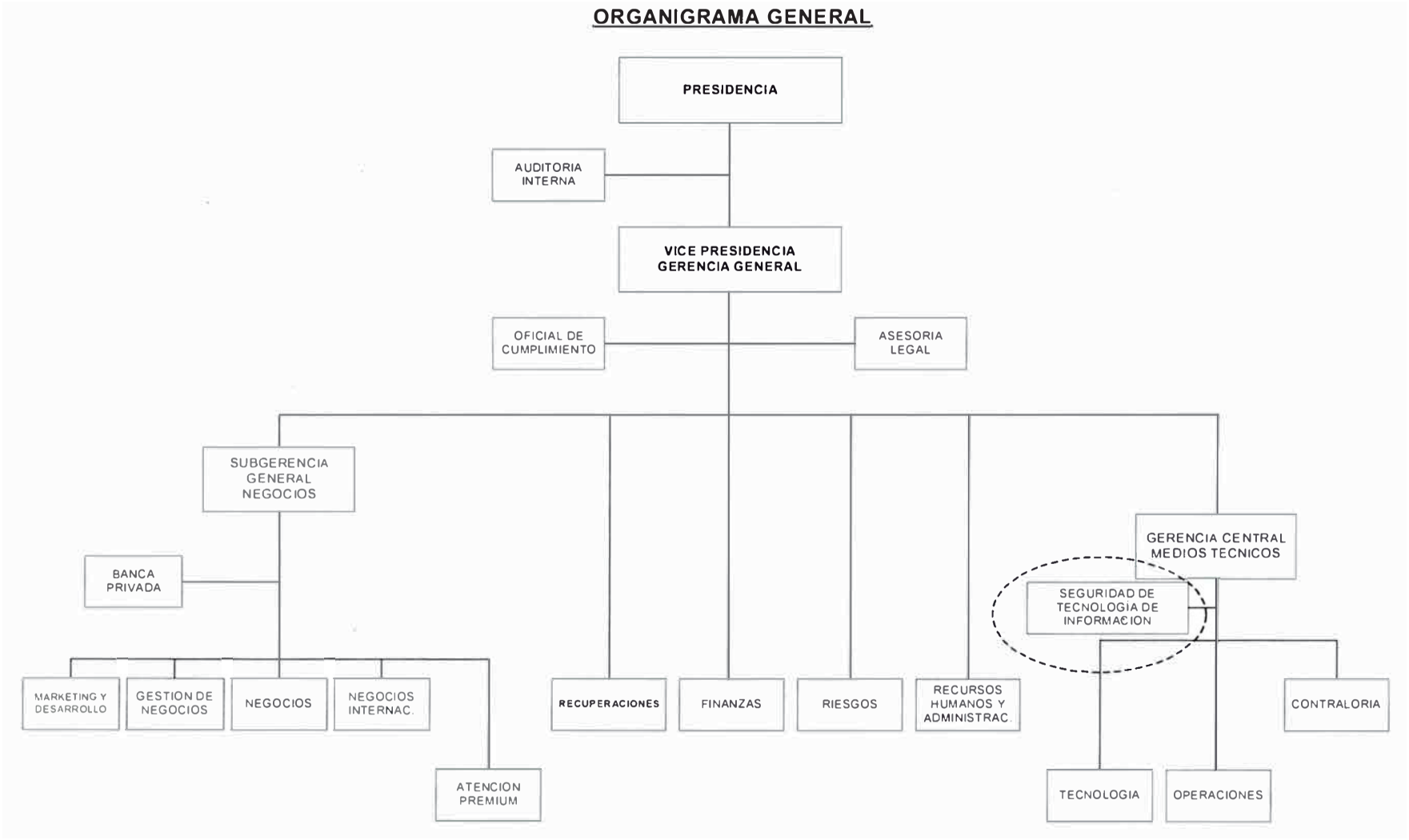
La comunicación y consulta involucra un diálogo en ambas direcciones entre los interesados, con el esfuerzo focalizado en la consulta más que un flujo de información en un sólo sentido del tomador de decisión hacia los interesados.

Es importante la comunicación efectiva interna y externa para asegurar que aquellos responsables por implementar la administración de riesgos, y aquellos con intereses creados comprenden la base sobre la cual se toman las decisiones y por qué se requieren ciertas acciones en particular.

Las percepciones de los riesgos pueden variar debido a diferencias en los supuestos, conceptos, las necesidades, aspectos y preocupaciones de los interesados, según se relacionen con el riesgo o los aspectos bajo discusión. Los interesados probablemente harán juicios de aceptabilidad de los riesgos basados en su percepción de los mismos.

Dado que los interesados pueden tener un impacto significativo en las decisiones tomadas, es importante que sus percepciones de los riesgos, así como, sus percepciones de los beneficios, sean identificadas y documentadas y las razones subyacentes para las mismas comprendidas y tenidas en cuenta.

ANEXO 6


ORGANIGRAMA GENERAL
PRESIDENCIA
AUDITORIA INTERNA
VICE PRESIDENCIA GERENCIA GENERAL
OFICIAL DE CUMPLIMIENTO
ASESORIA LEGAL
SUBGERENCIA GENERAL NEGOCIOS
BANCA PRIVADA
MARKETING Y DESARROLLO
GESTION DE NEGOCIOS
NEGOCIOS
NEGOCIOS INTERNAC.
ATENCION PREMIUM
RECUPERACIONES
FINANZAS
RIESGOS
RECURSOS HUMANOS Y ADMINISTRAC.
GERENCIA CENTRAL MEDIOS TECNICOS
SEGURIDAD DE TECNOLOGIA DE INFORMACION
CONTRALORIA
TECNOLOGIA
OPERACIONES

ANEXO 7

FUNCIONES DISEÑADAS PARA EL JEFE DE UNIDAD DE SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN DEL BANCO

FUNCIONES PRINCIPALES

Administrar en el Banco los riesgos de tecnología de información y la seguridad de la información según los lineamientos aprobados por la Alta Dirección.

FUNCIONES ESPECIFICAS

1. Evaluar y proponer políticas y procedimientos necesarios para la administración adecuada y prudente de los riesgos asociados a la tecnología de información.

2. Establecer y mantener un sistema de administración que asegure la confidencialidad, integridad, exactitud y disciplina de la información del Banco, en niveles concordantes con la importancia que revista para el desarrollo de su misión, y el cumplimiento de la legislación y normatividad vigente.

3. Identificar los riesgos a que pueda estar expuesta la información, ya sea durante su almacenamiento, manipulación o comunicación, y recomendar los controles más adecuados, para eliminarlos o reducir sus efectos.

4. Evaluar periódicamente si han aparecido nuevos riesgos asociados a la tecnología de información y plantear los controles pertinentes.

5. Evaluar periódicamente en las diferentes unidades del Dpto. Central de Tecnología la aplicación y efectividad de los procedimientos y controles de sus procesos críticos, proponiendo al Comité de Riesgo Operativo su ajuste o adecuación, según se determine su necesidad.

6. Establecer, normar y actualizar los criterios bajo los cuales se identificarán y clasificarán a los usuarios de la información y a la información en sí, y supervisar su aplicación evaluando y ajustando si fuera pertinente las clasificaciones asignadas.

7. Definir y administrar, en coordinación con la Departamento de Organización y Métodos y otras unidades si fuera necesario, los perfiles

de acceso a la información propia de cada puesto de trabajo, según la sensibilidad de la información y las funciones y nivel propios del puesto.

8. Monitorear y rastrear la actividad de los usuarios a fin de detectar y corregir desviaciones en el uso correcto de la información, o en el cumplimiento de las normas y procedimientos asociados a la seguridad de la información; solicitando de ser pertinente la aplicación de las sanciones a que hubiera lugar.

9. Evaluar periódicamente, en las diferentes unidades organizativas del Banco, la aplicación y efectividad de los procedimientos y controles, tantos físicos como lógicos, relacionados con la seguridad de información, proponiendo su ajuste, adecuación o implantación según se determinara necesario.

10. Controlar por la oportunidad, calidad y confidencialidad en que se proporciona la información a las diferentes unidades organizativas del Banco.

11. Definir los controles lógicos y físicos de seguridad necesarios para que sólo el personal autorizado pueda acceder a la información, dentro de niveles de atención que no entorpezcan la operativa del Banco; y elaborar los procedimientos normativos para el control de los accesos a los recursos.

12. Controlar para que el acceso, modificación, divulgación, destrucción o mantenimiento de la información solo se efectúe mediante procedimientos operativos y programas computarizados idóneos, probados y autorizados.

13. Supervisar que se conserven en medios magnéticos el registro de los accesos a la información por periodos que guarden relación con la necesidad de acceso a tales registros.

14. Definir estándares de seguridad que formen parte de las especificaciones básicas de las aplicaciones computarizadas que se desarrollen en el Banco.

15. Participar en el desarrollo de nuevos procedimientos ya sean operativos o computarizados, controlando que se consideren los aspectos relacionados con la seguridad de la información, y definiendo los niveles de acceso que corresponderá asignar a cada usuario de la información involucrada.

16. Evaluar las medidas de control incluidas en el software que se considere utilizar en el Banco, desarrollado internamente o por terceros, de manera que se garantice la coherencia entre los objetivos y las especificaciones de seguridad que se haya considerado en el diseño.

17. Supervisar que los elementos de manejo de información y colaterales (equipo, software, sistemas de comunicación, entre otros) que utilice el Banco, reúnan características que no debiliten la seguridad de la información, sino que más bien contribuya a ésta.

18. Participar activamente en el desarrollo del Plan de Continuidad del Negocio, y supervisar que mantenga vigencia y viabilidad mediante la evaluación de sus procedimientos de actualización y de los resultados de las revisiones, pruebas y simulacros que se programen en las diferentes unidades organizativas del Banco.

19. Establecer las políticas de respaldo de información en concordancia con las necesidades operativas del Banco, la legislación vigente, y las exigencias específicas del Plan de Continuidad del Negocio.

20. Evaluar la seguridad de los medios de almacenamiento de información del Banco, de los ambientes y locales en que éstos se conserven y de los procedimientos aplicados para su control y traslado.

21. Evaluar y seleccionar, en coordinación con el Dpto. Central de Tecnología herramientas para apoyar las funciones de la Unidad de Seguridad de Tecnología de la Información.

22. Establecer o evaluar las políticas para la destrucción de la información, especificando los medios a utilizar, procedimientos a aplicar y la oportunidad en que se ejecutará

23. Supervisar la adecuada administración y uso de los usuarios con atributos especiales del sistema principal

24. Controlar la administración (altas, bloqueos, modificaciones y bajas) de los accesos de los usuarios establecidos en el ambiente de producción de la Plataforma AS/400 y entorno de Redes.

25. Cumplir con las demás funciones inherentes a su cargo que le sean asignadas por su jefe inmediato superior.

ANEXO 8

DISEÑO DEL PLAN INTEGRAL DE SEGURIDAD DE INFORMACIÓN DEL BANCO

INDICE

EXTRACTO DEL PLAN DE SEGURIDAD DE INFORMACIÓN

1. GENERALIDADES

1.1. INTRODUCCIÓN

El presente documento es una propuesta inicial para el desarrollo del ***"Plan Integral de Seguridad de Información del BANCO****".*

Las políticas de seguridad de la información, que forman parte del plan, son estrategias frente a los riesgos que pueden atentar contra la confidencialidad, la integridad y la disponibilidad de los recursos informáticos; dichas estrategias fueron elaboradas en base a la identificación de los riesgos tanto internos como externos de toda la infraestructura informática del BANCO.

El presente documento presenta las políticas de seguridad de la información a ser tomadas en cuenta por el BANCO, siendo la base para el desarrollo de normas, procedimientos y controles, con el objetivo de tener las fuentes de información funcionando y atendiendo de una manera segura, lo que permitirá lograr la continuidad en los servicios informáticos de las unidades organizativas del Banco.

1.2. OBJETIVOS

Los objetivos de este documento son:

a. *Resumir las políticas, procedimientos y estándares relacionados con la seguridad de información, que deben cumplir todos los niveles de la administración del Banco, que intervienen en los diversos procesos de negocio del Banco.*
b. *Definir los procedimientos y estándares de seguridad de información para lograr un adecuado aseguramiento de la información en términos de confidencialidad, integridad y disponibilidad.*

1.3. ALCANCES

Para los propósitos de este documento, la seguridad está definida como la capacidad para proteger la integridad, disponibilidad y confidencialidad de la información, y para proteger los activos de tecnología de información. Ello incluye la seguridad de las instalaciones y servicios de TI, sistemas de aplicación, almacenamiento de datos, telecomunicaciones, aplicaciones relacionadas a Internet.

2. CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

CATEGORÍA DE ACTIVO	TIPO DE ACTIVO
I. Ambiente físico (infraestructura)	1. Cómputo
	2. Almacén de Cintas
II. Software	1. De Base
	2. Paquete
	3. De Aplicación
	4. Instaladores
III. Hardware	1. AS/400
	2. Servidores de red
	3. Workstations
	4. Dispositivos de almacenamiento
	5. Equipos de control fisico y ambiental
	6. Generadores de energía
	7. Cajeros automáticos y kioskos virtuales
	8. Dispositivos de backup
	9. Impresoras
	10. Equipos de comunicación
IV. Información de seguridad	1. Contraseñas AS/400
	2. Contraseñas servidores
V. Información de las Unidades Funcionales	1. En medio magnético
	2. En medio físico
VI. De soporte	1. Equipos de oficina
	2. Gabinetes
	3. Proyectores

3. OBJETIVOS DE CONTROL Y CONTROLES

3.1. OBJETIVOS DE CONTROL

En base a la identificación de los riesgos de seguridad de información, se han identificado los siguientes objetivos de control:

CATEGORÍA / SUBCATEGORIA		OBJETIVOS DE CONTROL
1. Política de seguridad		
1.1.	Política de seguridad de información	O.1.1.
2. Organización de la seguridad		
2.1.	Infraestructura de seguridad de información	O.2.1.
2.2.	Seguridad de acceso a terceros	O.2.2.
3. Clasificación y control de Activos		
3.1.	Responsabilidad por los activos	O.3.1.
3.2.	Clasificación de la información	O.3.2.
4. Seguridad del Personal		
4.1.	Seguridad en la definición de trabajo y provisión de recursos	O.4.1.
4.2.	Capacitación del usuario	O.4.2.
4.3.	Respuesta en caso de incidentes y fallas de seguridad	O.4.3.
5. Seguridad física y ambiental		
5.1.	Área seguras	O.5.1.
5.2.	Seguridad de Equipo	O.5.2.
5.3.	Controles Generales	O.5.3.
6. Administración de Comunicaciones y Operaciones		
6.1.	Procedimientos y responsabilidades de la Operación	O.6.1.
6.2.	Planeamiento y aceptación del sistema	O.6.2.
6.3.	Protección contra software malicioso	O.6.3.
6.4.	Tareas de reorganización	O.6.4.
6.5.	Administración de Redes	O.6.5.
6.6.	Manejo y seguridad de los medios	O.6.6.
6.7.	Intercambio de información y software	O.6.7.
7. Control de acceso a los sistemas		
7.1.	Requerimientos de negocios para el acceso a los sistemas	O.7.1.
7.2.	Administración de acceso de los usuarios	O.7.2.
7.3.	Responsabilidades de los	O.7.3.

	usuarios	
7.4.	Control de acceso a la red	O.7.4.
7.5.	Control de acceso al computador central	O.7.5.
7.6.	Control de acceso a los sistemas aplicativos	O.7.6.
7.7.	Monitoreo de los accesos y uso del sistema	O.7.7.
7.8.	Computación Móvil y Telecomunicación	O.7.8.
8. Desarrollo y mantenimiento de sistemas		
8.1.	Requerimientos de seguridad de los sistemas	O.8.1.
8.2.	Seguridad en los sistemas de aplicación	O.8.2.
8.3.	Controles Criptográficos	O.8.3.
8.4.	Seguridad de los archivos de los sistemas de aplicación	O.8.4.
8.5.	Seguridad en los ambientes de desarrollo y soporte	O.8.5.
9. Gestión de contingencias y continuidad de negocios		
9.1.	Planeamiento de Continuidad de Negocios	O.9.1.
10. Cumplimiento normativo y de regulación		
10.1.	Cumplimiento de Requerimientos Legales	O.10.1.
10.2.	Revisiones de la política de seguridad y cumplimiento técnico	O.10.2.
10.3.	Consideraciones de auditoria de los sistemas	O.10.3.

4. POLÍTICAS GENERALES DE SEGURIDAD DE INFORMACIÓN

1. La información del Banco es un activo intangible vital que debe ser protegido y custodiado.
2. La información relacionada a nuestros clientes y sus operaciones debe tratarse respetando la privacidad de los mismos.
3. La información debe ser completa y exacta, y estar a disposición del personal operativo, clientes, u órganos de control internos o externos, en la oportunidad y modalidad requerida.
4. El Banco es propietario de toda la información que genera su personal dentro de la misma o representándola, y de la que se genere mediante la utilización de sus equipos de cómputo, telefonía, oficina u otros.
5. Los incidentes de seguridad de información deben ser adecuadamente registrados, reportados e investigados

ANEXO 9

METODOLOGÍA ADOPTADA PARA LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DE INFORMACIÓN

El proceso de administración de riesgos asociados a la seguridad de información, nos debe permitir, particularmente:

- *La identificación de los activos*
- *La estimación de los estados de la seguridad: confidencialidad, integridad y disponibilidad*
- *La interdependencia de los diversos activos para cumplir su misión*
- *La detección de las amenazas que puedan atacar a los activos*
- *Los factores que pueden incrementar la vulnerabilidad*
- *La magnitud que un impacto provoca sobre un activo al materializarse una amenaza*
- *El establecimiento de un umbral aceptable de riesgo para los activos*
- *La especificación de los mecanismos de reducción de riesgos ya implantados y las recomendadas y/o diseñadas.*

Esta metodología toma como base la Metodología de Administración de Riesgos de Operación, descrita en el Manual de Riesgos de Operación, habiéndose adaptado para ello, algunos conceptos y actividades para su aplicación a los riesgos de seguridad de información.

Consta de las siguientes etapas, cada una compuesta de un conjunto de actividades:

1.1. PLANIFICACIÓN DEL ANÁLISIS Y GESTIÓN DE RIESGOS

En esta etapa se establecen las consideraciones necesarias para iniciar el proyecto de evaluación de riesgos, investigando la oportunidad de realizarlo, definiendo los objetivos que ha de cumplir y el ámbito (alcance) que abarcará, planificando los recursos materiales y humanos para su realización; e iniciando el lanzamiento del proyecto de evaluación.

Consta de las siguientes actividades:

1.1.1. Definición del alcance y objetivos

- *Especificar los objetivos*
- *Definir el alcance y los límites*
- *Identificar el entorno y restricciones generales*

1.1.2. Organización y planificación

- *Evaluar cargas de trabajo y planificar entrevistas*
- *Planificar el trabajo*

1.1.3. Lanzamiento

- *Adaptar los cuestionarios para la recogida de datos y elaborar los formatos de matriz respectivas*
- *Asignar los recursos necesarios*
- *Sensibilizar (campaña informativa)*

1.2. ANÁLISIS DE RIESGOS

En esta etapa se identifican y valoran los diversos elementos que intervienen en el riesgo, obteniendo una evaluación de éste y estimando los umbrales de riesgo deseables.

Consta de las siguientes actividades:

1.2.1. Recogida de información

- *Preparar la información*
- *Realización de las entrevistas*
- *Analizar la información recogida*

1.2.2. Identificación y agrupación de ACTIVOS

- *Identificar activos*
- *Identificar mecanismos de reducción de riesgos existentes*
- *Valorar activos (de ser posible)*

1.2.3. Identificación y evaluación de AMENAZAS

- *Identificar y agrupar amenazas*
- *Evaluar amenazas*

1.2.4. Identificación y estimación de VULNERABILIDADES

- *Identificar vulnerabilidades*
- *Estimar vulnerabilidades*

1.2.5. Identificación y valoración de IMPACTOS

- *Identificar impactos*
- *Tipificar impactos*
- *Valorar impactos*

1.2.6. Evaluación del RIESGO

- *Evaluar el riesgo intrínseco*
- *Analizar las acciones reductoras de los riesgos existentes*
- *Evaluar el riesgo efectivo*

1.3. GESTIÓN DE RIESGOS

Se identifican las posibles acciones reductoras del riesgo detectado, se seleccionan las aceptables en función de las existentes y de las restricciones y se especifican los elegidos finalmente.

Consta de las siguientes actividades:

1.3.1. Interpretación del RIESGO

- Interpretar los riesgos

1.3.2. Identificación y estimación de las acciones reductoras de riesgo

- Identificar acciones reductoras de riesgo
- Estimar la efectividad de las acciones de reducción de riesgos

1.3.3. Selección de las acciones reductoras de riesgo

- Aplicar los parámetros de selección
- Evaluar el riesgo

1.3.4. Cumplimiento de objetivos

- Determinar el cumplimiento de los objetivos

1.4. SELECCIÓN DE MECANISMOS DE REDUCCIÓN DE RIESGOS (PROCEDIMIENTOS O DISPOSITIVOS MITIGADORES)

Se escogen los mecanismos de reducción de riesgos a implantar, se elabora una orientación del plan de implantación de los mecanismos de reducción de riesgos elegidos, se establecen los procedimientos de seguimiento para la implantación y se recopila la información necesaria para obtener los productos finales del proyecto de evaluación y realizar las presentaciones de resultados.

Consta de las siguientes actividades:

1.4.1. Identificación de mecanismos de reducción de riesgos

- Identificar mecanismos posibles que materialicen las acciones reductoras de riesgo elegidos
- Estudiar mecanismos implantados
- Incorporar restricciones

1.4.2. Selección de mecanismos de reducción de riesgos

- Identificar mecanismos a implantar
- Evaluar el riesgo de los mecanismos elegidos
- Seleccionar mecanismos a implantar

1.4.3. Especificación de los mecanismos a implantar

- Identificar mecanismos a implantar

1.4.4. Planificación de la implantación

- Priorizar mecanismos
- Evaluar los recursos necesarios
- Elaborar cronogramas tentativos

1.5. SEGUIMIENTO Y CONTROL

En esta etapa se efectúa el seguimiento y control o monitoreo de las acciones y/u objetivos de control sea que estén implantados o en proceso de implantación, a fin de informar de modo concreto y oportuno

sobre el grado de alcance y éxito de las acciones y controles diseñados así como el cumplimiento de los objetivos.

1.1.1. Evaluación de reportes de actividades y acciones de control
1.1.2. Elaboración de matriz de seguimiento y reporte de riesgos de Seguridad de información
1.1.3. Evaluación de resultados
1.1.4. Correcciones a las actividades y acciones de control

ANEXO 10

ESTRUCTURA DEL PLAN DE ACTIVIDADES PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE INFORMACIÓN DE ACUERDO A LAS POLÍTICAS ESTABLECIDAS (MATRIZ ACTIVIDADES POR CONTROL)

1. POLÍTICA DE SEGURIDAD

	CATEGORÍA	CONTROLES	PRIORIDAD A: ALTA M: MEDIA B: BAJA	ACTIVIDADES	ESTADO ACTIVID. S: EJECUTADO N: NO EJECUT P: EN PROCESO	FECHA ESTIM. INICIO IMPLEM	FECHA ESTIM. FIN IMPLEM
1.1	Política de Seguridad de Información						

2. ORGANIZACIÓN DE LA SEGURIDAD

	CATEGORÍA	CONTROLES	PRIORIDAD A: ALTA M: MEDIA B: BAJA	ACTIVIDADES	ESTADO ACTIVID. S: EJECUTADO N: NO EJECUT P: EN PROCESO	FECHA ESTIM. INICIO IMPLEM	FECHA ESTIM. FIN IMPLEM
2.1	Infraestructura de la seguridad de información						