UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS

ADMINISTRACION DE RIESGOS DE TECNOLOGIA DE INFORMACION EN UNA INSTITUCION FINANCIERA

INFORME DE SUFICIENCIA

PARA OPTAR EL TITULO DE INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

OSWALDO MANUEL COHAILA BRAVO

LIMA – PERU

2004

DEDICATORIA

A Dios, por tantas cosas buenas.

A Magdalena y Oswaldo, mis queridos padres por su dedicación, por su esperanza y por su entrega. Hoy les dedico el fruto de su esfuerzo, todo lo que soy se lo debo a ustedes.

A Fátima, porque su sonrisa y alegría son la energía que mueve toda mi vida.

A Rosario, por ser mi punto de apoyo, por su amor y su paciencia.

A mis hermanos, Ninoska y Jorge por ser mis mejores amigos, por su aliento y sus consejos.

A mi recordada mamá grande.

AGRADECIMIENTO

Quiero agradecer de manera especial al equipo de Riesgos del BN, y con mayor énfasis al grupo de RTI, por su apoyo y compañerismo.

Igualmente quiero agradecer a aquellas personas que a lo largo de mi experiencia profesional me han brindado su amistad, han compartido sus conocimientos y me han dado un consejo, especialmente a la gente de la SBS y el BNML.

ADMINISTRACION DE RIESGOS DE TECNOLOGIA DE INFORMACION EN UNA INSTITUCION FINANCIERA

INDICE

DESCRIPTORES TEMATICOS

- Riesgo
- Tecnología de Información
- Riesgo de Operación
- Seguridad de información
- Confidencialidad
- Disponibilidad
- Integridad
- Riesgo residual
- Gestión Integral de riesgos
- Continuidad de Negocio

ADMINISTRACION DE RIESGOS DE TECNOLOGIA DE INFORMACION EN UNA INSTITUCION FINANCIERA

RESUMEN EJECUTIVO

El Banco de la Nación es la institución del Estado Peruano que brinda servicios financieros al sector público y clientes en general. Sus actividades principales pasan por el rol social que cumple al satisfacer las necesidades de interconexión financiera en más de 250 provincias y distritos del país como única oferta bancaria, así como cumplir con los pagos al personal público activo y cesante del país.

El Banco, como integrante del sistema financiero nacional y, siendo necesario garantizar la adecuada administración de la información y la tecnología en que ésta se sustenta, las buenas prácticas aplicadas al sector tecnología de información a nivel nacional e internacional, las recomendaciones de empresas especializadas en consultoría de riesgos y adecuándose a las exigencias de la Circular Nº G-105-2002 de la Superintendencia de Banca y Seguros ha considerado necesario tomar las medidas para administrar apropiadamente los riesgos de tecnología de información.

La administración de Riesgos de tecnología de información es parte fundamental del tratamiento de Riesgos de Operación, tratamiento relativamente nuevo en nuestro país, por lo cual si bien es cierto no existe un estándar de adecuación en el sistema financiero nacional, se han puesto bases sólidas que garantizan la seguridad de los procesos, la información y la continuidad del negocio.

A ello, es necesario agregar que las disposiciones reguladoras en el país exigen la cuantificación de los riegos para implementar herramientas que

hagan posible cumplir con las provisiones operativas que se agregaran a las provisiones crediticias y financieras.

El modelo de administración de los Riesgos de Tecnología de Información y los resultados aquí presentados se ejecutará aplicando las siguientes etapas de desarrollo de procesos:

Etapa 1.- Estructura Organizacional y procedimiento de tratamiento de riesgos
Etapa 2.- Gestión de Riesgos de Tecnología de Información.
Etapa 3.- Tratamiento de Procesos críticos de Negocio

Este desarrollo nos permitirá alcanzar los siguientes resultados: Permitir la administración de los riesgos estructurales y coyunturales a los que está expuesto la institución, cumplimiento de la regulación vigente (Superintendencia de banca y Seguros); Implementar medidas de mitigación de los riesgos de tecnología de información; clasificar los procesos críticos de negocio y alcanzar resultados económicos, sociales y operativos.

INTRODUCCION

El presente trabajo, tiene como objetivo establecer los lineamientos generales para el adecuado tratamiento de los riesgos de tecnología de información en el Banco de la Nación. Estos lineamientos deben permitir establecer todos los mecanismos y acciones para cuantificar y calificar los niveles de riesgo a los cuales está expuesta la institución, esto permitirá garantizar la gestión de actividades para mitigar las posibles pérdidas que podría ocasionar la materialización de eventos clasificados como riesgo. Otro de los objetivos fundamentales es el referido al cumplimiento de los requerimientos reguladores.

La adecuada administración de riesgos, se origina en las actividades de evaluación de procesos, requerimientos legales, contractuales y reguladores, los principios propios de la actividad inherente al negocio de la empresa, los diversos incidentes ocurridos en la seguridad de activos tanto a nivel del entorno como a los activos de información y los sistemas y la percepción de fallas por parte de los involucrados en el proceso del negocio. Con una planificación integral, anticipada, efectiva, es posible responder rápida y apropiadamente cualquier tipo de riesgo que atente en contra de los sistemas de información dada las cambiantes condiciones y nuevas plataformas de computación disponibles.

La actual Administración del Banco afirma la necesidad de dar alta prioridad a la seguridad de las operaciones sociales del gobierno y de los respectivos activos que soportan estas operaciones. De esta manera, un adecuado

tratamiento de los riesgos operativos, surgen como una herramienta para concientizar a los miembros de una organización sobre la importancia y sensibilidad de los procesos, las personas, las actividades externas y la información y servicios críticos que permiten al Banco desarrollarse y mantenerse en su sector de negocios. Este proceso debe mantener el compromiso de todo el personal para con la organización.

La Administración de Riesgos de Tecnología de Información, ha sido delegada al Departamento de Riesgos, quien aplica una metodología de desarrollo de procesos que se resume en una etapa inicial de recopilación y evaluación de información; un proceso continuo de gestión de riesgos y el desarrollo de la estructura organizacional que da soporte a la Gestión de actividades enmarcadas dentro de la mejores prácticas exigidas por las normas internacionales y la regulación peruana.

Es necesario indicar sin embargo, que siendo el Banco de la Nación una entidad pública, existen factores que dificultan que la institución tenga una cultura de riesgos definida y asumida por todo el personal, factores como la resistencia al cambio por parte de empleados con un enfoque tradicional de trabajo, con más de veinte años de servicio o con la prestación de servicios bancarios distinto al de la banca comercial, hacen de este proceso un reto aun mayor que el asumido por el resto de empresas financieras.

DEFINICIONES

Para efectos del presente documento, se aplicarán las siguientes definiciones:

Ley General: Ley Nº 26702, Ley General del Sistema Financiero y del Sistemas de Seguros y Orgánica de la Superintendencia de Banca y Seguros.

Superintendencia: Superintendencia de Banca y Seguros.

Circular: Circular Nº G-105-2002 del 22 de febrero de 2002, dirigida por la Superintendencia y referida a riesgos de tecnología de información.

El Banco: Banco de la Nación

SIAF: Sistema Integrado de Administración Financiera.

CAPITULO I
ANTECEDENTES

1.1.- DIAGNOSTICO ESTRATEGICO

1.1.1.- HISTORIA

El 27 de enero de 1966, el Congreso de la República aprobó la Ley 16000 por la cual creaba el Banco de la Nación. Días después el Poder Ejecutivo, bajo la firma del Presidente de la República, Fernando Belaunde Terry la pone en vigencia, culminando así un largo proceso cuyos antecedentes históricos datan del siglo XIX, pero que recién a partir de 1914, surge verdaderamente la preocupación de crear un Banco que centralice las actividades operativas, económicas y financieras.

El Banco de la Nación encuentra sus antecedentes inmediatos en el año 1905, durante el gobierno de don José Pardo, en el que se crea la Caja de Depósitos y Consignaciones. Esta Institución amplió sus actividades en 1927 cuando se le encargó la administración del Estanco del Tabaco y Opio, así como la recaudación de las rentas del país, derechos e impuestos del alcohol, defensa nacional y otros. Finalmente, en diciembre del mismo año se le encarga la recaudación de la totalidad de las rentas de toda la República.

El Decreto Supremo N° 47, del 9 de agosto de 1963, estatiza la Caja de Depósitos y Consignaciones, declarándola de necesidad y utilidad pública. Mediante este dispositivo se recupera para el Estado las funciones de

recaudación de las rentas fiscales y la custodia de los depósitos administrativos y judiciales. Tal estatización se realizó cuando la Caja contaba entre sus accionistas con diez Bancos: Crédito, Popular, Internacional, Wiese, Comercial, Continental, Gibson, De Lima, Unión y Progreso.

Las facilidades financieras que otorga el Banco no están sujetas a los límites que establece la Ley General de Instituciones Bancarias, Financieras y de Seguros y las funciones principales que realiza el Banco de la Nación son:

- Recaudar las rentas del Gobierno Central y de la entidades del Sub-Sector Público independiente y de los Gobiernos Locales
- Recibir en forma exclusiva y excluyente depósitos de fondos del Gobierno Central y del Sub-Sector Público, con excepción de los Bancos Estatales.
- Hacer efectivas las órdenes de pago contra sus propios fondos que expidan las entidades del Sector Público Nacional.
- Recibir en consignación y custodia todos los depósitos administrativos y judiciales y efectuar el servicio de la deuda pública.
- Efectuar en forma exclusiva por cuenta y en representación del estado, operaciones de crédito activas y pasivas con Instituciones Financieras del país y del exterior y participar en las operaciones de comercio exterior del Estado.
- Otorgar facilidades financieras al Gobierno Central, y a los Gobiernos Regionales y Locales.
- Brindar Servicios de Corresponsalía.
- Brindar Servicios de Cuentas Corrientes a las Entidades del Sector Público Nacional y a Proveedores del Estado y otorgar Créditos al Sector Público.

1.1.2.- VISIÓN

Ser un Banco moderno y eficiente con capacidad innovadora, reconocido por la calidad en la atención a sus clientes, con personal proactivo y de altos valores éticos, que apoya sustancialmente a los Organismos del Estado en la descentralización y el desarrollo nacional.

1.1.3.- VALORES INSTITUCIONALES

El Banco, tiene como práctica constante el Respeto a la persona humana, la Gerencia permanente por resultados, la Honestidad y puntualidad, la Búsqueda constante de valor agregado, la Vocación de servicio y solidaridad en el trabajo, el Impulso al trabajo en equipo y el cumplimiento de compromiso.

1.1.4.- MISIÓN

Somos el Banco del Estado, que brinda servicios financieros eficientes al Sector Público y Clientes en general, preocupándonos en satisfacer las necesidades de interconexión financiera en distritos donde la banca privada no presta sus servicios, coadyuvando a profundizar el sistema financiero peruano y participando activamente en el desarrollo nacional.

1.1.5.- ANALISIS FODA

FORTALEZAS

1. La mayor Red de Oficinas en el Sistema Financiero Nacional, especialmente en distritos de provincias, con operaciones registradas al 100% en teleproceso.
2. Atención en 254 distritos donde somos única oferta bancaria.
3. Centralización de las cuentas y subcuentas del Tesoro Público (Sunat y Entidades Públicas).
4. Personal con amplia experiencia.

OPORTUNIDADES

1. La necesidad del Estado de incluir a todos los distritos del País en la economía nacional.
2. La demanda de los pueblos del país por más y mejores servicios bancarios.
3. interconexión con nuestro principal cliente en el Sistema Integrado de Administración Financiera (SIAF).
4. El desinterés de la banca privada, por llegar directamente a distritos pocos rentables del País.
5. La necesidad de la banca privada de contar con servicios de corresponsalía.
6. Aprovechamiento de medios electrónicos para cancelación de obligaciones que contraen las unidades ejecutoras.
7. Integrarnos al nuevo modelo de Gestión Pública e-Government, a fin de participar eficientemente dentro proyecto electrónico gubernamental.

DEBILIDADES

1. Limitación legal en los servicios bancarios ofrecidos.
2. Infraestructura, número de personal, procesos y sistemas de información inadecuados para los volúmenes de operación atendidos, que generan formación de largas colas en Agencias, presentando una imagen negativa.
3. Deficiencia de canales de comunicación en niveles jerárquicos.
4. Estructura de cargos y categorías deficientes y regímenes pensionarios dispersos.
5. Normatividad Legal y Administrativa que dificulta la decisión para la gestión de recursos humanos y materiales.
6. Perfil atareo y profesional inadecuado para algunos cargos y categorías, lo que reduce la calidad de los servicios que presta el banco.

AMENAZAS

1. Sector público autorizado a realizar servicios bancarios con la banca privada.
2. El no ser el principal agente financiero del Estado.
3. Reducciones presupuestales para el sector público y limitaciones en su ejecución.
4. Variación de la Política Gubernamental.
5. Búsqueda de plazas rentables por parte de la banca privada.
6. Medidas que delimiten las funciones del Banco a las estrictamente subsidiarias, sin competir con la banca privada en servicios que éstos podrían brindar (tesorería y pagaduría en plazas donde existe presencia de banca privada).
7. Ocurrencia de siniestros de carácter social por pertenecer al Estado.
8. Crisis financiera internacional.
9. Dispositivo legal de un poder del Estado, de equilibrar las pensiones de los trabajadores comprendidos en la Ley 20530, con los trabajadores activos.

1.1.6.- OBJETIVOS ESTRATÉGICOS

- Satisfacer la demanda de nuestros clientes, brindándoles servicios de calidad.
- Apoyar al Estado en el proceso de descentralización y desarrollo del país, abordando preferentemente las necesidades de interconexión de las comunidades sin acceso a servicios bancarios.
- Fortalecer en la cultura organizacional de la institución la creatividad, el cambio de actitud y valores, generando una organización con mayor valor.

1.1.7.- OBJETIVOS ESPECÍFICOS

- Participar activamente en el proyecto gobierno electrónico, para el pago de los derechos por los servicios y procedimientos de las entidades públicas.
- Innovar productos financieros que cumplan con un rol social.
- Mejorar los Servicios de Pagaduría, mediante adecuación de aplicativos de interconexión del Banco de la Nación con el SIAF del M.E.F.
- Optimizar el proceso de la administración del registro de operaciones en cajeros automáticos.
- Implementación de (9) agencias en Lima y (43) en provincias durante los años 2003-2005.
- Implementar un nuevo software de servicios bancarios, integrando todas las plataformas, que permita acercar el Banco a los clientes atendiéndolos a través de diversos canales.
- Automatización de los procesos de intermediación financiera de sus diversas operaciones con el exterior.
- Automatización de reportes de transacciones en efectivo, así como archivo virtual del mismo y calificación de clientes exceptuados.
- Mejorar y ampliar el sistema de información en la página web del Banco.
- Establecer una política de optimización de costos, identificar y mejorar los procesos críticos, con el fin de lograr eficiencia y control de los riesgos.
- Contar con una estructura organizacional flexible en el tiempo y alineada a la misión del Banco.
- Fomentar mayor identificación, compromiso efectivo y motivación para elevar la eficiencia y productividad del personal.
- Lograr una óptima imagen en la calidad de servicios mediante la aplicación de estándares de producción y presentación de agencias a nivel nacional.

- Obtener certificaciones de calidad ISO para el desarrollo de software y el procesamiento de datos.
- Implementar un sistema de flujo de trabajo a fin de propender a establecer la "oficina sin papeles".
- Proponer y promover la promulgación de una ley que defina claramente el rol y misión del Banco dentro de la nueva política de modernización estatal.
- Contar con la nueva Sede Principal del Banco debidamente implementada con tecnología moderna.
- Crear la Fundación Cultural del Banco

1.1.8.- ESTRATEGIAS

- Ampliar la red de oficinas y la presencia del Banco de la Nación a nivel nacional.
- Implantar 2 turnos en las agencias de mayor carga operativa, con la finalidad de mejorar la imagen y calidad de servicio.
- Innovar canales de distribución de servicios, acercándolos al cliente y ampliando la capacidad de atención, mejorando la calidad y costo de los servicios que el Banco de la Nación presta.
- Implementar un sistema de comunicaciones amplio y confiable a través de una conexión directa que permita integrarnos con los clientes.
- Mantener un soporte informático integrado y oportuno a las necesidades del cliente, basado en la aplicación de tecnologías de información de vanguardia.
- Aplicar mecanismos que conlleven a perfeccionar integralmente al personal, incrementar la productividad, mejorar la calidad de atención, logrando una organización competitiva, proactiva, moderna y eficiente

1.2.- DIAGNOSTICO FUNCIONAL

1.2.1.- ESTRUCTURA ORGANIZACIONAL

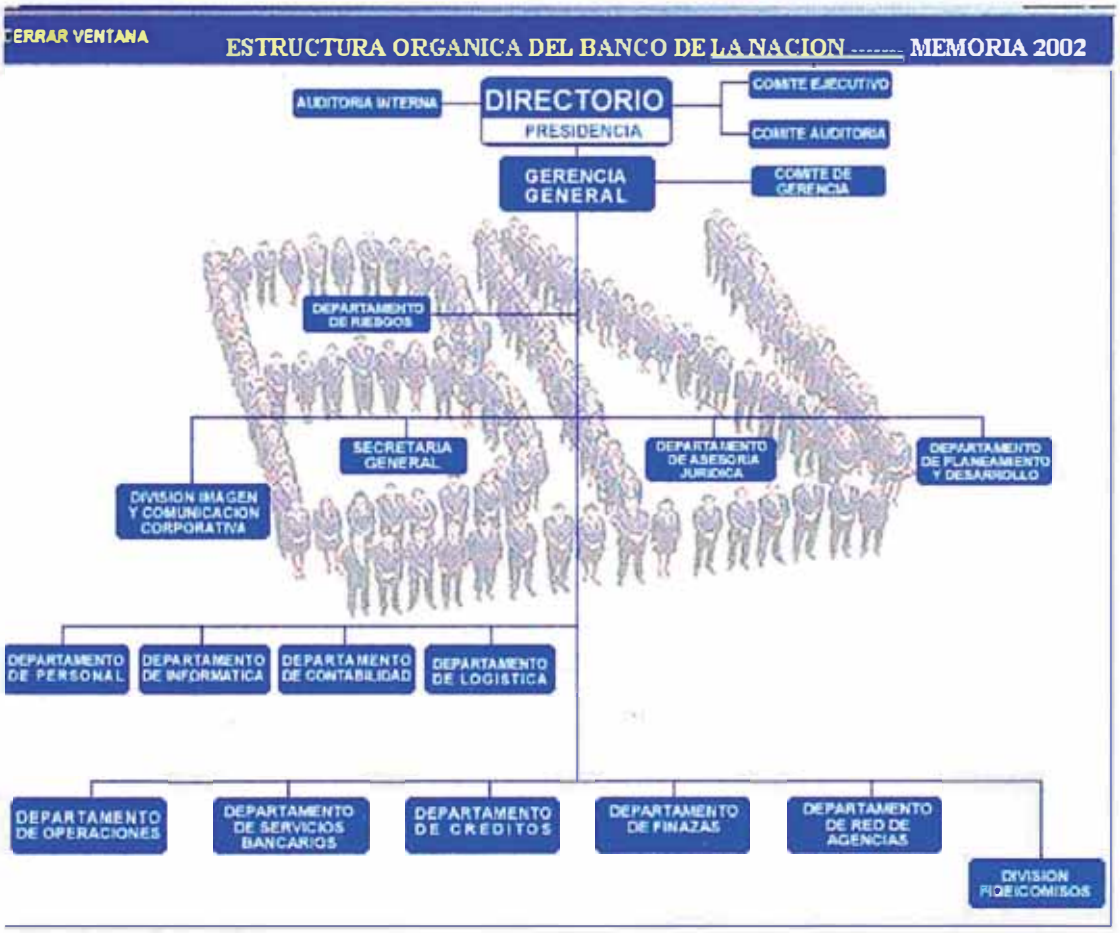


Figura 1: Estructura Organizacional del Banco de la Nación

1.2.2.- PRODUCTOS Y SERVICIOS

1.2.2.1.- MULTIRED

Es la red propia del Banco de la nación que permite realizar operaciones de consulta y retiro de dinero en efectivo, es la única red que brinda las denominaciones de 10, 20, 50 y 100 nuevos soles. El Banco brinda el servicio de pagaduría a trabajadores y pensionistas de entidades públicas con un único instrumento de cobro que es la tarjeta MULTIRED. El Banco de la Nación cuenta actualmente con una red de 220 cajeros automáticos distribuidos a nivel nacional 96 en Lima y 124 en Provincias, pudiendo

realizar operaciones los 7 días las 24 horas. Mediante la red multired, es posible realizar:

- Retiros de dinero diario hasta un máximo de S/. 1500
- Consulta de saldo y últimos movimientos
- Cambio de clave

1.2.2.2.- PRÉSTAMO MULTIRED

Es un servicio que brinda el Banco de la Nación a los trabajadores activos y pensionistas del Sector Público de menores ingresos que tienen cuenta de ahorros en el Banco con el propósito de mejorar su capacidad adquisitiva y nivel de vida, contribuyendo así al proceso de reactivación económica nacional.

1.2.2.3.- TELEGIROS:

Es un servicio mediante el cual se realizan transferencias de dinero a cualquier parte del país.

1.2.2.4.- CAJEROS MULTITASAS

El cajero de autoservicio Multitasas fácil de usar, que le permite pagar tributos y tasas a empresas públicas, aceptan monedas y billetes.

1.2.2.5.- RECAUDACIÓN

Es un sistema mediante el cual, el Banco recibe los depósitos por operaciones de las principales empresas recaudadoras, tales como: Sunat, Aduanas, Entidades públicas, Reniec, etc.

1.2.2.6.- CORRESPONSALÍA

El Banco actúa como Banco Corresponsal de las entidades del Sistema Financiero para atender la demanda insatisfecha de servicios bancarios en donde no existe oferta bancaria. Mediante la corresponsalía, se presta los siguientes servicios:

- Depósitos en Cuenta Corriente
- Pago de Cheques.
- Cobranza de Cupones.
- Depósitos especiales
- Cobranza de Facturas y letras
- Pago de Servicios.
- Telegiros.
- Pago de Planillas.
- Desembolso y Recuperación de Créditos.

1.2.2.7.- SERVICIOS DE CRÉDITO

El Banco de la Nación realiza Prestamos y sobregiros a gobiernos locales. Es otro de los servicios que el Banco de la Nación ofrece en apoyo a los gobiernos locales. Buscando favorecer la descentralización otorgando créditos a las municipalidades, con tasas de interés preferencial.

1.2.2.8.- SERVICIOS DE PAGADURÍA

El Banco de la Nación efectúa el servicio de pagaduría a los servidores y pensionistas de diversos organismos públicos en competencia con la Banca Comercial. Este servicio se realiza a través de cuentas corrientes y por cuentas de ahorros con tarjetas MULTIRED.

El pago a los proveedores y contratistas del Estado por concepto de bienes y servicios es realizado con cheques u órdenes de pago con cargo a las cuentas corrientes de las unidades ejecutoras.

1.2.2.9.- AGENTE FINANCIERO DEL ESTADO

El Banco, realiza las siguientes actividades como agente del Estado:

- Intervención del Banco de la Nación como agente financiero en los créditos y donaciones concertados por el Gobierno.

- Atención del Servicio de la Deuda Pública Externa de mediano y largo plazo por cuenta del Gobierno Central
- Atención del Servicio de la Deuda Interna

1.2.2.10.- TRANSFERENCIA A MUNICIPIOS

Este servicio se presta a todos los municipios a nivel nacional canalizando los recursos que le son asignados por el Fondo de Compensación Municipal y otros asignados por ley, Impuesto Promoción Municipal y Vaso de Leche. Para ello el Banco cuenta con un sistema a través de Teleproceso que permite su acreditación en forma simultánea.

1.2.2.11.- SERVICIOS BANCARIOS LOCALES

El Banco, presta los servicios de:

- Ahorros al sector público: pagaduría de remuneraciones y pensiones a trabajadores activos y pensionistas de las entidades públicas, que tienen convenio suscrito con el Banco.
- Ahorros sector privado en oficinas únicas ofertas bancarias: brinda el servicio de ahorros en moneda nacional a personas naturales en comunidades sin acceso a éstos.
- Cuentas corrientes: brindar servicios de cuentas corrientes referente a la apertura y cierre de cuentas, registro y actualización de firmas y venta de chequeras.

1.2.2.12.- SERVICIOS BANCARIOS INTERNACIONALES

- Remesas de cheques en cobranzas
- Transferencia de fondos al exterior
- Transferencia de fondos del exterior
- Créditos y cobranzas documentarias
- Fianzas bancarias

1.2.3.- CLIENTES

El principal cliente del Banco de la Nación es el estado peruano, esto incluye al sector público, destacando en su mayoría los trabajadores activos y cesantes de los diferentes regímenes tales como el personal del magisterio, ministerios, fuerzas armadas y policiales. Otro grupo importante de clientes es el conformado por las universidades públicas, la totalidad de gobiernos regionales y municipales, organismos reguladores y receptores de ingresos del estado, entre otros.

1.2.4.- PROVEEDORES

Los principales proveedores del Banco de la Nación son las siguientes empresas:

No.	No. R.U.C.	PROVEEDORES	PYME	IMPORTE
1	20100093759	SUL AMERICA COMPANIA DE SEGUROS SA.	-	10,242,228.78
2	20100017491	TELEFONICA DEL PERU S.A.A.	-	5,790,746.16
3	20100148162	CIA. DE SEGURIDAD PROSEGUR S.A.	-	5,513,229.82
4	20100101522	CIA. DE NEGOCIACIONES MOBILIARIAS E INMOBILIARIA	-	5,048,920.13
5	20100075009	IBM DEL PERU S.A.C.	-	3,451,099.42
6	20100077044	HERMES TRANSPORTES BLINDADOS S.A.	-	3,112,197.28
7	20100977380	TECNOLOGIA & GERENCIA DEL PERU SAC	-	1,848,095.04
8	20100128218	PETROLEOS DEL PERU S.A.	-	1,788,321.34
9	20423195119	GILAT TO HOME PERU S.A.	-	1,170,019.51
10	20101029442	INCOT S.A.C.	-	981,710.27
11	20100137985	OLIVETTI PERUANA S.A.	-	719,983.97
12	20100151384	SOFTWARE S.A.	-	705,540.05
13	20111035530	SERVICE Y MARKETING E.I.R.L.	-	617,492.87
14	20504629601	SAN MARTIN SOCIED. DE ING. & CONST.	-	584,854.48
15	20331898008	LUZ DEL SUR S.A.A.	-	462,853.00
16	20100128137	NCR DEL PERU S.A.	-	435,929.34
17	20332273532	B. Y F. POWER S.A.	-	415,899.02
18	20212149145	EFCO DEL PERU LTD., SUCURSAL	-	358,497.11
19	20101054986	SYSTEMS SUPPORT & SERVICES S.A.	-	347,793.64
20	20143229816	EMPRESA EDITORA EL COMERCIO	-	334,090.97

Figura 2: Principales Proveedores del Banco

1.2.5.- RIESGOS DE TECNOLOGIA DE INFORMACIÓN EN EL BANCO

1.2.5.1.- ÁMBITO

Para poder tener una primera visión de la importancia de la administración de riesgos de tecnología de información, es necesario considerar las siguientes características inherentes al Banco de la Nación:

EL ROL SOCIAL DEL BANCO DE LA NACIÓN.

El Banco administra los medios de pago de más de un millón de personas, éstas utilizan los medios que provee el Banco para el cobro de sus abonos mensuales.

OPERACIONES

Las distintas operaciones que realiza el Banco, tanto a nivel interno como las que realiza con las empresas del estado y las municipalidades; así como las operaciones externas como las que realiza el gobierno central con organismos internacionales, son parte fundamental de las operaciones del Banco.

1.2.5.2.- EL AMBIENTE EN EL PAÍS

Es necesario indicar que las formalidades de la administración de riesgos de operación y tecnología de información en nuestro país son relativamente nuevas. Aunque si bien es cierto, las instituciones financieras, aplican medidas de control, éstas no están firmemente desplegadas y puestas en ejecución.

La Superintendencia de Banca y Seguros (SBS), ha implementado un proceso de estandarización de procesos de control que las entidades del sistema financiero deben cumplir para adecuarse a los estándares internacionales y a las mejores prácticas con relación a la administración de estos riesgos.

La Superintendencia, emitió el año 2002, la Circular Nº G-105-2002 – Ver Anexo 1- la misma que estipula los puntos de partida que se debe considerar para la adecuada administración de los riesgos de tecnología de información y la elaboración de los respectivos documentos de apoyo el plan de seguridad de información y el plan de continuidad de negocio.

La SBS, enmarcada en la Ley General, recientemente ha incluido al Banco de la Nación en los procedimientos de adecuación a regulaciones de este tipo. En ese sentido, el Banco al igual que el resto de las instituciones financieras, están iniciando los proyectos relativos a la administración de riesgos de tecnología de información, ello conllevará a lograr un ambiente seguro en el negocio financiero.

CAPITULO II
MARCO TEORICO

2.1.- RIESGOS DE TECNOLOGIA DE INFORMACION

2.1.1.- RIESGO

Existe una gran variedad de definiciones o conceptos asociados a lo que es un riesgo, este se puede definir como:

- La proximidad o posibilidad de que ocurra un daño o peligro.
- Cada uno de los imprevistos y/o hechos desafortunados que puede cubrirse con un seguro.

Asimismo, al hablar de riesgos comúnmente relacionamos este concepto con las siguientes palabras: amenaza, emergencia, urgencia, apuro, etc.

Sin embargo, es necesario que podamos tratar de obtener, utilizando las anteriores ideas, un concepto formal y tal vez uno de los más usados y que involucra tanto los hechos como las pérdidas que éstos podrían originar se adecua al siguiente: Un Riesgo es aquel evento que genera incertidumbre o pérdida en términos económicos, sociales, profesionales o de imagen.

2.1.2.- CALIFICACION Y CUANTIFICACION DE UN RIESGO

Son también variadas las formas y métodos para medir un riesgo, se presume que según el tipo de riesgo en análisis, existen distintas maneras de medir el nivel de riesgo al que está expuesto el proceso o servicio en evaluación.

Al hablar de calificación, se puede considerar los objetivos del negocio, por ejemplo para los clientes de una entidad financiera, la calificación de riesgo para acceder a un crédito se mide en términos de clasificar al cliente a quien se otorga un préstamo (por ejemplo, normal, deficiente, potencial pérdida, etc.).

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 pueden ser ajustables para adaptarlas a las circunstancias que el análisis establezca. El análisis cualitativo se utiliza:

Como una actividad inicial de matiz, para identificar los riesgos que requieren de un análisis más detallado.

Cuando el nivel de riesgo no justifica el tiempo y esfuerzo requerido para un análisis más completo y

Cuando los datos numéricos son inadecuados para un análisis cuantitativo.

Al hablar de cuantificación, el objetivo es medir numéricamente la probabilidad de que un evento de riesgo se concrete, asimismo se mide el impacto que generaría en términos monetarios, de imagen institucional, social hacia la organización, etc. Es necesario asimismo tener en cuenta las medidas que la organización adopte para mitigar en cualquier forma la ocurrencia de algún evento de riesgo.

En este contexto, es factible relacionar los niveles de calificación con la cuantificación de un riesgo a ello se denomina análisis semi cuantitativo, por ejemplo un riesgo que tiene una probabilidad de ocurrencia de 40 en 100 casos y que genera una pérdida de 200 nuevos soles cada vez que ocurre podría considerarse como un Riesgo Alto. Considerando el mismo ejemplo y conociendo que la organización ha implementado un mecanismo de control que reduce las pérdidas de 200 a 15 nuevos soles, y una ocurrencia de 12

en 100 casos, el riesgo puede adoptar un nivel de Riesgo Medio. Este ejemplo muestra una de las maneras de tratar un riesgo y ese es uno de los retos de la Administración de Riesgos.

2.1.3.- CONCEPTO DE RIESGO DE TECNOLOGIA DE INFORMACION

La definición de los riesgos de tecnología de información, está sustentado en dos pilares fundamentales, el primero de ellos enlazado a los riesgos de operación y el segundo a las definiciones internacionales de riesgo en si.

En el primer pilar, los riesgos de tecnología de información son componentes de los riesgos de operación, entiéndase por riesgos de operación a la 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.

Esta primera definición, está sustentada en la declaración de Basilea II, la misma que propone diez principios para una adecuada administración de los riesgos de operación, estos principios incluyen la adecuada estructura organizacional, la participación de la alta gerencia, la sujeción a revisión de auditoría, la generación de políticas de mitigación de riesgos y un proceso de gestión de los riesgos.

En el segundo pilar, los riesgos de tecnología de información se definen además como aquellos asociados a actividades con soporte en recursos de tecnología de información, sistemas informáticos y tecnología inherente a estos sistemas, los mismos que afectan el desarrollo de las actividades del negocio contra los principios de integridad, confidencialidad y disponibilidad de la información.

Como todo componente de riesgo, los asociados a tecnología de información están inmersos dentro de aquellos eventos que generan incertidumbre o pérdida en términos económicos, sociales, profesionales o de imagen.

2.1.4.- GESTION INTEGRAL DE RIESGOS

Según el avance en las buenas prácticas para la administración de riesgos, éste se ha ido incrementando en el alcance de su evaluación. En primer lugar, el riesgo tradicional que evaluaban las empresas financieras, se basó en el riesgo de créditos. El 15 de Julio de 1988 el Comité de Basilea publica el ACB ó Basilea I, el cual establecía el acuerdo de convergencia que uniforma medir la adecuación del capital en los bancos para asegurar su solvencia. Este ACB sólo tenía en cuenta el riesgo de crédito y no hacía ninguna referencia al riesgo de mercado.

En Enero de 1996 se efectuó la enmienda al ACB88 que incorpora el Riesgo de Mercado con lo cual la gestión de riesgos adopta un esquema financiero, de créditos y de mercado.

Posteriormente, a finales de la década de los noventa, Basilea II introduce novedades en el Riesgo Crediticio y además por primera vez tiene en cuenta el Riesgo de Operación que incluye los Riesgos de tecnología de información, aspecto que cada día tiene más importancia en la operatoria de los Instituciones Financieras. A partir de esa fecha, se inicia el tratamiento integral de Riesgos y su administración da origen a la Gestión Integral de Riesgos.

La Gestión Integral de Riesgos, ha dado origen al tratamiento de los riesgos estratégicos, los riesgos legales y morales que las empresas deben considerar.

Figura 3: Nivel de Evolución de la Gestión Integral de Riesgos

2.2.- CONCEPTOS INMERSOS EN LOS RIESGOS DE TECNOLOGIA

2.2.1.- SEGURIDAD DE INFORMACION

No existe una definición estricta de lo que se entiende por seguridad de información, puesto que ésta abarca múltiples y muy diversas áreas relacionadas con los procesos, su entorno y los sistemas de información. Consideraciones que van desde la protección física de las aplicaciones como componentes hardware, de su entorno, hasta la protección de la información que estos sistemas contienen o de las redes que lo comunican con el exterior.

Son muy diversos los tipos de amenazas contra los que debemos protegernos. Desde amenazas físicas, como los cortes eléctricos, hasta errores no intencionados de los usuarios, pasando por los virus informáticos o el robo, el fraude interno, destrucción o modificación de la información.

No obstante, existen tres aspectos fundamentales que definen la seguridad de información: la confidencialidad, la integridad y la disponibilidad.
Sobre esta base, podemos definir a la seguridad de información como la adecuada interrelación de normas, procedimientos, cultura organizacional, mecanismos y recursos informáticos para garantizar los principios de confidencialidad, disponibilidad e integridad.

La seguridad de información, incluye en su análisis, un gran número de factores, por ejemplo, la British Estándar BS7799[1], establece 10 puntos clave en el control de la seguridad de información:

- Documento de Política de Seguridad de Información.
- Asignación de Responsabilidades de Seguridad.
- Capacitación y Difusión en Seguridad de Información.
- Reporte de Incidentes de Seguridad.

[1] BS 7799 : http://www.peopsoft.com/Servicio_Security.htm

- Controles Antivirus.
- Proceso de Planeación de Continuidad del Negocio.
- Control de copias Propietarias.
- Salvaguarda de los registros de la Empresa.
- Cumplimiento de la Legislación para la Protección de Datos.
- Cumplimiento de la Política de Seguridad.

2.2.2.- PLAN DE CONTINUIDAD DE NEGOCIOS

Un plan que direcciona la continuidad y el mantenimiento de todos los procesos del negocio requeridos para mantener un nivel aceptable de operación en el momento de ocurrencia de un evento de interrupción de los mismos y/o de los recursos que lo soportan.

Un plan de continuidad de negocios incluye los siguientes documentos como requerimiento mínimo de adecuación:

- Plan de Emergencias: Un mecanismo de respuesta centralizada que asegura la ejecución de las instrucciones y el control durante una interrupción operacional (Ej. Instrucciones y actividades manuales). Este plan incluye: identificación de incidentes, evaluación, escalamiento, declaración, plan de activación y desactivación inmediato y procedimientos iniciales de restauración.

- Plan de Contingencia: Un plan de ejecución y revisión constante que direcciona las acciones, personas, servicios y recursos informáticos o de comunicación disponibles para la atención de un evento de interrupción de los servicios con base en la evaluación de riesgos, disponibilidad de recursos y capacidad de respuesta.

- Plan de Recuperación: Un plan que direcciona la restauración de las aplicaciones de sistemas, software, datos e infraestructura de las mismas y procesos operativos del negocio (por ejemplo, hardware,

comunicaciones, redes, servicios bancarios, etc.) después que la contingencia o desastre ha ocurrido.

2.2.3.- ORÍGENES DE LA ADMINISTRACION DE LOS RIESGOS DE TECNOLOGIA

- Requerimientos legales, regulatorios, contractuales
- Acelerados avances tecnológicos
- Incidentes de seguridad (comunicaciones divulgadas)
- Preocupación de los usuarios
- Pérdidas económicas
- Crecimiento generalizado de procesos de negocio soportados en tecnología de información.

2.2.4.- INFORMACIÓN Y SISTEMA INFORMÁTICO

Entendemos por información el conjunto de datos que sirven para tomar una decisión. En consecuencia, su necesidad es evidente tanto en la planificación estratégica a largo plazo como en la fijación de estándares para la planificación a corto. La información también es necesaria para el estudio de las desviaciones y de los efectos de las acciones correctoras; es un componente vital para el Control.

En cuanto a su implantación, se puede hablar de:

• Subsistema formalizado: Normas, procedimientos e información de negocio.

• Subsistema no formalizado: Flujos de información que no pasan por el sistema de información formalizado (rumores, charlas informales, llamadas telefónicas, etc.).

El sistema informático es un subconjunto del subsistema formalizado, con distinto grado de cobertura. Por otra parte, se puede ver el sistema informático como el conjunto de los recursos técnicos (máquinas y utensilios), financieros (ingresos, gastos y patrimonio) y humanos (plantilla

de informáticos y personal auxiliar), cuyo objetivo consiste en el almacenamiento, procesamiento y transmisión de la información de la empresa.

Los aspectos clave en la seguridad de información, están asociados a dos niveles:

- Aspectos de Negocio (Procesos de negocio y Organización)
- Aspectos tecnológicos (soluciones e Infraestructura)

Adicionado a esto, los riesgos fundamentales asociados con la incorrecta protección de la información como la revelación a personas no autorizadas, la inexactitud de los datos. La dificultad en el acceso a la información cuando se necesita, el fraude interno y externo, el costo financiero y social como los más importantes. Estos aspectos se relacionan con las tres características que debe cubrir un sistema de información seguro: *confidencialidad, integridad y disponibilidad*.

2.2.5.- CONFIDENCIALIDAD

Se entiende por confidencialidad el servicio o condición, que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

En entornos de negocios, la confidencialidad asegura la protección en base a disposiciones legales o criterios estratégicos de información privada, tal como datos de las nóminas de los empleados, documentos internos sobre estrategias, nuevos productos o campañas, etc. Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son, por ejemplo:

• El uso de técnicas de control de acceso a los sistemas.
• El cifrado de la información confidencial o de las comunicaciones.

2.2.6.- INTEGRIDAD

Se entiende por integridad el servicio que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado. Esta modificación debe ser permisible a revisiones o controles de auditoria que permitan identificar a los responsables de su modificación.
Suelen integrarse varios conceptos análogos en este segundo aspecto de la seguridad:
• *Precisión accuracy,*
• *Integridad integrity,*
• *Autenticidad auntenticity.*

El concepto de integridad asimismo, significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado. De hecho el problema de la integridad no sólo se refiere a modificaciones *intencionadas*, sino también a *cambios accidentales* o no intencionados.

En el entorno financiero o bancario, este aspecto de la seguridad es el más importante. En los Bancos, cuando se realizan transferencias de fondos u otros tipos de transacciones, normalmente es más importante mantener la integridad y precisión de los datos que evitar que sean interceptados o conocidos.

2.2.7.- DISPONIBILIDAD

Se entiende por disponibilidad el grado en que la información está en el lugar, momento y forma en que es requerido por el usuario autorizado.

Asimismo en términos de Sistema de Información cuando se puede acceder a un SI en un periodo de tiempo considerado aceptable.

Un sistema seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo. Lógicamente, la información debe estar en los formatos adecuados para los usuarios al momento de encontrarse disponible para su uso.

Lo opuesto a disponibilidad, y uno de los posibles métodos de ataque a un sistema informático, se denomina "denegación de servicio" (*denial of service*). Una denegación de servicio significa que los usuarios no pueden obtener del sistema los recursos deseados.

2.2.8.- AMENAZAS A LA INFORMACIÓN

Una amenaza es cualquier elemento que afecta a los sistemas de información y a todo lo que involucra dicha información (procesos, eventos, etc.), el efecto de una amenaza es un daño, el mismo que no sólo incluye el efecto en si de la amenaza, sino también el hecho de no tomar acciones correctivas necesarias.

En la Figura 1, se puede encontrar un esquema de los diversos tipos de amenaza a la seguridad de información.

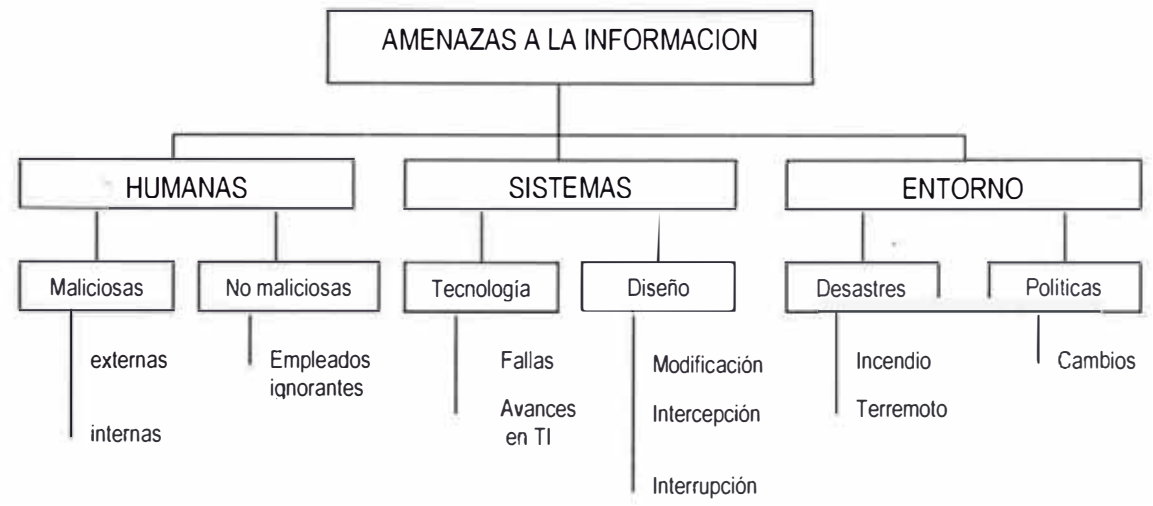


Figura 4: Amenazas a la Información

Una amenaza es también una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produzca una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). El análisis de riesgos identificará las amenazas que han de ser contrarrestadas.

Las cuatro categorías generales de amenazas o ataques son las siguientes:

- interrupción: Se produce cuando un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad.
- Interceptación: Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o una computadora.
- Modificación: Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad.
- Fabricación: Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad.

2.2.9.- ATAQUES PASIVOS

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o controla, para obtener información que está siendo transmitida. Sus objetivos son la interceptación de datos y el análisis de tráfico.

2.2.10.- ATAQUES ACTIVOS

Los ataques activos implican algún tipo de modificación del flujo de datos transmitido, o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

1.- Suplantación de Identidad: El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo.
2.- Repetición Indeterminada: Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
3.- Modificación de Mensajes: Una porción del mensaje legítimo es alterado, o los mensajes son retardados o reordenados, para producir un efecto no autorizado.
4.- Degradación fraudulenta del servicio: Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones.

2.2.11.- OTROS ASPECTOS RELACIONADOS

Existen otros aspectos considerados en el tratamiento de los riesgos de tecnología de información y que son especialmente importantes en el entorno bancario y en el uso del comercio digital, aunque pueden asimilarse a uno de los tres aspectos fundamentales, es necesario considerarlos con especial énfasis debido a su importancia en el negocio, entre ellos tenemos:

a) AUTENTICIDAD: Esta propiedad permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quién dice ser.

b) IMPOSIBILIDAD DE RECHAZO (no-repudio): Esta propiedad permite asegurar que cualquier entidad que envía o recibe información, no puede alegar ante terceros que no la envió o la recibió.

c) CONSISTENCIA: Asegurar que el sistema se comporta como se supone que debe hacerlo con los usuarios autorizados.

d) AISLAMIENTO: Regula el acceso al sistema, impidiendo que personas no autorizadas entren en él.

e) AUDITORÍA: Capacidad de determinar qué acciones o procesos se han llevado a cabo en el sistema, y quién y cuándo las han llevado a cabo.

f) RECUPERACIÓN: En caso de emergencia o pérdida de información, deben existir los mecanismos necesarios para recuperar la información.

g) CUSTODIA Y PROPIEDAD: Es necesario tener identificado a quien custodia la información y establecer solidamente las características de propiedad y depositario de la información.

CAPITULO III

TOMA DE DECISIONES

3.1.- PLANTEAMIENTO DE LA PROBLEMÁTICA

La administración y tratamiento de los riesgos de operación y por ende los riesgos de tecnología de información es un requerimiento oficial relativamente nuevo en nuestro país, si bien es cierto, en los sistemas informáticos y centros de cómputo de las diferentes empresas se han tomado medidas para prevenir la ocurrencia de eventos que puedan significar pérdidas de equipos, información o sistemas, estos procedimientos de control y resguardo, en la mayoría de casos se realizaban de manera convencional pues era natural resguardar los equipos y la información que éstos contenían. Cuando empiezan a aparecer las normas y procedimientos de mejores prácticas, las regulaciones y los estándares relacionados a riesgos de operación, es que el proceso de administración de riesgos adopta realmente la dimensión que tiene ahora.

En el siguiente esquema se puede visualizar las razones por las cuales es necesario realizar una adecuada administración de los riesgos de operación y de tecnología de información y el porqué se ha convertido en una práctica necesaria, obligatoria y competitiva para las empresas financieras del país.

Figura 5: Necesidad de Administrar los Riesgos de Tecnología de Información

Si bien es cierto, las instituciones financieras han mantenido niveles de mitigación de riesgo, no existía un enfoque general y estándar para el tratamiento de los mismos, por ello y a pesar de los esfuerzos del órgano regulador, las empresas han adoptado diversos mecanismos para el tratamiento de los riesgos de tecnología de información y en general para cualquier tipo de riesgo, sin embargo, existe documentación exigida por la superintendencia que posibilita en cierta medida hablar de un tratamiento uniforme de riesgos.

El Banco de la Nación, como integrante del sistema financiero nacional y eje fundamental de la economía social en el país, ha considerado implementar en su estructura orgánica y en su plan operativo, la administración de los riesgos de tecnología de información considerando la importancia y la necesidad de garantizar una adecuada administración de los activos de información que permiten la continuidad operativa del negocio.

Asimismo, considerando la necesidad de cumplir con las exigencias de la Circular relacionada a la adecuada implementación de políticas y procedimientos para administrar los riesgos de tecnología de información, el

Banco se somete a los requerimientos regulatorios con el claro objetivo de salvaguardar la información que administra sobre todo destinada a satisfacer la demanda social del país.

3.1.1.- COSTOS ASOCIADOS A EVENTOS DE RIESGO DE TECNOLOGIAS DE INFORMACION

a) COSTO ECONÓMICO

- Elevado costo por pérdida y recuperación de activos de información por ser la entidad con mayor número de operaciones en el país.
- Altos costos de adquisición de equipos tecnológicos, tales como los servidores principales, los servidores corporativos, servidores de banca electrónica, servidores de aplicativos en cajeros automáticos, etc.
- Pérdidas financieras asociadas a recursos del estado peruano
- Alto costo por servicios de recuperación de dispositivos físicos

b) COSTO OPERATIVO Y FINANCIERO:

- Pérdida de información o detención de actividades operativas
- Detención de procesos de recaudación (pérdidas de ingresos de comisiones).
- Problemas con las operaciones del Banco en cajeros, ventanillas, etc.
- Salida del negocio

c) COSTO SOCIAL

- Problemas con los pagos a servidores públicos (más de 1.200.000 personas)
- Elevado costo por efecto de las actividades públicas
- Actividades en contra de instituciones públicas gubernamentales
- Vandalismo, huelgas, atentados.
- Pérdida de reputación
- Suspensión de servicio al cliente

Esta problemática además considera los siguientes factores:

- Sanciones regulatorias
- Responsabilidades legales
- Riesgos y exposición a las amenazas internas y externas
- Preocupación de los usuarios considerando el mercado del Banco.
- Difusión de las comunicaciones

3.1.2.- NIVEL DE IMPACTO

a) EN EL AMBIENTE INTERNO

Las implicaciones con relación al personal, su seguridad y las actividades que realizan dentro de la institución se verían seriamente afectados, ya que la mayoría de los procesos de negocio hoy en día son soportados por aplicaciones tecnológicas.

b) EN EL AMBIENTE SOCIAL

Siendo una institución que brinda una gran cantidad de servicios sociales y con la importante posición en el sistema financiero, es necesario asegurar las operaciones con el público y con las empresas clientes del Banco, un problema crítico, sería dejar de prestar los servicios de pago a los trabajadores del sector público y los cesantes del estado. Asimismo, las operaciones y administración de fondos de las municipalidades y las operaciones con entidades externas.

Del mismo modo, la pérdida de confiabilidad, arrastraría una fuerte crisis en el sector financiero por corrida de depósitos, sobrecarga en las operaciones de la banca comercial en el caso de que ésta asuma operaciones del Banco, descrédito de la imagen del Banco y obviamente del estado peruano.

3.2.- ALTERNATIVAS DE SOLUCIÓN

El Banco, para adecuarse a las disposiciones de la Superintendencia, y en la búsqueda de alcanzar los niveles que estipulan las buenas prácticas, efectúo dos importantes acciones, formó la División de Riesgos, aunque sólo con la participación del Gerente de Riesgos y contrató los servicios de una consultora externa quien realizó un levantamiento de información sobre los riesgos de operación y de tecnología de información. A partir de allí y siendo necesario continuar con la administración de los riesgos, se consideró las siguientes alternativas para continuar el proceso de administración de riesgos:

OPCIÓN 1:
Terminar de conformar y equipar, tanto a nivel de recursos técnicos y humanos a la Gerencia de Riesgos y encargarle la administración y gestión de los riesgos de tecnología de información que actualmente afectan al Banco.

OPCIÓN 2:
Continuar con la labor de la consultoría externa especializada que realizó el levantamiento de información, la misma que propuso un plan de trabajo para los componentes de la administración de los riesgos de tecnología.

3.3.- METODOLOGÍA DE SOLUCIÓN

La solución que el Banco definió fue materia de discusión por parte de la Alta Dirección. Los criterios considerados para elegir la solución adecuada incluyeron los factores económicos, operativos y el más importante de todos fue el análisis corporativo relacionado con la administración directa de los riesgos en el Banco en el corto y mediano plazo.

3.3.1.- CRITERIOS ECONÓMICOS

Los principales criterios económicos a evaluar comprendían el costo – beneficio del proyecto en el corto y mediano plazo, donde están incluidas las dos alternativas de gestión de riesgos antes indicadas, las facultades que tenía el Banco en materia económica y los costos legales por el concurso público necesario en el caso de la opción de consultoría.

Adicionalmente, se ha incluido dentro de la evaluación económica los gastos y los beneficios aplicados a los principales recursos tecnológicos y las operaciones asociadas a los mismos.

En este sentido, como puede apreciarse en el cuadro Evaluación Costo-Beneficio (Ver Figura A), se muestran los gastos y los ahorros estimados de la gestión a un periodo de 3 años. Esta evaluación nos muestra un Valor Actual Neto de S/. 124.461.47 en un escenario muy conservador de beneficios y una TIR de 38% para la inversión.

3.3.2.- CRITERIOS OPERATIVOS

Con relación a la parte operativa, el Banco evaluó los siguientes factores:

a) PERSONAL A CARGO

En la opción de finalizar la conformación de la División de Riesgos, el personal sería personal especializado y con experiencia que el Banco contrate para esta función.

FIGURA A

FLUJO DE CAJA BASICO: ADMINISTRACION DE RIESGOS DE TI
Expresado en Nuevos Soles

RUBROS	AÑO 0	AÑO 1	AÑO 2	AÑO 3
Gastos de la Gestión				
Inversión inicial en equipos y muebles	-16,190.00	0.00	0.00	0.00
Otros gastos de inversión y mantenimiento	-2,000.00	-2,000.00	-2,000.00	-2,000.00
Gastos de Personal	-240,000.00	-240,000.00	-240,000.00	-240,000.00
Gastos logísticos	-10,965.00	-10,965.00	-10,965.00	-10,965.00
Otros gastos de Gestión	-7,500.00	-7,500.00	-7,500.00	-7,500.00
Capacitación y actualización	0.00	-25,000.00	-25,000.00	-25,000.00
Total Gastos de la Gestión	-276,655.00	-285,465.00	-285,465.00	-285,465.00
Beneficios del Proyecto				
Beneficios Tangibles				
Ahorro en capacitación interna (cultura de riesgos)	17,732.43	59,108.11	59,108.11	59,108.11
Ahorro por mitigación de riesgos en reclamos		10,928.33	10,928.33	10,928.33
Ahorro por diseño e implementación de Plan de Seguridad y Plan de Continuidad de Negocio		115,847.31	19,307.89	0.00
Ahorro por cumplimiento normativo (Estim 11 UIT)		35,200.00	35,200.00	35,200.00
Reducción de Contingencias en ATM's		10,527.29	10,527.29	10,527.29
Beneficios de Infraestructura tecnológica		8,007.69	8,007.69	8,007.69
Adecuación y formalización de procesos operativos		70,371.60	10,555.74	12,139.10
Reducción de riesgos de T.I. (procesos criticos)	36,840.00	122,800.00	122,800.00	122,800.00
Reducción de riesgos de T.I. (estimados por mitigaciónes en otros procesos)	5,526.00	30,700.00	38,375.00	47,968.75
Beneficios Intangibles (estimados)				
Incremento de valor de marca "Banco de la Nación"	10,000.00	15,000.00	15,000.00	15,000.00
Aseguramiento de niveles de continuidad operativa		18,000.00	21,000.00	24,000.00
Valor de difusión y adecuación de cultura de riesgos		10,000.00	11,000.00	12,000.00
Incremento de Imagen y aceptación institucional		12,000.00	15,000.00	18,000.00
Total Beneficios del Proyecto	70,098.43	518,490.33	376,810.04	375,679.27
Flujo de caja	-206,556.57	233,025.33	91,345.04	90,214.27
Factor de descuento (15%)	1	0.87	0.76	0.66
Flujo de caja Neto descontado	-206,556.57	202,630.72	69,069.97	59,317.34

VALOR ACTUAL NETO	124,461.47	RETORNO 13 MESES

TIR:	1	-206,556.57
	2	202,630.72
	3	69,069.97
	4	59,317.34
	TIR	38%

Nota:
El valor del factor de descuento, esta considerado sobre la base de cifras de proyectos en el país, basados en: Riesgo País, Riesgo político, tasa forward de descuento en tipo de cambio y tasa de interes, valor de la moneda en el tiempo, devaluación de la moneda nacional. En nuestro país cualquier proyecto lleva consigo una tas de descuento aproximadamente superior al 15%.

FIGURA A1: GASTOS DE LA GESTION
(Expresado en Nuevos Soles)

INVERSION EN EQUIPOS Y MUEBLES ENSERES

Nº	Descripción	Cantidad	PU	Total
1	Pc Pentium IV Compaq 2.0 GHz , DD 40Gb, Monitor 14" Compaq, CD-R	3	3,132.00	9,396.00
2	Pc Pentium IV Compaq 2.4 GHz , DD 60 GB, Monitor 17" Compaq, CD-R	1	3,654.00	3,654.00
3	Escritorios de madera 3 divisiones	4	350.00	1,400.00
4	Sillas giratorias de metal	4	60.00	240.00
5	Otros Muebles y enseres	-	1,500.00	1,500.00

Total gasto	16,190.00

INVERSION EN RECURSOS HUMANOS

Nº	Descripción	Cantidad	PU	Total
1	Sub Gerente de RTI	1	8,500.00	8,500.00
2	Analista de Riesgos de TI	2	5,500.00	11,000.00
3	Practicante de Riesgos de TI	1	500.00	500.00

Total Mensual	20,000.00
Total Anual	240,000.00

Nota: Los ingresos estan incluyendo Impuestos, Aportaciones Sociales

INVERSION EN RECURSOS LOGISTICOS

Nº	Descripción	Cantidad	PU	Total
1	Papeles para impresión (millares)	3	11.00	33.00
2	Impresoras y suministros de impresión	3	243.60	730.80
3	Fax, telefono, otros recursos de comunicación		150.00	150.00

Total Mensual	913.80
Total Anual	10,965.60

Tip. Cam.	3.48

FIGURA A2

PROGRAMA DE CAPACITACION INTERNA BANCO DE LA NACION

Costos de capacitación en el Mercado

	Moneda	Costo	Costo Hora
Seguridad de Información - Common Tech (15 horas - May 2003)	US$	120.00	8.00
Diplomado en Auditoria y Seguridad - Common Tech (120 horas) Ene 2004	US$	1,487.50	12.40
Curso Internac.Administración de Riesgos y seguridad (40 horas) ASIS Jun 2003	US$	1,071.00	26.78
Promedio en el Mercado de Cursos de Capacitación relacionados al Tema	US$		15.72
	T.C.		3.48
	SOLES		54.72

Costos por capacitacion Dentro del Banco (*)
(Expresado en Nuevos Soles)

(*) Capacitación de 24 horas académicas dentro de la Institución
(3 días de capacitación)
Realizado en 6 ciudades y con un total de 186 personas

	PU	CANT	TOTAL
Gastos por Viaticos terrestres (personal asistente)	360.00	175	63,000.00
Gastos por Viaticos aereos (personal asistente)	865.20	11	9,517.20
Gastos por Viaticos terrestres (personal capacitador interno)	360.00	1	360.00
Gastos por Viaticos aereos (personal capacitador interno)	865.20	5	4,326.00
Otros Gastos de Capacitación			10,000.00

Total		87,203.20
Promedio persona		468.83
Promedio pers/hora		19.53

Cálculo de Ahorro por capacitación interna
(Expresado en Nuevos Soles)

(*) Curso de 24 horas para 70 personas

	Costo/hora		costo total
COSTO EN EL MERCADO	54.72		91,926.52
COSTO CAPACITACION EN EL BANCO	19.53		32,818.41

AHORRO NETO	59,108.11

Se Estima Realizar 1 capacitación cada año
excepto el primer año donde se estima un ahorro inicial de 30% del total

FIGURA A3

ESTIMACIONES DE AHORRO POR MITIGACION EN RECLAMOS BN
(Expresado en Nuevos Soles)

SITUACION ACTUAL DE RECLAMOS EN EL BANCO A FAVOR DEL CLIENTE - 2003

	Cantidad	Monto Perdida promedio	Total
Bloqueo de Cuenta - Ahorros	7	23.45	164.15
Dinero falso - Ahorros	1	120.00	120.00
Dinero retenido - Ahorros	24	435.68	10,456.32
Pago comisión reposición de tarjeta - Ahorros	1	345.00	345.00
Pago de menos - Ahorros	1	460.00	460.00
Retiro no reconocido - Ahorros	9	135.20	1,216.80
Transposicion de cuenta - Ahorros	1	170.00	170.00
Dinero falso en ventanillas	11	260.45	2,864.95
Cobro indebido de intereses	2	11.60	23.20
Dinero falso en giros y transferencias	3	1,430.00	4,290.00
Dinero retenido en giros y transferencias	1	340.00	340.00
Retiro no reconocido en giros y transferencias	1	700.00	700.00
Caida del Sistema - Multired	24	289.70	6,952.80
Cobro Tarifario - Multired	4	11.56	46.24
Dinero falso - Multired	150	190.00	28,500.00
Dinero retenido - Multired	861	56.00	48,216.00
entrega incompleta de efectivo	4	125.00	500.00
Operación no procesada	5	140.00	700.00
Pago comisión reposición de tarjeta	435	5.00	2,175.00
Pago de menos	2	132.00	264.00
Retiro no reconocido - Multired	276	36.40	10,046.40
Trato al cliente - Recaudacion	6	31.00	186.00
Otros reclamos	132	94.36	12,455.52
		TOTAL 2003	131,192.38
Porcentaje estimado de Ahorro por implementación de medidas de mitigación			8.33%
		Total Ahorro est.	10,928.33

Nota:
1.- Los ahorros se estiman a partir del año 1
2.- El porcentaje estimado de ahorro corresponde Aprox. al 20% de la meta operativa de reducción de pérdidas por reclamos para el año 2004

FIGURA A4

PLAN DE SEGURIDAD DE INFORMACION Y PLAN DE CONTINUIDAD DE NEGOCIO

ESTIMACION DE AHORRO POR EJECUCION DE PROYECTOS
(Expresado en Nuevos Soles)

Consultora Price Waterhouse Coopers

Trabajo a 10 meses (2 equipos de proyecto)		Total Dólares	Total
Personal y gastos de consultoría	US$	96,000.00	334,080.00
impuestos		18,240.00	63,475.20
gastos de licitación			10,600.00
gastos diversos			7,000.00

	TC. 3.48
Total	415,155.20

Desarrollo de proyectos por personal del BN

Trabajo a 14 meses			280,000.00

Nota: No se incluyen gastos logísticos porque en ambos casos sería el mismo

Ahorro Neto	135,155.20
Ahorro prorrata mensual	9,653.94
Ahorro Primer Año (12)	115,847.31
Ahorro segundo año (2)	19,307.89

FIGURA A5

CONTINGENCIAS EN ATM

ESTIMACION DE AHORRO POR REDUCCION DE CONTINGENCIAS EN ATM
(Expresado en Nuevos Soles)

Número de contingencias en ATM

	Total Cont.	Perdida promedio	Total Mens
Contingencias Mensual (Ene-Dic 2003) Promedio	14,042.00	0.75	10,531.50
Total Anualizado	168,504.00	0.75	126,378.00

Estimado a reducir en contingencias	8.33%
Neto Ahorro Anual	10,527.29

Incluye
bandeja llena
dinero
dispensador
lectora
fuera de linea
wincha
recibos
fuera de linea

Nota:
1.- Los ahorros se estiman a partir del año 1
2.- El porcentaje estimado de ahorro corresponde Aprox. al 20% de la meta operativa de reducción de pérdidas en ATM para el año 2004

FIGURA A6

INFRAESTRUCTURA TECNOLOGICA

ESTIMACION DE BENEFICIOS POR ADECUACION DE INFRAESTRUCTURA TECNOLOGICA
(Expresado en Nuevos Soles)

Gastos:

Licitación Internacional Fibra Optica entre Centro de Computo principal y de respaldo	1,500,000.00
Licitación Internacional de Adecuación a Franquicia Internacional VISA	1,200,000.00
Otros gastos de licitación	15,000.00
	2,715,000.00

Nota: Incluye infraestructura a adquirir, equipos, personal, Sw y Hw

Ingresos	Actual	Ingresos Op	Ingresos Act	% Increm Estim.	Beneficios
Estimación de ingresos por número de operaciones transaccionales en ventanilla	5,409,623	0.60	3,245,774	10%	324,577
Estimación de ingresos por número de operaciones recaudación	26,449,586	0.33	8,728,363	8%	698,269
Estimación de ingresos por número de operaciones en ATM	3,486,746	0.3	1,046,024	18%	188,284
Beneficios por ahorro en Emergencia (Redundancia) equipos tecnológicos (*)	0				1,600,000

TOTAL BENEFICIOS	2,811,131
NETO BENEFICIO	96,130.73
% Beneficio por Participación de Rieg	8.33%
Beneficio	8,007.69

Nota:
1.- Los ahorros se estiman a partir del año 1
2.- El porcentaje estimado de ahorro corresponde Aprox. al 20% de la meta operativa evaluada por los comités de las licitaciones públicas.

FIGURA A7

EVALUACION DE PROCESOS

ESTIMACION DE AHORRO POR FORMALIZACION DE PROCESOS
(Expresado en Nuevos Soles)

Consultora BDO (PROPUESTA) TC. 3.48

Trabajo a 4 meses (1 equipos de proyecto)		total en dólares	Total
Personal y gastos de consultoría	US$	43,000.00	149,640.00
impuestos		8,170.00	28,431.60
gastos de licitación			5,300.00
gastos diversos			7,000.00
		Total	190,371.60

Desarrollo de proyectos por personal del BN

Trabajo a 6 meses (Riesgos + P y D)			120,000.00

Nota: No se incluyen gastos logísticos porque en ambos casos sería el mismo

Ahorro Neto	70,371.60

Nota:
Los beneficios se estiman para el Año 1con el 100% del ahorro neto
Para el año 2, se estima un 15% del ahorro del año 1, considerando procesos más trabajados. Para el año 3, se estima un 15% del ahorro del año 1 más el ahorro del año 2

FIGURA A8

GESTION DE RIESGOS DE TI

ESTIMACION DE AHORROS EN RIESGOS DE TI
(expresado en Nuevos Soles)

Mitigación de riesgos en procesos críticos (Sobre eventos de riesgo ocurridos a la fecha)

Dependencia	Macroproceso	Subproceso en análisis	Mitigación de riesgos
Operaciones	Captaciones	Administración de transacciones	12,600.00
Servicios Banc.	Recaudación		15,000.00
Tesoreria	Caja y Bancos	Abastecimiento de agencias y medios electrónicos	18,500.00
Administración de TI	Administración de red inform.	Monitoreo y control de agencias y cajeros	11,800.00
Servicios Banc.	Administración de cuentas del Tesoro		3,300.00
Servicios Banc.	Corresponsalia		2,100.00
Operaciones	Captaciones	Canje	25,500.00
Operaciones	Operaciones con el Exterior	Operaciones moneda extranjera	11,200.00
Logística	Seguridad	seguridad	19,800.00
Administración de TI	Administración de red inform.	Mantenimiento de equipos de la red	3,000.00

TOTAL DE AHORRO ASOCIADO A ACTIVIDADES DE MITIGACION	122,800.00

NOTA: (los porcentajes de mitigación estan entre niveles estimados de 5 a 10% de la pérdida asociada al proceso critico)

Para el Año 0, se estima un nivel de beneficio de 30% del ahorro estimado
Para las aplicaciones de medidas de mitigación en otros procesos de negocio, se sigue el siguiente esquema:
año 0: 15% del ahorro en el año 0 de procesos críticos ocurridos en el Banco
año 1: 25% del ahorro en el año 1 de procesos críticos ocurridos en el Banco
año 2 y año 3: Incremento de 25% con respecto al año anterior

Ello haría que la dependencia entre los trabajadores y el Banco sería directa.

En la opción de contratar a una consultora, el personal era derivado por ésta, los tiempos y realización de operaciones quedaban a entera disponibilidad de la consultora.

b) INFORMACIÓN Y ACCESO A INFORMACIÓN:

En la primera opción, la información sería administrada por el nuevo personal del Banco, en la segunda opción la información sería administrada por una entidad exterior al Banco.

c) USO DE INFORMACIÓN RECOPILADA

En la primera opción, los nuevos empleados debían validar el Relevamiento de información realizado por la consultora, en la segunda opción, de ser el caso que la consultora fuera distinta a quien realizó este relevamiento, igualmente sería necesaria la validación de la información.

En el caso que la consultora ganadora de la licitación sea la misma que realizó el proceso de levantamiento de información, el uso de la información sería mejor aprovechado, ya que sería continuar con el proceso ya iniciado.

3.3.3.- ANÁLISIS CORPORATIVO

La Alta Dirección del Banco, con la creación de la División de Riesgos, ha iniciado con buen paso el proceso de difundir la cultura de riesgos en el Banco, para ello, y en vista de los requerimientos normativos y la necesidad de preservar los activos del Banco, sujetos al objetivo corporativo de hacer del Banco de la Nación una entidad reconocida por la calidad de sus servicios a la ciudadanía y a las empresas del estado, consideró los siguientes factores dentro de su evaluación corporativa:

a) IMAGEN DEL BANCO

En las dos opciones, se evaluó lo que significaba para el Banco delegar la realización de sus actividades que estaban bajo el esquema de visitas de la SBS a un tercero y que significaba asumirlas directamente.

b) GESTIÓN DE RIESGOS

La Gestión de Riesgos en el Banco, no sólo incluían los riesgos de tecnología de información, el Banco consideró igualmente que es necesario la adecuada gestión de los riesgos de operación y los riesgos crediticios y financieros, en este sentido, la primera opción representaba cubrir dichos tipos de riesgo, ya que la División de Riesgos estaría implementada sobre la base de los tres tipos de riesgo. En el caso de la segunda opción, ésta sólo incluía los servicios especializados a tecnología de información y específicamente a uno de los proyectos de ésta.

3.4.- TOMA DE DECISIONES

El Banco, después de evaluar los factores antes mencionados, llegó a las siguientes conclusiones:

- Si bien es cierto que los costos de la gestión son altos, éstos se compensan con el beneficio a mediano plazo ya que la administración general de los riesgos por parte del Banco permitía incluir mayor realización de actividades que están especificadas en los requerimientos de la SBS, entre ellos se encuentran el Plan de Continuidad de Negocio, el Plan de Administración de Riesgos Operativos, el Proyecto de Cumplimiento Normativo, el Plan de Gestión de Riesgos Crediticios y Financieros, las Políticas de Evaluación de Cartera, entre otros.
- Considerar la opción de contratar una consultora significaría un gasto para cada concepto por separado, ya que es necesario personal con

dedicación exclusiva para cada uno de los requerimientos antes mencionados.

- Podría existir discordancias entre las diversas evaluaciones de las consultoras, ya que por ley, el Banco está imposibilitado de entregar todas sus licitaciones a la misma empresa, en este caso a la misma consultora.
- Consideró como un reto la administración directa de los riesgos en el Banco en el corto y mediano plazo.
- Era más flexible el control del personal dedicado a las labores de la gestión de riesgo, y esto permitía orientar a solucionar problemas adicionales que se puedan presentar en el tiempo, entre estos problemas pueden estar los riesgos por nuevos servicios, operaciones y el análisis de oportunidad de dichos nuevos lanzamientos.
- El hecho de que la mayoría de entidades financieras están asumiendo directamente las acciones necesarias a implementar los requerimientos normativos, hacen del reto de asumir la Gestión de riesgos ser partícipe en la mejoría de la imagen de la institución.

3.5.- ESTRATEGIAS ADOPTADAS

3.5.1.- ESTRUCTURA ORGANIZACIONAL Y PROCEDIMIENTO DE TRATAMIENTO DE RIESGOS

En esta etapa, se ha definido de manera clara los lineamientos de la organización con respecto al tratamiento de los riesgos, así como conseguir el compromiso de participación de la Alta Gerencia y mostrar la importancia y la necesidad de una adecuada administración de los riesgos a nivel general.

a) DEFINICIÓN DE LA ESTRUCTURA ORGANIZACIONAL

Teniendo en cuenta lo estipulado en la normativa, donde se indica la necesidad por parte de las empresas de establecer e implementar las políticas y procedimientos necesarios para administrar de manera adecuada y prudente los riesgos de tecnología de información, incidiendo en los procesos críticos asociados a dicho riesgo, la Gerencia de Riesgos del Banco delega esta responsabilidad a la División de Riesgos de tecnología de Información.

La estructura Organizacional del Departamento de Riesgos y la descripción de funciones se puede apreciar en el Anexo 2 del presente informe.

b) DEFINICIÓN DE LA VISIÓN Y ESTRATEGIA ORGANIZACIONAL

VISIÓN

La administración de riesgos de tecnología de información, será reconocida como ente gestor de un ambiente seguro en el manejo de la tecnología y la información asociada a ella dentro del Banco, alcanzando adecuados niveles que garanticen la seguridad de información, la continuidad de negocio y la participación de toda la organización, contribuyendo con el desarrollo de mecanismos y servicios financieros seguros e innovadores que permitan mejorar la competitividad empresarial y la calidad en el servicio.

ESTRATEGIA ORGANIZACIONAL

La estrategia organizacional para la gestión y difusión de una cultura de riesgo, se sustenta en un proceso continuo de concientización que se inicia con la verificación de todos los sistemas, aplicaciones y procesos actuales. La elaboración y despliegue de las políticas, los procesos y arquitectura de seguridad con la participación de las diversas áreas involucradas en las operaciones y servicios que requieren de tecnología y finalmente, la estrategia general de riesgos que considera los sub planes de adecuación bajo un enfoque de gestión de riesgos orientado a la estrategia del Banco.

Figura 6: Estrategia Organizacional

c) CONCIENTIZACIÓN EN LA ALTA DIRECCIÓN

Debido a la importancia de la Administración de riesgos, y a las implicancias que tiene en la institución, como es la emisión de políticas, normas y procedimientos, entre otros; se hace necesario el respaldo de la Alta Dirección. Al respecto, la Gerencia General ha mostrado el total apoyo a la Gerencia de Riesgos y está participando activamente en la difusión de los

planes a las demás gerencias. Hay que resaltar la ubicación del Departamento de Riesgos como órgano de línea de la Gerencia General.

3.5.2.- GESTION DE RIESGOS DE TECNOLOGIA DE INFORMACION

La metodología a ser usada por la División de Riesgos de Tecnologías de Información, está basada en recomendaciones de reconocidas empresas de consultoría de riesgos[2], así como la recopilación de metodologías aplicadas por empresas financieras y la recolección de información de los estándares internacionales relacionados.

El equipo de Riesgos de Tecnología de Información del Banco de la Nación la ha denominado METODOLOGIA RMC "RISK MANAGEMENT AND CONTROL" basada en la revisión del negocio orientado a los procesos que la conforman.

Nuestra metodología incluye las siguientes fases:

1.- Diagnóstico Inicial de procesos críticos.

2.- Un proceso continúo de evaluación de vulnerabilidades y riesgos, diseño e implementación de medidas de mitigación y el control de los riesgos.

3.- Un proceso de capacitación y concientización como soporte a los dos anteriores

[2] Metodologías Aplicadas por Price Waterhouse Coopers, KPMG, VMC, Audisys, Oracle Perú.

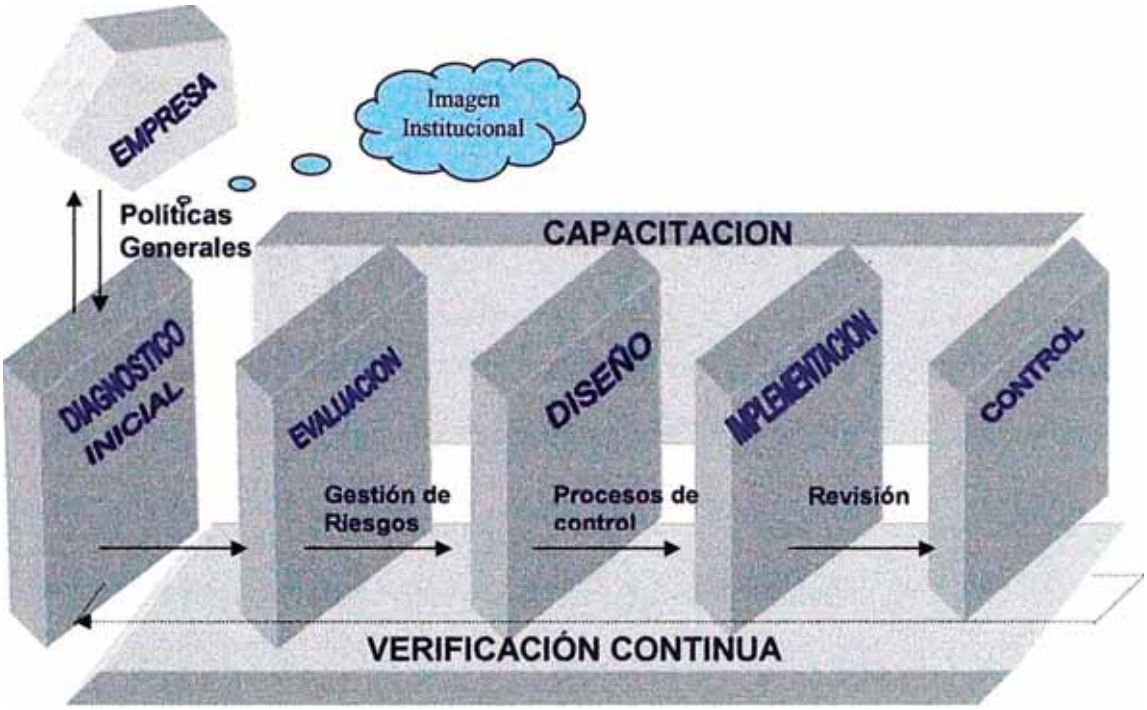


Figura 7: Esquema de la Metodología RMC

3.5.2.1.- DIAGNÓSTICO INICIAL DE PROCESOS CRÍTICOS

En está fase, se realizó un levantamiento total de información sobre los procesos del negocio, con énfasis especial en las áreas de TI y sobre la base del flujo de las políticas generales del Banco. Para ello, se utilizó un plantilla de Relevamiento de información para cada uno de los puntos críticos asociados con riesgos de tecnología de información y se consolidaron en un documento inicial de evaluación de la situación en la que el Banco se encontraba con relación a la Administración de los riesgos de tecnología de información. Los puntos críticos fueron:

- Servicios prestados por terceros
- Seguridad lógica
- Seguridad de personal
- Seguridad física
- Clasificación de seguridad
- Desarrollo de Sistemas
- Flujo de información interna y externa

- Procesos de respaldo
- Seguridad en operaciones y comunicaciones
- Eventos externos asociados a la operatividad y gestión del Banco.

El desarrollo de esta etapa nos ha permitido detectar cuales son los factores críticos hacia los cuales la Gerencia orientará un plan de tratamiento y control de riesgos. Para la recopilación de información, se han realizado entrevistas con personal de las siguientes dependencias:

- Departamento de Informática.
- Departamento de Logística – División de Seguridad.
- Departamento de Personal – División Administración de Personal.
- Departamento de Finanzas – División de Tesorería.

Asimismo, se han complementado con visitas a las siguientes oficinas e instalaciones físicas:

- Centro de Cómputo principal.
- Centro de Cómputo alterno.
- Central de grabación de circuito cerrado de TV.
- Central de monitoreo de circuito cerrado de TV.
- Oficinas de Personal, Logística, Finanzas, Informática.

Posteriormente, se ha enviado a las áreas involucradas una encuesta de autoevaluación conteniendo los mismos tópicos incluidos en el levantamiento de información con el objetivo de validar nuestra percepción y minimizar la sensibilidad a los resultados de la evaluación de información.

Los resultados del diagnóstico muestran de manera detallada y en resumen los puntos críticos considerados en relación con el nivel de control de los Riesgos de Tecnología a los que se encuentran expuestos. Este diagnóstico nos ha permitido determinar lo siguiente:

- El Banco, se encuentra en un nivel de Control Parcial de los Riesgos de Tecnología de Información. Alcanzando un nivel porcentual de control de 53,03%.
- La evaluación muestra la existencia de mecanismos de control que no están formalizados o actualizados y algunos se encuentran en desuso. Estos controles no son del total conocimiento de las partes o usuarios involucrados, existiendo posibilidad de materialización de los riesgos.
- Existen documentos y normas asociados, sin embargo están desactualizados o no se conocen.
- Por el lado de las actividades de control, éstas se encuentran con una tendencia a mejorar.
- Según la evaluación de Riesgos, los factores con mayor nivel de control, alcanzan un valor de 70% y 61% respectivamente.
- Según la evaluación de Riesgos, los factores con menor nivel de control y que requieren de medidas de mitigación inmediatas alcanzan 25% y 38% respectivamente.
- La autoevaluación realizada por los departamentos usuarios (antes de la publicación de los resultados obtenidos por riesgos) alcanza un nivel de 56,06% de control, valor que como se puede apreciar es ligeramente superior al evaluado por la división de riesgos. Esta variación es reducida por lo que se concluye que la evaluación de los puntos críticos realizada por el Departamento de Riesgos, es razonablemente aceptable.

3.5.2.2.- EVALUACIÓN DE VULNERABILIDADES Y RIESGOS, DISEÑO E IMPLEMENTACIÓN DE MEDIDAS DE MITIGACIÓN Y CONTROL DE RIESGOS

Este proceso está inmerso en un programa retroalimentado denominado VERIFICACION CONTINUA el mismo que enlaza los procesos anteriores utilizando herramientas de gestión de riesgo, procesos de emisión de reportes a la Alta Dirección y control a través de hojas de verificación y control.

Como herramientas de gestión de riesgo, se están usando usado:

- La matriz de evaluación de riesgos.
- La matriz de clasificación de nivel de control de riesgo.
- La matriz de riesgos residuales.
- Plantilla de Registro y Evaluación de Activos de Información.
- Plantilla de Evaluación de Riesgos.
- Plantilla de Registros de eventos de pérdida.
- Plantilla de alertas de riesgo histórico.

Estas herramientas permitirán apreciar tanto cualitativa como cuantitativamente el impacto del riesgo asociado a los procesos críticos de negocio, con lo cual se recomendarán las medidas correctivas y preventivas necesarias

En esta fase se ha realizado el análisis de los activos de información del Banco y el análisis de cada uno de los factores críticos.

A) CLASIFICACIÓN Y CONTROL DE ACTIVOS DE INFORMACIÓN

El objetivo de esta fase fue la recopilación y continua actualización de los activos de información, tanto a nivel del centro de cómputo, central de almacenamiento de dispositivos de respaldo y otras ubicaciones físicas y remotas.

Asimismo, se ha implementado niveles de clasificación, impacto y criticidad para los activos inventariados, lo que ha permitido documentar formalmente lo relativo a activos de información.

Para el proceso, se ha considerado el valor de medición de nivel de Impacto asociado a un valor que puede tener en la empresa la ocurrencia de un incidente que afecte al activo en evaluación. Dicho valor ha sido ponderado en una escala del 1 al 5; donde 1 se refiere al de menor impacto y 5 al máximo. Asimismo, para la Igualmente para la Clasificación de la información documentaria asociada a cada uno de los activos, se ha considerado los valores de USO INTERNO, CONFIDENCIAL, RESTRINGIDA, SIN RESTRICCIONES. Finalmente, para la clasificación de criticidad, se ha utilizado IMPRESCINDIBLE, ALTA, REEMPLAZABLE, NO CRÍTICO Y PRESCINDIBLE como niveles de medición.

Esta clasificación se realizó utilizando el inventario de activos existente en el Banco, la valorización de los activos considerando los factores de impacto, clasificación y criticidad fue realizada utilizando técnicas de Top-down (basado en la experiencia del personal que administra directamente el riesgo) en este caso, el trabajo fue directamente ejecutado con el personal experto del Departamento de Informática y la División de Seguridad del Banco, esta primera clasificación nos permitirá generar una base de datos de clasificación histórica que permitirá más adelante aplicar técnicas estadísticas para medir con menor sensibilidad a fallas la criticidad de activos de información.

En la Figura B, se muestra el resultado consolidado de los principales activos de información, la cual nos ha permitido administrar formalmente un esquema de criticidad y clasificación de activos.

FIGURA B

Plantilla 1	RTI	EVALUACION DE ACTIVOS DE INFORMACION

Proyecto	Gestión de Riesgos de Tecnología de Información
Etapa en desarrollo	Clasificación y Control de Activos de Información

Nombre	Tipo	Servicios que brinda (de comunicación, de B/D, transaccional, de seguridad, etc.)	Propietario / Responsable	Contrato de Mantenimiento (S/N)	Esquema de Respaldo (S/N)	Impacto	Clasificación	CRITICIDAD
Servidores Centrales	Tangible	transaccional	Informatica	S	S	5	Restringida	Imprescindible
Unidades de Almacenamiento	Tangible	Segundad	Informatica	S	S	3	Restringida	Alto
Unidades de comunicación	Tangible	comunicación	Informatica	S	S	3	Restringida	Imprescindible
Unidades de control terminales	Tangible	Seguridad	Banca elect.	S	S	3	Uso interno	Alto
Unidades de Impresión	Tangible		Informatica	S		2	Uso interno	No critico
ATM	Tangible	transaccional	Informatica - BE	S	S	5	Confidencial	Imprescindible
Equipos de aire acondicionado	Tangible	Segundad	Seguridad	S		4	Uso interno	Alto
Kioskos	Tangible	transaccional	Informatica	S	S	2	Confidencial	Alto
Servidores de sistema critico	Tangible	transaccional	Informatica	S	S	5	Restringida	Imprescindible
Sistema Operativo	Intangible	B/D	Informatica		S	5	Restringida	Imprescindible
Sistemas de Seguridad	Tangible	segundad	Seguridad	S		4	Uso interno	Imprescindible
Subsistemas	Intangible	transaccional	Informatica		S	4	Uso interno	No critico
Servicios de comunicación	Tangible	comunicación	Informatica	S	S	4	Uso interno	Alto
Servicios transaccionales	Intangible	transaccional	Informatica		N	4	Sin Restricciones	Reemplazable
Editor / Visualizador	Intangible		Informatica	S	N	3	Sin Restricciones	Reemplazable
Software de B.D.	Intangible	B/D	Informatica			3	Confidencial	Alto
Servicios de B.D.	Intangible	B/D	Informatica	S	S	4	Restringida	Alto
Servidores de red	Tangible	comunicación	Informatica	S	S	4	Restringida	Alto
Equipos diversos	Tangible		informatica		N	3	Sin Restricciones	No critico
Sistema de atención al público	Intangible	transaccional	Informatica		S	5	Uso interno	Alto
Software distribuido	Intangible	transaccional	Informatica		S	3	Uso interno	No critico
Equipos de comunicación LAN	Tangible	comunicación	Informatica	S	S	4	Restringida	Reemplazable
Equipos de comunicación WAN	Tangible	comunicación	Informatica	S	S	4	Restringida	Reemplazable
Servidores de dominio	Tangible	comunicación	Informatica	S	S	4	Restringida	Reemplazable
Servicio de B.D. administrativo	Tangible	B/D	Informatica		S	3	Restringida	Alto
Estaciones personales	Tangible	transaccional	Usuario	S	S	3	Confidencial	No critico
Datos de usuario final	Intangible		Usuario		N	2	Confidencial	No critico
Insumos internos	Tangible		Todas		N	2	Uso interno	No critico

B) IDENTIFICACIÓN Y EVALUACIÓN DE VULNERABILIDADES, RIESGOS Y MEDIDAS DE MITIGACIÓN

El procedimiento para la identificación y evaluación de riesgos y vulnerabilidades se ha realizado sobre la base de los puntos críticos asociados con tecnología y se ha desarrollado un proceso sistemático estructurado buscando abarcar la praxis de los usuarios finales y los responsables de los procesos críticos, los conceptos basados en la experiencia, un análisis de escenarios y un inventario inicial de riesgos asociados a la naturaleza implícita del proceso.

El análisis ha involucrado las fuentes de riesgo, sus consecuencias y un completo proceso que involucra la posibilidad de la ocurrencia del evento de riesgo asociada con el impacto hacia la institución y además considera los procedimientos actuales de control con orientación a incluir aquellas medidas de mitigación que puedan ser resultado de la evaluación de los riesgos.

Las medidas de control o mitigación de los riesgos evalúan todas aquellas actividades que permitan reducir el riesgo asociado a los factores de negocio, tales como controles preventivos, planes de contingencia, transferencia de impactos a seguros, y guardan correlación con la primera etapa de la metodología donde se recogieron las medidas de mitigación naturales al Banco.

Considerando que en el Banco, no existía a la fecha ninguna aplicación de registro de eventos de riesgo, se ha implementado un servicio de registro e identificación de eventos de riesgo, mediante el cual, las diversas áreas del Banco pueden ir incrementando la base de datos de riesgos de operación y de tecnología de información que se ha desarrollado considerando las bases de datos pre establecidas por la BBA Operacional Risk Database Association[3], el sistema de objetivos de control de COBIT y las normas ISO

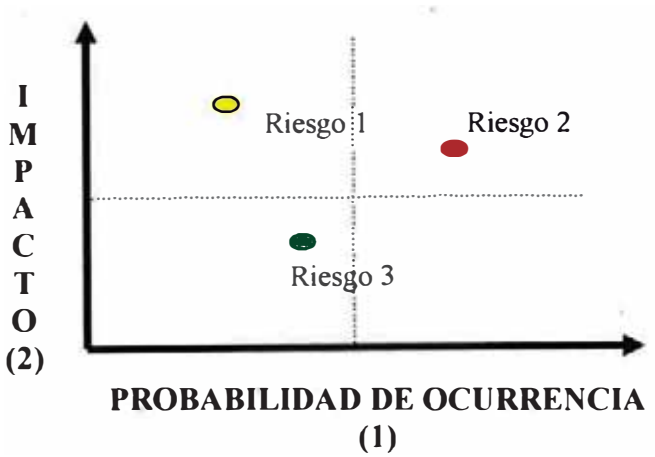
[3] British Bankers Association: Management and Supervi ion of Operational Risk http://www.bba.org.uk

17799. Los nuevos eventos de riesgo a registrar, están sustentados en la naturaleza del negocio particular y la experiencia de los responsables de los procesos y servicios en el Banco con quienes se tuvo reuniones de coordinación en las cuales se recopiló los demás eventos de riesgo componentes del registro de riesgos.

A continuación, se muestra las herramientas aplicadas y en las Figura C1 a C9 los resultados del proceso para cada uno de los puntos críticos evaluados.

MATRIZ DE EVALUACIÓN DE RIESGOS:

Es una matriz que refleja el nivel del riesgo asociado a un proceso de negocio, está basada en el impacto que generaría en el negocio la ocurrencia de amenazas u oportunidades y la probabilidad de ocurrencia de éstas.



El impacto será medido como la consecuencia de las amenazas y las oportunidades en los aspectos económicos, políticos, sociales y en los objetivos de la empresa. El impacto ha sido calificado en 5 niveles:

NIVEL DE IMPACTO	CALIFICACION	DESCRIPCION
BAJO	0	Impacto irrelevante, a nivel económico y operativo es poco significativo, a nivel social no se percibe.
MEDIO BAJO	1	El impacto es percibido a nivel interno, existen pérdidas operativas y económicas aceptables.
MEDIO	2	Impacto moderado en los niveles económico, operativo y de servicios
MEDIO ALTO	3	El impacto a nivel operativo es significativo, a nivel económico puede ocasionar pérdidas sustanciales, existencia de detención de procesos.
ALTO	4	El impacto en el negocio es totalmente negativo, la empresa puede finalizar sus operaciones, las acciones correctivas son irrelevantes, peligro total en la reputación y situación en el mercado.

La probabilidad es la medida de la posibilidad de ocurrencia de la amenaza u oportunidad. Esta ha sido calificada en 5 niveles:

PROBABILIDAD	CALIFICACION	DESCRIPCION Y CARACTERISTICAS
BAJO	0	Ocurrencia muy improbable, no se conocen casos asociados al negocio, periodos de tiempo largos de ocurrencia
MEDIO BAJO	1	Ocurrencia poco probable, se conocen casos aislados, los periodos de ocurrencia son en periodos largos.
MEDIO	2	Probabilidad de ocurrencia a nivel significativo, existe varios casos asociados, la ocurrencia se da en periodos ciclicos conocidos.
MEDIO ALTO	3	Los acontecimientos ocurren con frecuencia, conocimiento de casos
ALTO	4	La ocurrencia en este nivel es continua, existencia importante de factores externos asociados, existencia muy significativa de casos similares.

Por lo cual, el nivel de riesgo asociado se reflejará en aplicación de los dos componentes antes mencionados en la relación de importancia del 60% para el impacto y 40% para la probabilidad de ocurrencia, esto sustentado en la naturaleza social del Banco:

PROBABILIDAD

IMPACTO	BAJO	MEDIO BAJO	MEDIO	MEDIO ALTO	ALTO
BAJ0	BAJO	BAJO	MEDIO BAJO	MEDIO BAJO	MEDIO
MEDIO BAJO	BAJO	MEDIO BAJO	MEDIO BAJO	MEDIO	MEDIO
MEDIO	MEDIO BAJO	MEDIO	MEDIO	MEDIO	MEDIO ALTO
MEDIO ALTO	MEDIO	MEDIO	MEDIO ALTO	MEDIO ALTO	MEDIO ALTO
ALTO	MEDIO	MEDIO	MEDIO ALTO	ALTO	ALTO

Riesgo Asociado = P*0.4 + I*0.6

MATRIZ DE IDENTIFICACIÓN DE CONTROLES EXISTENTES:

Las medidas de control o mitigación de los riesgos evalúan todas aquellas actividades que permitan reducir el riesgo asociado a los factores de negocio, tales como controles preventivos, planes de contingencia, transferencia de impactos a seguros, etc.

NIVEL DE CONTROL	CARACTERISTICAS PRINCIPALES	OBSERVACIONES DOCUMENTARIAS	ESQUEMA GRÁFICO
0: No Controlado	No existe mecanismos formales o informales de control, no existen medidas de ningún tipo para el control de riesgos. No se reconocen los factores de riesgo asociados a los procesos. Es muy probable la materialización del riesgo	No existen documentos	 rojo
1: Nivel de Control bajo.	Existen indicios informales de control de riesgos, generalmente se llevan a cabo por costumbre, no cubre la totalidad de los grupos involucrados, está en proceso de formación. El riesgo se puede materializar.	Existen documentos asociados no relativos directamente al punto crítico	 naranja
2: Nivel de Control parcial	Existen mecanismos de control, éstos no están formalizados o están en desuso, asimismo éstos no son de conocimiento de los involucrados. Se están formando equipos de control. Existen posibilidades de la ocurrencia de las amenazas	Existen documentos y normas asociados, éstos están desactualizados o no se conocen	 amarillo
3.- Nivel de Control razonable	Existencia regular de mecanismos formales de control de riesgos, éstos se difunden a casi todos los usuarios involucrados, existen equipos encargados del control de riesgos.	Existen documentos publicados actualizados y formalizados, definición de roles y responsabilidades.	 verde
4.- Nivel de control óptimo	Se tiene participación total de los involucrados, distribución eficiente de documentos de sustento y mecanismos formales de control, monitoreo y seguimiento del nivel de control de riesgos. Muy poca posibilidad de materialización del riesgo.	Existen documentos formales, estándares, de seguimiento dual, con definición de roles, responsabilidades y certificados	 azul

MATRIZ DE RIESGO RESIDUAL

Es la medida del nivel de riesgo, que se realiza posteriormente a la ejecución de las actividades de mitigación de riesgos.

Matriz de Riesgos Residuales:

CONTROL DE RIESGOS

NIVEL RIESGO

	OPTIMO	RAZON.	PARCIAL	BAJO	SIN CON.
BAJO	BAJO	BAJO	BAJO	BAJO	BAJO
MEDIO BAJO	BAJO	BAJO	BAJO	MEDIO BAJO	MEDIO BAJO
MEDIO	BAJO	BAJO	MEDIO BAJO	MEDIO	MEDIO
MEDIO ALTO	BAJO	MEDIO BAJO	MEDIO BAJO	MEDIO	MEDIO ALTO
ALTO	BAJO	MEDIO BAJO	MEDIO	MEDIO ALTO	ALTO

Efectividad: Es el resultado de la evaluación de los riesgos del negocio teniendo en consideración las medidas de control y mitigación, ello permitirá las medidas a tomar por parte de las dependencias del Banco.

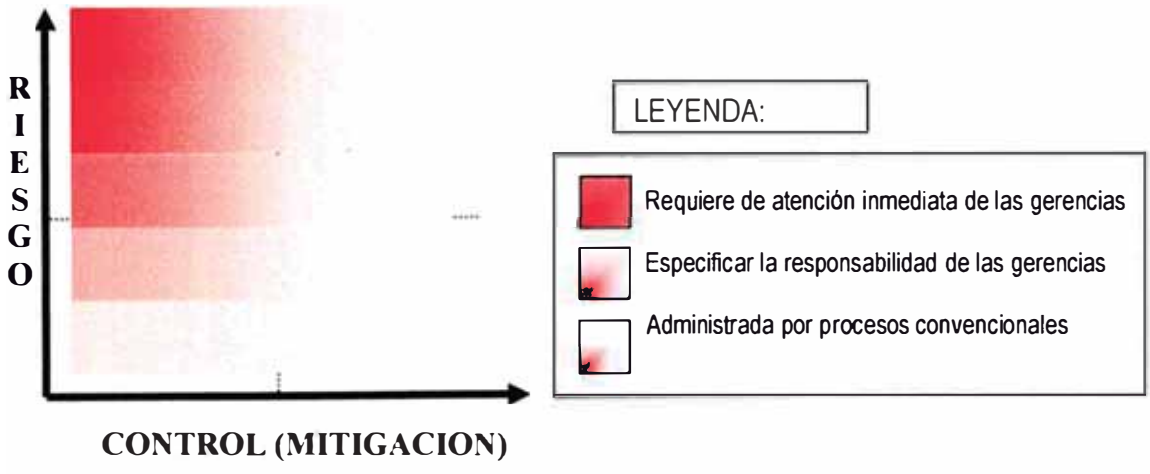


FIGURA C1

Plantilla 2	RTI	EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Critico / Proceso en Evaluación:	Desarrollo de Sistemas

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	DS001	Ausencia de requerimientos funcionales de validación de la información de entrada para generación o modificación de sistemas	2: Medio	3: Medio Alto	MEDIO ALTO	No se está validando ni realizando pruebas de validación de información de entrada, se utiliza información continua	0: No Controlado	MEDIO ALTO
002	DS002	Ausencia de planeamiento de sistemas de información	2: Medio	4: Alto	MEDIO ALTO	Se está desarrollando el PETI	2: Parcial	MEDIO BAJO
003	DS003	Ausencia o deficiencia de metodología de desarrollo de sistemas	1: Medio Bajo	3: Medio Alto	MEDIO	La metodología de desarrollo de sistemas está en proceso de formalización y despliegue	1: Bajo	MEDIO
004	DS004	Ausencia o no utilización de estándares de desarrollo	2: Medio	2: Medio	MEDIO	Aun no se han establecido mecanismos de procesos estándares.	0: No Controlado	MEDIO
005	DS005	Ausencia de documentos de sustento en las solicitudes de nuevos sistemas	3: Medio Alto	3: Medio Alto	MEDIO ALTO	Las solicitudes de generación o modificación tienen un proceso de "sentido Comun" con firmas del usuarios solicitante, no existen formatos	2: Parcial	MEDIO BAJO
006	DS006	Ausencia de procesos formales de control de cambios	3: Medio Alto	3: Medio Alto	MEDIO ALTO	Existen niveles de control de cambios, pero no están estandarizados ni formalizados, dependen mucho del responsable y del jefe de división	2: Parcial	MEDIO BAJO
007	DS007	Fallas en la implementación de cambios a sistemas desarrollados	1: Medio Bajo	3: Medio Alto	MEDIO	Los cambios en los sistemas se prueban antes del pase a producción	3: Razonable	BAJO
008	DS008	Ausencia de auditorías de calidad y pruebas a nuevos sistemas	1: Medio Bajo	3: Medio Alto	MEDIO	Los cambios en los sistemas se prueban antes del pase a producción y son revisados por auditoria	3: Razonable	BAJO
009	DS009	Ausencia de tecnología de administración de proyectos	2: Medio	2: Medio	MEDIO	Se tiene un módulo de administracion de proyectos, pero no se está utilizando	1: Bajo	MEDIO
010	DS010	Información critica no protegida en los sistemas de información	3: Medio Alto	2: Medio	MEDIO	La información crítica se mantiene aislada, sin embargo se realiza por buenas prácticas, aun no se tiene establecida una clasificación adecuada.	2: Parcial	MEDIO BAJO

Actividad/Servicio/Proceso en evaluación:
Requerimientos de nuevos sistemas
Control en uso de aplicaciones
Cifrado a información critica
Control antes de ingreso a producción
Control de acceso a programas fuente
Requerimientos de nuevos sistemas
Mejoras y actualización de los sistemas actuales

FIGURA C2

Plantilla 2 RTI	EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION
Factor Critico / Proceso en Evaluación:	Servicios Prestados por Terceros

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	ST001	Mal uso de información del banco por parte de terceras empresas	1: Medio Bajo	4: Alto	MEDIO ALTO	No existen politicas de acuerdos de confidencialidad formal, el control es muy informal	1: Bajo	MEDIO
002	ST002	Fraude	1: Medio Bajo	3: Medio Alto	MEDIO	Se hace seguimiento y control en base a sentido común de los responsables, no existen controles formales	2: Parcial	MEDIO BAJO
003	ST003	Robo y divulgación de información	2: Medio	3: Medio Alto	MEDIO ALTO	No se están ejecutando controles	0: No Controlado	MEDIO ALTO
004	ST004	Contratos sin inclusión de compromisos, responsabilidades y clausulas de penalidad	3: Medio Alto	2: Medio	MEDIO	Los contratos tienen clausulas de penalidad, pero no establecen mecanismos de confidencialidad.	1: Bajo	MEDIO
005	ST005	Ausencia de controles a la seguridad de terceros	2: Medio	3: Medio Alto	MEDIO ALTO	No existen mecanismos de control	0: No Controlado	MEDIO ALTO
006	ST006	No se realizan procesos de control de la sensibilidad de información en manos de terceros.	1: Medio Bajo	2: Medio	MEDIO	No existen mecanismos de control	0: No Controlado	MEDIO
007	ST007	Dependencia excesiva de terceros para la realización de diversos procesos	2: Medio	4: Alto	MEDIO ALTO	En los casos criticos, se ha buscado mas de dos proveedores (ATM), en los demas, se ha considerado no imprescindible	3: Razonable	MEDIO BAJO
008	ST008	No se realizan procesos de medición de desempeño o estos son deficientes y no documentados	1: Medio Bajo	1: Medio Bajo	MEDIO BAJO	Se realiza verificación de trabajos realizados y evaluación de objetivos alcanzados para el pago.	2: Parcial	BAJO
009	ST009	No existen procesos de monitores de servicios o estos son deficientes	2: Medio	3: Medio Alto	MEDIO ALTO	No se monitorea permanentemente el servicio, unicamente en el caso de reportes de falla.	1: Bajo	MEDIO
010	ST010	No se lleva un adecuado registro de contratos según sensibilidad de información expuesta a terceros	3: Medio Alto	2: Medio	MEDIO	Se tiene un inventario de contratos, pero no tiene clasificación de importancia y sensibilidad, el responsable aplica muchas veces su experiencia.	1: Bajo	MEDIO

Actividad/Servicio/Proceso en evaluación:
Proceso de contratación
Relación con proveedores
Contratos
Controles de Seguridad en los servicios prestados por terceros
Medidas de desempeño
Programas de mejoramiento
Monitoreo de servicios

FIGURA C3

Plantilla 2 RTI	EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Critico / Proceso en Evaluación:	Seguridad de Operaciones y Comunicaciones

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	SO001	Ausencia de control de cambios al ambiente operativo : los sistemas de informacion, instalaciones de procesamiento y procedimientos.	2: Medio	2: Medio	MEDIO	Existen niveles de control de cambios, pero no están estandarizados ni formalizados, dependen mucho del responsable y del jefe de división	2: Parcial	MEDIO BAJO
002	SO002	No disponibilidad de los sistemas y servicios	1: Medio Bajo	3: Medio Alto	MEDIO	Se tiene implementado mecanismos Non Stop y control permanente del servidor principal	3: Razonable	BAJO
003	SO003	Tiempo de respuesta alto en sistemas en linea	1: Medio Bajo	3: Medio Alto	MEDIO	No se están ejecutando procesos de control mas alla de verificar la linea en los incidentes	1: Bajo	MEDIO
004	SO004	Planificacion ineficiente en procesos batch	0: Bajo	3: Medio Alto	MEDIO	Los procesos se encuentran planificados pero no se lleva un monitoreo de los mismos	2: Parcial	MEDIO BAJO
005	SO005	Fallas en los equipos y/o aplicaciones	1: Medio Bajo	3: Medio Alto	MEDIO	Se dispone de mecanismos de seguimiento y revisión permanente, hay deficiencias en soporte.	2: Parcial	MEDIO BAJO
006	SO006	Cambios no autorizados a la información en produccion	0: Bajo	3: Medio Alto	MEDIO	Todo cambio en producción debe estar acompañado de la solicitud de cambio, falta documentar y formalizar el proceso.	3: Razonable	BAJO
007	SO007	Inexistencia o deficiencias notables en ambiente de desarrollo	1: Medio Bajo	2: Medio	MEDIO	El personal es responsable del control de los procesos.	2: Parcial	MEDIO BAJO
008	SO008	Pruebas y control de calidad de los nuevos sistemas en produccion	2: Medio	2: Medio	MEDIO	Los controles no permiten pruebas en producción	3: Razonable	BAJO
009	SO009	Insuficiente capacidad de procesamiento de los equipos y medios de almacenamiento	1: Medio Bajo	4: Alto	MEDIO ALTO	Procesos Merge, Procesos continuos de reasignación y optimizacion de espacio fisico.	3: Razonable	MEDIO BAJO
010	SO010	Introduccion de software malicioso o no autorizado	1: Medio Bajo	4: Alto	MEDIO ALTO	Se controla en las PC principales y administrativas, no asi en las PC operativas	2: Parcial	MEDIO BAJO

Actividad/Servicio/Proceso en evaluación:
Registro de Control de Cambios
Metodologia de Desarrollo de Sistemas
Separacion de Ambientes (Producción - Desarrollo)
Inventario de Infraestructura Tecnologica
Revisión manual de funciones
Manejo de Licencias de Software
Manejo de Problemas
Seguridad Correo Electronico
Seguridad de Red
Seguridad en Cajeros
Aplicación Banca Electronica
Sw permitido - adquisicion, uso, administracion Virus y Transmición

FIGURA C4

Plantilla 2 RTI	EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Critico / Proceso en Evaluación:	Seguridad Lógica

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	SL001	Acciones y/o actividades no autorizadas en los servicios de red	1: Medio Bajo	2: Medio	MEDIO	Se ha implementado visores de control de red, apliaciones de seguimiento por usuario.	2: Parcial	MEDIO BAJO
002	SL002	Ausencia o deficiencia en la identificación de usuarios en los sistemas	3: Medio Alto	2: Medio	MEDIO	En los sistemas administrativos se maneja por sistema operativo, en las sedes operativas no hay control	2: Parcial	MEDIO BAJO
003	SL003	Ausencia o deficiencia de validación de contraseñas de acceso a los sistemas	0: Bajo	2: Medio	MEDIO BAJO	En los sistemas administrativos se maneja por sistema operativo, en las sedes operativas no hay control	2: Parcial	BAJO
004	SL004	Ausencia o deficiencia de herramientas de auditoria	4: Alto	3: Medio Alto	MEDIO ALTO	Existen programas log en los servidores principales, no en los aplicativos desarrollados	2: Parcial	MEDIO BAJO
005	SL005	Ausencia de autenticación de usuarios en comunicaciones remotas	3: Medio Alto	1: Medio Bajo	MEDIO	Se valida por Host, no se autentica	3: Razonable	BAJO
006	SL006	Ingreso de virus, gusanos, caballos de troya, etc.	4: Alto	3: Medio Alto	MEDIO ALTO	Se tiene instalado antivirus en todas las PC	3: Razonable	MEDIO BAJO
007	SL007	Administración de derechos de perfiles no realizado por un área especializada en seguridad informática	2: Medio	3: Medio Alto	MEDIO ALTO	No existe area de seguridad informatica implementada, solo el MOF	0: No Controlado	MEDIO ALTO
008	SL008	Uso de distintas claves y perfiles distintos para cada aplicativo	4: Alto	2: Medio	MEDIO ALTO	No hay planificación para uso de Single SignOn	0: No Controlado	MEDIO ALTO
009	SL009	Ausencia de documentos de sustento de solicitudes de alta de usuarios	3: Medio Alto	2: Medio	MEDIO	La solicitud de alta de usuarios viene firmada por el jefe de departamento solicitante	3: Razonable	BAJO
010	SL010	Ausencia de documentos de clasificación de perfiles de usuario para cada aplicativo	3: Medio Alto	2: Medio	MEDIO	Se implementara una base de datos de perfiles de usuario, se administra actualmente de modo informal.	1: Bajo	MEDIO

Actividad/Servicio/Proceso en evaluación:
Procedimientos de concesión, administración de derechos y perfiles
Revocación de usuarios
Monitoreo de cuentas de usuario y administración de servicios
Identificación y vigilancia de usuarios
Utilidades del sistema y herramientas de auditoría
Acceso y uso del sistema
Usuarios remotos y computación móvil
Control sobre cuentas propias (por usuario)
Control de incidentes
Reacreditación de seguridad

FIGURA C5

Plantilla 2 RTI	EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Critico / Proceso en Evaluación:	Seguridad Física

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	SF001	Ocurrencia de desastres que destruyan o deterioren de manera parcial o total ambientes físicos del banco	1: Medio Bajo	4: Alto	MEDIO ALTO	Se tiene un plan de seguridad física y de emergencia en oficinas, no se han hecho simulacros	2: Parcial	MEDIO BAJO
002	SF002	Ocurrencia de actos vandálicos que dañen los ambientes físicos del banco	3: Medio Alto	3: Medio Alto	MEDIO ALTO	Se tiene un plan de seguridad física y de emergencia en oficinas, no se han hecho simulacros o acciones preventivas	1: Bajo	MEDIO
003	SF003	Ausencia de equipos de seguridad (alarmas, detectores de humo o agua, extintores, etc) adecuados	0: Bajo	3: Medio Alto	MEDIO	Se tiene implementado equipos de seguridad en todas las agencias	3: Razonable	BAJO
004	SF004	Inoperatividad de equipos de seguridad adecuados	2: Medio	3: Medio Alto	MEDIO ALTO	Se tiene controles preventivos y correctivos para equipos.	3: Razonable	MEDIO BAJO
005	SF005	No se realiza mantenimiento de equipos de seguridad o de ambientes físicos	1: Medio Bajo	3: Medio Alto	MEDIO	Se tiene controles preventivos y correctivos para equipos.	3: Razonable	BAJO
006	SF006	Presencia no generalizada en todo el banco de equipos de seguridad	0: Bajo	3: Medio Alto	MEDIO	Todas las agencias tienen equipos de seguridad implementados	3: Razonable	BAJO
007	SF007	Inexistencia de áreas físicas seguras en caso de desastre o no señalización de las mismas	0: Bajo	3: Medio Alto	MEDIO	Se encuentran señalizadas las zonas de seguridad, y los puntos de seguridad.	3: Razonable	BAJO
008	SF008	No existencia de control físico de acceso a los ambientes no públicos del banco	2: Medio	3: Medio Alto	MEDIO ALTO	Vigilancia privada y controles visuales con camaras de video en CCTV	2: Parcial	MEDIO BAJO
009	SF009	Inadecuada distribución y clasificicación de ambientes físicos según tipo de acceso permitido	2: Medio	2: Medio	MEDIO	No se tienen planos adecuados de distribución en algunas agencias, la mayoria de las nuevas están implementando dicho esquema de trabajo.	2: Parcial	MEDIO BAJO
010	SF010	Equipos mal ubicados en ambientes físicos	1: Medio Bajo	1: Medio Bajo	MEDIO BAJO	No se tienen planos adecuados de distribución en algunas agencias, la mayoria de las nuevas están implementando dicho esquema de trabajo.	2: Parcial	BAJO

Actividad/Servicio/Proceso en evaluación:
Acceso Físico
Administración de instalaciones físicas
Acciones de personal en áreas de trabajo
Equipamiento y bienes físicos
Centro de Procesamiento
Zonas de seguridad
Estructura Física
Controles de disposición documentana
Servicios de respaldo de llaves, usuarios y contraseñas
Resguardo especializado de salud de personal crítico
Escolta de visitantes

FIGURA C6

Plantilla 2 RTI	EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Crítico / Proceso en Evaluación:	Seguridad de Personal

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	SP001	Error en la manipulacion de los sistemas de informacion utilizados en personal	2: Medio	3: Medio Alto	MEDIO ALTO	No existen mecanismos de control formales	1: Bajo	MEDIO
002	SP002	Fraude Interno	2: Medio	3: Medio Alto	MEDIO ALTO	Se realizan validaciones por totales y en informática se evalúa el archivo de personal	2: Parcial	MEDIO BAJO
003	SP003	Sabotaje	2: Medio	3: Medio Alto	MEDIO ALTO	Se realizan validaciones por totales y en informática se evalúa el archivo de personal	2: Parcial	MEDIO BAJO
004	SP004	Robo de informacion	1: Medio Bajo	2: Medio	MEDIO	No existen mecanismos de control formales	1: Bajo	MEDIO
005	SP005	Abuso de accesos a los sistemas de informacion	1: Medio Bajo	2: Medio	MEDIO	Se controla via aplicativo host pero no hay limites de acceso.	1: Bajo	MEDIO
006	SP006	Manipulacion de la informacion	1: Medio Bajo	3: Medio Alto	MEDIO	Se realizan validaciones por totales y en informática se evalúa el archivo de personal	2: Parcial	MEDIO BAJO
007	SP007	Mal uso de la plataforma tecnologica	3: Medio Alto	3: Medio Alto	MEDIO ALTO	La experiencia de los usuarios finales limita el nivel de riesgo sin embargo no hay mecanismos de control	2: Parcial	MEDIO BAJO
008	SP008	Desconocimiento de las amenazas y problemas de seguridad de informacion	1: Medio Bajo	2: Medio	MEDIO	No hay programas de despliegue implementados actualmente	0: No Controlado	MEDIO
009	SP009	No existen definidas politicas de reemplazo de personal ausente	2: Medio	3: Medio Alto	MEDIO ALTO	Se aplican reemplazos ante la necesidad, no hay planes de reemplazo ni escalabilidad	1: Bajo	MEDIO
010	SP010	Ausencia por motivos no definidos de personal en cualquier area o agencia.	1: Medio Bajo	2: Medio	MEDIO	Se tiene establecido el reportar su ausencia a tiempo.	2: Parcial	MEDIO BAJO

Actividad/Servicio/Proceso en evaluación:
Responsabilidades y límites de contratación de los recursos humanos
Acuerdos privados de confidencialidad
Contingencias de personal
Sistemas de Administracion de Personal

FIGURA C7

Plantilla 2 RTI	EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Crítico / Proceso en Evaluación:	Procesos de Respaldo

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	PR001	No se realizan procedimientos de respaldo de información critica	3: Medio Alto	3: Medio Alto	MEDIO ALTO	Se realizan los backup, hay problemas asociados con la ubicación de estos	2: Parcial	MEDIO BAJO
002	PR002	No existe redundancia en los respaldos de información	4: Alto	4: Alto	ALTO	Se realizan dos copias de respaldo sin embargo no en todos los aplicativos	2: Parcial	MEDIO
003	PR003	No se realizan procesos de respaldo a la totalidad de sistemas criticos.	3: Medio Alto	2: Medio	MEDIO	Se realizan los backup, hay problemas asociados con la ubicación de estos	2: Parcial	MEDIO BAJO
004	PR004	No existencia de redundancia en los equipos de comunicación y líneas de comunicación	4: Alto	2: Medio	MEDIO ALTO	No existe dicho mecanismo de redundancia a la fecha.	0: No Controlado	MEDIO ALTO
005	PR005	Pérdida de información de respaldo (por robo, deterioro de dispositivos de almacenamiento)	2: Medio	3: Medio Alto	MEDIO ALTO	No hay mecanismos de control	0: No Controlado	MEDIO ALTO
006	PR006	Daños en los equipos de grabación y generación de respaldo	2: Medio	3: Medio Alto	MEDIO ALTO	No se tienen mecanismos de control, existe un control correctivo de equipos	1: Bajo	MEDIO
007	PR007	Ineficiente sistema de rotación de respaldo de información	3: Medio Alto	2: Medio	MEDIO	No hay mecanismos de rotación establecidos, se realizan de manera primaria unicamente	1: Bajo	MEDIO
008	PR008	Inadecuado inventario de dispositivos de almacenamiento	2: Medio	2: Medio	MEDIO	Los inventarios de dispositivos de almacenamiento se realizan solo para algunos servicios y servidores	2: Parcial	MEDIO BAJO
009	PR009	Inadecuado rotulado de dispositivos de almacenamiento	1: Medio Bajo	1: Medio Bajo	MEDIO BAJO	Existe un rotulado establecido	3: Razonable	BAJO
010	PR010	No existencia de procesos de recuperación y pruebas de efectividad de respaldo de información	3: Medio Alto	3: Medio Alto	MEDIO ALTO	La restauración del servidor principal es diaria, otra pruebas se realizan de manera permanente	2: Parcial	MEDIO BAJO

Actividad/Servicio/Proceso en evaluación:
Procedimientos de respaldo
Procedimientos de Recuperación
Ubicación Remota
Periodos de almacenamiento – Ciclos
Administración Física de ambientes para proceso de respaldo
Inventario de librería de almacenamiento
Respaldo de dispositivos de acceso
Respaldo documentario

FIGURA C8

Plantilla 2 RTI	EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Critico / Proceso en Evaluación:	Flujo de Información

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	FI001	Existencia de medios inseguros para trasladar información	3: Medio Alto	2: Medio	MEDIO	No se tiene un control sobre los mecanismos de traslado de información	1: Bajo	MEDIO
002	FI002	Recepción/envio de correos electrónicos no deseados	3: Medio Alto	3: Medio Alto	MEDIO ALTO	Se ha implementado un analizador de contenidos y servicios antispam	3: Razonable	MEDIO BAJO
003	FI003	Deficiencias en el transporte fisico a entidades externas	2: Medio	2: Medio	MEDIO	No se tiene un control sobre los mecanismos de traslado de información	1: Bajo	MEDIO
004	FI004	Inexistencia de acuerdos y responsabilidades	3: Medio Alto	2: Medio	MEDIO	Existencia de contratos con responsabilidades pero que no enfocan el factor confidencialidad.	2: Parcial	MEDIO BAJO
005	FI005	Inexistencia de documentación de nivel de sensibilidad de información	2: Medio	2: Medio	MEDIO	No existen clasificación de información	0: No Controlado	MEDIO
006	FI006	Inexistencia de registro de circulación de documentos (bitacoras fisicas, actas, base de datos de documentos)	2: Medio	1: Medio Bajo	MEDIO BAJO	No existen mecanismos formales, se almacenan de modos distintos en cada area.	1: Bajo	MEDIO BAJO
007	FI007	Inexistencia de grados de dependencia e interrelación entre documentos circulantes (información)	1: Medio Bajo	3: Medio Alto	MEDIO	No se tiene mecanismos de seguimiento.	0: No Controlado	MEDIO
008	FI008	Procesos de seguimiento de información inadecuados	1: Medio Bajo	2: Medio	MEDIO	No se tiene mecanismos de seguimiento.	0: No Controlado	MEDIO
009	FI009	Existencia de redundancia en flujos de información	2: Medio	2: Medio	MEDIO	No se tiene mecanismos establecidos	0: No Controlado	MEDIO
010	FI010	Procesos de recepción de información (cargos) no adecuados o no establecidos	2: Medio	2: Medio	MEDIO	Hay normas con relación a la entrega de documentos.	3: Razonable	BAJO

Actividad/Servicio/Proceso en evaluación:
Información circulante en cualquiera de sus formas
seguimiento documentario
Procesos de distribución
Niveles de flujo de información

FIGURA C9

Plantilla 2 RTI	EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Critico / Proceso en Evaluación:	Clasificación de Información

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	CS001	Ausencia de inventario clasificado de recursos de tecnologia de informacion	3: Medio Alto	2: Medio	MEDIO	Se tiene un inventario con una clasificación primaria	2: Parcial	MEDIO BAJO
002	CS002	Ausencia de responsables de los activos de informacion	2: Medio	2: Medio	MEDIO	Se tiene definido las responsabilidades, y esta se actualiza permanentemente.	3: Razonable	BAJO
003	CS003	Ausencia de proteccion adecuada a los activos de informacion	3: Medio Alto	2: Medio	MEDIO	En el C.C. se tiene mecanismos de protección de activos, en otras instancias aun no.	2: Parcial	MEDIO BAJO
004	CS004	Inadecuada manipulacion de los medios que contienen la informacion clasificada	2: Medio	3: Medio Alto	MEDIO ALTO	No hay mecanismos de seguimiento de información critica.	1: Bajo	MEDIO
005	CS005	Inexistencia o procedimientos inadecuados de asignacion de responsabilidades de activos de informacion	2: Medio	2: Medio	MEDIO	Se tiene definido las responsabilidades, y esta se actualiza permanentemente.	3: Razonable	BAJO
006	CS006	No se ejecutan procedimientos para clasificar la información circulante en físico o electrónico	2: Medio	2: Medio	MEDIO	No se tiene establecida una política de clasificación de información.	0: No Controlado	MEDIO
007	CS007	No hay un plan de despliegue de clasificación de seguridad operativo	3: Medio Alto	3: Medio Alto	MEDIO ALTO	No se tiene establecida una política de clasificación de información.	0: No Controlado	MEDIO ALTO
008	CS008	Ausencia o desuso de metodologia de clasificacion de seguridad	3: Medio Alto	2: Medio	MEDIO	No se tiene establecida una política de clasificación de información.	0: No Controlado	MEDIO

Actividad/Servicio/Proceso en evaluación:
Existencia de Inventario actualizado de activos asociados a T.I.
Diseño e implementacion del esquema de Clasif. de la Información

IMPLEMENTACION DE MEDIDAS DE MITIGACION

Como se ha indicado, la implementación de las medidas de mitigación, son recomendaciones a aplicar en el Banco posterior a la validación de la efectividad de los procedimientos de control existentes. Para este proceso, se ha simplificado en dos tipos de evaluación de riesgo:

1.- Para aquellos eventos de riesgo que tienen medidas de mitigación implementada s o en ejecución.- En este caso, las medidas de mitigación adicionales se han recomendado considerando la efectividad del mecanismo de mitigación actual y cuando el riesgo residual mantenga un nivel superior al nivel MEDIO. Este proceso, se ha realizado de la siguiente manera: Si la medida de mitigación actual no es efectiva, es decir, no reduce efectivamente el nivel de riesgo del evento en análisis, se evaluará la posibilidad de modificarlo o repotenciarlo.

2.- Para aquellos eventos de riesgo que actualmente no tienen ninguna medida de mitigación implementada o en ejecución.- En este caso, las medidas de mitigación se han recomendado cuando el riesgo residual mantenga un nivel superior al nivel MEDIO.

Para ambas opciones, se ha evaluando el costo beneficio de la implementación o modificación de las medidas de mitigación. El resultado se muestra en el Detalle de Evaluación de medidas de mitigación en la Figura C10.

FIGURA C1O

RTI	MEDIDAS DE MITIGACION A IMPLEMENTAR - EVALUACION DE RIESGOS DE TI					
NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE RIESGO	RIESGO RESIDUAL ACTUAL	CONTROLES ASOCIADOS	CONTROLES A IMPLEMENTAR
001	DS001	Ausencia de requerimientos funcionales de validación de la información de entrada para generación o modificación de sistemas	Medio Alto	Medio Alto	No se está validando ni realizando pruebas de validación de información de entrada, se utiliza información continua	Implementar piloto de pruebas de calidad de información, Se está requiriendo formatos estándares a usuarios que envían información
002	DS003	Ausencia o deficiencia de metodología de desarrollo de sistemas	Medio	Medio	La metodología de desarrollo de sistemas está en proceso de formalización y despliegue	Implementación de Plan de Desarrollo de Sistemas, dentro del marco del PSI
003	DS004	Ausencia o no utilización de estándares de desarrollo	Medio	Medio	Aun no se han establecido mecanismos de procesos estándares.	Implementación de Plan de Desarrollo de Sistemas, dentro del marco del PSI
004	DS007	Ausencia de tecnología de administración de proyectos	Medio	Medio	Se tiene un módulo de administracion de proyectos, pero no se está utilizando	Actualización del módulo de proyectos en NOTES, documentar los perfiles de SW.
005	ST001	Mal uso de información del banco por parte de terceras empresas	Medio Alto	Medio	No existen políticas de acuerdos de confidencialidad formal, el control es muy informal	Implementar documento de acuerdo de confidencialidad adendum a principales contratos
006	ST003	Robo y divulgación de información	Medio Alto	Medio Alto	No se están ejecutando controles	Implementación de Políticas de seguridad en contratos con terceros, aplicación de programas de elica profesional aplicadas en contratos vigentes
007	ST004	Contratos sin inclusión de compromisos, responsabilidades y clausulas de penalidad	Medio	Medio	Los contratos tienen clausulas de penalidad, pero no establecen mecanismos de confidencialidad.	Adecuar las clausulas de penalidad con los acuerdos de confidencialidad
008	ST005	Ausencia de controles a la seguridad de terceros	Medio Alto	Medio Alto	No existen mecanismos de control	Solicitar esquemas de seguridad de información y negociar la adecuación a los sistemas de seguridad del Banco, agregar adendum al contrato
009	ST006	No se realizan procesos de control de la sensibilidad de información en manos de terceros.	Medio	Medio	No existen mecanismos de control	Formar el comité de evaluación (testeo) de sensibilidad de información
010	ST009	No existen procesos de monitoreo de servicios o estos son deficientes	Medio Alto	Medio	No se monitorea permanentemente el servicio, unicamente en el caso de reportes de falla.	Implementar los grupos de seguimiento de servicios prestados por terceros, adecuar formatos de eventos de riesgo y formatos de ocurrencia de incidencias
011	ST010	No se lleva un adecuado registro de contratos según sensibilidad de información expuesta a terceros	Medio	Medio	Se tiene un inventario de contratos, pero no tiene clasificación de importancia y sensibilidad, el responsable aplica muchas veces su experiencia.	Automatizar los registros de contratos, aplicar clasificación de nivel de importancia y sensibilidad propuesto por riesgos.
012	SO003	Tiempo de respuesta alto en sistemas en linea	Medio	Medio	No se están ejecutando procesos de control mas alla de verificar la linea en los incidentes	Inicio de proceso Batch despues de las 5 PM, utilizar y reportar usando formato de ocurrencia de incidencias, evaluar y clasificar segmentos de ocurrencia mayor
013	SL007	Administración de derechos de perfiles no realizado por un área especializada en seguridad informática	Medio Alto	Medio Alto	No existe area de seguridad informatica implementada, solo el MOF	Implementar de personal al area ya aprobada
014	SL008	Uso de distintas claves y perfiles distintos para cada aplicativo	Medio Alto	Medio Alto	No hay planificación para uso de Single SignOn	Implementar politicas de seguridad de accesos bajo la administración de seguridad de información
015	SL010	Ausencia de documentos de clasificación de perfiles de usuario para cada aplicativo	Medio	Medio	Se implementara una base de datos de perfiles de usuario, se administra actualmente de modo informal.	Se está implementando el documento de perfil de aplicativo via formato de Planeamiento Estratégico de TI

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE RIESGO	RIESGO RESIDUAL ACTUAL	CONTROLES ASOCIADOS	CONTROLES A IMPLEMENTAR
016	SP001	Error en la manipulacion de los sistemas de informacion utilizados en personal	Medio Alto	Medio	No existen mecanismos de control formales	Asignación de responsabilidades formales a nivel de usuario, especificación de niveles de escalamiento
017	SP004	Robo de informacion	Medio	Medio	No existen mecanismos de control formales	Diseñar módulos de autenticidad y auditoría para acceso a sistemas de usuario. Difusión de políticas de seguridad
018	SP005	Abuso de accesos a los sistemas de informacion	Medio	Medio	Se controla via aplicativo host pero no hay limites de acceso.	Implementar máximo número de accesos por día
019	SP008	Desconocimiento de las amenazas y problemas de seguridad de informacion	Medio	Medio	No hay programas de despliegue implementados actualmente	Difusión y capacitacion de cultura de riesgos
020	SP009	No existen definidas polltlcas de reemplazo de personal ausente	Medio Alto	Medio	Se aplican reemplazos ante la necesidad, no hay planes de reemplazo ni escalabilidad	Implementación de mecanismos de escalabilidad para procesos y actividades de personal
021	PR002	No existe redundancia en los respaldos de información	Alto	Medio	Se realizan dos copias de respaldo sin embargo no en todos los aplicativos	Implementación de red de fibra óptica entre centros de cómputo, politicas de respaldo de información
022	PR004	No existencia de redundancia en los equipos de comunicación y líneas de comunicación	Medio Alto	Medio Alto	No existe dicho mecanismo de redundancia a la fecha.	Implementación de red de fibra óptica entre centros de cómputo, politicas de respaldo de información
023	PR005	Pérdida de información de respaldo (por robo, deterioro de dispositivos de almacenamiento)	Medio Alto	Medio Alto	No hay mecanismos de control	Esquema formal de procedimiento dual
024	PR006	Daños en los equipos de grabación y generación de respaldo	Medio Alto	Medio	No se tienen mecanismos de control, existe un control correctivo de equipos	Revisar contratos de mantenimiento preventivo o correctivo, contactos de servicios menores
025	PR007	Ineficiente sistema de rotación de respaldo de información	Medio	Medio	No hay mecanismos de rotación establecidos, se realizan de manera primaria unicamente	Documentar los procesos aplicando controles de copia, ciclos de rotación y actualización según politicas de respaldo
026	FI001	Existencia de medios inseguros para trasladar información	Medio	Medio	No se tiene un control sobre los mecanismos de traslado de información	Esquema formal de procedimiento dual
027	FI003	Deficiencias en el transporte físico a entidades externas	Medio	Medio	No se tiene un control sobre los mecanismos de traslado de información	Esquema formal de procedimiento dual
028	FI005	Inexistencia de documentación de nivel de sensibilidad de información	Medio	Medio	No existen clasificación de información	Implementar proyecto de clasificación de información y difundirlo a la institución
029	FI008	Procesos de seguimiento de información inadecuados	Medio	Medio	No se tiene mecanismos de seguimiento.	Implementar proyecto de clasificación de información y difundirlo a la institución, adecuar sistema de control documentario en NOTES
030	FI009	Existencia de redundancia en flujos de información	Medio	Medio	No se tiene mecanismos establecidos	adecuar sistema de control documentario en NOTES
031	CS004	Inadecuada manipulacion de los medios que contienen la informacion clasificada	Medio Alto	Medio	No hay mecanismos de seguimiento de información crítica.	Implementar proyecto de clasificación de información y difundirlo a la institución
032	CS006	No se ejecutan procedimientos para clasificar la información circulante en físico o electrónico	Medio	Medio	No se tiene establecida una política de clasificación de información.	Implementar proyecto de clasificación de información y difundirlo a la institución
033	CS007	No hay un plan de despliegue de clasificación de seguridad operativo	Medio Alto	Medio Alto	No se tiene establecida una política de clasificación de información.	Implementar proyecto de clasificación de información y difundirlo a la institución
034	CS008	Ausencia o desuso de metodologia de clasificacion de seguridad	Medio	Medio	No se tiene establecida una política de clasificación de información.	Implementar proyecto de clasificación de información y difundirlo a la institución

3.5.2.3.- PROCESO DE CAPACITACIÓN Y CONCIENTIZACIÓN

Un proceso de capacitación y concientización como soporte a las dos anteriores etapas, el mismo que incluye al personal general del Banco y a la Gerencia General la misma que permitirá la expansión de la cultura de riesgo, la misma que incrementará nuestra imagen institucional.

Esta fase se orientará a cubrir la necesidad de concientizar acerca de la importancia de una cultura de riesgos, así como también a capacitar para el correcto despliegue y manejo descentralizado de los riesgos en cada una de las sucursales y agencias en todo el país.

3.5.3.- TRATAMIENTO DE PROCESOS CRITICOS DE NEGOCIO

Una de las principales consideraciones dentro de la Administración de riesgos de Tecnología de información y relacionados con el Plan de Continuidad de Negocios, es el tratamiento de los procesos críticos del negocio, para la consecución de este objetivo, se ha logrado Identificar los factores externos e internos de interrupción del negocio y los parámetros para la clasificación y priorización de procesos críticos relacionados a la actividad y naturaleza del Banco.

Esta identificación es el punto de partida para la identificación tanto de los procesos críticos del negocio, como también la tecnología que está ligada a cada uno de los mismos.

3.5.3.1.- IDENTIFICACION DE LOS FACTORES DE INTERRUPCION

Para el proceso de identificación de los factores que de materializarse podrían interrumpir la Continuidad del Negocio se ha creído conveniente hacer una distinción entre los factores internos, es decir, los que se generan por eventos propios del Banco; y los factores externos, cuya causa son eventos que se encuentran fuera del control del Banco.

FACTORES INTERNOS

Como su nombre lo indica, son factores producidos por eventos que se generan dentro del Banco, en el proceso operativo constante. Por ser de origen interno, se puede realizar un control adecuado a cada unos de estos factores, es decir, está dentro de la capacidad del Banco poder aplicar medidas de control interno para preveerlos de manera adecuada.

Dentro de esta clasificación hemos identificado los siguientes:

- **Robo Físico**: Robo de infraestructura de vital importancia para el normal desarrollo de las operaciones del banco, incluye equipos informáticos, información, entre otros. Esta también considerado como factor externo, cuando la sustracción es perpetrada por personas ajenas al Banco.
- **Paralización de labores**: Relacionado con huelgas y demás tipos de protesta que pudieran paralizar la actividad dentro de la institución.
- **Falla en los dispositivos de conectividad:** Se refiere a cualquier eventualidad que se pudiese producir con los equipos críticos de interconexión como router, switch, firewall, entre otros.
- **Falla en los enlaces de comunicación:** Hace referencia a fallas que podrían ocasionarse durante la transmisión de la información, en especial se consideran, las fallas de comunicación con el servidor central.
- **Sabotaje:** Relacionado con la destrucción o deterioro de equipos, maquinaria e instalaciones del Banco por parte de los empleados, se incluye en este rubro el ataque informático interno
- **Inadecuada manipulación de dispositivos críticos:** Factor de interrupción producido por un error, falla o manejo inadecuado de los equipos y dispositivos críticos por parte de los responsables de éstos.

FACTORES EXTERNOS

Son factores generados por eventos que se encuentran fuera del alcance y del control del Banco. Estos factores son los que se muestran a continuación:

- **Factor Regulatorio:** Cambios de la regulación en la industria/país.
- **Factor Político:** Guerra, política económica, bloqueo de negocios.
- **Factor Legal:** Interpretación, emisión o modificación de leyes.
- **Desastres:** Relacionado con desastres naturales a los cuales por la ubicación geográfica estamos propensos, siendo los más perjudiciales terremoto, inundación, entre otros.
- **Vandalismo:** Guarda relación con ataques originados por terceras personas, que no tienen vinculación alguna con el banco, sobre la infraestructura del mismo, se incluyen aquí las protestas y marchas violentas ajenas a la institución.
- **Delitos informáticos:** Considera los ataques informáticos perpetrados por los conocidos hackers, crackers, y/o cualquier otro tipo de pirata informático que violase las barreras de seguridad establecidas por el Banco.
- **Ataques de ex empleados:** Considera cualquier tipo de ataque, en su mayoría informáticos, perpetrado por ex empleados del Banco. Su conocimiento de los niveles de seguridad, así como de claves y vías de acceso, facilitan la violación de las barreras de seguridad del Banco. Este factor es una variante de los delitos informáticos.
- **Acciones Terroristas: Ocasionado** por ataques terroristas, en toda su variedad.
- **Contingencias de energía:** Relacionado con caídas del fluido eléctrico, apagones, pulsos de tensión, entre otros.
- **Contingencias de comunicación:** Relacionado con la dependencia de comunicación con otras empresas.

3.5.3.2.- PARAMETROS PARA CLASIFICACION DE PROCESOS

Para priorizar de manera correcta los procesos sensibles a la ocurrencia de los factores tanto internos como externos, se hace necesario hacer uso de ciertos parámetros que permitan medir de manera adecuada la criticidad de estos procesos.

Los parámetros ha ser usados, de acuerdo a su nivel de importancia, son los siguientes:

Impacto Económico (IE)

Relacionado con el impacto económico total que generaría la ocurrencia de un factor de interrupción. Este parámetro está conformado por el gasto de recuperación, la pérdida por interrupción, el número de operaciones y el volumen marginal de operaciones.

- **Gasto por Recuperación (GR):** Gasto económico necesario para la recuperación de la continuidad del proceso.
- **Pérdida por Interrupción (PI):** Pérdida económica ocasionada durante el periodo en el que un proceso se encuentre no operativo.
- **Número de Operaciones (NO):** Número total de operaciones que se realiza a través de un proceso en una unidad de tiempo de interrupción.
- **Monto de Operaciones (MO):** Monto de las operaciones que se realiza a través de un proceso en una unidad de tiempo de interrupción.

Por tanto, el impacto económico se expresa de la siguiente manera:

$$IE = (GR + PI + NO + MO) / 4$$

Tiempo Mínimo de Recuperación (TMR)

Relacionado con el período de tiempo que un proceso se encuentra no operativo. Para este parámetro se debe considerar el tiempo mínimo requerido para que el proceso se reestablezca, asimismo debe de realizase el calculo de tiempo mínimo del peor caso que se pudiese presentar en la ocurrencia de un factor de interrupción.

Impacto Social (IS)

Todos aquellos factores que por la naturaleza y misión del banco podrían significar dejar de cumplir con el soporte, servicio y beneficios a los empleados activos y pasivos del sector público y la necesidad de asegurar la prestación de servicios como única oferta bancaria.

Afección a la Imagen Institucional (II)

Relacionado con los efectos que podría tener, la ocurrencia de un factor de interrupción, sobre los clientes, proveedores y demás entes que tengan relación, directa o indirecta, con el Banco.

Ubicación Geográfica (UG)

Relacionado con el ámbito geográfico en el cual está incluido el proceso afectado por un factor de interrupción.

Otros (OT)

Relacionado con cualquier otro parámetro adicional o propio para cada proceso que tenga relevancia en cuanto a la ocurrencia de un factor de interrupción del negocio.

3.5.3.3.- CALCULO DE PUNTUACION DE PROCESOS

El cálculo de la puntuación de un proceso, será obtenido en función de la ponderación de los parámetros identificados anteriormente; es así que esta puntuación se obtiene considerando ponderadamente cada uno factor.

El modelo matemático del cálculo de la puntuación de un proceso crítico se expresa de la siguiente manera:

Puntuación del Proceso (X) =	100* **IE(x)** + 40***TMR(x)** + 100***IS(x)** + 50***II(x)** + 30***UG(x)** + 10* **0T(x)**

Donde:

Puntuación del Proceso(X): Puntuación total del nivel de criticidad que posee el proceso "X" dado que está siendo afectado por un factor de interrupción. Esta puntuación permitirá ubicar de manera jerarquizada cada uno de los procesos desde los más críticos para la continuidad del negocio, hasta los menos críticos, de tal manera que se orienten los planes de recuperación a los más importantes según el resultado ordenado de la evaluación, Siempre que haya ocurrido un factor de interrupción.

IE(x): Impacto económico que causaría la interrupción del proceso "X", frente a la ocurrencia del factor de interrupción".

TMR(x): Tiempo mínimo de recuperación que necesitaría el proceso "X", de ser interrumpido por la ocurrencia del factor de interrupción".

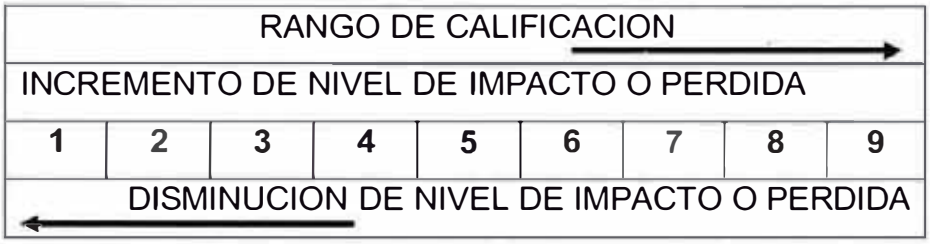
IS(x): Impacto social que por la naturaleza del banco generaría la interrupción del proceso "X", a causa de la ocurrencia del factor de interrupción.

II(x/y): Medición del nivel en que afecta a la imagen institucional la interrupción del proceso ""X", a causa de la ocurrencia del factor de interrupción.

UG(x): Medición del nivel en que afecta por la ubicación geográfica la interrupción del proceso "X", a causa de la ocurrencia del factor de interrupción.

OT(x): Cualquier otro parámetro propio del proceso ""x", frente a la ocurrencia del factor de interrupción.

Rango de Calificación: El rango de calificación para cada uno de los factores de cuantificación se realizará en escala numérica de 1 a 9 considerando para ello que el nivel de impacto o pérdida aumenta con la escala.



En la Figura D, se muestra el resultado de la evaluación aplicando la puntuación de procesos a los Servicios externos del Banco. Esta evaluación se realizó en trabajo conjunto con el Departamento de Operaciones quienes brindaron la información de número de operaciones, monto de operaciones por servicio en evaluación y lo referente a los tiempos de recuperación y pérdidas estimadas aplicando un primer nivel de gastos según volumen de operaciones y aplicando técnicas de Top-Down basado en la experiencia del personal a cargo de los procesos críticos de negocio. El impacto social ha sido evaluado en trabajo conjunto con el Departamento de Servicios Bancarios, mientras que el factor geográfico ha tenido un primer desarrollo a nivel de la Red de Agencias, en estos casos igualmente se han utilizado técnicas de Top-Down en vista que no existe un trabajo previo que permita iniciar o aplicar metodologías estadísticas basadas en registros históricos.

FIGURA D

Plantilla 3	RTI	CALCULO DE PUNTUACION DE CRITICIDAD DE PROCESOS

Proyecto	*Plan de Continuidad de Negocios*
Etapa en desarrollo	*Análisis de Impacto de Negocio*

PROCESO / SERVICIO	IMPACTO ECONOMICO				TIEMPO MINIMO DE RECUPERACION	IMPACTO SOCIAL	IMAGEN INSTITUCIONAL	UBICACIÓN GEOGRAFICA	OTROS FACTORES	PUNTUACION DE CRITICIDAD
	Gasto por recuperación	Pérdida por Interrupción	Número de Operaciones	Volumen Marginal de Operaciones						
Abono Masivo	5	6	9	8	5	9	9	8	6	2550
Retiro de ahorros	6	5	8	8	5	9	6	8	6	2375
Cobro de tasas a entidades públicas	4	7	7	8	6	7	7	6	6	2180
Recaudaciones SUNAT	4	7	6	8	5	7	5	5	6	1985
Depósito de Ahorros	3	4	3	4	5	8	7	4	5	1870
Corresponsalia Telefónica del Perú	5	5	3	6	6	5	6	4	5	1685
Compra Venta de M.E.	7	5	1	3	6	6	5	4	3	1640
Pago de Cheques	3	6	5	6	4	5	7	5	5	1710
Tarjetas-pago FONAHPU	4	3	1	4	6	7	5	3	4	1620
Corresponsalia	3	5	5	6	3	5	8	4	5	1665
Depósitos Cuenta Corriente	4	6	2	6	5	4	6	4	4	1510
Emisión giro bancario/telefónico	5	5	2	5	4	4	6	5	4	1475
Pago giro bancario/telefónico	4	4	2	4	5	4	6	3	4	1380
Emisión depósitos judiciales y administrativos	6	6	1	3	5	3	5	5	4	1340
Documentos Valorados	6	5	1	4	4	4	4	3	4	1290
Aduanas	3	3	1	5	5	3	6	4	3	1250
Pago depósitos judiciales y administrativos	4	4	1	1	4	3	6	5	3	1190

CAPITULO IV
EVALUACION DE RESULTADOS

La estrategia para el adecuado tratamiento de los riesgos de tecnología de información permitirá al Banco diseñar mecanismos de respuesta y control para minimizar el impacto de la ocurrencia de eventos de riesgo. Asimismo, llevar un adecuado control de las falencias asociadas a los procesos y servicios bancarios soportados por recursos de información y de tecnología.

El detalle de los resultados se ha dividido en cuatro grandes grupos de resultados:

- Cumplimiento de la regulación vigente (Superintendencia de banca y Seguros).
- Permitir la administración de los riesgos estructurales y coyunturales a los que está expuesto la institución e implementar medidas de mitigación.
- Clasificar los procesos críticos de negocio.
- Resultados operativos, económicos y sociales.

4.1.- CUMPLIMIENTO DE LA REGULACION VIGENTE

Con la aplicación de la metodología para la administración de los riesgos de Tecnología, el Banco cumplirá lo estipulado en la Circular G-105 y que involucra básicamente la estructura organizacional para el tratamiento de los RTI, la evaluación de riesgos, la selección de controles y objetivos de control, el desarrollo e implementación de los respectivos planes de adecuación que involucran la seguridad de información y finalmente el plan de continuidad de negocios.

4.2.- PERMITIR LA ADMINISTRACIÓN DE LOS RIESGOS ESTRUCTURALES Y COYUNTURALES A LOS QUE ESTÁ EXPUESTO LA INSTITUCIÓN E IMPLEMENTAR MEDIDAS DE MITIGACIÓN

Mediante la aplicación de la metodología de Administración de Riesgos, y según los resultados mostrados en el presente informe, el Banco ha logrado:

- Determinar la posibilidad de ocurrencia y el impacto de los riesgos asociados a tecnología de información.
- Determinar y formalizar los mecanismos actuales de control y mitigación de RTI y determinar el riesgo residual actual.
- Determinar los mecanismos para la mitigación de los riesgos residuales actuales.
- Clasificar los principales activos de información.

Por otro lado, estos resultados nos permitirán en el corto plazo:

- Monitorear continuamente las vulnerabilidades y las medidas de control aplicadas para mitigar los riesgos.
- Establecer adecuados y formales procedimientos de almacenamiento, distribución, intercambio y mantenimiento de información en los sistemas de soporte.

Asimismo, con relación a los riesgos coyunturales, es decir aquellos que puedan presentarse durante la actividad diaria del negocio, se aplicará el mismo esquema metodológico con evaluación inmediata del proceso o servicio que se evalúe entre ellos tenemos la operatividad de sistemas y los proyectos tecnológicos a proponer.

4.3.- CLASIFICAR LOS PROCESOS CRÍTICOS DE NEGOCIO.

Dentro de las actividades logradas en el tratamiento de los procesos críticos de negocio, se ha logrado establecer una clasificación para los principales servicios que la Institución presta a sus clientes. En el corto plazo, esta clasificación será ampliada tanto a los procesos críticos internos como a las operaciones y procesos del negocio.

4.4.- RESULTADOS OPERATIVOS, ECONOMICOS Y SOCIALES

Con relación a la rentabilidad a nivel económico, si bien es cierto la administración de los riesgos de tecnología, al igual que el resto de los riesgos a los que se encuentra sujeto el Banco, no reporta beneficios directos de manera tangible, el adecuado tratamiento de los mismos representará para el Banco:

- Reducir significativamente los costos de recuperación de archivos que contengan información (en cualquiera de sus formas).
- Asegurar el mantenimiento preventivo y correctivo a nivel de recursos de tecnología de información.
- Incrementar la calidad en los servicios operativos asegurando la disponibilidad, integridad y confidencialidad de la información.

- Definir y estructurar los procedimientos para garantizar el correcto desarrollo de operaciones nacionales e internacionales.
- Garantizar y reducir el costo de pérdida de información en operaciones internas (personal, logística, comunicaciones, entre otros).
- Mejora de la imagen institucional al mantener un adecuado control de la información soportada en sus aplicaciones tecnológicas.
- Asegurar la disponibilidad de información para las actividades de orden social inherentes al negocio
- Implementación y medición de adecuados ratios de disponibilidad de información, ya que actualmente no existe ninguno.
- Incrementar el porcentaje de aceptación de operaciones bancarias seguras.
- Poseer mejores y más controlados sistemas internos.
- Capacitar internamente al personal del Banco para que sea parte de la cultura de riesgos de la institución.

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES

La administración integral de riesgos ha cobrado importante valor dentro de las actividades de una empresa, considerando además que las empresas financieras son un nicho de negocio sustantivamente crítico por la información, los servicios y los activos a proteger relacionados con su naturaleza, en este sentido y considerando el soporte a las operaciones y servicios que brinda la tecnología, es fundamental garantizar la adecuada administración de los riesgos inherentes al nivel de servicio y continuidad del negocio que ésta presta. Por ello, administrar los riesgos de tecnología de información, permitirá cubrir aquellos aspectos que conlleven a lograr minimizar cualquier efecto de vulnerabilidad o evento externo que signifique riesgos y que traigan consigo pérdidas de algún tipo a la empresa.

Se conseguirá mantener un adecuado programa continuo de evaluación de los riesgos a los que está expuesta la tecnología de información, los recursos asociados a ella, los activos de información y los procesos con soporte en equipos tecnológicos. El Banco, aplicará un control permanente a aquellos factores estructurales y en aquellos casos coyunturales donde sea necesario un análisis de proceso en especial, se aplicará la misma metodología considerando el riesgo coyuntural como un tipo especial de riesgo al cual se le hará el seguimiento respectivo.

Se logrará disponer de un registro permanentemente y actualizado de los principales activos de información a proteger de modo que se garantice la

continuidad operativa vía los planes de adquisición. Esto nos permitirá una adecuada sinergia con los procedimientos de continuidad del negocio.

Los Alcances a nivel organizacional, implican resultados en el corto y mediano plazo a nivel de Resultados de infraestructura tecnológica y seguridad de información soportada en esta infraestructura, servicios y operaciones con soporte en tecnología, los requerimientos de la superintendencia.

El Banco dispondrá de información clasificada, pudiendo orientar la atención de las Gerencias respectivas hacia los eventos de riesgos que pudieran significar mayores pérdidas para el negocio, Se podrá disponer de herramientas de alerta que nos permitan monitorear permanentemente el hallazgo de nuevos eventos de riesgo y a los cuales se les dará el tratamiento respectivo.

Para lograr estos resultados, se tiene en cuenta factores estratégicos como el apoyo de la Alta Dirección, la necesidad de disponer de amplios espacios de difusión, la fácil implementación de los mecanismos de administración de riesgos, la necesidad de orientar a la institución hacia la formalización de procesos y actividades, una permanente verificación y pruebas de control que garanticen la disponibilidad, integridad y confidencialidad de información y finalmente un adecuado plan de despliegue de la cultura de riesgos que garantice la participación general de los empleados.

BIBLIOGRAFIA

FRANCESE ROSES – Risk Management, Una nueva forma de asegurar el éxito empresarial. ACV Ediciones Barcelona 2002.

COBIT – Objetivos de Control para la Información y tecnologías afines - Control Objectives - 3ra. Edición. COBIT, Julio 2000.

COBIT – Objetivos de Control para la Información y tecnologías afines - Control Objectives - 2ra. Edición. COBIT, Abril 1998.

ISO/IEC 17799 International Standard, Información Technology – Code of practice for information security management, first edition, ISO/IEC 2000.

ALBERTO CANCELADO G. - Sistema De Administración De Riesgos En Tecnología Informática, Noviembre 2003.

HEIDI RICHARDS - Federal Reserve Board, Information Technology Risks, Marzo 2001

ESTANDAR AUSTRALIANO – Administración de Riesgos AS/NZS 4360:1999.

INEI – Instituto Nacional de Estadística e Informática Perú - Lineamientos de Política Nacional de Seguridad de la Información en el Estado Peruano, Diciembre 2000.

INEI – Instituto Nacional de Estadística e Informática Perú – Conceptos sobre Seguridad de la Información, Marzo 2000.

BETTY INFANTE – Evade ITESM México – Banca por Internet, una nueva forma de hacer negocios, 2003.

RU SECURE – Information Security Policies V. 2.0 – Securing Information In The Digital Age, Abril 2003.

GALLO, PORTUGAL, PARRONDO, SANCHEZ - La Protección de Datos Personales, Soluciones en Entornos Microsoft ®, Microsoft Ibérica S.R.L. 2003.

IT BASELINE PROTECTION MANUAL - Standard Security Safeguards - Bundesanzeiger – Verlag, Alemania. 2001.

BORGHELLO CRISTIAN F. – TESIS: Seguridad Informática: Sus Implicancias e Implementación- Universidad Tecnológica Nacional de Argentina, Licenciatura en Sistemas, 2001.

JOSÉ MANUEL BADÍA CONTELLES, ÓSCAR COLTELL SIMON - Seguridad Y Protección de la Información - Ingeniería Técnica en Informática de Gestión, 1998.

ALLAN R. PALIOTTA – CISA, CFE, CFSA - A Total-Process View of information Security Risk Management, Agosto 2001

GUIAS DE REFERENCIA:

SBS- Superintendencia De Banca y Seguros Perú – Circular Nº G-105-2002 – Riesgos de Tecnología de Información, 2002.

CHARLES CRESSON WOOD, Cisa, Cissp – Information Security Policies Made Easy V. 6 Baseline Software, Inc., USA 1997.

EDPACS - The Edp Audit, Control, And Security- A view of international IT Security Standards, Especially ISO/IEC17799, Diciembre 2001.

PROTECTING VALUE – Study 2003 Managing Business Risks

ERNST & YOUNG - Global Information Security Survey 2002 -Technology And Security Risk Services

ANDRES CORREAL – Plan de Contingencias, Fundación Universitaria de Boyacá, Nov. 2002

M. FARIAS – ELINOS - Auditoría de los Sistemas de Información - LIDETEA, Universidad de la Salle México,

RODOLFO OCONITRILLO BRENES - Gestión De Riesgos, Una propuesta práctica para Cooperativas de Ahorro y Crédito

GABRIEL CASAS SAAVEDRA – Evaluación de Riesgos, IV Reunión de Auditores Internos de Banca Central – CEMLA Cartagena de Indias, Colombia julio de 1998.

SITIOS DE REFERENCIA EN INTERNET:

ISACA: The Information Systems Audit and Control Association & Foundation
http://www.isaca.org/

Normas NIST: Requerimientos de seguridad para módulos criptográficos.
http://csrc.nist.gov

IT Baseline Proteccion Manual
http://www.bsi.bund.de/gshb/english/etc/inhalt.htm

Información sobre las normas ISO 17799
http://www.puntonetsoluciones.com.ar/is017799.htm

Plan De Continuidad De Negocio
http://www.novagestion.cl/html_nova/Planes_negocio.html

Elaboración de mapas de riesgo
http://www.securitymanagement.com/library/001147.html

Riesgos del Software - tutorial
http://www.cs.virginia.edu/~knabe/riesgos.html

Guía para la evaluación de riesgos
http://www.istas.net/sl/bajar/rspsc2.pdf

Minimizar los riesgos en el uso de la tecnología
http://www.aceproject.org/main/espanol/et/ete.htm

Análisis de Riesgos y plan de respuesta a contingencias

http://www.transredes.com/pdfs/MedioAmb/eeia/eeiaColpaMineros/08_AnalRiesgosPlanContin.PDF

10 Características Claves De Seguridad De Información
http://www.peopsoft.com/Servicio_Security.htm

Links De Seguridad De Información
http://www.security.kirion.net/seguridad/

Seguridad De Información
http://www.lpsi.eui.upm.es/SInformatica/SInformatica.htm

Cybsec Security Systems – Empresa consultora en Seguridad de Información
http://www.cybsec.com

Guía para plan de seguridad Informático para ONG's
http://personal2.iddeo.es/alcazaba/normas/planseguridadinformatico.pdf
http://guiaong.cjb.net

La Importancia de la Seguridad Informática: Las políticas y la Legislación
http://seguridad.internet2.ulsa.mx/

Definición de Políticas de Seguridad
http://www.rediris.es/cert/

ANEXOS

ANEXO 1

CIRCULAR Nº G–105–2002 RIESGOS DE TECNOLOGIA DE INFORMACIÓN

Lima, 22 de febrero de 2002

CIRCULAR Nº G - 105 - 2002

Ref.: Riesgos de tecnología de información

Señor
Gerente General

Sírvase tomar nota que, en uso de las atribuciones conferidas por el numeral 7 del artículo 349º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley Nº 26702 y sus modificatorias, en adelante Ley General, y por la Resolución SBS N° 1028-2001 del 27 de diciembre de 2001, con la finalidad de establecer criterios mínimos para la identificación y administración de los riesgos asociados a la tecnología de información, a que se refiere el artículo 10º del Reglamento para la Administración de los Riesgos de Operación, aprobado mediante la Resolución SBS Nº 006-2002 del 4 de enero de 2002, esta Superintendencia ha considerado conveniente establecer las siguientes disposiciones:

Alcance
Artículo 1º.- Las disposiciones de la presente norma son aplicables a las empresas señaladas en los artículos 16° y 17° de la Ley General, al Banco Agropecuario, a la Corporación Financiera de Desarrollo S.A. (COFIDE), al Banco de la Nación, a la Fundación Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI) y a las derramas y cajas de beneficios que se encuentren bajo la supervisión de esta Superintendencia, en adelante empresas.

Definiciones
Artículo 2º .- Para efectos de la presente norma, serán de aplicación las siguientes definiciones:

a. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.
b. Ley General: Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.
c. Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la empresa, y cuya falta o ejecución deficiente puede tener un impacto financiero significativo para la empresa.

d. Reglamento: Reglamento para la Administración de los Riesgos de Operación aprobado por Resolución SBS N° 006-2002 del 4 de enero de 2002.

e. Riesgos de operación: Entiéndase por riesgos de operación a la 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.

f. Riesgos de tecnología de información: Los 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.

g. 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.

h. Objetivo de control: Una declaración del propósito o resultado deseado mediante la implementación de controles apropiados en una actividad de tecnología de información particular.

Responsabilidad de la empresa

Artículo 3°.- Las empresas deben establecer e implementar las políticas y procedimientos necesarios para administrar de manera adecuada y prudente los riesgos de tecnología de información, incidiendo en los procesos críticos asociados a dicho riesgo, considerando las disposiciones contenidas en la presente norma, en el Reglamento, y en el Reglamento del Sistema de Control Interno aprobado mediante la Resolución SBS Nº 1040-99 del 26 de noviembre de 1999.

La administración de dicho riesgo debe permitir el adecuado cumplimiento de los siguientes criterios de control interno:

i. Eficacia. La información debe ser relevante y pertinente para los objetivos de negocio y ser entregada en una forma adecuada y oportuna conforme las necesidades de los diferentes niveles de decisión y operación de la empresa.
ii. Eficiencia. La información debe ser producida y entregada de forma productiva y económica.
iii. Confidencialidad. La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
iv. Integridad. La información debe ser completa, exacta y válida.
v. Disponibilidad. La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.
vi. Cumplimiento normativo. La información debe cumplir con los criterios y estándares internos de la empresa, las regulaciones definidas externamente por el marco legal aplicable y las correspondientes entidades reguladoras, así como los contenidos de los contratos pertinentes.

Estructura organizacional y procedimientos

Artículo 4°.- Las empresas deben definir y mantener una estructura organizacional y procedimientos que les permita administrar adecuadamente los riesgos asociados a la tecnología de información, consistente con su tamaño y naturaleza, asi como con la complejidad de las operaciones que realizan.

Administración de la seguridad de información

Artículo 5º.- Las empresas deberán establecer, mantener y documentar un sistema de administración de la seguridad de la información, en adelante "Plan de Seguridad de la información - (PSI)". El PSI debe incluir los activos de tecnología que deben ser protegidos, la metodología usada, los objetivos de control y controles, así como el grado de seguridad requerido.

Las actividades mínimas que deben desarrollarse para implementar el PSI, son las siguientes:

a. Definición de una política de seguridad.
b. Evaluación de riesgos de seguridad a los que está expuesta la información
c. Selección de controles y objetivos de control para reducir, eliminar o evitar los riesgos identificados, indicando las razones de su inclusión o exclusión.
d. Plan de implementación de los controles y procedimientos de revisión periódicos.
e. Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoria.

Las empresas bancarias y las empresas de operaciones múltiples que accedan al módulo 3 de operaciones a que se refiere el artículo 290º de la Ley General deberán contar con una función de seguridad a dedicación exclusiva.

Subcontratación (outsourcing)

Artículo 6º.- La empresa es responsable y debe verificar que se mantengan las características de seguridad de la información contempladas en la presente norma, incluso cuando ciertas funciones o procesos críticos puedan ser objeto de una subcontratación. Para ello se tendrá en cuenta lo dispuesto en la Primera Disposición Final y Transitoria del Reglamento. Asimismo, la empresa debe asegurarse y verificar que el proveedor del servicio sea capaz de aislar el procesamiento y la información objeto de la subcontratación, en todo momento y bajo cualquier circunstancia.

En caso que las empresas deseen realizar su procesamiento principal en el exterior, requerirán de la autorización previa y expresa de esta Superintendencia. Las empresas que a la fecha de vigencia de la presente norma se encontrasen en la situación antes señalada, deberán solicitar la autorización correspondiente. Para la evaluación de estas autorizaciones, las empresas deberán presentar documentación que sustente lo siguiente:

a) La forma en que la empresa asegurará el cumplimiento de la presente circular y la Primera Disposición Final y Transitoria del Reglamento.

b) La empresa, así como los representantes de quienes brindarán el servicio de procesamiento en el exterior, deberán asegurar adecuado acceso a la información con fines de supervisión, en tiempos razonables y a solo requerimiento.

Aspectos de la seguridad de información

Artículo 7°.- Para la administración de la seguridad de la información, las empresas deberán tomar en consideración los siguientes aspectos:

7.1 Seguridad lógica

Las empresas deben definir una política para el control de accesos, que incluya los criterios para la concesión y administración de los accesos a los sistemas de información, redes y sistemas operativos, así como los derechos y atributos que se confieren.

Entre otros aspectos, debe contemplarse lo siguiente:

a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios. Revisiones periódicas deben efectuarse sobre los derechos concedidos a los usuarios.
b) Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.
c) Controles especiales sobre utilidades del sistema y herramientas de auditoria.
d) Seguimiento sobre el acceso y uso de los sistemas y otras instalaciones físicas, para detectar actividades no autorizadas.
e) Usuarios remotos y computación móvil.

7.2 Seguridad de personal

Las empresas deben definir procedimientos para reducir los riesgos asociados al error humano , robo, fraude o mal uso de activos, vinculados al riesgo de tecnología de información. Al establecer estos procedimientos, deberá tomarse en consideración, entre otros aspectos, la definición de roles y responsabilidades establecidos sobre la seguridad de información, verificación de antecedentes, políticas de rotación y vacaciones, y entrenamiento.

7.3 Seguridad física y ambiental

Las empresas deben definir controles físicos al acceso, daño o interceptación de información. El alcance incluirá las instalaciones físicas, áreas de trabajo, equipamiento, cableado, entre otros bienes físicos susceptibles a riesgos de seguridad.

Se definirán medidas adicionales para las áreas de trabajo con necesidades especiales de seguridad, como los centros de procesamiento, entre otras zonas en que se maneje información que requiera de alto nivel de protección.

7.4 Clasificación de seguridad

Las empresas deben realizar un inventario periódico de activos asociados a la tecnología de información que tenga por objetivo proveer la base para una posterior clasificación de seguridad de dichos activos. Esta clasificación debe indicar el nivel de riesgo existente para la empresa en caso de falla sobre la seguridad, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.

Administración de las operaciones y comunicaciones

Artículo 8º.- Las empresas deben establecer medidas de administración de las operaciones y comunicaciones que entre otros aspectos contendrán lo siguiente:

- Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.
- Control sobre los cambios del ambiente de desarrollo al de producción.
- Separación de funciones para reducir el riesgo de error o fraude.
- Separación del ambiente de producción y el de desarrollo.
- Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.
- Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.
- Seguridad sobre correo electrónico.
- Seguridad sobre banca electrónica.

Desarrollo y mantenimiento de sistemas informáticos - Requerimientos de seguridad

Artículo 9º.- Para la administración de la seguridad en el desarrollo y mantenimiento de sistemas informáticos, se debe tomar en cuenta, entre otros, los siguientes criterios:

a) Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.
b) Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.
c) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.
d) Controlar el acceso a las librerías de programas fuente .
e) Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.

Procedimientos de respaldo

Artículo 10º.- Las empresas deben establecer procedimientos de respaldo regulares y periódicamente validados. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con lo requerido en el Plan de Continuidad.

La empresa debe conservar la información de respaldo y los procedimientos de restauración en una ubicación remota, a suficiente distancia para no verse comprometida ante un daño en el centro principal de procesamiento.

Planeamiento para la continuidad de negocios

Artículo 11º.- Las empresas, bajo responsabilidad de la Gerencia y el Directorio, deben desarrollar y mantener un "Plan de Continuidad de Negocios" (PCN), que tendrá como objetivo asegurar un nivel aceptable de operatividad de los procesos críticos, ante fallas mayores internas o externas.

Criterios para el diseño e implementación del Plan de Continuidad de Negocios

Artículo 12º.- Para el desarrollo del PCN se debe realizar previamente una evaluación de riesgos asociados a la seguridad de la información. Culminada la evaluación, se desarrollarán sub-planes específicos para mantener o recuperar los procesos críticos de negocios ante fallas en sus activos, causadas por eventos internos (virus, errores no esperados en la implementación, otros), o externos (falla en las comunicaciones o energía, incendio, terremoto, proveedores, otros).

Prueba del Plan de Continuidad de Negocios

Artículo 13º.- La prueba del PCN es una herramienta de la dirección para controlar los riesgos sobre la continuidad de operación y sobre la disponibilidad de la información, por lo que la secuencia, frecuencia y profundidad de la prueba del PCN, deberá responder a la evaluación formal y prudente que sobre dicho riesgo realice cada empresa.

En todos los casos, mediante una única prueba o una secuencia de ellas, según lo considere adecuado cada empresa de acuerdo a su evaluación de riesgos, los principales aspectos del PCN deberán ser probados cuando menos cada dos años.

Anualmente, dentro del primer mes del ejercicio, se enviará a la Superintendencia el programa de pruebas correspondiente, en que se indicará las actividades a realizar durante el ciclo de 2 años y una descripción de los objetivos a alcanzar en el año que se inicia.

Cumplimiento normativo

Artículo 14º.- La empresa deberá asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.

Privacidad de la información

Artículo 15º .- Las empresas deben adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme la normatividad vigente sobre la materia.

Auditoría Interna y Externa

Artículo 16º.- La Unidad de Auditoría Interna deberá incorporar en su Plan Anual de Trabajo la evaluación del cumplimiento de lo dispuesto en la presente norma.

Asimismo, las Sociedades de Auditoría Externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la entidad cuenta con políticas y procedimientos para la administración de los riesgos de tecnología de información, considerando asimismo, el cumplimiento de lo dispuesto en la presente norma.

Auditoría de sistemas

Artículo 17º.- Las empresas bancarias y aquellas empresas autorizadas a operar en el Módulo 3 conforme lo señalado en el artículo 290° de la Ley General, deberán contar con un servicio permanente de auditoría de sistemas, que colaborará con la Auditoría interna en la verificación del cumplimiento de los criterios de control interno para las tecnologías de información, así como en el desarrollo del Plan de Auditoría.

El citado servicio de auditoría de sistemas tomará en cuenta, cuando parte del procesamiento u otras funciones sean realizadas por terceros, que es necesario conducir su revisión con los mismos estándares exigidos a la empresa, por lo que tomará en cuenta las disposiciones indicadas en la Primera Disposición Final y Transitoria del Reglamento.

Las empresas autorizadas para operar en otros módulos, para la verificación del cumplimiento antes señalado, deberán asegurar una combinación apropiada de auditoría interna y/o externa, compatible con el nivel de complejidad y perfil de riesgo de la empresa. La Superintendencia dispondrá un tratamiento similar a las empresas pertenecientes al módulo 3, cuando a su criterio la complejidad de sus sistemas informáticos y su perfil de riesgo así lo amerite.

Información a la Superintendencia

Artículo 18°.- El informe anual que las empresas deben presentar a la Superintendencia, según lo dispuesto en el Artículo 13° del Reglamento, deberá incluir los riesgos de operación asociados a la

tecnología de información, como parte integral de dicha evaluación, para lo cual se sujetará a lo dispuesto en dicho Reglamento y a lo establecido en la presente norma.

Sanciones

Artículo 19°.- En caso de incumplimiento de las disposiciones contenidas en la presente norma, la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Plan de adecuación

Artículo 20°.- En el Plan de Adecuación señalado en el segundo párrafo de la Cuarta Disposición Final y Transitoria del Reglamento, las empresas deberán incluir un sub-plan para la adecuación a las disposiciones contenidas en la presente norma.

Plazo de adecuación

Artículo 21°.- Las empresas contarán con un plazo de adecuación a las disposiciones de la presente norma que vence el 30 de junio de 2003

Atentamente,

SOCORRO HEYSEN ZEGARRA
Superintendente de Banca y Seguros (e)

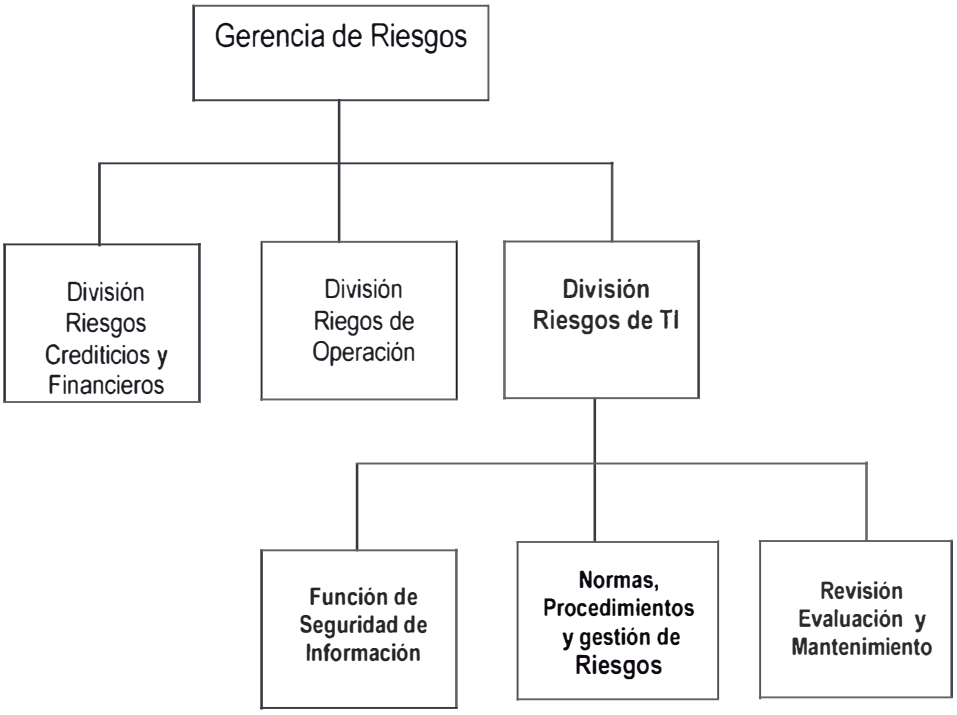
ANEXO 2

ESTRUCTURA ORGANIZACIONAL DEPARTAMENTO DE RIESGOS Y DIVISION DE RIESGOS DE TECNOLOGIA DE INFORMACION

Ubicación En La Empresa

En la Figura 1, se puede visualizar la ubicación actual de la División de Riesgos de Tecnología de Información en el Banco, dentro de la Gerencia de Riesgos, y se puede notar de igual modo la ubicación de la Función de Seguridad de Información.

Figura 1 : Estructura Organizacional



Descripción De Funciones

Función de Seguridad de Información (FSI)

Responsable de cumplir los requerimientos de la SBS con relación al diseño, desarrollo, implementación y seguimiento del Plan de Seguridad de Información y el Plan de Continuidad de Negocio. Asimismo corresponde la concientización y difusión de la función de seguridad de información en el Banco.

Normas Procedimientos Riesgos (NPR)

Establece normas, procedimientos, directivas. Participa en proyectos interdisciplinarios, encargado de la gestión del Plan de Seguridad y del Plan de Continuidad de Negocio, despliegue de estos a todo el Banco.

Revisión, Evaluación y Mantenimiento (REM)

Realiza la evaluación y el monitoreo de las actividades y procedimientos establecidos, para ello deberá gestionar los mecanismos apropiados para informar a la Alta Dirección y a las instancias que así lo requieran.

Funciones De La División De Riesgos De Tecnología De Información

- Elaborar y mantener las Políticas relacionadas a los Riesgos de Tecnología de Información.
- Definir, establecer e implementar metodologías relacionadas a la Gestión de Riesgos de Tecnología de Información.
- Recomendar alternativas de solución que permitan reducir los riesgos tecnológicos que puedan afectar los objetivos de negocio.
- Identificar los riesgos asociados a los procesos operativos del Banco que están en relación con sistemas, aplicativos y recursos de tecnología
- Definir, mantener y actualizar las políticas de seguridad relacionadas a tecnología de Información.
- Diseñar, desarrollar, implementar y verificar el cumplimiento del Plan de Seguridad de información.
- Diseñar, desarrollar y verificar el cumplimiento Plan de Continuidad de Negocios coordinando con las áreas ejecutoras lo relativo a la implementación del mismo y participando en las pruebas.
- Facilitar los reportes e informes de Administración y Control de Riesgos de Tecnología de Información, a Auditoria Interna, Externa y a Órganos reguladores, cuando así lo requieran.
- Comunicar y concientizar al personal del Banco sobre aspectos básicos asociados a riesgos en los procesos que tienen como soporte a tecnología de información y sobre la seguridad de información.
- Participar en el diseño de la arquitectura de seguridad y en los aspectos relacionados a la seguridad de la infraestructura tecnológica (equipos, sistemas, recursos, etc.).
- Participar en el comité de Riesgos.
- Monitorear de manera continua el cumplimiento de las Políticas de Seguridad y de los Controles propuestos a los Riesgos de T.I.
- Otras que sean delegadas por la Gerencia.