

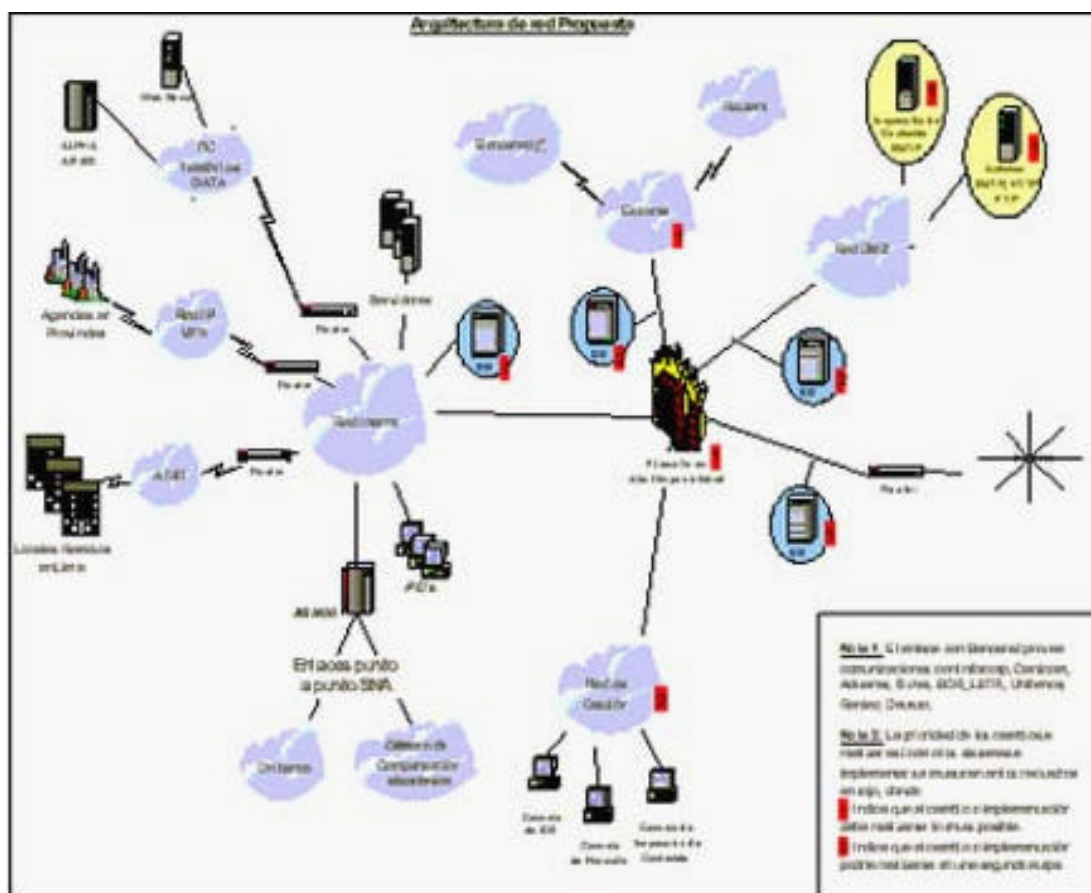
ANEXOS

A. DISEÑO DE ARQUITECTURA DE SEGURIDAD DE RED

ARQUITECTURA DE SEGURIDAD DE RED

Con el propósito de incrementar la seguridad de la plataforma tecnológica del Banco, se realizó un análisis de su actual arquitectura de red principalmente en el control de conexiones con redes externas. Producto de dicho análisis se diseñó una nueva arquitectura de red, la cual posee controles de acceso para las conexiones y la ubicación recomendada para los detectores de intrusos a ser implementados por el Banco.

A continuación se muestra el diagrama con la arquitectura de red propuesta.



Para lograr implementar esta arquitectura de red, se deben realizar un conjunto de cambios los cuales se detallan a continuación:

1. Creación de la Extranet: Controlar mediante un firewall la comunicación entre la red del Banco y redes externas como Banca Red y Reuters, para evitar actividad no autorizada desde dichas redes hacia los equipos de la red del Banco.
2. Implementar una red DMZ para evitar el ingreso de conexiones desde Internet hacia la red interna de datos. Adicionalmente implementar un sistema de inspección de contenido con el propósito de monitorear la información que es transmitida vía correo electrónico entre el Banco e Internet.

En la red DMZ se debe ubicar un servidor de inspección de contenido, el cual trabajaría de la siguiente manera:

- a. Ingreso de correo electrónico: El servidor de inspección de contenido, recibirá todos los correos enviados desde Internet, revisará su contenido y los enviará al servidor Lotus Notes, quién los entregará a su destinatario final.
- b. Salida de correo electrónico: El Servidor Lotus Notes enviará el correo electrónico al servidor de inspección de contenido, quién revisará el contenido del mensaje, para transmitirlo a través de Internet a su destino final.

Esta nueva red DMZ puede ser empleada para ubicar nuevos equipos que brindarán servicios a través de Internet en el futuro tales como FTP, Web, etc.

3. Para controlar el ingreso de virus informáticos desde Internet, así como para prevenir el envío de mensajes electrónicos conteniendo virus informático, se recomienda implementar un primer nivel de protección

antivirus mediante un sistema de inspección de servicios de Internet. Este sistema inspeccionará la información recibida desde Internet, así como la información enviada hacia otras entidades vía Internet. Este sistema debe inspeccionar la navegación de los usuarios (HTTP - HyperText Transfer Protocol), la transferencia de archivos (FTP – File Transfer Protocol) y el intercambio de correo electrónico (SMTP – Simple mail Transfer Protocol).

4. Luego de implementados los cambios previamente detallados, el Firewall se torna en un punto crítico para las comunicaciones del Banco, por lo cual se requiere implementar un sistema de Alta Disponibilidad de Firewalls, el cual permita garantizar que el canal de comunicación permanezca disponible en caso de falla de uno de los Firewalls.
5. Con el propósito de prevenir la realización de actividad no autorizada desde redes externas hacia la red del Banco y desde la red interna del Banco hacia los servidores y hacia Internet, se debe implementar un sistema de detección de intrusos que inspeccione el tráfico que circula por segmentos de red estratégicos tales como:
 - Internet, para detectar la actividad sospechosa proveniente desde Internet.
 - Red DMZ, para detectar la actividad dirigida contra los servidores públicos que logró atravesar el Firewall.
 - Extranet, para detectar actividad realizada desde las redes externas con las que se posee conexión.
 - Puntos estratégicos de la red interna, los cuales permitan detectar la actividad realizada contra los equipos críticos del Banco.

**B. CIRCULAR N° G-105-2002 PUBLICADA POR LA SUPERINTENDENCIA
DE BANCA Y SEGUROS (SBS) SOBRE RIESGOS DE TECNOLOGÍA DE
INFORMACIÓN**

Lima, 22 de febrero de 2002

CIRCULAR N° 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 349° de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley N° 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 10° del Reglamento para la Administración de los Riesgos de Operación, aprobado mediante la Resolución SBS N° 006-2002 del 4 de enero de 2002, esta Superintendencia ha considerado conveniente establecer las siguientes disposiciones:

Alcance

Artículo 1°.- 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 N° 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 4º.- 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, así 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 auditoría.

- 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 formativo

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.

Auditoria Interna y Externa

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

Asimismo, las Sociedades de Auditoria 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.

Auditoria de sistemas

Artículo 17º.- Las empresas bancarias y aquellas empresas autorizadas a operar en el Módulo 3 conforme lo señalado en el artículo 290º de la Ley General, deberán contar con un servicio permanente de auditoria de sistemas, que colaborará con la Auditoria 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 Auditoria.

El citado servicio de auditoria 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 auditoria 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 18º.- El informe anual que las empresas deben presentar a la Superintendencia, según lo dispuesto en el Artículo 13º 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)

C. DETALLE: DIAGNOSTICO DE LA SITUACION ACTUAL DE LA ADMINISTRACIÓN DE LOS RIESGOS DE TECNOLOGIA DE LA INFORMACION


La siguiente matriz muestra puntos específicos de la situación actual en cuanto a la administración de seguridad y los compara contra los requerimientos de la Circular G-105-2002 de la Superintendencia, contempla los siguientes aspectos:


1. Estructura de la organización de seguridad de la información
 - 1.1 Roles y responsabilidades
2. Plan de seguridad de la información
 - 2.1 Políticas, estándares y procedimientos de seguridad
 - 2.2 Seguridad lógica
 - 2.3 Seguridad de personal
 - 2.4 Seguridad física y ambiental
 - 2.5 Clasificación de seguridad
3. Administración de las operaciones y comunicaciones.
4. Desarrollo y mantenimiento de sistemas informáticos.
5. Procedimientos de respaldo.
6. Subcontratación (Relación y status de los contratos con terceros en temas críticos)
7. Cumplimiento normativo
8. Privacidad de la información
9. Auditoria interna y externa



El detalle de la evaluación de las áreas mencionadas se muestra en una matriz cuyo contenido es el siguiente:


- Situación Actual: Muestra un resumen de la situación encontrada en el Banco a partir de la información relevada durante las entrevistas y de los documentos entregados.
- Mejores Practicas: Muestra un resumen de las mejores prácticas en el sector y los requerimientos mencionadas en la Circular G105-2002 de la SBS uno de los motivos del presente trabajo.
- Análisis de Brecha: Muestra de manera gráfica la brecha existente entre la situación actual y los requerimientos de la SBS y las mejores prácticas del sector.


	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
1 ESTRUCTURA ORGANIZACIONAL PARA LA ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN			
1.	<p>El Banco cuenta con las siguientes unidades:</p> <p>División de Riesgo: Órgano dependiente de la Gerencia General, encargado de medir y controlar la calidad y capacidad de endeudamiento de los clientes, con el objeto de mantener adecuados niveles de riesgo crediticio, tanto para aquellos que se encuentren en evaluación, como aquellos que ya han sido utilizados y se encuentran en pleno proceso de cumplimiento de reembolsos. Asimismo, los riesgos denominados genéricamente Riesgos de Mercado. Cuenta con un departamento de Riesgos Operativos y Tecnológicos a cargo de la Srta. Patricia Pacheco.</p> <p>Area de Seguridad: Órgano encargado de velar por la seguridad de las instalaciones del Banco, así como del personal y Clientes que se</p>	<p>Se debería contemplar los siguientes aspectos:</p> <ul style="list-style-type: none"> - Definición y mantenimiento de una estructura organizacional que permita administrar adecuadamente los riesgos asociados a la tecnología de información. - La unidad de riesgo deberá contar con un responsable de la administración del riesgo de TI. - La responsabilidad de la seguridad de la Información debería ser ejercida de forma exclusiva. - El Departamento de Riesgos Operativos y Tecnológicos 	


	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
	<p>encuentran y transitan en ellas.</p> <p>Area de Seguridad Informática: Enfocada a los aspectos de accesos a los aplicativos y sistemas. Área que originalmente formo parte de Soporte Técnico (Agosto 2001). No considera en sus funciones las referentes a seguridad de la plataforma y de la información.</p> <p>Auditoria de Sistemas: Entre otras, sus funciones son las de:</p> <ul style="list-style-type: none"> - Efectuar evaluaciones periódicas de la capacidad y apropiada utilización de los recursos de cómputo. - Verificar el cumplimiento de las normas y procedimientos referidos a las Áreas de Desarrollo de Sistemas y Soporte Tecnológico, participando junto con estas instancias y los usuarios directos durante el ciclo de desarrollo de sistemas para la implantación de adecuados controles internos y pistas de auditoria, incluyendo su posterior evaluación y seguimiento. <p>Se ha observado que la documentación existente con respecto a las distintas áreas se encuentra desactualizada.</p> <p>No existe dentro de la estructura roles equivalentes al de Oficial de Seguridad.</p>	<p>debería contar con una estructura acorde con los riesgos de tecnología evaluados para Banco y definir indicadores que ayuden a monitorear los mismos.</p> <ul style="list-style-type: none"> - El Departamento de Riesgos Operativos y Tecnológicos debería definir los mencionados indicadores en conjunto con el área de sistemas del Banco. 	
2 PLAN DE SEGURIDAD DE LA INFORMACIÓN			

	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
2	El Banco no cuenta con un plan de Seguridad de la Información formalmente documentado que guíe las distintas normas con que cuenta el Banco referentes a los riesgos y seguridad de la Tecnología de Información.	<p>Se deberían contemplar los siguientes aspectos:</p> <ul style="list-style-type: none"> - Definición de una política de seguridad. - Evaluación de riesgos de seguridad a los que está expuesta la información. - Inventario de riesgos de seguridad de la información. - Selección de controles y objetivos de control para reducir, eliminar y evitar los riesgos identificados, indicando las razones de su inclusión o exclusión - Plan de implementación de los controles y procedimientos de revisión periódicos. - 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 de auditoría. 	
2.1 POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS DE SEGURIDAD			
2.1	El Banco no cuenta con políticas de seguridad formalmente documentadas que indiquen los procedimientos de seguridad a ser adoptados	<p>La definición de una política de seguridad debería contemplar:</p> <ul style="list-style-type: none"> - Declaración escrita de la 	


	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
	<p>para salvaguardar la información de posibles pérdidas en la integridad, disponibilidad y confidencialidad.</p> <p>Sin embargo, se ha observado la existencia de controles específicos en distintos aspectos de la seguridad de la Información, que detallamos a continuación.</p>	<p>política.</p> <ul style="list-style-type: none"> - Definición de la propiedad de la Política. - Políticas debidamente comunicadas. - Autoridad definida para realizar cambios en la Política. - Aprobación por el área legal. - Alineamiento de la política con la organización. - Definición de responsabilidades de la seguridad. - Confirmación de usuarios de conocimiento de la política. 	
2.2 SEGURIDAD LÓGICA			
2.2	<p>Hemos observado la existencia, entre otros aspectos, de:</p> <ul style="list-style-type: none"> - Procedimientos definidos en el área de sistemas para la concesión y administración de perfiles y accesos a usuarios, incluyendo la revocación y revisiones periódicas de los mismos. - Accesos a los sistemas de información del Banco controlados al nivel de red de datos y aplicación, para lo cual cada usuario cuenta con IDs y contraseñas de uso estrictamente personal y de responsabilidad de los usuarios. - Controles de acceso a herramientas de 	<p>La Seguridad Lógica debería contemplar los siguientes aspectos:</p> <ul style="list-style-type: none"> - Definición de procedimientos formales para la administración de perfiles y usuarios. - Identificación única de usuarios. - Controles sobre el uso de herramientas de auditoría y utilidades sensibles del sistema. - Controles sobre el acceso y uso de los sistemas y otras instalaciones físicas. 	

	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
	<p>auditoria en los sistemas de información.</p> <ul style="list-style-type: none"> - Controles de acceso parciales a utilidades sensibles del sistema. - Generación parcial de pistas de auditoria en los sistemas de información. <p>Hemos observado que no cuenta con:</p> <ul style="list-style-type: none"> - Controles de acceso a utilidades sensibles del sistema sobre estaciones de trabajo Win98/95. - Habilitación de opciones de auditoria en los sistemas operativos de red. - Procedimientos de revisión de pistas de auditoria que contemplen no solo los registros del computador central. 	<ul style="list-style-type: none"> - Controles sobre usuarios remotos y computación móvil. - Administración restringida de los equipos de acceso remoto y configuración de seguridad del mismo. 	
2.3 SEGURIDAD DE PERSONAL			
	<p>Hemos observado que el Banco se encuentra en un proceso de normalización llevado a cabo por el área de RRHH y la de OyM el cual incluye entre otros aspectos:</p> <ul style="list-style-type: none"> - Formalización de normas y procedimientos de las distintas áreas del Banco. - Identificación de información relevante a entregar a los nuevos trabajadores por área de trabajo. - Normalización de entrega de dicha información a los actuales trabajadores incluyendo documento de confirmación de conocimiento. 	<p>Se debería considerar:</p> <ul style="list-style-type: none"> - Procedimientos de revisión de datos en el proceso de selección de personal previo a su contratación (Ex. Referencias de carácter, verificación de estudios, revisión de crédito –si aplica- y revisión independiente de identidad) - Entrega formal de las políticas de manejo de información confidencial a los nuevos 	

	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
	Adicionalmente hemos observado que RRHH considera dentro del proceso de evaluación de personal nuevo, la verificación de distintos aspectos de personales a modo de preselección o filtro de personal idóneo para el Banco.	<p>integrantes del Banco.</p> <ul style="list-style-type: none"> - Definición apropiada de responsabilidad sobre la seguridad es parte de los términos y condiciones de la aceptación del empleo (ex. Términos en el contrato). - Difusión de las políticas con respecto al monitoreo de actividades en la red y sistemas de información, antes entregar IDs a usuarios. 	
2.4 SEGURIDAD FÍSICA Y AMBIENTAL			
	<p>Hemos observado la existencia, entre otros aspectos, de:</p> <ul style="list-style-type: none"> - Controles de acceso adecuados a sus activos físicos e instalaciones - Normas de control de acceso físico a áreas sensibles establecidos y en proceso de mejora en el caso de la oficina principal. - Monitoreo constante de las instalaciones del Banco. - Controles ambientales así como medidas preventivas y correctivas ante incendios. - Existen procedimientos definidos para el deshecho de papeles de trabajo. - Las copias de respaldo son almacenadas de manera segura. - Generadores de respaldo y UPS para red de 	<p>Se debería considerar los siguientes aspectos:</p> <p>Áreas seguras</p> <p>Procedimientos de reubicación de empleados</p> <ul style="list-style-type: none"> - Controles de áreas de carga y descarga. - Controles físicos de entrada. - Seguridad del perímetro físico de las instalaciones. - Procedimientos de Remoción o reubicación de activos. - Aseguramiento de oficinas, áreas de trabajo y facilidades. 	

	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
	<p>datos .</p> <p>Sin embargo encontramos deficiencias en los siguientes aspectos:</p> <ul style="list-style-type: none"> - Las medidas de seguridad existentes no se extienden a la Información como activo de valor del Banco y no existen normas adecuadas con respecto al resguardo de la misma cuando se trata de activos físicos (equipos o elementos de almacenamiento de información, documentos impresos, etc.). - No existe un programa de concientización para el usuario con respecto al cuidado necesario para con la información. - No existe una norma en uso sobre “mesas y pantallas limpias”. <p>El programa de mantenimiento preventivo de los equipos del Banco se encuentra incompleto al considerar únicamente al computador central.</p>	<p>Seguridad de Equipos</p> <p>Aseguramiento de Cableado</p> <ul style="list-style-type: none"> - Acciones y planes de mantenimiento de equipos <p>Protección de equipos</p> <p>Normas de seguridad para laptops.</p> <ul style="list-style-type: none"> - Fuentes de poder redundantes. - Procedimientos de eliminación o uso reiterado seguro de equipos de manera segura <p>Controles generales</p> <ul style="list-style-type: none"> - Política de “mesa limpia” - Política de “pantallas limpias” 	
2.5 CLASIFICACIÓN DE SEGURIDAD			
	<p>El Banco cuenta con inventarios de software, licencias y hardware razonablemente actualizados</p> <p>Sin embargo carece de inventarios de información, servicios y proveedores así como de una clasificación de los elementos mencionados con respecto a su nivel de riesgo dentro del Banco.</p>	<p>Se debería considerar los siguientes aspectos:</p> <ul style="list-style-type: none"> - Un catálogo de todos los activos físicos de la organización, indicando tipo de activo, ubicación física, responsable y nivel de criticidad. - Un catálogo de todos los activos de software tales como 	


	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
		<p>herramientas de desarrollo, aplicaciones, etc. Debe indicar entre otros, vendedor, ubicación lógica y física, responsable, nivel de criticidad, clasificación de la información, etc.</p> <ul style="list-style-type: none"> - Un catálogo o descripción de alto nivel de todos los activos de información mas importantes de la organización. Debe indicar información como tipo de data, ubicación lógica o física, responsable o dueño de la información, clasificación de la información y nivel de criticidad. - Un listado de todos los servicios tales como comunicaciones, cómputo, servicios generales, etc. y documentar la información relativa a los proveedores del servicio. Debería incluir entre otros, persona de contacto con el proveedor, procedimientos de servicios de emergencia, criticidad y unidades de negocio afectadas por el servicio. - Clasificación de los sistemas de información y/o grupos de 	

	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
		<p>data según su criticidad y sus características de confidencialidad, integridad y disponibilidad.</p> <ul style="list-style-type: none"> - Asignación de la responsabilidad de clasificación - Procedimientos de mantenimiento de la clasificación 	
3 ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES			
	<p>El Banco cuenta con:</p> <p>Procedimientos y responsabilidades de operación.</p> <ul style="list-style-type: none"> - Documentación no formalizada relativa a los procedimientos de operaciones en los sistemas de información - Procesos de revisión y reporte de conformidad de dichas operaciones. Controles establecidos relativos a cambios en los sistemas de información. <p>Control en cambios operacionales.</p> <ul style="list-style-type: none"> - Adecuada separación de las facilidades de los ambientes de producción y las de desarrollo. - Un Sistema a través del cual se administran las actividades de: <ul style="list-style-type: none"> - Cambios a los programas; - Pase a producción; y 	<p>Se deberían considerar los siguientes aspectos:</p> <p>Procedimientos y responsabilidades de operación.</p> <ul style="list-style-type: none"> - Documentación formal de todos los procedimientos de operación así como procedimientos y niveles de autorización definidos para su mantenimiento. - Programación de trabajos o procesos debe ser correctamente documentada, así como el resultado de dichas ejecuciones. <p>Administración de facilidades externas.</p> <ul style="list-style-type: none"> - Todo procesos realizado en o por un tercero, debe ser 	

	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
	<ul style="list-style-type: none"> - Administración de versiones - Adecuada segregación de funciones en labores de pase a producción de sistemas. - Limitación de operadores a través de menús de acceso. <p>Protección contra software malicioso.</p> <ul style="list-style-type: none"> - Controles de protección contra virus y software malicioso y procedimientos de revisión periódica del cumplimiento o efectividad de dichos controles, tanto por parte del área de sistemas como por parte del auditor de sistemas. <p>Segregación de funciones</p> <ul style="list-style-type: none"> - Todas las funciones mencionadas se mantienen independientes. Sin embargo, cabe mencionar que el actual Auditor de Sistemas del Banco perteneció al equipo de soporte del área de sistemas y mantiene acceso a datos de producción y desarrollo. Posee acceso también a la línea de comandos de ambos entornos. - Asimismo, eventualmente usuarios finales tienen acceso a la línea de comandos; restringida a tareas puntuales. No existe control formal sobre estas actividades. <p>Operaciones de verificación</p>	<p>evaluado con respecto a los riesgos y seguridad para desarrollar procedimientos que mitiguen dichos riesgos.</p> <p>Control en cambios operacionales.</p> <ul style="list-style-type: none"> - Todo cambio en la red de datos, incluyendo software, dispositivos, cableado o equipos de comunicación debe seguir procedimientos formales definidos y adecuadamente registrados. - Roles y responsabilidades deben ser claramente definidos y las funciones adecuadamente segregadas. - Los cambios deben ser adecuadamente aprobados. - Los resultados de todo cambio deben ser correctamente documentados. Roles y responsabilidades en las actividades de pase a producción correctamente definidos y segregados. - Adecuada separación de ambientes de producción y desarrollo. - Estándar de administración de 	


	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
	<ul style="list-style-type: none"> - Procedimientos de generación y almacenamiento de copias de contingencia definidos. - Se usan formatos de reporte de las actividades de operación y generación de copias de respaldo. <p>Administración de Red</p> <ul style="list-style-type: none"> - Se cuenta con un sistema Proxy y un filtro de paquetes como elementos de protección de red. No se cuenta con una DMZ ni con una arquitectura de seguridad red apropiada con respecto a la Internet. <p>Manipulación y seguridad de dispositivos de almacenamiento de información.</p> <ul style="list-style-type: none"> - Las copias de respaldo se encuentran en una localidad distinta y son aseguradas por un tercero. - No existen políticas con respecto al manejo de otros dispositivos de almacenamiento de información en el área de sistemas. <p>Intercambio de información y seguridad</p> <ul style="list-style-type: none"> - Controles y restricciones establecidas, no documentadas ni formalizados, respecto al uso del correo electrónico. 	<p>cambios definido, incluyendo cambios de emergencia.</p> <ul style="list-style-type: none"> - Control de accesos a escritura sobre sistemas en producción. <p>Administración de incidentes de seguridad.</p> <ul style="list-style-type: none"> - Definición de procedimientos y equipos de respuesta ante incidentes de seguridad. <p>Segregación de funciones.</p> <ul style="list-style-type: none"> - Las actividades de desarrollo, migración y operación de sistemas, así como las de administración de aplicaciones, helpdesk, administración de red y de IT deben ser correctamente segregadas. <p>Planeamiento de sistemas.</p> <ul style="list-style-type: none"> - Procedimientos formales definidos de planeamiento de recursos. <p>Protección contra software malicioso.</p> <ul style="list-style-type: none"> - Controles preventivos y detección sobre el uso de software de procedencia dudosa, virus, etc.). 	


	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
		<p>Operaciones de verificación</p> <ul style="list-style-type: none"> - Adecuado registro de fallas. - Adecuados procedimientos de generación de copias de respaldo. - Registros adecuados de todas las actividades de operación. <p>Administración de Red</p> <ul style="list-style-type: none"> - Adecuados controles de operación de red implementados. - Protección de la red y comunicaciones usando dispositivos de control de accesos, procedimientos y sistemas de monitoreo de red (Detección de intrusos) y procedimientos de reporte. <p>Manipulación y seguridad de dispositivos de almacenamiento de información.</p> <ul style="list-style-type: none"> - Aseguramiento sobre medios de almacenamiento y documentación de sistemas. <p>Intercambio de información (Correo electrónico y otros) y seguridad</p>	


	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
		<ul style="list-style-type: none"> - Controles de seguridad en el Correo electrónico y cualquier otro medio de transferencia de información (Ex. Normas, filtros, sistemas de protección contra virus, etc.). - Seguridad en la Banca Electrónica. 	
4 DESARROLLO Y MANTENIMIENTO			
	<p>El Banco cuenta con:</p> <ul style="list-style-type: none"> - Metodología de Desarrollo y Mantenimiento de Aplicaciones que especifica las siguientes actividades como tareas dentro de un proyecto: <ul style="list-style-type: none"> ▪ Definiciones ▪ Perfil ▪ Definiciones funcionales ▪ Especificaciones funcionales ▪ Diagrama de procesos ▪ Prototipo ▪ Plan de Trabajo ▪ Definiciones técnicas ▪ Diagrama de Contexto ▪ Diagrama de flujo de datos ▪ Modelo de datos ▪ Cartilla técnica ▪ Cartilla de operador ▪ Cartilla de usuario ▪ Pruebas y capacitación ▪ Acta de conformidad de pruebas 	<p>Se debería considerar lo siguiente:</p> <ul style="list-style-type: none"> - Contar con metodologías y estándares formales de desarrollo y mantenimiento de sistemas. - Los requerimientos deben ser definidos antes de la fase de diseño y se debe determinar un apropiado ambiente de control para la aplicación, estos requerimientos deben incluir: <ul style="list-style-type: none"> ▪ Control de acceso ▪ Autorización ▪ Criticidad del sistema ▪ Clasificación de la información ▪ Disponibilidad del sistema ▪ Integridad y confidencialidad de 	



	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
	<ul style="list-style-type: none"> ▪ Pase a producción - Las aplicaciones cuentan con controles de edición y cuando se requiere de controles en totales, cuadros, etc. Estos son generalmente definidos en las etapas de definición del proyecto por los responsables de las áreas usuarias y se deja documentado dichos requerimientos de control. - Procesos en lote ("batch") mantienen actividades iniciales que validan la información a procesar. Asimismo, para el caso específico de Lotes Contables, se valida la información inicial a procesar durante el día, para evitar se retrase el procesamiento por dicha actividad. - Rutinas de consistencia de información que se remite a otras entidades como COFIDE y SBS, realizadas a través de un sistema llamado SUCAVE. - Librerías de rutinas ya estandarizadas y revisadas para controles de fechas, campos numéricos y cadenas de caracteres, totales numéricos, cálculo de intereses, entre otros. Sin embargo, cabe señalar que en algunos casos estas rutinas se mantienen independientes en cada programa y no en una librería de rutinas que invoca todo programa que lo necesite. - Técnicas de encriptación para intercambio de información con Unibanca, con la Cámara de Compensación Electrónica y SUNAD 	<p>la información.</p> <ul style="list-style-type: none"> - Todas las aplicaciones deberán tener rutinas de validación de data. - Toda la data debe ser revisada periódicamente, a fin de detectar inexactitud, cambios no autorizados e integridad de la información. - Se deben definir controles para prevenir que la data se vea afectada por un mal procesamiento. - Se deben definir controles que permitan revisar toda información obtenida por un sistema de información, asegurando que sea completa, correcta y solo disponible para personal autorizado. - Uso de técnicas de encriptación estándar. - Controles para el acceso a las librerías de programa fuentes. - Mantener un estricto y formal control de cambios, que sea debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios. 	

	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
	<ul style="list-style-type: none"> - Entornos independientes de desarrollo y producción. - La metodología de desarrollo y mantenimiento de aplicaciones indica la necesidad de una actividad de prueba de los cambios y/o nuevos requerimientos; sin embargo, no existe procedimientos específicos definidos para la documentación de las pruebas realizadas ni para la conformidad de las mismas. <p>Cabe señalar que se mantiene versiones de los programas fuente y compilados en los entornos de Desarrollo y Producción. El sistema Fenix administra los cambios y versiones del entorno de desarrollo y la actualización en el entorno de producción se encuentra a cargo del Jefe de Soporte Técnico.</p> <p>Los estándares de mantenimiento y desarrollo no se encuentran completos.</p>	<ul style="list-style-type: none"> - Procedimientos formales y adecuados para las pruebas y reportes de las mismas. 	
5 PROCEDIMIENTOS DE RESPALDO			
	<p>Se cuenta con un procedimiento formalizado para el respaldo de información del computador central y de usuario final, este procedimiento establece:</p> <ul style="list-style-type: none"> - Para archivo de datos, se realiza con una frecuencia diaria, dos copias y tres generaciones. - Para software base, se realiza con una frecuencia diaria, dos copias y tres generaciones. 	<p>Los procedimientos de generación de copias de respaldo deberían contar con los siguientes controles clave:</p> <ul style="list-style-type: none"> - Aseguramiento de que el proceso de generación de copias de respaldo haya culminado exitosamente. - Procedimientos que 	



	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
	<ul style="list-style-type: none"> - Para los programas fuente, se realiza de forma diaria, una copia en tres generaciones. - Para la información de usuarios finales, se realiza de forma diaria, una copia en tres generaciones. <p>Todas las copias se guardan en la bóveda central del Banco y de forma mensual se remiten a almacenar en la empresa PROSEGUR.</p> <p>Se encuentra en proceso de definición un procedimiento de verificación de cintas, por la antigüedad de las mismas.</p> <p>Se mantiene información histórica desde el inicio de actividades del Banco.</p>	<p>contemplan pruebas periódicas de las copias de respaldo.</p> <ul style="list-style-type: none"> - El tiempo de almacenamiento de las copias de respaldo debe estar en concordancia con los requisitos legales y normativos vigentes. 	
	-	<p>Se debería considerar:</p> <ul style="list-style-type: none"> - Generación de Plan de Contingencias que abarque todos los procesos críticos del Banco y que se ha desarrollado siguiendo una metodología formal. - Procedimientos revisión periódica del plan. - Creación de un equipo para implementar el plan en el que todos los miembros conocen 	

	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
		<p>sus responsabilidades y cómo deben cumplir con las tareas asignadas.</p> <ul style="list-style-type: none"> - Existencia de preparativos adecuados para asegurarse de la continuidad del procesamiento computadorizado (existe centro de procesamiento alterno). - Una copia del plan de contingencias se almacena en una sede remota y será de fácil acceso en caso de que ocurriera cualquier forma de desastre. - Preparativos de contingencia para el hardware y software de comunicaciones y redes. - Realización periódica un back-up de los archivos de datos críticos, los sistemas y bibliotecas de programas almacenándolo en una sede remota cuyo tiempo de acceso sea adecuado. - Identificación del equipamiento requerido por los especialistas y se hicieron los preparativos para su reemplazo. 	
	-	Se debería considerar lo siguiente:	

	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
		<ul style="list-style-type: none"> - Revisión del impacto sobre el negocio, previo al diseño del Plan de continuidad de negocios, identificando las partes más expuestas a riesgo. - Realizar revisión del impacto en el negocio, estableciendo los procedimientos a seguirse en el caso de que ocurriera un desastre (por ej. Explosión, incendio, daño por tormenta, pérdida de personal clave) en cualquiera de las dependencias operativas de la organización. - Deberían existir planes de contingencia para cada recurso computadorizado. - El plan de contingencias debería contemplar las necesidades de los departamentos usuarios en términos de traslados, ubicación y operación. - El plan de contingencias debería asegurar que se observen normas de seguridad de información en caso de que ocurriera un desastre. - El cronograma para la recuperación de cada función debería ser revisado asegurando 	

	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
		que sea adecuado.	
		El plan de contingencias debería probarse periódicamente para asegurarse de que aún es viable y efectivo.	
6 SUBCONTRATACIÓN			
	<p>Encontramos que el Banco tiene principalmente, los siguientes servicios contratados:</p> <ul style="list-style-type: none"> - UNIBANCA: Procesamiento de transacciones de tarjetas (diario) - HERMES: Distribución de tarjetas de crédito y débito. Información necesaria y tarjetas recibidas de UNIBANCA. (diario) - NAPATEK: Impresión de estados de cuenta y "ensobrado". Recibe información vía una transferencia electrónica de archivos - "File Transfer" (mensual). - Rehder: Se transmite información de monto facturado por cada cliente (e-mail) para el seguro de desgravámenes (mensual). - TELEFONICA: Centro de procesamiento de datos de respaldo. Entrará en operatividad el 31 de Mayo. - PROSEGUR: Almacenamiento de copias de respaldo. <p>No se obtuvo información (contratos) relativa a los servicios prestados por UNIBANCA.</p>	<p>El plan de contingencias debe incluir la pérdida del servicio prestado por terceros.</p> <p>Los contratos de servicios con terceros deberían incluir entre otros aspectos, los siguientes:</p> <ul style="list-style-type: none"> - Requerimientos de seguridad y las acciones que se tomarán de no cumplirse el contrato. - Acuerdos de controles de seguridad y políticas a aplicarse para garantizar el cumplimiento de los requerimientos. - Determinación de los niveles de servicio requeridos (Service Level Agreements o SLA). - El derecho de la entidad, y la Superintendencia de Banca y Seguros, o las personas que ellos designen, de auditar el ambiente de la empresa que 	

	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
	El Banco no cuenta con un procedimiento definido para la inclusión de cláusulas relativas a la confidencialidad, niveles de servicio, etc., en los contratos de servicios prestados por terceros al Banco.	<p>brinda el servicio, para verificar los controles de seguridad aplicados a la data y los sistemas.</p> <ul style="list-style-type: none"> - Documentación sobre los controles físicos y lógicos, empleados por la empresa que brinda el servicio, para proteger la confidencialidad, integridad y disponibilidad de la información y equipos de la entidad. - Determinación de los requerimientos legales, incluyendo privacidad y protección de la data. - Procedimiento que asegure que la empresa que brinda el servicio realizará pruebas periódicas para mantener la seguridad de la data y los sistemas. - Cláusula sobre exclusividad de equipos que procesan información del Banco. 	
7 CUMPLIMIENTO NORMATIVO			
	<p>El Banco ha implementado controles para el cumplimiento normativo relativo al uso de software licenciado, tales como:</p> <ul style="list-style-type: none"> - Controles manuales periódicos por parte del área de sistemas y el área de auditoria de sistemas. 	<p>Se debería contar con:</p> <ul style="list-style-type: none"> - Definición de responsable del cumplimiento de las normas emitidas por la Superintendencia. 	

	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
	<ul style="list-style-type: none"> - Compromiso firmado por los usuarios referente al software autorizado, tipificando el incumplimiento como falta grave. - Evaluación de software para auditorías de software de forma automática. - La información, tanto física como digital es almacenada según períodos determinados por ley. - Existe un procedimiento de comunicación de las normas legales emitidas aplicables a las distintas áreas del Banco y el área de auditoría interna realiza labores de control con respecto a la implementación de dichas normas. <p>Sin embargo:</p> <ul style="list-style-type: none"> - No existe un responsable definido en la estructura del Banco encargado de mantener actualizada sobre las normas emitidas por organismos reguladores. 	<ul style="list-style-type: none"> - Procedimientos de control establecidos para el cumplimiento de las normas emitidas por la Superintendencia. - Control de cumplimiento de normas sobre la propiedad intelectual (licenciamiento de software). 	
8 PRIVACIDAD DE LA INFORMACIÓN			
	<p>El Banco no cuenta con:</p> <ul style="list-style-type: none"> - Un responsable asignado para la salvaguarda de la privacidad de la información. <p>Si bien durante las diversas charlas realizadas en los Comités se tocan temas referentes al secreto bancario, no se han implementado controles específicos en todas las áreas del Banco con el fin de evitar la exposición de información sensible</p>	<p>Se debería contar con:</p> <ul style="list-style-type: none"> - Definición de responsabilidades con respecto a la aplicación del secreto bancario y de la privacidad de la Información. - Restricciones de acceso a información en salvaguarda de su privacidad y del secreto bancario. 	

	Situación Actual	SBS, Mejores Prácticas	Análisis De Brecha
	<p>de los clientes y del Banco así como limitar el acceso del personal a dicha información.</p> <p>En el área de sistemas se han implementado controles respecto a la limitación de acceso a información de clientes y se ha registrado evidencia de incidentes y acciones tomadas por auditoría interna, dicha situación no se replica en las distintas áreas del Banco.</p>	<ul style="list-style-type: none"> - Existencia de autorizaciones internas para la entrega y transferencia de información. 	
9 AUDITORIA INTERNA Y EXTERNA			
	<p>El Banco no cuenta con:</p> <ul style="list-style-type: none"> - Un área de auditoría interna que esta incluyendo en su plan de auditoría el cumplimiento de lo dispuesto en la norma G-105-2002 de la Superintendencia. 	<p>Se debería considerar:</p> <ul style="list-style-type: none"> - La Unidad de Auditoría Interna deberá incorporar en su Plan Anual de Trabajo la evaluación del cumplimiento de lo dispuesto en la norma G-105-2002 de la Superintendencia. - 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. <p>El Banco deberá contar con un servicio permanente de auditoría de sistemas.</p>	