ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Desarrollo de un marco de control interno para la administración del riesgo operativo relacionado con la tecnología de información como modelo para el Banco CoopNacional S.A. en base a la norma ISO 17799"

TESIS DE GRADO

Previa a la obtención del Titulo de:

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

Presentado por:

Ricardo Arturo Salazar Almeida

Guayaquil-Ecuador

2013

AGRADECIMIENTO

A DIOS por permitirme culminar la tesis de una manera satisfactoria.

A mis padres y hermanos por poner su entera confianza en mi, aprendiendo de ellos que nada es imposible y que con perseverancia se llega a cumplir lo que deseamos.

A mi esposa Rosita por su paciencia, comprensión, preocupación y apoyo incondicional.

A mis hijos Keyla, Bianca y Ricardito por ser mi ayuda en todo momento

DEDICATORIA

A mis padres, por su comprensión, apoyo y consejos cada vez que los necesité.

A mis hermanos, por sus consejos que me orientaron a tomar las mejores decisiones.

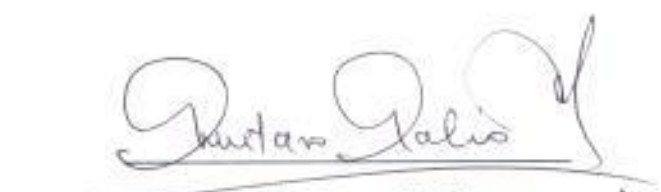
A mi esposa Rosita por su apoyo y amor.

A mis hijos Keyla, Bianca y Ricardito por ser mi ayuda en todo momento, las razones de mi vida.

TRIBUNAL DE GRADUACIÓN

Ing. Lenin Freire Cobo
DIRECTOR MSIG

Ing. Robert Andrade
DIRECTOR DE TESIS



Dr. Gustavo Galio
MIEMBRO SUPLENTE

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL."

(Reglamento de Graduación de la ESPOL.)

Ricardo Arturo Salazar Almeida

RESUMEN

El crecimiento acelerado que ha tenido el Banco CoopNacional S.A. la ha convertido en una institución financiera muy respetable y de amplia aceptación para muchos ciudadanos, quienes acuden a ellas en busca de un servicio de ahorro para sus recursos financieros y en la oportunidad de poder acceder a un crédito en forma oportuna y eficaz. Dicho crecimiento operacional y financiero ha significado también una expansión en su cobertura, productos y servicios mediante el uso de la tecnología y los sistemas de información.

Dicho uso creciente de la tecnología de información por parte del Banco CoopNacional S.A. conlleva también una mayor dependencia hacia ella y por lo tanto, los riesgos relacionados a la tecnología de información se transfieren a los procesos del negocio; lo cual, involucra una responsabilidad para la Alta Dirección respecto a la administración de los riesgos relacionados con la tecnología de información ya que el no hacerlo podría poner en riesgo la seguridad de uno de sus activos más importantes: la información; y, la continuidad de sus operaciones, acarreando incuantificables pérdidas financieras y hasta la desaparición de la Entidad.

Es por ello, que tanto organizaciones internacionales como gubernamentales de nuestro País han emitido una serie de normas, estándares y mejores prácticas que permitan al Banco CoopNacional S.A. poder hacer frente al desafío de lograr una adecuada administración de los procesos, las personas, la tecnología y los eventos externos en forma efectiva y sustentable, bajo un adecuado ambiente de control interno.

Por consiguiente, para el éxito dentro de la administración del riesgo tecnológico es necesario el liderazgo de la Alta Dirección y el compromiso de todos quienes conforman la Entidad hacia una cultura de

control interno y prevención del riesgo, basado en los diferentes lineamientos, marcos de referencia, estándares y regulaciones vigentes, adaptado a las necesidades y requerimientos de cada Entidad, buscando la seguridad de la información y la continuidad del negocio en forma sustentable, de tal manera, que se agregue valor y ventaja competitiva a las operaciones que realizan.

Es necesario que el Banco CoopNacional S.A. diseñe, implemente y mejore una metodología para la administración del riesgo operativo, considerando en forma especial el factor de la tecnología con la finalidad de mejorar la seguridad de la información y la continuidad de las operaciones, conscientes de la importancia que tiene la tecnología de información y el control interno dentro de la cadena de valor del negocio y en la estructura organizacional que la conforma.

Para una adecuada administración del riesgo existe una variedad de herramientas informáticas para dicho fin, de tal manera que se maximice el monitoreo y control de las operaciones, se mejore el control en el acceso a la información, se optimice la gestión de riesgos y auditoría interna y se proporcione información de calidad a la alta dirección para la toma oportuna de decisiones.

La presente tesis busca establecer un marco de control de gestión del riesgo operativo relacionado con la tecnología de información que sirva de guía para Directivos, Gerentes de TI, Auditores y Analistas de Riesgo en el desempeño de sus funciones dentro del gobierno y administración del riesgo tecnológico dentro del Banco CoopNacional S.A., tomando en consideración que se busca proteger los recursos financieros de los socios que han puesto su confianza en dicho sector financiero.

Índice General

Índice de Figuras

Índice de Tablas

ÍNDICE DE ABREVIATURAS

COBIT	Objetivos de Control para Tecnología de Información y Tecnologías relacionadas
DBA	Administrador de Bases de Datos
ISO	Organización Internacional de Normalización
COSO	Sponsoring Organizations of the Treadway Commission
BSI	Instituto Británico de Estandarización
SGSI	Sistema de Gestión de Seguridad de la Información
OHSAS	Requisitos de Sistema de Gestión de Seguridad y Salud
PDCA	Plan, Do, Check, Act – Planear Hacer Chequear Actuar
VPN	Virtual Private Network - Red Privada Virtual
ID	Identificación del Usuario
DPI	Derechos de Propiedad Intelectual
UPS	Uninterruptible Power Supply
TI	Tecnología de Información
SPARC	Scalable Processor ARChitecture
DVD	Disco de Video Digital
USB	Universal Serial Bus
PCI	Peripheral Component Interconnect
FBDIMMs	Fully Buffered DIMM – Son memorias DDR2 diseñadas para aplicarlas en Servidores
RoHS	Restriction of Hazardous Substances – Restricción de ciertas Sustancias Peligrosas
SATA	Serial Advanced Technology Attachment
VGA	Video Graphics Array

INTRODUCCIÓN

Luego de diversos eventos que ocurrieron hace casi una década, como los escándalos financieros que ocurrieron en Estados Unidos con las Instituciones Financieras y no Financieras que cotizaban en la Bolsa de Valores y la caída de las Torres Gemelas, a nivel mundial se formó una nueva corriente sobre la forma en que debe realizarse el Control Interno dentro de las Instituciones Financieras. Dicho Control Interno se basaba en el ***Riesgo***.

Riesgo es el daño potencial que puede surgir por un proceso presente o suceso futuro. El riesgo está latente en cualquier actividad que se realice sin que podamos determinar el momento de su ocurrencia pero sí tomar ciertas medidas preventivas para minimizar la probabilidad de ocurrencia y el impacto que esta pueda tener.

Las organizaciones sin importar su actividad se enfrentan constantemente a diversos tipos de riesgos con los cuales deben convivir, sin que exista un mecanismo 100% confiable que permita evitar dichos riesgos.

En el caso de las Instituciones Bancarias, el riesgo es parte integral dentro de las diversas operaciones que realizan, principalmente porque su materia prima fundamental es el dinero. El manejo del dinero proveniente de las captaciones es una responsabilidad demasiado alta para las instituciones financieras, debido a que para ellos representa la mayor parte de sus pasivos y deben tener la capacidad suficiente para poder almacenarlo, cuidarlo y después devolverlo a sus clientes.

En el Ecuador, luego del "remezón" que hubo a finales de los '90, durante la crisis financiera en el que muchos bancos cayeron, el sector financiero a base de confianza y apoyo al microcrédito comenzó a escalar considerablemente hasta posicionarse como una parte importante dentro de la masa monetaria circulante en el País.

Dicho crecimiento ha ocasionado que dichas instituciones incorporen dentro de sus procesos de negocio, dos componentes que para los bancos ya habían sido parte de su existir: la tecnología y la administración del riesgo.

Conscientes de la evolución de las Instituciones Bancarias, la Superintendencia de Bancos y Seguros comenzó a realizar controles más exhaustivos a las operaciones que estas realizaban y comenzó a delinear mecanismos de control básicos para gestionar su adecuado funcionamiento.

Poco a poco las Instituciones Bancarias dejaron de lado los procesos manuales y fueron incorporando diversas herramientas tecnológicas como bases de datos, computadores de última generación, redes privadas entre oficinas y hasta sistemas integrados de comunicaciones bancarias.

Por otro lado, la planificación y la toma de decisiones gerenciales que con muy buenos resultados, se basaba solamente en el manejo eficiente de la cartera y la liquidez, ahora debía considerar aspectos internos y externos que pudieran significar un riesgo. Es así, que aparecen dentro de la administración del riesgo: el riesgo de mercado, el riesgo de liquidez y el riesgo de crédito.

Sin embargo, ha surgido un nuevo componente dentro de la gestión del riesgo conocido como Riesgo Operacional, que busca minimizar el riesgo dentro de los diversos procesos y operaciones del negocio, enfocándose principalmente en la base donde se sustentan todos los procesos dentro de las Instituciones Bancarias: la tecnología.

La presente Tesis tiene como uno de sus objetivos específicos, estudiar la forma en que las Instituciones Bancarias han incorporado la tecnología dentro de sus procesos de negocio, la forma en que les ha permitido una

eficiente toma de decisiones y sobre todo la manera en que esto ha significado un mejor servicio para sus clientes.

Así mismo, se busca establecer los lineamientos básicos para una adecuada gestión de los recursos tecnológicos tomando en consideración el riesgo operativo, los estándares internacionales y la legislación vigente en el País, buscando interrelacionarlos y determinando los aspectos que son aplicables y que podrían ser incorporados por las Instituciones Bancarias.

Además, se buscará establecer los mecanismos de control, herramientas y recursos disponibles para uso de gerentes, directores de tecnología, responsables de seguridad y auditores dentro de un ambiente de procesamiento electrónico de datos dentro de las Instituciones Bancarias.

Por consiguiente, la presente Tesis podría convertirse en una referencia para los diversos sujetos dentro de los procesos de negocio de las Instituciones Bancarias para una segura, eficiente y confiable gestión de tecnología de información que permita el desarrollo operacional y financiero de dichas instituciones en forma sustentable.

CAPÍTULO 1.

GENERALIDADES

Capítulo 1.

Generalidades

1.1. Antecedentes

El crecimiento acelerado que ha tenido el Banco CoopNacional S.A. la ha convertido en una institución financiera muy respetable y de amplia aceptación para la ciudadanía. Este crecimiento operacional y financiero ha significado una expansión en su cobertura, productos y servicios mediante el uso de la tecnología y los sistemas de información.

El uso creciente de tecnología de información por parte del Banco CoopNacional S.A. conlleva a una mayor dependencia de la TI y por lo tanto, los riesgos relacionados se transfieren a los procesos del negocio; lo cual, involucra una responsabilidad para la Alta Dirección, respecto a la administración de los riesgos relacionados con la tecnología de información ya que el no hacerlo podría poner en riesgo la seguridad de sus activos más importantes: la información; y, la continuidad de las operaciones, acarreando incuantificables pérdidas financieras de la Entidad.

La presente tesis tiene como objetivo crear un marco de control interno para la administración del riesgo operativo, relacionado con la tecnología de información optimizando la seguridad de la información y la continuidad de las operaciones, conscientes de la importancia que tiene la tecnología de información y el control interno dentro de la cadena de valor del negocio y en su estructura organizacional.

1.2. Objetivos de la Tesis.

1.2.1. Objetivos generales.

Establecer los lineamientos de control para la Gestión Integral de Riesgos Tecnológicos y determinar la factibilidad de implementación de los controles de la gestión tecnológica bajo el marco de regulación de la norma ISO 17799.

1.2.2. Objetivos específicos.

a) Identificar el impacto que tienen los sistemas de información y su aprovechamiento dentro de sus operaciones así como en la toma de decisiones a nivel gerencial.
b) Analizar la forma en que el control interno interviene dentro de la gestión de tecnología de información.
c) Gestionar la evolución y aplicación de las normas y lineamientos sobre la gestión del riesgo operativo.
d) Establecer las diferentes variables que se debe considerar para la implementación de los controles tecnológicos.
e) Analizar la forma en que las herramientas informáticas apoyan en la gestión del riesgo operativo tecnológico.
f) Definir un Marco de Control Integral para la gestión del riesgo tecnológico dentro de las Instituciones Bancarias.

1.3. Misión.

Brindar al microempresario de Guayaquil y de los cantones aledaños financiamiento de forma oportuna, transparente, con respeto y disciplina apoyados en adecuadas tecnologías de información que permitan obtener una rentabilidad para los accionistas y un sueldo digno y justo para todo el personal, respetando y protegiendo al medio ambiente.

1.4. Visión.

Ser la primera y mejor opción de financiamiento que facilite el desarrollo económico y mejore la calidad de vida de nuestros clientes.

1.5. Descripción del problema.

El Banco CoopNacional S.A. actualmente realiza la administración del riesgo a nivel de Tecnología en Información. El objetivo de esta tesis es identificar los riesgos que se presentan en los procesos de Tecnología de Información, para que a través del análisis y de la evaluación de los mismos, se optimicen los controles actuales que llegue a reducir o mitigar estos riesgos inherentes.

1.6. Características.

La principal característica del proyecto es la minimización del riesgo de tecnología de información estableciendo un correcto marco de control el cual se maneja en los siguientes puntos:

a) Analizar y evaluar los riesgos.
b) Asegurar la integridad, disponibilidad y confidencialidad de la información ingresada, procesada, almacenada y generada.
c) Aplicar las medidas preventivas y correctivas de gestión de replicación y respaldos.
d) Gestionar de forma segura el Control de Acceso y cambios en los ambientes de desarrollo y pruebas.

1.7. Alcance.

Gestionar el riesgo operativo en el área de Tecnología de Información definiendo un marco general de control para la minimización de los riesgos a

través de directrices, políticas y procedimientos aplicables a toda la organización, optimizando los procesos internos del Banco así como el establecimiento los controles de seguridad de información en todas las áreas de la institución.

1.8. Controles.

El Banco CoopNacional S.A. actualmente maneja diferentes controles de tecnología de información que permite la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitando la interrupción del negocio y logrando que la información sea integra, confidencial y esté disponible para una apropiada toma de decisiones.

El principal control que se usará en esta tesis se encuentra basado en las mejores prácticas de la Norma ISO 17799 que incluye los siguientes puntos:

1.8.1. Gestionar que la administración de la tecnología de información soporte adecuadamente los requerimientos de operación actuales y futuros de la entidad.

a) Crear un plan integral de tecnología de la información alineado con el plan estratégico institucional.
b) Crear un plan operativo que establezca las actividades a ejecutar en el corto plazo (un año), de manera que se asegure el logro de los objetivos institucionales propuestos.
c) Tener una adecuada tecnología de información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la institución.
d) Definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos.
e) Definir bajo la aplicación de estándares, las políticas, procesos y procedimientos de tecnología de información.

f) Difundir y comunicar al personal involucrado en las políticas, procesos y procedimientos, de tal forma que se asegure su implementación.

g) Capacitar al personal del área de tecnología de información y a los usuarios de la misma.

1.8.2. Definir políticas que permitan que las operaciones de tecnología de información satisfagan los requerimientos de la entidad.

a) Crear y actualizar los manuales o reglamentos internos, debidamente aprobados por el directorio u organismo que haga sus veces, que establezcan como mínimo las responsabilidades y procedimientos para la operación, el uso de las instalaciones de procesamiento de información y respuestas a incidentes de tecnología de información.

1.8.3. Administrar los recursos y servicios provistos por terceros, cumpliendo con responsabilidades claramente definidas y que estén sometidas a un monitoreo de su eficiencia y efectividad.

a) Definir la propiedad de la información de las aplicaciones; y, la responsabilidad de la empresa proveedora de la información.

b) Definir los requerimientos contractuales convenidos que establezcan que las aplicaciones sean parametrizables, que exista una transferencia del conocimiento y que se entregue documentación técnica y de usuario, a fin de reducir la dependencia de las instituciones controladas con proveedores externos y los eventos de riesgo operativo que esto origina.

1.8.4. Con el objeto de administrar la continuidad de las operaciones, las instituciones controladas deben contar al menos con lo siguiente.

a) Establecer políticas y procedimientos de respaldo de información periódicos, que aseguren al menos que la información crítica pueda

ser recuperada en caso de falla de las tecnologías de la información, o con posterioridad, a un evento inesperado.

b) Manejar los respaldos y procedimientos de restauración de base de datos en una ubicación remota, a una distancia adecuada que garantice su disponibilidad ante eventos de desastre en el centro principal de procesamiento.

1.8.5. Apoyar en el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones para que satisfagan los objetivos del negocio.

a) Establecer una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados.

b) Administrar una documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución.

c) Establecer controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción.

d) Establecer controles que permitan asegurar que la calidad de la información sometida a migración, cumple con las características de integridad, disponibilidad y confidencialidad.

CAPÍTULO 2.

MARCO TEÓRICO

Capítulo 2.

Marco Teórico

2.1. Marco conceptual.

Las instituciones financieras, además de estar en permanente evolución y desarrollo, requieren estar acorde con las regulaciones legales y técnicas del entorno, deben implementar normas que les permita cumplir estos preceptos, y desarrollar controles para evitar quedarse rezagadas de las demás.

La información es vulnerable; puede perderse debido a fallas en elementos físicos, y ser afectada por virus informáticos, desastres naturales, etc.

La correcta aplicación de las Políticas de Seguridad de la Información mantiene la integridad, confidencialidad y disponibilidad de la misma; esta investigación, involucra un subconjunto de éstos lineamientos, que ayudan a establecer las Políticas de Seguridad de la Información.

2.2. Descripción de la norma ISO 17799.

Figura 2.1. Norma ISO 17799

La norma ISO 17799 es una guia de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a Seguridad de la Información. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. A continuación se presenta un resumen de la Norma.

2.2.1. Política de Seguridad.

2.2.1.1. Política de Seguridad de la Información.

2.2.1.1.1. Documento de la Política de Seguridad de la Información.

El documento de la Política de Seguridad de la Información enuncia el compromiso de la gerencia el cual maneja los siguientes puntos:

a) Una definición de la seguridad de la información, sus objetivos, alcance generales y la importancia.
b) La intención de la gerencia, sus objetivos y los principios de la Seguridad de la Información en línea con la estrategia y los objetivos comerciales.
c) Un marco referencial para establecer los objetivos de control y controles incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo.
d) Una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad.
e) Una definición de las responsabilidades generales y específicas para la gestión de la Seguridad de la Información incluyendo el

reporte de incidentes de Seguridad de la Información.

f) Referencias a la documentación que fundamente la política; por ejemplo, políticas y procedimientos de seguridad más detallados para sistemas de información específicos o reglas de seguridad que los usuarios debieran observar y cumplir.

2.2.1.1.2. Revisión de la Política de Seguridad de la Información.

Evaluar la Política de Seguridad de la Información a intervalos de tiempo planificados o cuando existen cambios significativos relacionados con la información, esta revisión debe estar enfocada al mejoramiento del documento.

2.2.2. Aspectos organizativos de la seguridad de la información.

2.2.2.1. Organización Interna.

La gerencia establece una gestión para iniciar y controlar la implementación de la Seguridad de la Información, aprobando la política de Seguridad de la Información, asignando las funciones de seguridad, coordinando y revisando la implementación de la seguridad en toda la organización.

2.2.2.1.1. Compromiso de la Dirección con la Seguridad de la Información.

La dirección apoya activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado y el

conocimiento de las responsabilidades de la Seguridad de la Información. Las responsabilidades se manejan través de un comité de dirección dedicado a esta labor.

2.2.2.1.2. Coordinación de la Seguridad de la Información.

Las actividades de la Seguridad de la Información son coordinadas por los representantes de todas las áreas de la organización, esta coordinación involucra la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad. La coordinación identifica la forma en que se manejan los incumplimientos, evalúa la efectividad de los controles para recomendar acciones para responder a incidentes identificados.

2.2.2.1.3. Asignación de Responsabilidades para la Seguridad de la Información.

La asignación de responsabilidades para la Seguridad de la Información se realiza de acuerdo con la política de Seguridad de la Información. Se definen claramente las responsabilidades para la protección de activos y para realizar procesos específicos de seguridad. Las personas con responsabilidades de seguridad asignadas delegan las labores de seguridad a otros; pero continúan siendo responsables en verificar la correcta ejecución de las tareas asignadas.

2.2.2.1.4. Proceso de Autorización para los Servicios de Procesamiento de Información.

Se recomienda tener en cuenta las siguientes directrices para el proceso de autorización:

a) Los servicios nuevos tendrán autorización de la dirección para el usuario apropiado, autorizando su propósito y uso.
b) Cuando sea necesario, tanto hardware como software serán verificados para asegurar que son compatibles con otros componentes del sistema;
c) Se identificarán e implementarán controles necesarios contra posibles vulnerabilidades introducidas por equipos personales tales como laptops, computadores domésticos y otros dispositivos manuales.

2.2.2.1.5. Acuerdos sobre confidencialidad.

Los acuerdos de confidencialidad abordan los requisitos para proteger la información confidencial. Se consideran los siguientes elementos para establecer los requisitos:

a) Definir la información que se ha de proteger (información confidencial)
b) Tiempo de duración esperada del acuerdo, incluyendo los casos en que puede ser necesario mantener la confidencialidad de manera indefinida.

c) Acciones requeridas cuando se termina un acuerdo.
d) Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información.
e) Propiedad de la información, secretos comerciales y propiedad intelectual y como se relaciona con la protección de la información confidencial.
f) Derecho de auditar y monitorear las actividades que involucran a la información confidencial.
g) Proceso para el reporte de divulgación no autorizada o violación de la información confidencial.
h) Términos para la devolución o la destrucción de la información al terminar el acuerdo.
i) Acciones esperadas a tomar en caso de incumplimiento de este acuerdo.

2.2.2.1.6. Contacto con las autoridades.

Las empresas tienen procedimientos que especifiquen cuándo y a través de qué autoridades una persona se contacta y la forma en que se reporta oportunamente los incidentes identificados de la Seguridad de la Información, o la sospecha de incumplimiento de la ley.

El contacto también implica relación con organismos de regulación, esto sirve para prepararse a los cambios futuros en la ley. Puede

también incluir los servicios públicos, servicios de emergencia, seguridad, entre otros.

2.2.2.1.7. Contactos con Grupos de Intereses Especiales.

La pertenencia a foros o grupos de intereses especiales, se constituyen en un medio para:

a) Renovar el conocimiento sobre la información referente a la seguridad.
b) Garantizar que la comprensión del entorno de Seguridad de la Información es actual y completa.
c) Recibir advertencias oportunas de alertas, avisos y parches relacionados con ataques y vulnerabilidades.
d) Obtener acceso a asesoría especializada sobre Seguridad de la Información.
e) Compartir información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.
f) Suministrar puntos adecuados de enlace cuando se trata de incidentes de Seguridad de la Información.

2.2.2.1.8. Revisión Independiente de la Seguridad de la Información.

Esta revisión es hecha por una persona ajena al área sometida a revisión; así se puede conseguir eficacia, idoneidad y propiedad del enfoque de la organización para la gestión de la Seguridad de la Información.

2.2.2.2. Terceros.

Cuando existe la necesidad de trabajar con partes externas que pueden requieren acceso a la información de la organización y a sus servicios de procesamiento de información, se realizará una evaluación de riesgos para determinar las implicaciones para la Seguridad de la Información y los requisitos de control. Los controles se definen en un convenio con la parte externa.

2.2.2.2.1. Identificación de los riesgos derivados del acceso de terceros.

Cuando existe la necesidad de permitir el acceso de una parte externa a los servicios de procesamiento de información o a la información de la organización, se llevará a cabo una evaluación de riesgos, para identificar los controles necesarios. Se considera:

a) Los servicios de procesamiento de información a los cuales requiere acceso la parte externa.
b) El tipo de acceso que tendrá la parte externa a la información y a los servicios de procesamiento de información (fisico, lógico o conexión de red).
c) El valor y la sensibilidad de la información involucrada.
d) Los controles necesarios para que información no autorizada no esté disponible para la parte externa.
e) La forma en que se puede identificar al personal autorizado a tener acceso, la manera

de verificar la autorización, y la forma de confirmar esta verificación.

f) Los medios y controles utilizados por la parte externa para almacenar, procesar, comunicar, compartir e intercambiar la información.
g) El impacto del acceso denegado a la parte externa cuando lo requiere y la recepción o el acceso de la parte externa a la información engañosa.
h) Los procedimientos para tratar los incidentes de Seguridad de la Información, los daños potenciales y las condiciones para la continuación del acceso de la parte externa.

2.2.2.2.2. Tratamiento de la seguridad en la relación con los clientes.

Los siguientes términos se consideran para abordar la seguridad antes de dar acceso a los clientes a cualquiera de los activos de la organización.

a) Protección de activos.
b) Descripción del producto o servicio a proveer.
c) Las diversas razones, requisitos y beneficios del acceso del cliente.
d) Política del control de acceso (uso de ID, contraseñas, privilegios, o revocar derechos).
e) Convenios para el reporte, la notificación y la investigación de las en exactitudes de la información (por ejemplo los datos personales de los clientes), incidentes y violaciones de la seguridad de la información.
f) Descripción de cada servicio disponible.

g) La meta del nivel de servicio y los niveles aceptables de servicio.
h) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.
i) Las respectivas responsabilidades civiles de la organización y del cliente.
j) Derechos de Propiedad Intelectual (DPI) y asignación de derechos de copia y la protección de cualquier trabajo en colaboración.

2.2.2.2.3. Tratamiento de la seguridad en contratos con terceros.

Se garantiza que no existen malos entendidos entra la organización y la tercera parte. Se recomienda tener en cuenta los siguientes puntos para la inclusión en el acuerdo con el objeto de cumplir los requisitos de seguridad identificados:

a) La política de Seguridad de la Información y los controles para asegurar la protección del activo.
b) Asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información.
c) Disposiciones para la transferencia del personal, cuando es apropiado.
d) Responsabilidades relacionadas con la instalación y mantenimiento del software y hardware.

e) La estructura clara y los formatos acordados para la presentación de los informes.
f) La política de control de acceso.
g) Disposiciones para la notificación y la investigación de incidentes, incumplimientos y violaciones de los requisitos establecidos en el acuerdo.
h) La descripción de cada servicio que va a estar disponible y los objetivos del servicio.
i) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.
j) El derecho a auditar las responsabilidades definidas en el acuerdo, a que dichas auditoria sean realizadas por una tercera parte y a enumerar los derechos estatutarios de los auditores.
k) El establecimiento de un proceso de escalada para la solución de problemas.
l) Los requisitos de la continuidad del servicio, incluyendo las medidas para la disponibilidad y confiabilidad, de acuerdo con las prioridades de negocio de la organización.
m) Las responsabilidades civiles correspondientes de las partes del acuerdo.
n) Los Derechos de Propiedad Intelectual (DPI) y la asignación de derechos de copia y la protección de cualquier trabajo en colaboración.
o) La participación de una tercera parte con los subcontratistas y los controles de seguridad que estos subcontratistas necesiten implementar.

p) Las condiciones para la regeneración / terminación del acuerdo.

2.2.3. Gestión de Activos

2.2.3.1. Responsabilidad sobre los activos.

Se identifica que los dueños para todos los activos y la asignación de la responsabilidad para el mantenimiento de los controles adecuados. La implementación de los controles específicos puede ser delegada por el dueño, pero éste sigue siendo responsable de la protección adecuada de los activos.

2.2.3.1.1. Inventario de activos.

La organización identifica todos los activos y documenta su importancia. El inventario de activos incluye toda la información necesaria para recuperarse de los desastres, incluyendo el tipo de activo, el formato, la ubicación, la información de soporte, la información sobre licencias y el valor para el negocio.

2.2.3.1.2. Propiedad de los activos.

El propietario del activo es responsable de:

a) Garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente.
b) Definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

2.2.3.1.3. Uso aceptable de los activos.

Los empleados, contratistas y usuarios de tercera parte que tienen acceso a los activos de la organización están conscientes de los límites que existen para el uso de los recursos de procesamiento de información y de cualquier uso efectuado bajo su responsabilidad.

2.2.3.2. Clasificación de la información.

La información se clasifica para indicar la necesidad, las prioridades y el grado esperado de protección. Es recomendable utilizar un esquema de clasificación para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas especiales en caso que sea necesario.

2.2.3.2.1. Directrices de clasificación.

Las directrices de clasificación incluyen convenciones para la clasificación inicial y la reclasificación con el paso del tiempo, de acuerdo con alguna política predeterminada de control de acceso. Es responsabilidad del propietario del activo definir la clasificación del activo, revisarlo periódicamente y asegurarse de que se mantiene actualizado y en el nivel adecuado.

2.2.3.2.2. Etiquetado y manipulado de la información.

Es necesario que los procedimientos para el etiquetado de la información comprendan los activos de información en formatos físico y

electrónico. El etiquetado reflejará la clasificación según las reglas y directrices establecidas. Para la manipulación de la información es recomendable definir los procedimientos de manejo, incluyendo procesamiento, almacenamiento, transmisión, desclasificación y destrucción seguros.

2.2.4. Seguridad ligada a los Recursos Humanos.

2.2.4.1. Antes del empleo.

Las responsabilidades de la seguridad se definen antes de iniciar la contratación laboral, describiendo adecuadamente el trabajo, los términos y condiciones del mismo. Los candidatos para el empleo, contratistas y usuarios de terceras partes se seleccionan adecuadamente en especial cuando se trata de trabajos que sean de mucha importancia para la empresa.

2.2.4.1.1. Funciones y responsabilidades.

Las funciones y responsabilidades incluyen los requisitos para:

a) Implementar y actuar de acuerdo con las políticas de Seguridad de la Información de la organización.
b) Proteger los activos contra acceso, divulgación, modificación, destrucción o interferencia no autorizados.
c) Ejecutar actividades particulares de seguridad.
d) Garantizar que se asigna la responsabilidad a la persona para que tome las acciones.
e) Informar los eventos de seguridad u otros riesgos de seguridad para la organización.

2.2.4.1.2. Investigación de antecedentes.

Para seguridad en la selección del personal se considera, siempre y cuando se autorice en la legislación, lo siguiente:

a) Referencias de comportamiento satisfactorio.
b) Verificación de la hoja de vida del candidato.
c) Verificación de las calificaciones profesionales y académicas declaradas.
d) Verificación de la identidad.
e) Verificación de los detalles adicionales tales como créditos o antecedentes criminales.

2.2.4.1.3. Términos y condiciones de contratación.

Los términos y condiciones laborales reflejan la política de seguridad de la organización, y tienen en cuenta elementos como:

a) Todos los empleados, contratistas y usuarios de terceras partes que tengan acceso a información sensible firman un acuerdo de confidencialidad antes de tener acceso a la información.
b) Los derechos y responsabilidades legales de los empleados, los contratistas y cualquier otro usuario, por ejemplo con respecto a las leyes de derechos de copio o la legislación sobre protección de datos.
c) Responsabilidades para la clasificación de la información y la gestión de los activos de

información manejados por el empleado, el contratista o el usuario de tercera parte.

d) Responsabilidades del empleado, el contratista o el usuario de tercera parte para el manejo de la información recibida de otras empresas o de partes externas.
e) Responsabilidades de la organización para el manejo de toda la información personal, durante el contrato laboral con la organización.
f) Responsabilidades que van más allá de las instalaciones de la organización y de las horas laborales, por ejemplo en el caso de trabajo en domicilio.
g) Acciones a tomar si el empleado, el contratista o el usuario de tercera parte hace caso omiso de requisitos de seguridad de la organización.

2.2.4.2. Durante el empleo.

Se concientiza, educa y forma a todos los empleados para que apliquen correctamente las políticas de Seguridad de la Información y utilicen correctamente los servicios de procesamiento de información para minimizar los posibles riesgos de seguridad. Es conveniente establecer un proceso disciplinario formal para el manejo de las violaciones de la seguridad.

2.2.4.2.1. Responsabilidades de la Dirección.

Las responsabilidades de la dirección velan que los empleados, los contratistas y los usuarios de terceras partes:

a) Estén adecuadamente informados sobre las funciones y responsabilidades respecto a la Seguridad de la Información antes de que se les otorgue acceso a la información.
b) Tengan las directrices para establecer las expectativas de seguridad de sus funciones dentro de la organización.
c) Estén motivados para cumplir las políticas de seguridad de la organización.
d) Logren un grado de concientización sobre la seguridad correspondiente a sus funciones y responsabilidades dentro de la organización.
e) Estén de acuerdo con los términos y las condiciones laborales, las cuales incluyen la política de Seguridad de la Información de la organización y los métodos apropiados de trabajo.
f) Sigan teniendo las calificaciones y las habilidades apropiadas.

2.2.4.2.2. Concienciación, formación y capacitación en seguridad de la información.

Se empieza con un proceso de introducción en el cual se presentan las políticas de seguridad de la organización y las expectativas, antes de otorgar el acceso a la información. En esta introducción se incluye puntos como requisitos de seguridad, controles, proceso disciplinario.

2.2.4.2.3. Proceso disciplinario.

El proceso disciplinario establece la imparcialidad y el tratamiento correcto para los

empleados de quienes se sospecha han cometido violaciones de la seguridad. El proceso disciplinario formal brinda una respuesta gradual, de tal forma que se sancione conforme a la mala conducta presentada y si es reiterado.

2.2.4.3. Cese del empleo o cambio de puesto de trabajo.

Se establece responsabilidades para asegurar la gestión de la salida de los empleados, contratistas o usuario de terceras partes de la organización y que se complete la devolución de todo el equipo y la cancelación de todos los derechos de acceso.

2.2.4.3.1. Responsabilidad del cese o cambio.

La comunicación de las responsabilidades en la terminación incluye las responsabilidades legales y las responsabilidades contenidas en cualquier acuerdo de confidencialidad, los términos y condiciones laborales continúan durante un periodo definido después de terminar la contratación laborar del empleado, el contratista o el usuario de terceras partes.

2.2.4.3.2. Devolución de activos.

Se tiene un proceso de terminación para incluir la devolución del software previamente publicado, los documentos corporativos, manuales y los equipos. También es necesaria la devolución de otros activos de la organización tales como dispositivos móviles, tarjetas de crédito, tarjetas de acceso, y la información almacenada en medios electrónicos.

2.2.4.3.3. Retirada de los derechos de acceso.

Después de la terminación del convenio con un empleado, se consideran los derechos de acceso de la persona a los activos asociados con la información y de ser necesario retirarlos. Si un empleado, contratista o usuario de terceras partes que se retira tiene contraseñas conocidas para permanecer activo, éstas deben ser cambiadas en la terminación o el cambio de empleado, contrato o acuerdo.

2.2.5. Seguridad Física y Ambiental.

2.2.5.1. Áreas seguras.

La información crítica para la empresa está ubicada en áreas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad y controles adecuados. Dichas áreas están protegidas físicamente contra acceso no autorizado, daño e interferencia.

2.2.5.1.1. Perímetro de seguridad física.

Para la seguridad se considera:

a) Definir claramente los perímetros de seguridad; la ubicación y las fortalezas de cada perímetro dependen de los requisitos de seguridad de los activos.
b) Los perímetros de un lugar con servicios de procesamiento de información son robustos físicamente; las paredes sólidas y puertas

externas tienen protección adecuada contra el acceso no autorizado; las puertas y ventanas están cerradas con llave cuando no están atendidas y se tiene presente la protección externa para las ventanas, en especial cuando se está a nivel del suelo.

c) Se establece un área de recepción con personal para controlar el acceso físico al lugar; el acceso debe estar permitido únicamente al personal autorizado.
d) Cuando sea posible se deberá construir barreras físicas par evitar el acceso no autorizado.
e) Las puertas de incendio en el perímetro de seguridad debe tener alarma y someterse a pruebas para establecer el grado requerido de resistencia según las normas nacionales e internacionales; funcionan de manera segura de acuerdo con el código local de incendios.
f) Si es posible se instalará sistemas adecuados de detección de intrusos y someterlos a pruebas regularmente.
g) Los servicios de procesamiento de información dirigidos por la organización debe estar físicamente separados de los dirigidos por terceras partes.

2.2.5.1.2. Controles físicos de entrada.

Tienen las siguientes directrices:

a) Registrar la fecha y la hora de entrada y salida de visitantes, todos los visitantes son

controlados, dar acceso para propósitos específicos y autorizados.

b) Controlar el acceso a áreas en donde se procesa o almacena información sensible y restringir el acceso a personas autorizadas; se podría utilizar controles de autenticación como las tarjetas de control de acceso.
c) Exigir a todos los empleados, contratistas y usuarios de terceras partes la utilización de alguna forma de identificación visible y notificar inmediatamente al personal de seguridad si se encuentran visitantes sin acompañante o sin identificación visible.
d) Dar acceso restringido al personal del servicio de soporte de terceras partes a las áreas seguras o a los servicios de procesamiento de información sensible únicamente cuando sea necesario.
e) Revisar y actualizar los derechos de acceso a áreas seguras n con regularidad y revocarlos cuando sea necesario.

2.2.5.1.3. Seguridad de oficinas, despachos e instalaciones.

Se recomienda tener en cuenta las siguientes directrices para la seguridad de oficinas, recintos y servicios.

a) Tener presente los reglamentos y las normas pertinentes a la seguridad y la salud.
b) Ubicar las instalaciones claves de modo que se evite el acceso al público.
c) Cuando sea viable, las edificaciones mantenerse discretas y no tener indicaciones

sobre su propósito, sin señales obvias que identifiquen la presencia de actividades de procesamiento de información.

d) Los directorios y los listados telefónicos internos indiquen las ubicaciones de los servicios de procesamiento de información sensible no ser de fácil acceso al público.

2.2.5.1.4. Protección contra las amenazas externas y de origen ambiental.

Se recomienda tener en mente las siguientes directrices para evitar daño debido a incendio, inundación, terremoto, explosión, malestar social, y otras formas de desastre natural o artificial.

a) Almacenar los materiales inflamables a una distancia prudente del área de seguridad.
b) Los equipos de respaldo (backup) y los medios de soporte de seguridad ubicarlos a una distancia prudente para evitar daño debido a algún desastre que afecte a las instalaciones principales.
c) Suministrar equipo apropiado contra incendios y ubicarlo adecuadamente.

2.2.5.1.5. Trabajo en áreas seguras.

Se deberá considerar las siguientes directrices:

a) El personal sólo conocerá la existencia del área segura según las necesidades de la empresa.

b) Se evitará el trabajo no supervisado en áreas seguras tanto por razones de seguridad como para evitar las oportunidades de actividades maliciosas.
c) Las áreas seguras vacías tendrán bloqueo físico y se revisarán periódicamente.
d) No se permitirá equipo de grabación fotográfica, de audio ni otro equipo de grabación como cámaras en dispositivos móviles, a menos que esté autorizado.

2.2.5.1.6. Áreas de acceso público y de carga y descarga.

Se recomienda considerar las siguientes directrices:

a) Restringir el acceso al área de despacho y carga desde el exterior de la edificación a personal identificado y autorizado.
b) El área de despacho y carga designar y diseñar para que los suministros se puedan descargar evitando que el personal de despacho tenga acceso a otras partes de la organización.
c) Las puertas externas del área de despacho y entrega estarán aseguradas mientras las puertas internas estén abiertas.
d) Inspeccionar el material que llega para determinar posibles amenazas antes de moverlo desde el área de despacho y carga hasta el punto de uso.
e) Registrar materias que llegan de acuerdo con los procedimientos de gestión de activos a su entrada al lugar.

f) Separar físicamente cuando se posible, los envíos entrantes y salientes.

2.2.5.2. Seguridad de los equipos.

La protección del equipo debe ser contra amenazas físicas y ambientales, esto ayuda a reducir el riesgo de acceso no autorizado a la información y para proteger contra pérdida o daño. También se considera la ubicación de los equipos.

2.2.5.2.1. Emplazamiento y protección de equipos.

Se recomienda considerar las siguientes directrices para la protección de los equipos:

a) Los equipos se deben ubicar de modo tal que se minimice el acceso innecesario a las áreas de trabajo.
b) Los servicios de procesamiento de información que se manejan datos sensibles, deben estar ubicados de tal forma que se reduzca el riesgo de visualización de la información por personas no autorizadas.
c) Los elementos que requieran protección especial deben estar aislados para reducir el nivel general de protección requerida de los demás elementos.
d) Se recomienda adoptar controles para minimizar el riesgo de amenazas físicas potenciales (robo, explosión, falla en el suministro de agua, polvo, vibración, efectos químicos, falla en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo)

e) Se deberá establecer directrices para comer, beber y fumar en las cercanías de los servicios de procesamiento de información.

f) Es conveniente monitorear las condiciones ambientales, para determinar las condiciones que podrían afectar adversamente el funcionamiento de los servicios de procesamiento de información.

g) Aplicar protección contra rayos a todas las edificaciones y adaptar filtros protectores a las fuentes de energía entrantes y a las líneas de comunicación.

h) Es recomendable considerar la utilización de métodos especiales de protección para equipos en ambientes industriales, tales como membranas para los teclados.

i) Los equipos de procesamiento de información sensible deben estar protegidos para minimizar el riesgo de fuga de información.

2.2.5.2.2. Instalaciones de suministro.

Todos los servicios de suministro, tales como electricidad, agua, alcantarillado, calefacción, ventilación y aire acondicionado deben ser adecuados para los sistemas a los que dan apoyo.

Se recomienda tener UPS para garantizar el funcionamiento de los servicios y equipos principales hasta que se pueda apagarlos normalmente; o de ser posible, un generador.

2.2.5.2.3. Seguridad del cableado.

Se recomienda tener en cuenta las siguientes directrices para la seguridad del cableado:

a) Las líneas de energía y de telecomunicaciones en los servicios de procesamiento de información deben ser subterráneas, o tener protección alterna adecuada.
b) El cableado de la red deberá estar protegido contra interceptación no autorizada o daño, por ejemplo utilizando conductos o evitando rutas a través de áreas públicas.
c) Los cables de energía deben estar separados de los cables de comunicaciones para evitar transferencia.
d) Se deben utilizar rótulos de equipo y de cables claramente identificables para minimizar los errores en las conexiones de cables.
e) Es recomendable emplear un plano del cableado par reducir la posibilidad de errores.
f) Para sistemas críticos se debe considerar la instalación de conductos blindados, uso de fibra, e inspecciones periódicas.

2.2.5.2.4. Mantenimiento de los equipos.

Se recomienda considerar las siguientes directrices para el mantenimiento de los equipos.

a) El mantenimiento de los equipos debe estar acorde con las especificaciones y los intervalos de servicio recomendados por el proveedor.

b) Solo personal autorizado deberá realizar las reparaciones y el mantenimiento e los equipos.
c) Se recomienda conservar el registro de todas las fallas y de todo el mantenimiento preventivo y correctivo.
d) Es recomendable implementar controles apropiados cuando se programa el mantenimiento para los equipos, si el mantenimiento lo realiza el personal dentro o fuera de la organización y la clase de información que tiene el equipo.
e) Se deben cumplir todos los requisitos impuestos por las pólizas de seguros.

2.2.5.2.5. Seguridad de los equipos fuera de las *instalaciones.*

Se recomienda tener en cuenta las siguientes directrices para la protección del equipo por fuera de las instalaciones:

a) El equipo y los medios llevados fuera de las instalaciones no se dejarán solos en sitios públicos, los computadores portátiles se llevarán como equipaje de mano y camuflado.
b) Se deben observar en todo momento las instrucciones del fabricante para la protección del equipo, por ejemplo, protección contra la exposición a campos electromagnéticos.
c) Se recomienda determinar controles para el trabajo que se realiza en casa mediante una evaluación de riesgos y controles adecuados, por ejemplo gabinetes de archivos con seguro, política de escritorio despejado, controles de

acceso a computadores y comunicaciones seguras.

d) Se deberá contratar un seguro para proteger el equipo fuera de las instalaciones.

2.2.5.2.6. Reutilización o retirada segura de equipos.

Los dispositivos que contienen información sensible se distribuyen fisicamente o su información se destruye o sobrescribe usando técnicas que permitan que la información original no se pueda recuperar.

2.2.5.2.7. Retirada de materiales propiedad de la empresa.

Se recomienda tener presentes las siguientes directrices:

a) Los empleados, contratistas y usuarios de terceras partes, que tenga autoridad para retirar activos deben estar claramente identificados.
b) Se recomienda establecer límites de tiempo para el retiro de equipos y verificar el cumplimiento en el momento de la devolución.
c) Se debe verificar que el equipo retirado ha sido devuelto.

2.2.6. Gestión de comunicaciones y operaciones.

2.2.6.1. Responsabilidades y procedimientos de operación.

Se establece todas las responsabilidades y los procedimientos para la gestión y operación de todos los servicios de procesamiento de información.

2.2.6.1.1. Documentación de los procedimientos de operación.

Los procedimientos de operación especifican las instrucciones para la ejecución detallada de cada trabajo, incluyendo:

a) Procesamiento y manejo de información.
b) Copias de respaldo.
c) Instrucciones para el manejo de errores y otras condiciones que se pueden presentar durante la ejecución del trabajo, incluyendo las restricciones al uso de las utilidades del sistema.
d) Contactos de soporte en caso de dificultades técnicas u operativas inesperadas.
e) Instrucciones del manejo de medios, informes especiales, incluyendo los procedimientos, para la eliminación segura de los informes de tareas fallidas.
f) Procedimientos para el reinicio y la recuperación del sistema que se ha de usar en caso de falla del sistema.
g) Gestión de los registros de auditoria y de la información de registro del sistema.

2.2.6.1.2. Gestión de cambios.

Los sistemas operativos y el software de aplicación están sujetos a un control estricto de la gestión del cambio; se considera los siguientes elementos:

a) Identificación y registro de los cambios significativos.
b) Planificación y pruebas de los cambios
c) Evaluación de los impactos potenciales de tales cambios, incluyendo los impactos de la seguridad.
d) Procedimiento de aprobación formal para los cambios propuestos.
e) Comunicación de los detalles del cambio a todas las personas implicadas.
f) Procedimientos de emergencia, incluyendo los procedimientos y las responsabilidades de cancelar o recuperarse de cambios fallidos y eventos imprevistos.

2.2.6.1.3. Segregación de tareas.

La distribución de funciones es un método pare reducir el riesgo de uso inadecuado deliberado o accidental del sistema. Se tiene cuidado de que ninguna persona pueda tener acceso, modificar o utilizar los activos sin autorización o sin ser detectado.

2.2.6.1.4. Separación de los recursos de desarrollo, prueba y operación.

Se debe tener presentes los siguientes elementos:

a) Se recomienda definir y documentar las reglas para la transferencia de software, desde el estado de desarrollo al operativo.
b) El software de desarrollo y el operativo se ejecutará en diferentes sistemas o procesadores de computación, dominios o directorios.
c) Los compiladores, editores, herramientas de desarrollo o utilidades del sistema no deben ser accesibles desde los sistemas operativos cuando no se requiera.
d) El ambiente del sistema de prueba debe emular al ambiente del sistema operativo lo más estrechamente posible.
e) Los usuarios deben emplear perfiles de usuario diferentes para los sistemas operativos y de prueba y los menús mostrar mensajes de identificación adecuados para reducir el riesgo de error.
f) Los datos sensibles no se deben copiar en el entorno del sistema de prueba.

2.2.6.2. Gestión de la provisión de servicios por terceros.

La organización verifica la implementación de acuerdos, monitorear el cumplimiento de ellos y gestionar los cambios para asegurar que los servicios que se prestan cumplen los requisitos acordados con los terceros.

2.2.6.2.1. Provisión de servicios.

La prestación de servicios por terceros incluye los acuerdos sobre disposiciones de seguridad, definiciones del servicio y aspectos de la gestión del mismo. En el caso de contrataciones externas, la organización debe planificar las transiciones necesarias (de información, servicios de procesamiento de información y todo lo demás que se deba transferir) y garantizar que la seguridad se mantiene durante todo el periodo de transición.

2.2.6.2.2. Supervisión y revisión de los servicios prestados por terceros.

El monitoreo y la revisión de los servicios por terceros permiten el cumplimiento de los términos y condiciones de Seguridad de la Información de los acuerdos y que los incidentes y problemas de la Seguridad de la Información se manejan adecuadamente. La organización dispone que el tercero asigne responsabilidades para la verificación del cumplimiento y la aplicación de los requisitos de los acuerdos. Los servicios, reportes y registros suministrados por terceras partes controlan y revisan con regularidad, las auditorías se llevan a cabo a intervalos regulares.

2.2.6.2.3. Gestión del cambio en los servicios prestados por terceros.

Es necesario que el proceso de gestión de los cambios en el servicio prestado por el tercero tome en consideración:

a) Los cambios hechos por la organización para implementar mejora en servicios tales como: desarrollo de aplicaciones nuevas, actualizaciones de la política, nuevos controles para mejorar la seguridad.
b) Cambios en los servicios por el tercero para implementar cambios en las redes, usar nuevas tecnologías, adquirir nuevos productos, nuevas herramientas de desarrollo, cambio en la ubicación física o cambio de proveedores.

2.2.6.3. Planificación y aceptación del sistema.

Se requieren planificación y preparación para garantizar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño requerido del sistema.

2.2.6.3.1. Gestión de capacidades.

Se recomienda monitorear y adaptar el sistema para garantizar y mejorar la capacidad y la eficacia de los sistemas. Se establecen controles de indagación para indicar los problemas en el momento oportuno. En las proyecciones de los requisitos de capacidad futura se consideran los negocios nuevos y los requisitos del sistema, así como las tendencias actuales y proyectadas en la

capacidad de procesamiento de información de la organización.

2.2.6.3.2. Aceptación del sistema.

Los requisitos para la aceptación de nuevos sistemas están definidos, acordados, documentados y probados claramente. Los nuevos sistemas de información, las actualizaciones, se migra a producción después de obtener la aceptación formal, en la que se consideran:

a) Requisitos de desempeño y capacidad de los computadores.
b) Procesos de reinicio y de recuperación por errores, y planes de contingencia.
c) Preparación y prueba de procedimientos operativos de rutina para las normas definidas.
d) Establecimiento del conjunto de controles de seguridad acordados.
e) Procedimientos manuales eficaces.
f) Disposiciones para la continuidad del negocio.
g) Evidencia de que la instalación del nuevo sistema no afectará a los sistemas inexistentes, en especial en horas pico.
h) Evidencia de que se ha tenido en cuenta el efecto del nuevo sistema en toda la seguridad de la organización.
i) Formación en la utilización de los sistemas nuevos.
j) Facilidad de uso, en la medida en que afecte el desempeño del usuario y evite el error humano.

2.2.6.4. Protección contra el código malicioso y descargable.

El software y los servicios de procesamiento de información son vulnerables a códigos maliciosos tales como virus de computador, caballos troyanos, gusanos electrónicos. Los usuarios son conscientes de los peligros de estas vulnerabilidades. Se introduce controles para evitar, detectar y retirar los códigos maliciosos de la organización.

2.2.6.4.1. Controles contra el código malicioso.

La protección contra códigos maliciosos se basa en software de detección y reparación de códigos maliciosos, acceso apropiado al sistema y controles en la gestión de cambios. Se recomienda considerar las siguientes directrices.

a) Establecer una política formal que prohíba el uso de software no autorizado.
b) Establecer una política formal para la protección contra los riesgos ligados con la obtención de archivos y software, indicando las medidas de protección a tomar.
c) Llevar a cabo revisiones regulares del software y del contenido de los sistemas que dan soporte a los procesos críticos del negocio; se investiga la presencia de archivos no aprobados o modificaciones no autorizadas.
d) Instalación y actualización del software de detección y reparación de códigos maliciosos para explorar los computadores y los medios.
e) Definir responsabilidades y procedimientos de gestión para tratar la protección contra códigos maliciosos en los sistemas.

f) Preparación de planes adecuados para la continuidad del negocio con el fin de recuperarse de los ataques de códigos maliciosos.
g) Implementación de procedimientos para recolectar información periódicamente, como la suscripción a sitios Web y listados de correo que suministren información sobre códigos maliciosos.
h) Implementación de procedimientos para verificar la información relacionada con códigos maliciosos y garantizar que los boletines de advertencia sean exactos e informativos.

2.2.6.4.2. Controles contra el código descargado en el cliente.

Se recomienda tener en cuenta las siguientes consideraciones para la protección contra códigos móviles que ejecutan acciones no autorizadas.

a) Ejecución de los códigos móviles en un entorno con aislamiento lógico.
b) Bloqueo de cualquier uso de códigos móviles.
c) Bloqueo de la recepción de códigos móviles.
d) Activación de medida técnicas en un sistema especifico para garantizar la gestión del código móvil.
e) Control de recursos disponibles para el acceso a códigos móviles.
f) Controles criptográficos para autenticar de forma única el código móvil.

2.2.6.5. Copias de seguridad.

Se establece procedimientos de rutina para implementar la política y la estrategia de respaldo, para hacer copias de seguridad de los datos y probar sus tiempos de restauración.

2.2.6.5.1. Copias de seguridad de la información.

Es conveniente disponer de servicios de respaldo adecuados para garantizar que la información y el software esenciales se recuperan después de un desastre o una falla de los medios, se recomienda considerar los siguientes elementos:

a) Es recomendable definir el nivel necesario para la información de respaldo.
b) Hacer registros exactos y completos de las copias de respaldo y generar procedimientos documentados de restauración.
c) Almacenar los respaldos en un sitio lejano, a una distancia suficiente para escapar a cualquier daño debido a desastres en la sede principal.
d) Dar un grado apropiado de protección física y ambiental a la información de respaldo.
e) Es conveniente probar con regularidad los medios de respaldo para garantizar que sean confiables para uso en emergencias.
f) Verificar y probar los procedimientos de restauración para garantizar su eficacia y que se pueden completar dentro del tiempo designado en los procedimientos para la recuperación.

g) En situaciones donde es importante la confidencialidad, los respaldos se protegen por medio de encriptación.

2.2.6.6. Gestión de la seguridad de las redes.

La gestión segura de las redes, las cuales pueden sobrepasar las fronteras de la organización, exige la consideración del flujo de datos, las implicaciones legales, el monitoreo y la protección.

2.2.6.6.1. Controles de red.

Se implementan controles que garanticen la Seguridad de la Información en las redes y la protección de los servicios conectados contra el acceso no autorizado. Es conveniente tener en cuenta los siguientes elementos:

a) La responsabilidad operativa de las redes se administra independientemente del área de operaciones de computador, según sea el caso.
b) Es necesario establecer las responsabilidades y los procedimientos para la gestión de equipos remotos, incluyendo los equipos en áreas de usuarios.
c) Es conveniente establecer controles especiales para mantener la confidencialidad y la integridad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y las aplicaciones conectadas.
d) Aplicar el registro y el monitoreo adecuados para permitir y registrar las acciones de seguridad pertinentes.

e) Se recomienda coordinar las actividades de gestión para optimizar el servicio para la organización y garantizar que los controles se aplican consistentemente en toda la infraestructura del procesamiento de información.

2.2.6.6.2. Seguridad de los servicios de red.

Determinar y monitorear periódicamente la capacidad del proveedor del servicio de red para gestionar los servicios acordados de forma segura.

2.2.6.7. Manipulación de los soportes.

Se establecen procedimientos operativos adecuados para proteger documentos, medios de computador, datos de entrada/salida y documentación del sistema contra divulgación, modificación, remoción y destrucción no autorizadas.

2.2.6.7.1. Gestión de soportes extraíbles.

Se recomienda tener presentes las siguientes directrices:

a) Si ya no son necesarios, los contenidos de los medios reutilizables que se van a retirar de la organización deben ser irrecuperables.
b) Cuando se necesario, se debe exigir autorización para los medios retirados de la organización y conservar un registro de tales retiros.
c) La información almacenada en los medios que debe estar disponible por un tiempo mayor al

del ciclo de la vida del medio, se debe almacenar en otra parte para evitar la pérdida de información, debido al deterioro de dichos medios.

d) La información almacenada en los medios que debe estar disponible por un tiempo mayor al del ciclo de vida del medio, deberá almacenarse en otra parte para evitar la pérdida de información, debido al deterioro de dichos medios.
e) Se deberá tener en cuenta el registro de los medios removibles para evitar la oportunidad de que se presenta pérdida de datos.
f) Las unidades de medios removibles solo se habilitarán si existen razones para hacerlo.

2.2.6.7.2. Retirada de soportes.

Los procedimientos formales para la eliminación segura de los medios, debe minimizar el riesgo de fuga de información sensible. Se recomienda tener en cuenta los siguientes elementos.

a) Los medios que contienen información sensible se deberá eliminar de forma segura, por ejemplo mediante incineración.
b) Establecer procedimientos para identificar los elementos que pueden requerir eliminación segura.
c) Puede ser más fácil disponer de todos los elementos de los medios de almacenamiento que serán recogidos y liberados de forma

segura, que tratar de disponer sólo de los elementos sensibles.

d) Muchas organizaciones ofrecen servicios de recolección y eliminación de equipos y medios; se debe tener cuidado en seleccionar un contratista idóneo con control y experiencia adecuados.

e) Se deberá registrar la eliminación de los elementos sensibles.

2.2.6.7.3. Procedimientos de manipulación de la información.

Se debe elaborar procedimientos para manejar, procesar, almacenar y comunicar la información de acuerdo con su clasificación. Se debe considerar los siguientes elementos:

a) Manejo y etiquetado de todos los medios hasta su nivel indicado de clasificación.

b) Restricciones de acceso para evitar el acceso de personal no autorizado.

c) Mantenimiento de un registro formal de los receptores autorizados de los datos.

d) Garantizar que los datos de entrada están completos, que el procesamiento se completa adecuadamente y que se aplica la validación de la salida.

e) Protección de los datos de la memoria temporal que esperan su ejecución.

f) Almacenamiento de los medios según las especificaciones del fabricante.

g) Mantenimiento de la distribución de datos en un mínimo.

h) Rotulado de todas las copias de los medios para la autenticación del receptor autorizado.
i) Revisión de las listas de distribución y las listas de receptores autorizados a intervalos regulares.

2.2.6.7.4. Seguridad de la documentación del sistema.

Para asegurar la documentación del sistema, se debe tener en cuenta los siguientes elementos:

a) La documentación del sistema se deben almacenar con seguridad.
b) La documentación del sistema en la red pública, que se suministra a través de una red pública, debe tener protección adecuada.

2.2.6.8. Intercambio de información.

Se establecen procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito y que se van a compartir.

2.2.6.8.1. Políticas y procedimientos de intercambio de información.

Los procedimientos y controles a seguir cuando se utilizan servicios de comunicación electrónica para el intercambio de información consideran los siguientes elementos:

a) Procedimientos para proteger la información intercambiada contra interceptación, copiado,

modificación, enrutamiento inadecuado y destrucción.

b) Procedimientos para detección y protección contra códigos maliciosos que se pueden transmitir con el uso de comunicaciones electrónicas.

c) Procedimientos para proteger la información electrónica sensible comunicada en forma de adjunto.

d) Directrices que enfaticen el uso aceptable de los servicios de comunicación electrónica.

e) Procedimientos para el uso de comunicaciones inalámbricas, pensando en los riesgos particulares involucrados.

f) Responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la organización.

g) Uso de técnicas criptográficas para proteger la confidencialidad, la integridad y la autenticidad de la información.

h) Directrices de retención y eliminación para toda la correspondencia, incluyendo mensajes, según la legislación y reglamentos locales y nacionales correspondientes.

i) No dejar información sensible en los dispositivos de impresión como copiadoras, impresoras y máquinas de facsímil.

j) Controles y restricciones asociados con el envío de servicios de comunicación, como el envío automático de correo electrónico a direcciones de correo externas.

k) No revelar información sensible.

l) No dejar mensajes que contengan información sensible en el contestador automático.

2.2.6.8.2. Acuerdos de intercambio.

En los acuerdos de intercambio de información se toman en consideración las siguientes condiciones de seguridad:

a) Responsabilidades de la dirección para controlar y notificar la transmisión, el despacho y la recepción.
b) Procedimientos para notificar a quién envía, la transmisión, el despacho y la recepción.
c) Procedimientos para garantizar la trazabilidad y el no-repudio.
d) Normas técnicas mínimas para el empaquetado y la transmisión.
e) Acuerdos de fideicomiso.
f) Normas para identificar los servicios de mensajería.
g) Responsabilidades y deberes en caso de incidentes de Seguridad de la Información, como pérdidas de datos.
h) Uso de sistemas acordados de etiquetado de la información, garantizando que el significado de las etiquetas se entienda inmediatamente y que la información está protegida adecuadamente.
i) Propiedad y responsabilidades para la protección de datos, derechos de copia, conformidad de las licencias de software.
j) Normas técnicas para registrar y leer la información y el software.

k) Todos los controles especiales que se puedan requerir para proteger los elementos sensibles tales como las claves criptográficas.

2.2.6.8.3. Soportes físicos en tránsito.

Se recomienda tener en cuenta las siguientes directrices para la protección de los medios que se transporta entre los lugares.

a) Se recomienda utilizar transporte confiable o servicios de mensajería.
b) Acordar con la dirección una lista de servicios de mensajería.
c) Desarrollar procedimientos para verificar la identificación de los servicios de mensajería.
d) El embalaje debe ser suficiente para proteger el contenido contra cualquier daño físico que se pueda producir durante el transporte, por ejemplo protección contra todos los factores ambientales que puedan reducir la eficacia de la restauración de los medios (datos del fabricante).
e) Cuando sea necesario, se debe adoptar controles para proteger la información sensible contra divulgación o modificación no autorizada.

2.2.6.8.4. Mensajería electrónica.

Las consideraciones de seguridad para la mensajería electrónica incluyen las siguientes:

a) Proteger los mensajes de los accesos no autorizados, modificación o negación de los servicios.
b) Garantizar que la dirección y el transporte del mensaje son correctos.
c) Confiabilidad general y disponibilidad del servicio.
d) Consideraciones legales como, por ejemplo, los requisitos para las firmas electrónicas.
e) Obtención de aprobación antes de utilizar servicios públicos externos como la mensajería instantánea o el compartir de archivos.
f) Niveles sólidos de autenticación que controlen el acceso desde redes accesibles al público.

2.2.6.8.5. Sistemas de información empresariales.

Se establece, desarrolla e implementa políticas para proteger la información asociada con los sistemas de información del negocio, las consideraciones de tales servicios para la seguridad y para el negocio incluye:

a) Vulnerabilidades conocidas en los sistemas administrativos y de contaduría en donde la información es compartida entre diferentes partes de la organización.
b) Vulnerabilidades de la información en los sistemas de comunicación del negocio, por ejemplo la grabación de llamadas telefónicas, almacenamiento de facsímiles, distribución del correo.
c) Políticas y controles adecuados para gestionar la forma en que se comparte la información.

d) Categorías excluyentes de información sensible, si los sistemas no brindan un nivel adecuado de protección.
e) Restricción del acceso a la información diaria, relacionada con individuos seleccionados, por ejemplo el personal de proyectos sensibles.
f) Categorías de personal, contratistas o socios del negocio a quienes se permite usar el sistema y los sitios desde los cuales pueden tener acceso.
g) Restricción de los servicios seleccionados para categorías de usuarios específicos.
h) Identificación del estado de los usuarios en los directorios para el beneficio de otros usuarios.
i) Retención y copias de respaldo de la información contenida en el sistema.
j) Requisitos y disposiciones para los recursos de emergencia.

2.2.6.9. Servicios de comercio electrónico.

Es necesario considerar las implicaciones de seguridad asociadas al uso de servicios de comercio electrónico, incluyendo las transacciones en linea y los requisitos para los controles. También se considerará la integridad y disponibilidad de la información publicada electrónicamente a través de sistemas disponibles al público.

2.2.6.9.1. Comercio electrónico.

Las consideraciones de seguridad para el comercio electrónico incluyen:

a) El nivel de confianza que exige cada parte en la identidad declarada de las otras partes, por ejemplo por medio de autenticación.
b) Los procesos de autorización asociados con la persona que puede emitir o firmar documentos comerciales clave.
c) La garantía de que los socios comerciales están totalmente informados sobre sus autorizaciones.
d) La determinación y el cumplimiento de los requisitos de confidencialidad, integridad, prueba de despacho y recibo de documentos clave, y el no repudio de contratos, por ejemplo los asociados a los procesos de licitación.
e) El nivel de confianza exigido en la integridad de las listas de precios publicadas.
f) La confidencialidad de datos o información sensible.
g) La confidencialidad e integridad de las transacciones de orden de compra, información sobre pagos, detalles de las direcciones de entrega y confirmación de recibo.
h) El grado adecuado de verificación para comprobar la información sobre pagos suministrada por un cliente.
i) La selección del mejor convenio sobre la forma de pago más apropiada para evitar el fraude.
j) El nivel de protección exigido para mantener la confidencialidad e integridad de la información de orden de compra.

k) Evitar la pérdida o duplicación de la información sobre transacciones.
l) La responsabilidad asociada con transacciones fraudulentas.
m) Los requisitos de las pólizas de seguros.

2.2.6.9.2. Transacciones en línea.

Las consideraciones de seguridad para las transacciones en línea incluyen las siguientes:

a) Uso de firmas electrónicas por cada una de las partes implicadas en la transacción.
b) Todos los aspectos de la transacción (credenciales, transacción confidencial, privacidad).
c) Encriptación de la ruta para las comunicaciones entre todas las partes involucradas.
d) Seguridad de los protocolos utilizados para la comunicación entre todas las partes involucradas.
e) Garantizar que el almacenamiento de los detalles de la transacción está fuera de cualquier entorno de acceso público (Intranet), y que no se retiene ni expone en un medio de almacenamiento accesible directamente desde Internet.
f) Cuando se emplea una autoridad confiable (por ejemplo firmas digitales y/o certificados digitales) la seguridad se integra a través de todo el proceso completo de gestión del certificado/firma.

2.2.6.9.3. Información públicamente disponible.

El software y otra información que requiera un nivel alto de integridad y que están en sistemas públicos se protegen con mecanismos apropiados como firmas digitales. Los sistemas de acceso público deben probar frente a debilidades y fallas antes de que la información esté disponible, también se debe asegurar que:

a) La información que se obtenga de conformidad con la legislación sobre la protección de datos.
b) La entrada de información hacia el sistema editorial se procese completa y exactamente de forma oportuna.
c) La información sensible estará protegida durante la recolección, el procesamiento y el almacenamiento.
d) El acceso al sistema editorial no permite acceso involuntario a redes a las cuales se conecta el sistema.

2.2.6.10. Supervisión.

Se debe monitorear los sistemas y registrar los eventos de Seguridad de la Información. Los registros de operador y la actividad de registro de fallas se utilizan para garantizar la identificación de los problemas del sistema de información.

2.2.6.10.1. Registros de auditoría.

Los registros para auditoría incluyen:

a) Identificación del usuario.
b) Fecha, hora y detalles de los eventos clave
c) Identidad o ubicación de la terminal
d) Registros de los intentos aceptados y rechazados de acceso al sistema.
e) Registros de los intentos aceptados y rechazados de acceso a los datos y otros recursos.
f) Cambios en la configuración del sistema.
g) Uso de privilegios.
h) Uso de las utilidades y aplicaciones del sistema.
i) Archivos a los que se ha tenido acceso y tipo de acceso.
j) Direcciones y protocolo de red.
k) Alarmas originadas por el sistema de control de acceso.
l) Activación y desactivación de los sistemas de protección, como los sistemas antivirus y los sistemas de detección de intrusión.

2.2.6.10.2. Supervisión del uso del sistema.

El nivel de monitoreo se lo determina mediante una evaluación de riesgos. Las áreas que se deben considerar incluyen:

a) Acceso autorizado.
b) Intentos de acceso no autorizado.
c) Alertas o fallas del sistema
d) Cambios o intentos de cambio en la configuración y los controles de seguridad del sistema.

La frecuencia con la cual se revisan los resultados de las actividades de monitoreo depende de los riesgos involucrados. Los factores de riesgo que se consideran incluyen:

a) Importancia de los procesos de aplicación.
b) Valor, sensibilidad e importancia de la información implicada.
c) Experiencia previa de infiltración o uso inadecuado del sistema, y frecuencia de aprovechamiento de las vulnerabilidades.
d) Extensión de la interconexión del sistema.
e) Servicio de operación de registro que se desactiva.

2.2.6.10.3. Protección de la información de los registros.

Los servicios y la información necesitan proteger contra el acceso y manipulación no autorizados. Los controles tienen como objetivo la protección contra cambios no autorizados y problemas operativos con el servicio de registro incluyendo:

a) Alteraciones en los tipos de mensaje que se registran.
b) Archivos de registro que se editan o eliminan.
c) Capacidad de almacenamiento de los medios de archivo de registro que se exceden, lo que resulta en la falla para grabar eventos o sobre-escritura de eventos grabados anteriormente.

2.2.6.10.4. Registros de administración y operación.

Se registran las actividades tanto del operador como del administrador del sistema. Los registros incluyen:

a) La hora en que ocurrió el evento.
b) Información sobre el evento (por ejemplo archivos manipulados) o la falla (por ejemplo errores que se presentaron y acciones correctivas que se tomaron).
c) Cual cuenta y cual administrador estuvo involucrado.
d) Cuáles procesos fueron implicados.

2.2.6.10.5. Registro de fallos.

Se registra las fallas reportadas por los usuarios o por los programas del sistema relacionadas con el procesamiento de la información o sistemas de comunicación. Se manejan reglas para el manejo de las fallas reportadas, incluyendo:

a) Revisión de los registro de fallas para garantizar que éstas se han resuelto satisfactoriamente.
b) Revisión de las medidas correctivas para garantizar que no se han puesto en peligro los controles y que la acción tomada está totalmente autorizada.

2.2.6.10.6. Sincronización del reloj.

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de seguridad están sincronizados con una fuente de tiempo exacta y acordada.

2.2.7. Control de Acceso.

2.2.7.1. Requisitos de negocio para el control de acceso.

El acceso a la información, a los servicios de procesamiento de información y a los procesos del negocio se controla en base a los requisitos de seguridad y del negocio.

2.2.7.1.1. Política de control de acceso.

Las reglas y los derechos para el control de acceso para los usuarios se establecen en una política de control de acceso, los controles del acceso son tanto lógicos como físicos y se considera en conjunto. La política considera los siguientes aspectos:

a) Requisitos de seguridad de las aplicaciones individuales del negocio.
b) Identificación de toda la información relacionada con las aplicaciones del negocio y los riesgos a los que se enfrenta la información.
c) Políticas para la distribución y autorización de la información, por ejemplo, la necesidad de

conocer los principios, niveles de seguridad y clasificación de la información.

d) Consistencia entre el control de acceso y las políticas de clasificación de la información de sistemas y redes diferentes.
e) Legislación pertinente y obligaciones contractuales relacionadas con la protección del acceso a los datos o los servicios.
f) Perfiles estándar de acceso de usuario para funciones laborales comunes en la organización.
g) Gestión de los derechos de acceso en un entorno distribuido y con red que reconozca todos los tipos de conexiones posibles.
h) Distribución de las funciones de control de acceso, por ejemplo solicitud de acceso, autorización del acceso, administración del acceso.
i) Requisitos para la autorización formal de las solicitudes de acceso.
j) Requisitos para la revisión periódica de los controles de acceso.
k) Retiro de los derechos de acceso.

2.2.7.2. Gestión de acceso de usuario.

Se establecen procedimientos para controlar el acceso a los sistemas y servicios de información, éstos comprenden desde el registro inicial de los usuarios nuevos hasta la cancelación final del registro de usuarios que ya no requieren acceso a los servicios y sistemas de información. Se da énfasis a los usuarios con capacidad para modificar estos controles.

2.2.7.2.1. Registro de usuario.

Se maneja un procedimiento para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información. El procedimiento de control del acceso para el registro y cancelación de usuarios posee:

a) Uso de la identificación por usuario para permitir que los usuarios sean responsables de sus acciones; cuando se requieran identificaciones de grupos, se otorgará por razones del negocio pero se necesita la aprobación y documentación de la misma.
b) Verificación de que el usuario tenga autorización del dueño del sistema para el uso del sistema o servicio de información.
c) Verificación de que el nivel de acceso otorgado sea adecuado para que los propósitos del negocio sean consistentes con la política de seguridad de la organización, es decir, no pone en peligro la distribución de funciones.
d) Dar a los usuarios una declaración escrita de sus derechos de acceso.
e) Exigir a los usuarios firmar declaraciones que indiquen que aquellos entienden las condiciones del acceso.
f) Asegurar que los proveedores del servicio no otorguen el acceso hasta que se hayan terminado los procedimientos de autorización.
g) Mantenimiento de un registro formal de todas las personas registradas para usar el servicio.

h) Retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado la organización.
i) Garantizar que las identificaciones de usuario no se otorgan a otros usuarios.

2.2.7.2.2. Gestión de privilegios.

Para poder un usuario manejar un sistema de información se otorga una asignación y los privilegios necesarios para manejar la misma. Los sistemas de usuario múltiple que requieren protección contra el acceso no autorizado controlan la asignación de privilegios a través de un proceso formal de autorización. Se recomienda tener en cuenta los siguientes elementos:

a) Identificar los usuarios y sus privilegios de acceso asociados con cada producto del sistema.
b) Asignar los privilegios a los usuarios sobre los principios de necesidad de uso, de manera acorde con la política de control de acceso.
c) Crear un registro de todos los privilegios asignados. Los privilegios no se otorgarán hasta que el proceso de autorización esté completo.
d) Es conveniente promover el desarrollo y empleo de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.
e) Se recomienda promover también el desarrollo y empleo de programas que eviten la necesidad de funcionar con privilegios.

2.2.7.2.3. Gestión de contraseñas de usuario.

La asignación de contraseñas se controlará a través de un proceso formal de gestión. El proceso incluirá los siguientes requisitos:

a) Exigir a los usuarios la firma de una declaración para mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de éste.
b) Suministrar una contraseña temporal segura que estén forzados a cambiar inmediatamente.
c) Establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle una contraseña temporal, nueva.
d) Las contraseñas temporales se deben suministrar de forma segura a los usuarios; se recomienda evitar mensajes de correo electrónico de terceras partes o sin protección.
e) Las contraseñas temporales deben ser únicas para un individuo y no ser descifrables.
f) Los usuarios deben confirmar la entrega de las contraseñas.
g) Las contraseñas nunca se almacenan en sistemas de computador en un formato no protegido.
h) Las contraseñas predeterminadas por el proveedor se cambiarán inmediatamente después de la instalación de los sistemas o del software.

2.2.7.2.4. Revisión de los derechos de acceso de usuario.

La dirección establecerá un procedimiento formal de revisión periódica de los derechos de

acceso de los usuarios. Se considera las siguientes directrices:

a) Los derechos de acceso de los usuarios se revisan en intervalos regulares o después de cada cambio de funciones.
b) Los derechos de acceso de usuarios se revisan y se reasigna cuando hay cambios de un cargo a otro dentro de la misma organización.
c) Revisar las autorizaciones para derechos de acceso privilegiado a intervalos frecuentes.
d) Verificar la asignación de privilegios a intervalos regulares para garantizar que no se obtienen privilegios no autorizados.
e) Los cambios en las cuentas privilegiadas se registran para su revisión periódica.

2.2.7.3. Responsabilidades de usuario.

Concientizar a los usuarios sobre sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular con relación al uso de contraseñas y a la seguridad del equipo del usuario.

2.2.7.3.1. Uso de contraseñas.

Dar énfasis a los usuarios sobre el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas. Todos los usuarios necesitan cumplir con los siguientes elementos:

a) Mantener la confidencialidad de las contraseñas.

b) Evitar conservar registros de las contraseñas, a menos que éstas se puedan almacenar de forma segura y el método de almacenamiento esté aprobado.
c) Cambiar las contraseñas siempre que haya indicación de puesta en peligro del sistema o de la contraseña.
d) Seleccionar contraseñas de calidad.
e) Cambiar las contraseñas a intervalos regulares o con base en el número de acceso y evitar la reutilización de contraseñas antiguas.
f) Cambiar las contraseñas temporales en el primer registro de inicio.
g) No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un marco o en una clave de función.
h) No compartir las contraseñas de usuarios individuales.
i) No utilizar la misma contraseña para propósitos del negocio y para los que no lo son.

2.2.7.3.2. Equipo de usuario desatendido.

Concientizar a los usuarios sobre los requisitos y los procedimientos de seguridad para proteger los equipos desatendidos, así cubre sobre sus responsabilidades en la implementación de dicha protección. Los usuarios necesitan conocer los siguientes puntos:

a) Terminar las sesiones cuando finalice, a menos que se puedan asegurar por medio de un mecanismo de bloqueo (protector de pantalla con contraseña)

b) Realizar el registro de cierre en computadoras principales, servidores y computadores personales de oficina al terminar la sesión.
c) Cuando no están en uso, asegurar los terminales contra el uso no autorizado mediante una clave de bloqueo o una contraseña.

2.2.7.3.3. Política de puesto de trabajo despejado y pantalla limpia.

En la política de escritorio despejado y pantalla despejada se considera las clasificaciones de la información, los requisitos legales y contractuales, los riesgos correspondientes y los aspectos culturales de la organización. Es recomendable tener presentes las siguientes directrices:

a) Cuando no se requiere la información crítica del negocio, como por ejemplo los medios de almacenamiento electrónicos o en papel, asegurarlos bajo llave.
b) Las sesiones de los terminales se protegen con un mecanismo de bloqueo de pantalla y de teclado controlado por una contraseña, para que se activen automáticamente después de un lapso de inactividad.
c) Proteger los puntos de entrada y salida de correo y los fax desatendidos.
d) Evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción.
e) Los documentos que contengan información sensible, retirar inmediatamente de las impresoras

2.2.7.4. Control de acceso a la red.

Es recomendable controlar el acceso a los servicios en red. El acceso de los usuarios a las redes y a los servicios de red no debe comprometer la seguridad de los servicios de red garantizando que:

a) Existen interfaces apropiadas entre la red de la organización y las redes que pertenecen a otras organizaciones, y las redes públicas.
b) Se aplican mecanismos adecuados de autenticación para los usuarios y los equipos.
c) Se exige control de acceso de los usuarios a los servicios de información.

2.2.7.4.1. Política de uso de los servicios en red.

Los usuarios tendrán acceso a los servicios para cuyo uso están específicamente autorizados. Se creará una política con respecto al uso de las redes y los servicios de red. Esta política maneja:

a) Las redes y los servicios de red a los cuales se le permite el acceso.
b) Los procedimientos de autorización para determinar a quién se le permite el acceso a qué redes y qué servicios en red.
c) Los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y los servicios de red.

2.2.7.4.2. Autenticación de usuario para conexiones externas.

Se debe emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos. Se puede usar técnicas con base criptográficas, token de hardware o protocolos de desafío/respuesta. Las posibles implementaciones de dichas técnicas se pueden encontrar en diversas soluciones de red privada virtual (VPN).

Implementar controles de autenticación adicionales para controlar el acceso a redes inalámbricas debido a las grandes oportunidades para la interceptación y que no son detectadas en el tráfico de red.

2.2.7.4.3. Identificación de los equipos en las redes.

En la identificación automática de los equipos se considera un medio para autenticar conexiones de equipos y ubicaciones específicas. Un identificador en el quipo se puede usar para indicar si está permitido que este equipo se conecte a la red. Estos equipos indican con claridad a qué red está permitido conectar el equipo, si existe más de una red y si estas tienen sensibilidad diferente.

2.2.7.4.4. Protección de los puertos de diagnóstico y configuración remotos.

Los controles para el acceso a los puertos de diagnóstico y configuración, incluyen el uso de un bloqueo de clave y procedimientos de soporte

para controlar el acceso físico al puerto. Un ejemplo de un procedimiento de soporte es garantizar que los puertos de diagnóstico y configuración sólo sean accesibles mediante acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware/software que requiere el acceso.

2.2.7.4.5. Segregación de las redes.

En las redes es la responsable de manejar los grupos de servicios de información, usuarios y sistemas de información. Un método para el control en las redes grandes es dividirlas en dominios lógicos de red separados, cada uno protegido por un perímetro de seguridad. Se puede aplicar un conjunto graduado de controles en diferentes dominios lógicos de red para separar aún más los entornos de seguridad de la red, por ejemplo los sistemas de acceso público, las redes internas y los activos críticos.

Se puede implementar un perímetro de red instalando una puerta de enlace (Gateway) seguro entre las dos redes que se van a interconectar para controlar el acceso y el flujo de información entre los dos dominios. Esta puerta de enlace (Gateway) se configura para filtrar el tráfico entre estos dominios y para bloquear el acceso no autorizado, este tipo de puerta de enlace es lo que se conoce comúnmente como barrera de fuego (firewall). Otro método para apartar los dominios lógicos separados es restringir el acceso a la red usando redes privadas virtuales para grupos de usuarios

dentro de la organización, o para las redes inalámbricas procedentes de redes internas y privadas.

2.2.7.4.6. Control de la conexión a la red.

En el caso de ser una red compartida, se controla la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control de acceso y los requisitos de aplicación del negocio. Se puede restringir a través de puertas de enlace (Gateway) de red que filtren el tráfico por medio de reglas predefinidas. Los siguientes son algunos ejemplos de aplicaciones con restricciones:

a) Mensajería, por ejemplo, el correo electrónico.
b) Transferencia de archivos.
c) Acceso interactivo.
d) Acceso a las aplicaciones.

2.2.7.4.7. Control de encaminamiento (routing) de red.

Se implementan controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso de las aplicaciones del negocio. Las puertas de enlace (Gateway) de seguridad se pueden usar para validar la dirección fuente/destino en los puntos de control de las redes interna y externa.

2.2.7.5. Control de acceso al sistema operativo.

Se recomienda utilizar medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos.

a) Autenticar usuarios autorizados, de acuerdo con una política de control de acceso.
b) Registrar intentos exitosos y fallidos de autenticación del sistema.
c) Registrar el uso de privilegios especiales del sistema.
d) Emitir alarmas cuando se violan las políticas de seguridad del sistema.
e) Suministrar medios adecuados para la autenticación.
f) Cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

2.2.7.5.1. Procedimientos seguros de inicio de sesión.

El procedimiento de registro en un sistema operativo está diseñado para minimizar la oportunidad de acceso no autorizado. Por ello, el procedimiento de registro de inicio registra la información mínima sobre el sistema para evitar suministrar asistencia a un usuario no autorizado.

Cumple los siguientes aspectos:

a) No mostrar identificadores de aplicación ni de sistema hasta que el proceso de registro de inicio se haya completado exitosamente.
b) Mostrar una advertencia de notificación general indicando que solo pueden tener acceso al computador los usuarios autorizados.

c) No suministrar mensajes de ayuda durante el procedimiento de registro de inicio que ayuden a un usuario no autorizado.

d) Validar la información de registro de inicio únicamente al terminar todos los datos de entrada. Si se presenta una condición de error, el sistema indicará qué parte de los datos es correcta o incorrecta.

e) Limitar la cantidad de intentos permitidos de registro de inicio.

f) Limitar el tiempo máximo permitido para el procedimiento de registro de inicio.

g) Mostrar información de fecha y hora de registro exitoso y el detalle de intentos fallidos.

h) No mostrar la contraseña que se introduce o esconder los caracteres mediante simbolos.

i) No transmitir contraseñas en texto claro en la red.

2.2.7.5.2. Identificación y autenticación de usuario.

Todos los usuarios tendrán un identificador único para su uso personal, y elegir una técnica de autenticación para comprobar la identidad de un usuario no autorizado. Los identificadores de usuario se utilizan para rastrear las actividades de la persona responsable.

2.2.7.5.3. Sistema de gestión de contraseñas.

El sistema de gestión de contraseñas considera los siguientes puntos:

a) Hacer cumplir el uso de identificadores de usuario individual y de contraseñas para conservar la responsabilidad.
b) Permitir a los usuarios la selección y el cambio de sus contraseñas e incluir un procedimiento de confirmación para tener en cuenta los errores en los ingresos.
c) Imponer una elección de contraseñas de calidad.
d) Imponer cambios de contraseña.
e) Forzar a los usuarios a cambiar las contraseñas temporales en el primer registro de inicio
f) Conservar un registro de las contraseñas de usuario previas y evitar su reutilización
g) No mostrar contraseñas en la pantalla cuando se hace su ingreso.
h) Almacenar los archivos de contraseñas separadamente de los datos del sistema de aplicación
i) Almacenar y transmitir contraseñas en formatos protegidos (encriptados o codificadas)

2.2.7.5.4. Uso de los recursos del sistema.

Se restringe y controla estrictamente el uso de programas que pueden anular los controles del sistema de la aplicación. Se considera las siguientes directrices:

a) Uso de procedimientos de identificación, autenticación y autorización para las utilidades del sistema
b) Separación de las utilidades del sistema del software de aplicaciones

c) Limitación del uso de las utilidades del sistema a la cantidad mínima viable de usuarios de confianza autorizados.
d) Limitación de la disponibilidad de las utilidades del sistema, por ejemplo para la duración de un campo autorizado
e) Registro de todo uso de las utilidades del sistema
f) Definición y documentación de los niveles de autorización para las utilidades del sistema
g) Registro de todas las utilidades o el software del sistema basado en software innecesario
h) No poner a disposición las utilidades del sistema a usuarios que tangan acceso a aplicaciones en sistemas en donde se requiere distribución de funciones

2.2.7.5.5. Desconexión automática de sesión.

Una utilidad de tiempo de inactividad es inhabilitar la pantalla de sesión y también cerrar la sesión de la aplicación y la de red después de un periodo definido de inactividad.

2.2.7.5.6. Limitación del tiempo de conexión.

Se tiene en cuenta los controles de tiempo para las aplicaciones sensibles de computador, en especial las de lugares de alto riesgo, por ejemplo áreas públicas que están fuera de la gestión de seguridad de la organización. Los siguientes son algunos ejemplos de estas restricciones.

a) Uso de conexiones por tiempo predeterminados.

b) Restricción de los tiempos de conexión a las horas normales de oficina, si no se requiere tiempo extra u operaciones de horario prolongado.
c) Considerar la repetición de la autenticación a intervalos determinados.

2.2.7.6. Control de acceso a las aplicaciones y a la información.

Se considera utilizar medios de seguridad para restringir el acceso a los sistemas de aplicación tales como:

a) Controlar el acceso de usuarios a la información de acuerdo con la politica definida de control de acceso.
b) Suministrar protección contra acceso no autorizado por una aplicación, el software del sistema operativo o software malicioso que pueda anular o desviar los controles del sistema o de la aplicación.
c) No poner en peligro otros sistemas con los que se comparten los recursos de información.

2.2.7.6.1. Restricción del acceso a la información.

Restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios. Las restricciones del acceso se basan en los requisitos de las aplicaciones del negocio. Se considera la aplicación de las siguientes directrices:

a) Proporcionar menús para controlar el acceso a las funciones del sistema de aplicación
b) Controlar los derechos de acceso a los usuarios (leer, escribir, eliminar y ejecutar)

c) Controlar los derechos de acceso de otras aplicaciones.
d) Garantizar que los datos de salida de los sistemas de aplicación que manejan información sensible sólo contienen la información pertinente para el uso de la salida y que se envía únicamente a terminales autorizados

2.2.7.6.2. Aislamiento de sistemas sensibles.

Los sistemas sensibles se manejan en un entorno informático aislado. Se consideran los siguientes puntos para el aislamiento de los sistemas sensibles:

a) La sensibilidad de un sistema de aplicación se identifica y documenta por parte del dueño de la aplicación.
b) Cuando una aplicación se ejecute en un entorno compartido, los sistemas de aplicación con los cuales se maneja los recursos y los riesgos de la misma deben ser identificados y aceptados por el responsable de la aplicación sensible.

2.2.7.7. Ordenadores portátiles y teletrabajo.

La protección debe estar acorde con los riesgos que originan estas formas especificas de trabajo. Cuando se usa la computación móvil, se tiene en cuenta los riesgos de trabajar en un entorno sin protección y aplicar la protección adecuada, cuando se trabaja desde un sitio remoto, la organización aplica protección en el sitio del remoto y garantizar que se han establecido las disposiciones adecuadas para esta forma de trabajo.

2.2.7.7.1. Ordenadores portátiles y comunicaciones móviles.

Cuando se usan servicios de computación y de comunicaciones móviles (notebook, laptop, tarjetas inteligentes y teléfonos móviles) se tiene cuidado especial para asegurarse de que la información no se pone en riesgo. Se incluye los requisitos para la protección física, los controles de acceso, las técnicas criptográficas, las copias de respaldo y la protección contra virus.

El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación móvil solo tiene lugar después de la identificación y la autenticación exitosa. Los servicios de computación móvil también se deben proteger físicamente contra robo, especialmente cuando se deja, en automóviles y otros medios de transporte, habitaciones de hoteles, centros de conferencias y reuniones.

Es conveniente contratar un seguro para los casos de robo o pérdida de los servicios de computación móvil. El equipo que porta información sensible no se deja desatendido y se bloquea con algún medio físico o cerraduras especiales para asegurar el equipo.

Se recomienda disponer la formación del personal que utiliza computación móvil para concientizar sobre los riesgos adicionales que se

originan en este tipo de trabajo y los controles que se implementan.

2.2.7.7.2. Teletrabajo.

Se necesita implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto. Se recomienda considerar los siguientes aspectos:

a) La seguridad física en el sitio de trabajo remoto (seguridad física y del entorno)
b) El entorno físico de trabajo remoto propuesto.
c) Los requisitos de seguridad de las comunicaciones, pensando en la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la cual se tendrá acceso.
d) La amenaza del acceso no autorizado a la información o los recursos por parte de otras personas que usan el mismo espacio (familia y amigos)
e) El uso de redes domésticas y los requisitos en la configuración de servicios de red inalámbrica
f) Las políticas para evitar disputas con respecto a los derechos de propiedad intelectual desarrollados o al equipo de propiedad privada.
g) El acceso a equipo de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), si es permitido por la ley
h) Los acuerdos sobre licencias de software que permitan que la organización sea responsable de la licencia para software de clientes en estaciones de trabajo de propiedad privada de

los empleados, contratistas o usuarios de terceras partes.

i) Protección antivirus y requisitos de barreras contra fuego (firewall)

2.2.8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

2.2.8.1. Requisitos de seguridad de los sistemas de información.

Los sistemas de información incluyen sistemas operativos, infraestructura, aplicaciones del negocio, productos de vitrina, servicios y aplicaciones desarrolladas para usuarios. El diseño y la implementación del sistema de información que da soporte a los procesos del negocio pueden ser cruciales para la seguridad. Identificar los requisitos de seguridad antes del desarrollo y/o la implementación de los sistemas de información.

2.2.8.1.1. Análisis y especificación de los requisitos de seguridad.

En las especificaciones para los requisitos de control consideran los controles automatizados que se han de incorporar en el sistema de información y la necesidad de controles y manuales de apoyo. Los requisitos del sistema para la Seguridad de la Información y los procesos para implementarla se integran en las fases iniciales de los proyectos del sistema de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Si se adquieren productos, se sigue un proceso formal de adquisición y prueba. Los contratos con el proveedor abordan los requisitos de seguridad identificados. Cuando la funcionalidad de la seguridad de un producto determinado no satisface el requisito específico, entonces es conveniente considerar los controles de los riesgos, introducidos y asociados, antes de adquirir el producto.

2.2.8.2. Tratamiento correcto de las aplicaciones.

Se diseña controles apropiados en las aplicaciones, incluyendo las aplicaciones desarrolladas por el usuario para garantizar el procesamiento correcto. Estos controles incluyen la validación de los datos de entrada y de salida del procesamiento interno.

2.2.8.2.1. Validación de los datos de entrada.

Se validan los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados. Es recomendable realizar verificaciones de las entradas de las transacciones del negocio, de los datos permanentes (nombre y direcciones, límites de crédito, números de referencia del cliente) y de las tablas de parámetros (precios de venta, tasas de interés). Se recomienda tomar en consideración:

a) Verificaciones de entradas de datos para determinar (valores fuera de rango, caracteres no válidos, datos incompletos, datos inconsistentes)

b) Revisión periódica del contenido de los campos clave o de los archivos de datos para confirmar su validez e integridad.
c) Inspección de los documentos de entrada impresos para determinar cambios no autorizados (todos los cambios en los datos de entrada deben de estar autorizados)
d) Procedimientos de respuesta ante errores de validación.
e) Procedimientos para probar la credibilidad de los datos de entrada.
f) Definición de responsabilidades para todo el personal que participa en el proceso de entrada de datos.
g) Creación de un registro de las actividades implicadas en el proceso de entrada de datos.

2.2.8.2.2. Control del procesamiento interno.

Incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información. El diseño y la implementación de las aplicaciones garantizan que se minimizan los riesgos de falla en el procesamiento, los cuales originan pérdida de la integridad. Las áreas específicas que se han de considerar incluyen:

a) Utilización de las funciones agregar, modificar y borrar para implementar los cambios en los datos.
b) Procedimientos para evitar que los programas se ejecuten en orden erróneo o su ejecución después de falla previa del procesamiento.

c) Utilización de programas adecuados para la recuperación después de fallas con el fin de garantizar el procesamiento correcto de los datos.
d) Protección contra ataques empleando desbordamiento/exceso en el búfer.

2.2.8.2.3. Integridad de los mensajes.

Se identifica los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados. Se realiza una evaluación de los riesgos de seguridad para determinar si se requiere integridad del mensaje y para identificar el método más apropiado de implementación.

2.2.8.2.4. Validación de los datos de salida.

Se necesita validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias. La validación de los datos de salida incluye:

a) Verificaciones de la credibilidad para probar si los datos de salida son razonables
b) Asegurar el procesamiento de todos los datos
c) Suministro de información suficiente para que un lector o un sistema de procesamiento posterior determine la exactitud, precisión y clasificación de la información.

d) Procedimientos para responder las pruebas de validación de salidas
e) Definición de las responsabilidades del personal que participa en el proceso de la salida de datos
f) Creación de un registro de las actividades del procesamiento de validación de la salida de datos.

2.2.8.3. Controles criptográficos.

Proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos. Se desarrollará una política sobre el uso de los controles criptográficos y establecer una gestión de claves para dar soporte al empleo de técnicas criptográficas.

2.2.8.3.1. Política de uso de los controles criptográficos.

Se implementa una política sobre el uso de controles criptográficos para la protección de la información. Se recomienda tomar en consideración los siguientes aspectos al desarrollar una política criptográfica:

a) El enfoque de la dirección para el uso de controles criptográficos en la organización, incluyendo los principios generales bajo los cuales se protege la información del negocio.
b) La evaluación de riesgos ayuda a identificar el nivel requerido de protección teniendo en cuenta tipo, fortaleza y calidad del algoritmo de encriptación requerido.
c) Uso de encriptación para la protección de la información transportada por medios móviles o

removibles, por dispositivos o a través de líneas de comunicación.

d) Enfoque para la gestión de claves que incluya métodos para la protección de las claves criptográficas y la recuperación de información encriptada en caso de pérdida, amenaza o daño de las claves.
e) Funciones y responsabilidades, es decir, quién es el encargado de la implementación de la política y de la gestión de claves.

Los controles criptográficos se utilizan para lograr diferentes objetivos de seguridad:

a) Confidencialidad: uso de encriptación de la información para proteger información sensible o crítica, bien sea almacenada o transmitida.
b) Integridad/autenticidad: uso de firmas digitales o códigos de autenticación de mensajes para proteger la autenticidad e integridad de información sensible o crítica transmitida o almacenada.
c) No repudio: uso de técnicas criptográficas para obtener prueba de la ocurrencia o no ocurrencia de un evento o acción.

2.2.8.3.2. Gestión de claves.

Establecer la gestión de claves para apoyar el uso de técnicas criptográficas en la organización. Todas las claves criptográficas tienen protección contra modificación, pérdida o destrucción.

El equipo usado para generar, almacenar y archivar las claves está protegido por medios físicos. Un sistema de gestión de claves se basa en normas, procedimientos y método seguro para:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
b) Generar y obtener certificados de claves públicas.
c) Distribuir claves a los usuarios previstos, incluyendo la forma de activar y recibir las claves.
d) Almacenar las claves, incluyendo la forma en que los usuarios autorizados tendrán acceso a ellas.
e) Cambiar o actualizar las claves incluyendo reglas sobre cuándo cambiarlas y cómo hacerlo.
f) Tratar las claves perdidas.
g) Revocar las claves, incluyendo la forma de retirarlas o desactivarlas, por ejemplo, cuando las claves se han puesto en peligro o cuando un usuario se retira de la organización.
h) Recuperar las claves perdidas o corruptas como parte de la gestión de continuidad del negocio; por ejemplo, para la recuperación de información encriptada.
i) Archivar claves, por ejemplo para la información archivada o con copia de respaldo.
j) Destrucción de claves
k) Registro y auditoría de las actividades relacionadas con la gestión de claves.

2.2.8.4. Seguridad de los archivos de sistema.

Los accesos a los archivos del sistema y al código fuente del programa se encuentran protegidos, y los proyectos de tecnología de información y las actividades de soporte se ejecutan de forma segura.

2.2.8.4.1. Control del software en explotación.

Se establecen procedimientos para controlar la instalación de software en los sistemas operativos. Para minimizar los riesgos de corrupción de los sistemas operativos, se tiene en cuenta las siguientes directrices para controlar los cambios:

a) La actualización del software operativo, las librerías y los programas son realizadas por administradores capacitados y con la debida autorización de la dirección.
b) Los sistemas operativos tiene códigos ejecutables aprobados y no códigos en desarrollo ni compiladores.
c) El software de las aplicaciones y del sistema operativo se implementan después del ensayo exhaustivo y exitoso, los ensayos incluyen pruebas sobre capacidad de uso, seguridad, efectos en otros sistemas y facilidad para el usuario, se garantiza que todas las librerías fuentes del programa correspondiente estén actualizadas.
d) Usar un sistema de control de configuración para mantener el control del software

implementado, asi como de la documentación del sistema.

e) Conservar un registro para auditoría de todas las actualizaciones de las librerías de los programas operativos.

f) Es conveniente conservar las versiones anteriores del software de aplicación como medida de contingencia.

g) Archivar las versiones antiguas de software junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de soporte, en la medida en que los datos se retengan en archivo.

Los parches de software se aplican cuando pueden ayudar a eliminar o reducir las debilidades de la seguridad.

2.2.8.4.2. Protección de los datos de prueba del sistema.

Se evitará el uso de bases de datos operativos que contiene información sensible con propósitos de prueba. Si se utiliza información sensible para propósitos de prueba, todos los detalles y el contenido sensible se retiran o modifica antes del uso. Se recomienda seguir las siguientes directrices para proteger los datos operativos cuando se emplean con propósitos de prueba.

a) Los procedimientos de control de acceso que se aplican a los sistemas de aplicación operativos también se aplica a los sistemas de aplicación de pruebas.

b) Borrar la información operativa inmediatamente después de terminar la prueba.
c) Registrar el copiado y la utilización de la información operativa para brindar una pista para auditoría.

2.2.8.4.3. Control de acceso al código fuente de los programas.

El acceso al código fuente de programas y a los elementos asociados, se controla para evitar la introducción de la funcionalidad no autorizada y evitar los cambios involuntarios. Para el código fuente de programas esto se puede lograr con el almacenamiento central controlado de dicho código, preferiblemente en las librerías fuente de programas. Las siguientes directrices se consideran para controlar el acceso a fuentes de programas:

a) Las librerías fuente de programas no se mantienen en los sistemas operativos.
b) El código fuente de programas y las librerías fuente de programas se gestionan de acuerdo con los procedimientos establecidos.
c) El personal de soporte tiene acceso restringido a las librerías fuente de programas.
d) La actualización de las librerías fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, se ejecuta después de recibir la autorización apropiada.
e) Mantener los listados de programas en un entorno seguro.

f) Crear un registro para auditoria de todos los acceso a las librerías fuente de programas
g) Crear un procedimiento de control de cambios de las librerías fuente de programas.

2.2.8.5. Seguridad en los procesos de desarrollo y soporte.

Los entornos de soporte y de desarrollo necesitan ser controlados. Los directores responsables de los sistemas de aplicación controlan que todos los cambios propuestos en el sistema se revisan para comprobar que no ponen en peligro la seguridad del sistema no del entorno operativo.

2.2.8.5.1. Procedimientos de control de cambios.

Se controla la implementación de cambios utilizando procedimientos formales de control de cambios. Los procedimientos se documentan y se cumplen. La introducción de sistemas nuevos y de cambios importantes en los sistemas existentes sigue un proceso formal de documentación, especificación, prueba, control de calidad e implementación con gestión. Los procedimientos de control de cambios incluyen:

a) El mantenimiento de un registro de los niveles acordados de autorización.
b) La garantía de que los cambios son realizados por los usuarios autorizados.
c) La revisión de los controles y de procedimientos de integridad para asegurar que nos e pondrán en peligro debido a los cambios

d) La identificación de todo software, la información, las entidades de bases de datos y el hardware.

e) La obtención de la aprobación formal de las propuestas detalladas antes de iniciar el trabajo.

f) Los usuarios autorizados aceptan los cambios antes de las implementaciones

g) La documentación del sistema está actualizada al finalizar cada cambio y que la documentación antigua se archiva o elimina.

h) El mantenimiento de una versión de control para todas las actualizaciones del software.

i) El mantenimiento de un rastro para auditoria de todos los cambios solicitados.

j) La documentación operativa y los procedimientos de usuario se cambian en función de la necesidad con el objeto de mantener su idoneidad.

k) La implementación de los cambios tiene lugar en el momento oportuno y no perturba los procesos del negocio involucrados.

2.2.8.5.2. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se someten a una revisión y se realizan pruebas para asegurar que no hay un mal impacto en las operaciones ni en la seguridad de la organización. Este proceso comprende los siguientes aspectos:

a) Revisión de los procedimientos de integridad y control de la aplicación para asegurarse de que

nos se han puesto en peligro debido a los cambios en el sistema operativo.

b) Verificar que el plan y el presupuesto de soporte anual cubrirán las revisiones y pruebas del sistema que resulten de cambios en el sistema operativo.

c) Comunicar oportunamente sobre los cambios en el sistema operativo para permitir la realización de las pruebas y las revisiones apropiadas antes de la implementación.

2.2.8.5.3. Restricciones a los cambios en los paquetes de software.

Se minimiza y controla la realización de modificaciones a los paquetes de software, limitarlas a cambios necesarios. Los paquetes de software suministrador por el vendedor se utilizan sin modificaciones. Cuando sea necesario modificar un paquete de software, se tiene en cuenta los siguientes puntos:

a) El riesgo de que los procesos de integridad y de control incorporados se vean comprometidos.

b) Si es necesario obtener el consentimiento del vendedor.

c) La posibilidad de obtener los cambios requeridos del vendedor como un programa estándar de actualizaciones.

d) El impacto, si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios.

2.2.8.5.4. Fugas de información.

Toda entidad debe evitar que exista fuga de información, por ello se considera los siguientes aspectos:

a) Exploración de los medios y comunicaciones de salida para determinar la información oculta.
b) Comportamiento de las comunicaciones y del sistema de modulación y enmascaramiento para reducir la probabilidad de que una tercera parte pueda deducir información a partir de tal comportamiento.
c) Utilización de sistemas y software que se consideran con alta integridad.
d) Monitoreo regular de las actividades del personal y del sistema, cuando está permitido por la legislación o los reglamentos existentes.
e) Monitoreo del uso de los recursos en los sistemas de computador.

2.2.8.5.5. Externalización del desarrollo de software.

La organización debe supervisar y monitorear el desarrollo de software contratado externamente, se considera lo siguiente:

a) Acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad intelectual.
b) Certificación de calidad y exactitud del trabajo realizado.
c) Convenios de fideicomiso en caso de falla de la tercera parte.

d) Derechos de acceso para auditar la calidad y exactitud del trabajo realizado.
e) Requisitos contractuales para la calidad y la funcionalidad de la seguridad del código.
f) Realización de pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

2.2.8.6. Gestión de la vulnerabilidad técnica.

La gestión de la vulnerabilidad técnica se implementa de forma eficaz, sistemática y repetible con toma de mediciones para confirmar su eficacia. Estas consideraciones incluyen a los sistemas operativos y otras aplicaciones en uso.

2.2.8.6.1. Control de las vulnerabilidades técnicas.

Se obtiene información sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, determinar cuan expuesta está la empresa a estas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos. Se recomienda tener en cuenta las siguientes directrices:

a) Definir e implementar las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica.
b) Identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas.
c) Definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales.

d) Identificar los riesgos asociados y las acciones que se han de tomar.

e) Dependiendo de la urgencia con la que es necesario tratar la vulnerabilidad técnica, la acción a tomar se ejecuta de acuerdo con los controles relacionados con la gestión de cambios o siguiente los procedimientos de respuesta ante incidentes de Seguridad de la Información.

f) Si está disponible un parche de actualización de software, se evalúa los riesgos asociados con su instalación.

g) Probar y evaluar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables.

h) Conservar un registro para auditoría de todos los procedimientos efectuados.

i) Monitorear y evaluar a intervalos regulares para garantizar su eficacia y eficiencia.

j) Tratar primero los sistemas con alto riesgo.

2.2.9. Gestión de Incidentes en la Seguridad de la Información.

2.2.9.1. Notificación de eventos y puntos débiles de seguridad de la información.

Es conveniente establecer el reporte formal del evento y los procedimientos de escalada. Exigir a todos los miembros de una empresa que reporten todos los eventos de Seguridad de la Información y las debilidades tan pronto sea posible al punto de contacto designado.

2.2.9.1.1. Notificación de los eventos de seguridad de la información.

Todos los empleados, contratistas y usuarios de tercera parte tienen la responsabilidad para reportar todos los eventos de Seguridad de la Información lo más pronto posible a través de los canales de gestión apropiados y con el procedimiento definido. Los procedimientos de reporte incluye los siguientes aspectos:

a) Procesos adecuados de retroalimentación para garantizar que aquellos que reportan los eventos de Seguridad de la Información reciben notificación de los resultados después que se ha tratado y solucionado el problema
b) Formatos para el reporte de los eventos de Seguridad de la Información para soportar la acción de reporte y ayudar a que la persona que hace el reporte recuerde todas las acciones necesarias en caso de un evento de Seguridad de la Información.
c) El comportamiento correcto en caso de un evento de Seguridad de la Información (tomar nota sobre los detalles importantes, reportar inmediatamente)
d) Referencia a un proceso disciplinario formar establecido para tratar a los empleados, contratistas o usuarios de tercera parte que cometieron la violación de seguridad

2.2.9.1.2. Notificación de puntos débiles de seguridad.

Exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios tan pronto como sea posible a su director.

2.2.9.2. Gestión de incidentes y mejoras de seguridad de la información.

Es conveniente establecer las responsabilidades y los procedimientos para manejar los eventos y debilidades de la Seguridad de la Información de manera eficaz una vez se han reportado. Aplicar un proceso de mejora continua a la respuesta de monitorear, evaluar y gestionar en su totalidad estos incidentes de Seguridad de la Información.

2.2.9.2.1. Responsabilidades y procedimientos.

Establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de Seguridad de la Información. Se recomienda tener en cuenta las siguientes directrices:

a) Es conveniente instaurar procedimientos para manejar los diferentes tipos de incidentes de Seguridad de la Información
b) Comprender análisis e identificación de la causa, contención, planificación e implementación, comunicación con afectados, reporte de la acción a la autoridad.

c) Recolectar y asegurar los rastros para auditoria y la evidencia similar para el análisis de los problemas internos, uso de evidencia forense, negociación para la compensación de proveedores y servicios.

2.2.9.2.2. Aprendizaje de los incidentes de seguridad de la información.

Se necesitan crear mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de Seguridad de la Información. La Información obtenida de la evaluación de los incidentes de seguridad, se utiliza para identificar los incidentes recurrentes o de alto impacto.

2.2.9.2.3. Recopilación de evidencias.

Cuando una acción de seguimiento contra una persona u organización después de un incidente de Seguridad de la Información implica acciones legales, la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

En general, las reglas para la evidencia comprenden los siguientes aspectos:

a) Admisibilidad de la evidencia: si la evidencia se puede utilizar o no en la corte;
b) Peso de la evidencia: la calidad y cabalidad de la evidencia.

Para lograr la admisibilidad de la evidencia, la organización revisa que sus sistemas de información cumplen cualquier norma o código de práctica publicado para la producción de evidencia admisible.

Todo el trabajo forense se ejecuta únicamente en copias del material de evidencia. Se protege la integridad de todo el material de evidencia. El proceso de copia del material de evidencia esta supervisado por personal de confianza y se registra la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

2.2.10. Gestión de la Continuidad del Negocio.

2.2.10.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

Implementar un proceso de gestión de la continuidad del negocio para minimizar el impacto y la pérdida de activos de información en la organización. En este proceso es conveniente identificar los procesos críticos para el negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones.

2.2.10.1.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.

Desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trae los requisitos de Seguridad de la Información necesarios para la continuidad del negocio dentro de la organización. El proceso reúne los siguientes elementos para la gestión de la continuidad del negocio:

a) Comprensión de los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y determinación de la prioridad de los procesos críticos del negocio.
b) Identificación de todos los activos involucrados en los procesos críticos del negocio.
c) Comprensión del impacto que pueden tener las interrupciones causadas por incidentes de Seguridad de la Información, y establecer los objetivos del negocio para los servicios de procesamiento de información.
d) Consideración para adquirir pólizas de seguros adecuadas que puedan formar parte de todo el proceso de continuidad del negocio.
e) Identificación y consideración de la implementación de controles preventivos y mitigantes adicionales.
f) Identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la Seguridad de la Información.

g) Formulación y documentación de los planes de continuidad del negocio que abordan los requisitos de Seguridad de la Información acorde con la estrategia acordada de continuidad del negocio.

h) Prueba y actualización regular de los planes y procesos establecidos.

2.2.10.1.2. Continuidad del negocio y evaluación de riesgos.

Se identifican los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la Seguridad de la Información.

Los aspectos de Seguridad de la Información en la continuidad del negocio se basan en la identificación de los eventos que puedan causar interrupciones en los procesos del negocio de la organización.

Las evaluaciones de riesgos para la continuidad del negocio se efectúan con la plena participación de los dueños de los recursos y los procesos del negocio. Estas evaluaciones considera todos los procesos del negocio para identificar, cuantificar y priorizar los riesgos frente a los criterios y los objetivos pertinentes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridades de recuperación.

Dependiendo de los resultados, se desarrolla una estrategia de continuidad del negocio para determinar el enfoque para la continuidad del negocio. Una vez que se ha creado esta estrategia, la dirección la aprueba e implementa el plan.

2.2.10.1.3. Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.

Se desarrolla e implementa planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos críticos para el negocio. Se considera los siguientes aspectos:

a) Identificar y acordar todas las responsabilidades y los procedimientos para la continuidad del negocio.
b) Identificar la pérdida aceptable de información y servicios.
c) Implementar los procedimientos que permitan recuperar y restaurar las operaciones del negocio y la disponibilidad de la información en las escalas de tiempo requeridas.
d) Procedimientos operativos que se han de seguir en espera de la terminación de la recuperación y restauración.
e) Documentación de procedimientos y procesos acordados.

f) Formación apropiada del personal en los procedimientos y procesos acordados, incluyendo el manejo de las crisis.
g) Pruebas y actualización de los planes.

2.2.10.1.4. Marco de referencia para la planificación de la continuidad del negocio.

Se mantiene una sola estructura de los planes de continuidad del negocio para asegurar que todos los planes son consistentes, y considerar los requisitos de la Seguridad de la Información así como identificar las prioridades para pruebas y mantenimiento.

Cada plan de continuidad del negocio debe tener un enfoque definido, por ejemplo el enfoque para garantizar la disponibilidad y Seguridad de la Información, cada plan especifica el avance y las condiciones para su implementación, así como las personas responsables de ejecutar cada etapa del proyecto. Se considera los siguientes aspectos.

a) Las condiciones para la activación de los planes que describen el proceso a seguir antes de activar cada plan.
b) Los procedimientos de emergencia que describen las acciones por realizar tras un incidente que ponga en peligro las operaciones del negocio.
c) Los procedimientos de respaldo que describen las acciones por realizar para desplazar las actividades esenciales del negocio a lugares temporales alternos y para devolver la

operatividad de los procesos del negocio en los plazos requeridos.

d) Los procedimientos operativos temporales por seguir mientras se terminan la recuperación y la restauración.
e) Los procedimientos de reanudación que describen las acciones por realizar para que las operaciones del negocio vuelvan a la normalidad.
f) Una programación de mantenimiento que especifique cómo y cuando se realizarán pruebas al plan y el proceso para el mantenimiento del plan.
g) Actividades de concientización, educación y formación diseñadas para comprender los procesos de continuidad del negocio y garantizar que los procesos siguen siendo eficaces.
h) Los activos y recursos críticos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación.

2.2.10.1.5. Pruebas, mantenimiento y reevaluación de planes de continuidad.

Las pruebas del plan de continuidad del negocio sirven para asegurar que todos los miembros del equipo de recuperación son conscientes de los planes y sus responsabilidades para la continuidad del negocio y la Seguridad de la Información.

La programación de las pruebas para los planes de continuidad del negocio indica cómo y

cuándo se va a probar cada elemento del plan. Es conveniente utilizar una variedad de técnicas para garantizar que los planes funcionarán en condiciones reales. Estas incluyen:

a) La prueba sobre papel de varios escenarios.
b) Las simulaciones
c) Las pruebas de recuperación técnica
d) Las pruebas de recuperación en un lugar alterno.
e) Las pruebas de los recursos y servicios del proveedor
f) Los ensayos completos.

2.2.11. Cumplimiento.

2.2.11.1. Cumplimiento de los requisitos legales.

El diseño, el uso, la operación y la gestión de los sistemas de información pueden estar sujetos a requisitos de seguridad estatutarios, reglamentarios y contractuales. Se necesita la asesoría externa sobre estos requisitos.

2.2.11.1.1. Identificación de la legislación aplicable.

Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se definen explícitamente, documentar y mantener para desarrollar controles que cubran estas zonas.

2.2.11.1.2. Derechos de propiedad intelectual (DPI).

Se implementan procedimientos aprobados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual. Se toma en consideración las siguientes directrices:

a) Publicar una política de cumplimiento de los derechos de propiedad intelectual que defina el uso legal del software y de los productos de información.
b) Adquirir software únicamente a través de fuentes conocidas y de confianza para garantizar que no se violan los derechos de copia.
c) Mantener la concientización sobre las políticas para proteger los derechos de propiedad intelectual y notificar la intención de tomar acciones disciplinarias para el personal que los viole.
d) Mantener registros apropiados de los activos e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual.
e) Mantener prueba y evidencia sobre la propiedad de licencias, discos maestros, manuales, entre otros.
f) Implementar controles para asegurar que no se exceda el número máximo de usuarios permitidos.
g) Verificar que únicamente se instalan software autorizado y productos con licencia.
h) Suministrar una política para mantener las condiciones de licencia apropiadas.

i) Suministrar una política para la disposición o transferencia de software a otros.

j) Usar herramientas de auditoría adecuadas.

k) Cumplir los términos y condiciones para el software y la información obtenida de las redes públicas.

l) No copiar total ni parcialmente libros, artículos, informes ni otros diferentes a los permitidos por la ley de derechos de copia.

2.2.11.1.3. Protección de los documentos de la organización.

Los registros importantes se necesitan proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos reglamentarios, contractuales y del negocio. Se clasifican en tipos de registro, cada uno con detalles de los periodos de retención y los tipos de medio de almacenamiento. Los sistemas de almacenamiento de datos se seleccionan de forma tal que los datos requeridos se puedan recuperar en el periodo de tiempo y en forma aceptable, dependiendo de los requisitos que se deben cumplir.

Para cumplir estos objetivos de salvaguarda de registros, la organización sigue los siguientes aspectos.

a) Publicar directrices sobre retención, almacenamiento, manipulación y eliminación de registros de información.

b) Publicar una programación de retención que identifique los registros y el periodo de tiempo de su retención.

c) Crear un inventario de las fuentes de información clave.

d) Implementar los controles apropiados para proteger los registros y la información contra pérdida, destrucción y falsificación.

2.2.11.1.4. Protección de datos y privacidad de la información de carácter personal.

Se necesita desarrollar e implementar una política de protección y privacidad de los datos. Esta politica se comunica a todas las personas involucradas en el procesamiento de información personal. Con frecuencia esto se logra mejor nombrando a una persona responsable.

2.2.11.1.5. Prevención del uso indebido de recursos de tratamiento de la información.

Se da a conocer a los usuarios la importancia de no utilizar los servicios de procesamiento de información para propósitos no autorizados. Todo uso de estos servicios para propósitos no relacionados con el negocio sin autorización de la dirección, o para cualquier propósito no autorizado se considera uso inadecuado de los servicios.

Todos los usuarios conocen el alcance preciso de su acceso permitido y del monitoreo implementado para detectar el uso no autorizado.

Esto se puede lograr dando a los usuarios autorización escrita, una copia firmada por el usuario y la organización lo guarde en archivo.

2.2.11.1.6. Regulación de los controles criptográficos.

Se utilizan controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes. Se recomienda tener presentes los siguientes elementos:

a) Restricción de importaciones y/o exportaciones de hardware y software de computadores para la ejecución de funciones criptográficas.
b) Restricción de importaciones y/o exportaciones de hardware y software de computadores diseñados para adicionarles funciones criptográficas.
c) Restricciones al uso de encriptación.
d) Métodos obligatorios o discrecionales de acceso por parte de las autoridades del país a la información encriptado mediante hardware o software para brindar confidencialidad al contenido.

2.2.11.2. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.

La seguridad de los sistemas de información se revisa cada cierto período y se lleva a cabo frente a las políticas de seguridad apropiadas, también se realizan controles a las plataformas técnicas y los sistemas de información para determinar el cumplimiento de las normas aplicables sobre

implementación de la seguridad y los controles de seguridad documentados.

2.2.11.2.1. Cumplimiento de las políticas y normas de seguridad.

Los directores garantizan que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

2.2.11.2.2. Comprobación del cumplimiento técnico.

Los sistemas de información se verifican periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad, la verificación del cumplimiento técnico se puede hacer manualmente por un ingeniero de sistemas con experiencia y/o con la ayuda de herramientas automáticas que generan un informe técnico para la interpretación posterior por parte del especialista técnico.

2.2.11.3. Consideraciones sobre las auditorías de los sistemas de información.

Actualmente existen controles para salvaguardar los sistemas operativos y las herramientas de auditoría durante las auditorías de los sistemas de información.

2.2.11.3.1. Controles de auditoría de los sistemas de información.

Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se planifican para minimizar el riesgo de interrupciones de los procesos de negocio. Se posee las siguientes directrices:

a) Los requisitos de auditoría debe informar a la dirección correspondiente.
b) Controlar el alcance de las verificaciones.
c) El acceso diferente al de solo lectura únicamente se permite para copias aisladas de archivos del sistema que se puedan borrar al terminar la auditoría.
d) Los recursos para llevar a cabo las verificaciones se identifican explícitamente y estar disponibles.
e) Se identifican los requisitos para el procesamiento especial o adicional.
f) Todo acceso se monitorea y registra para crear un rastro para referencia; el uso de rastros de referencia de tiempo se considera para datos o sistemas críticos.
g) Se recomienda documentar todos los procedimientos, requisitos y responsabilidades.
h) El auditor es un ser independiente de las actividades auditadas.

2.2.11.3.2. Protección de las herramientas de auditoria de los sistemas de información.

Se necesita proteger el acceso a las herramientas de auditoria de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.

CAPÍTULO 3.

ENFOQUE DE LA NORMA ISO 17799 A LA ADMINISTRACIÓN RIESGO TECNOLÓGICO

Capítulo 3.

foque de la Norma ISO 17799 a la administración del Riesgo Tecnológico

3.1. Introducción.

Como se ha visto en el Capítulo II, la norma ISO 17799 está constituida por once dominios:

a. Política de seguridad
b. Aspectos Organizativos de la Seguridad de la Información
c. Gestión de Activos
d. Seguridad ligada a los recursos humanos.
e. Seguridad Física y del Entorno
f. Gestión de Comunicaciones y Operaciones
g. Control de Acceso
h. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
i. Gestión de Incidentes en la Seguridad de la Información
j. Gestión de la continuidad del Negocio
k. Cumplimiento.

La presente tesis es acerca del "***Desarrollo de un Marco de Control Interno para la Administración del Riesgo Operativo relacionado con la Tecnología de Información.***"

Por este motivo la Tesis se centra en el estudio del siguiente dominio:

Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

Hay que considerar que todos los dominios, objetivos de control y controles de la norma ISO son importantes pero se está tomando en consideración el alcance de la Tesis.

Figura 3.1. Constitución del dominio "Adquisición, desarrollo y mantenimiento de los Sistemas

3.2. Objetivo de Control "Requisitos de seguridad de los sistemas de información".

Tiene como objetivo asegurar que la seguridad se encuentra incorporada a los sistemas de información, esto incluirá aplicaciones desarrolladas por el usuario. Los requerimientos de seguridad deben ser identificados y aprobados antes del desarrollo de los sistemas de información.

Todos los requerimientos de seguridad, incluyendo la necesidad de planes de reanudación, deben ser identificados en la fase de requerimientos de un proyecto y justificados, aprobados y documentados como una parte de la totalidad del caso de negocios de un sistema de información.

3.2.1. Primer control "Análisis y especificación de los requisitos de seguridad".

Las comunicaciones de requerimientos para desarrollar nuevos sistemas o mejoras a los sistemas existentes deben especificar las necesidades de controles. Tales especificaciones deben considerar los controles automáticos a incorporar al sistema y la necesidad de controles manuales de apoyo.

Los requerimientos de seguridad y los controles deben reflejar el valor de los recursos de información involucrados y el potencial daño al negocio que pudiere resultar por una falla o falta de seguridad. El marco para analizar los requerimientos de seguridad e identificar los controles que los satisfagan son la evaluación y la administración de riesgo.

Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

3.3. Objetivo de Control "Tratamiento correcto de las aplicaciones".

Con este objetivo de control se desea prevenir la pérdida, modificaciones o uso inadecuado de los datos del usuario en los sistemas de aplicación. Se deben

diseñar en los sistemas de aplicación, incluyendo las aplicaciones realizadas por el usuario, controles apropiados y pistas de auditoria o registros de actividad. Esto debe incluir la validación de datos de entrada, procesamiento interno y salida de datos.

Pueden ser necesarios controles adicionales para sistemas que procesan o tienen impacto en recursos sensitivos, valiosos o criticos de la organización. Tales controles deben ser determinados sobre la base de requerimientos de seguridad y evaluación de riesgo.

3.3.1. Primer control "Validación de los datos de entrada".

Los datos de entrada en sistemas de aplicación deben ser validados para asegurar que son correctos y apropiados. Los controles deben ser aplicados a las entradas de las transacciones de negocios, datos permanentes (nombres y direcciones, límites de crédito, números de referencia al cliente) y tablas de parámetros (tasas de interés).

Se deben considerar los siguientes controles:

a) Entrada de datos y controles de entrada que abarca:
   Valores fuera de rango
   Caracteres inválidos en campos de datos
   Datos faltantes o incompletos
   Volúmenes de datos que exceden los limites inferior y superior
   Controles de datos no autorizados o inconsistentes
b) Revisión periódica de los contenidos de campos clave o archivos de datos para confirmar su validez e integridad.
c) Inspección de los documentos de entrada para detectar cambios no autorizados en los datos de entrada (todos los cambios a los documentos de entrada deben ser autorizados);
d) Procedimientos para responder a errores de validación;
e) Procedimientos para determinar la verosimilitud de los datos;

f) Determinación de las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

3.3.2. Segundo control "Control del procesamiento interno.".

El control del procesamiento interno lo podemos medir en dos grupos:

3.3.2.1. Áreas de Riesgo.

Los datos que han sido correctamente ingresados pueden generar errores o a través de actos deliberados. Para esto se necesita controles de validación que deben ser incorporados a los sistemas para detectar incidentes. El diseño de aplicaciones debe asegurar que las restricciones se implementen para minimizar los riesgos de fallas de procesamiento, dando como resultado una pérdida de la integridad. Las áreas especificas a considerar incluyen:

a) El uso y localización dentro de los programas, de funciones de cálculo para realizar cambios en los datos;
b) Los procedimientos para prevenir la ejecución de programas fuera de secuencia o cuando falló el procesamiento previo.
c) El uso de programas correctos para recuperación ante fallas, a fin de garantizar el procesamiento correcto de los datos.

3.3.2.2. Controles y verificaciones.

Los controles requeridos dependerán de la aplicación y del impacto de alteraciones de datos. Entre los ejemplos de verificaciones que pueden ser incorporadas se encuentran los siguientes:

a) Controles de sesión, para conciliar los saldos de las cuentas de los clientes después de una transacción realizada
b) Controles de saldos de cuentas de clientes por día, almacenando un archivo histórico diario, por ejemplo:

Controles ejecución a ejecución
Totales de actualización de datos
Controles programa a programa

c) Validación de datos generados por el sistema
d) Verificación de la integridad de los datos, entre computadoras centrales y remotas.
e) Control de los registros y archivos
f) Verificación para garantizar que los programas de aplicación se ejecutan en el momento correcto
g) Comprobar que los programas se ejecutan en el orden correcto y terminan en caso de producirse una falla, y que se detiene todo procesamiento posterior hasta que se resuelva el problema.

3.3.3. Tercer control "Integridad de los mensajes".

La validación a través de mensajes es una técnica utilizada para detectar cambios no autorizados en el contenido de un mensaje transmitido electrónicamente, o para detectar alteraciones en el mismo.

Puede implementarse en el código fuente de la aplicación en el cual se debe tener en cuenta la autenticación de mensajes de seguridad.

3.3.4. Cuarto control "Validación de los datos de salida".

Los datos que son utilizados de salida en un sistema de información debe ser validada para garantizar que el procesamiento sea correcto y adecuado a las circunstancias. Normalmente, los sistemas se desarrolla en base a una validación, verificación y prueba apropiada, la

salida siempre será correcta. Esto no siempre se cumple. La validación de salidas puede incluir:

a) Comprobación de la razonabilidad para probar si los datos de salida.
b) Control de manejo de cuentas para asegurar el procesamiento de todos los datos.
c) Manejo de información suficiente, para que el lector o sistema de procesamiento subsiguiente, determine la exactitud, totalidad, precisión y clasificación de la información.
d) Procedimientos para responder a las pruebas de validación de salidas.
e) Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

3.4. Objetivo de Control "Controles criptográficos".

Los controles criptográficos tienen como objetivo proteger la confidencialidad, autenticidad e integridad de la información y se debe utilizar sistemas y técnicas criptográficas para la protección de la información que se considera en estado de riesgo y para la cual otros controles no suministran una adecuada protección.

3.4.1. Primer control "Política de uso de los controles criptográficos".

Decidir si una solución criptográfica es apropiada, deber ser visto como parte de un proceso más amplio de evaluación de riesgos, para determinar el nivel de protección que debe darse a la información. Esta evaluación puede utilizarse posteriormente para determinar si un control criptográfico es adecuado, que tipo de control debe aplicarse y conque propósito, y los procesos de la empresa.

Una organización debe desarrollar una política sobre el uso de controles criptográficos para la protección de su información. Dicha política es necesaria para maximizar beneficios y minimizar los riesgos que ocasiona el uso de técnicas criptográficas, evitando un uso

inadecuado o incorrecto. Al desarrollar una política se debe considerar lo siguiente:

a) El enfoque gerencial respecto del uso de controles criptográficos en toda la organización, con inclusión de los principios generales según los cuales debe protegerse la información de la empresa.
b) El enfoque respecto de la administración de claves, con inclusión de los métodos para administrar la recuperación de la información cifrada en caso de pérdida, compromiso o daño de las claves.
c) Funciones y responsabilidades, por ej. quien es responsable de:

   La implementación de la política
   La administración de las claves

d) Como se determinara el nivel apropiado de protección criptográfica.
e) Los estándares que han de adoptarse para la eficaz implementación en toda la organización.

3.4.2. Segundo control "Gestión de claves".

La gestión de claves criptográficas es esencial para el uso de técnicas criptográficas.

Cualquier incidente de pérdida de proceso de criptografía de claves puede conducir a un riesgo de la confidencialidad, autenticidad y/o integridad de la información. Se debe implementar un sistema de administración para respaldar el uso por parte de la organización, de los dos tipos de técnicas criptográficas, los cuales son:

a) Técnicas de clave secreta, cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla. Esta clave tiene que mantenerse en secreto dado que una persona que tenga acceso a la misma podrá descifrar toda la

información contenida con dicha clave, o introducir información no autorizada;

b) Técnicas de clave pública, cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) y una clave privada (que debe mantenerse en secreto).

Todas las claves deben ser protegidas contra modificación y destrucción, y las claves secretas y privadas necesitan protección contra divulgación no autorizada. Las técnicas criptográficas también pueden aplicarse con este propósito. Se debe proveer de protección física al equipamiento utilizado para generar, almacenar y archivar claves.

Un sistema de administración de claves debe estar basado en un conjunto acordado de normas, procedimientos y métodos seguros para:

a) Generar claves para diferentes aplicaciones
b) Generar y obtener certificados de clave pública
c) Distribuir claves a los usuarios que corresponda, incluyendo como deben activarse las claves cuando se reciben.
d) Almacenar claves, incluyendo como obtienen acceso a las claves los usuarios autorizados.
e) Cambiar o actualizar claves incluyendo reglas sobre cuando y como deben cambiarse las claves.
f) Ocuparse de las claves comprometidas.
g) Revocar claves incluyendo como deben retirarse o desactivarse las mismas, por ej. cuando las claves están comprometidas o cuando un usuario se desvincula de la organización (en cuyo caso las claves también deben archivarse);
h) Recuperar claves perdidas o alteradas como parte de la administración de la continuidad del negocio.
i) Archivar claves, por ej. , para la información archivada o resguardada.
j) Destrucción de claves

k) Registrar un log de actividades y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves deben tener fechas de entrada en vigencia y de fin de vigencia, definidas de manera que solo puedan ser utilizadas por un periodo limitado de tiempo. Este periodo debe definirse según el riesgo percibido y las circunstancias bajo las cuales se aplica el control criptográfico.

3.5. Objetivo de Control "Seguridad de los archivos del sistema".

3.5.1. Primer control "Control del software en explotación".

Se debe proveer de control para la implementación de software en los sistemas en operaciones. A fin de minimizar el riesgo de alteración de los sistemas operacionales se deben tener en cuenta los siguientes controles:

a) La actualización de los programas fuentes y archivos ejecutables debe ser realizada por una persona designada y responsable de cuidar y proteger dicha información.
b) Si es posible, los sistemas en operaciones sólo deben guardar el código ejecutable.
c) El código ejecutable no debe ser implementado en un sistema operacional hasta tanto no se obtenga evidencia del éxito de las pruebas y de la aceptación del usuario, y se hayan actualizado las correspondientes bibliotecas de programas fuente.
d) Se debe mantener un registro de auditoria de todas las actualizaciones a las bibliotecas de programas operativos.
e) Las versiones previas de software deben ser retenidas como medida de contingencia en el caso que exista alguna eventualidad.

El mantenimiento del software debe contar con el soporte del mismo. Cualquier decisión referida a una actualización a una nueva versión debe tomar en cuenta la seguridad.

3.5.2. Segundo control "Protección de los datos de prueba del sistema".

Los datos de prueba deben ser protegidos y controlados. Las pruebas de aceptación del sistema normalmente requieren volúmenes considerables de datos de prueba, que sean tan cercanos como sea posible a los datos operativos. Se debe evitar el uso de bases de datos operativas que contengan información personal. Se deben aplicar los siguientes controles para proteger los datos operativos, cuando los mismos se utilizan con propósitos de prueba.

a) Los procedimientos de control de accesos, que se aplican a los sistemas de aplicación en operación, también deben aplicarse a los sistemas de aplicación de prueba.
b) Se debe llevar a cabo una autorización por separado cada vez que se copia información operativa a un sistema de aplicación de pruebas.
c) Se debe borrar la información operativa de un sistema de aplicación de prueba inmediatamente después de completada la misma.
d) La copia y el uso de información operacional deben ser registrado a fin de suministrar una pista de auditoría.

3.5.3. Tercer control "Control de acceso al código fuente de los programas".

A fin de evitar la manipulación de programas fuentes y ejecutables, se debe mantener un control estricto del acceso a las carpetas de los programas fuentes, según los siguientes puntos:

a) Se debe designar a una persona responsable de custodiar los programas fuentes de la institución.
b) El personal de soporte de TI no debe tener acceso a la carpeta de los archivos fuentes.
c) Los programas en desarrollo o mantenimiento no deben ser almacenados en la carpeta de producción, debe ser manejado en un ambiente de pruebas y pre-producción.

d) La actualización de los programas fuente sólo debe ser llevada a cabo por el supervisor responsable de custodiar la información, con la autorización del gerente de soporte de TI para la aplicación pertinente.

e) Se debe mantener un registro de auditoría de todos los accesos a las bibliotecas de programa fuente.

f) Las antiguas versiones de los programas fuente deben ser archivadas con una clara indicación de las fechas y horas precisas en las cuales estaban en operaciones, junto con todo el software de soporte, el control de tareas, las definiciones de datos y los procedimientos.

3.6. Objetivo de Control "Seguridad en los procesos de desarrollo y soporte".

Para cumplir con este objetivo se debe controlar estrictamente los entornos de los proyectos y el soporte a los mismos.

Los gerentes responsables de los sistemas de aplicación también deben ser responsables de la seguridad del ambiente del proyecto y del soporte. Los gerentes deben garantizar que todos los cambios propuestos para el sistema sean revisados, a fin de comprobar que los mismos no comprometen la seguridad del sistema o del ambiente operativo.

3.6.1. Primer control "Procedimientos de control de cambios".

El procedimiento de control de cambio debe incluir:

a) Mantener un registro de los niveles de autorización acordados.

b) Garantizar que los cambios son propuestos por usuarios autorizados.

c) Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.

d) Identificar todo el software, la información, las entidades de bases de datos y el hardware que requieran correcciones.

e) Obtener aprobación formal para las propuestas detalladas antes de que comiencen las tareas.

f) Garantizar que el usuario autorizado acepte los cambios antes de cualquier implementación.

g) Garantizar que la implementación se lleve a cabo minimizando la discontinuidad de las actividades de la empresa.

h) Garantizar que la documentación del sistema será actualizada cada vez que se completa un cambio y se archiva o elimina la documentación vieja.

i) Mantener un control de versiones para todas las actualizaciones de software.

j) Mantener una pista de auditoría de todas las solicitudes de cambios.

k) Garantizar que la implementación de cambios tenga lugar en el momento adecuado y no altere los procesos de la institución.

3.6.2. Segundo control "Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo".

Periódicamente es necesario hacer mejoras en el sistema operativo ya sea actualización de nuevas versiones en el Sistema de Información o instalar un nuevo parche de actualización. Cuando se realizan los cambios, los sistemas de aplicación deben ser revisados y probados para garantizar que no se produzca un impacto adverso en las operaciones o en la seguridad.

Este proceso debe cubrir:

a) Revisión de procedimientos de integridad y control de aplicaciones para garantizar que estos no hayan sido comprometidos por los cambios del sistema operativo.

b) Garantizar que el plan y presupuesto de soporte anual contemple las revisiones y las pruebas del sistema que deban realizarse como consecuencia del cambio en el sistema operativo.

c) Garantizar que se notifiquen los cambios del sistema operativo de manera oportuna antes de la implementación.

d) Garantizar que se realicen cambios apropiados en los planes de continuidad de la empresa.

3.6.3. Tercer control "Restricciones a los cambios en los paquetes de software".

El proceso de cambios de los paquetes de software debe ser restringido y únicamente la persona responsable de ejecutar dicha actualización tiene acceso para actualizar los programas fuentes de la institución.

Cuando se considere esencial modificar un paquete de software, se deben tener en cuenta los siguientes puntos:

a) Se debe obtener la aprobación por parte de la gerencia de sistemas.
b) La posibilidad de obtener los cambios requeridos como actualizaciones estándar de programas.
c) El impacto que se produciría si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios.

Si los cambios se consideran esenciales, se debe retener el software original y aplicar los cambios a una copia claramente identificada. Todos los cambios deben ser probados y documentados exhaustivamente, de manera que pueden aplicarse nuevamente, de ser necesario, a futuras actualizaciones de software.

3.6.4. Cuarto control "Fugas de información".

Para el control de fugas de información se debe considerar los siguientes puntos:

a) Sólo comprar programas de proveedores acreditados.
b) Comprar programas en código fuente de manera que el mismo pueda ser verificado.
c) Examinar todo el código fuente antes de utilizar operativamente el programa en la institución.

d) Controlar el acceso y las modificaciones al código una vez instalado el mismo.
e) Emplear personal de probada confiabilidad para trabajar en los sistemas críticos.

3.6.5. Quinto control "Externalización del desarrollo de software".

Cuando se realiza la tercerización de desarrollo de software, se deben considerar los siguientes puntos:

a) Acuerdos de licencias, propiedad de códigos y derechos de propiedad intelectual.
b) Certificación de la calidad y precisión del trabajo llevado a cabo.
c) Acuerdos de custodia en caso de quiebra de la tercera parte.
d) Derechos de acceso a una auditoria de la calidad y precisión del trabajo realizado.
e) Requerimientos contractuales con respecto a la calidad del código.
f) Realización de pruebas previas a la instalación para detectar códigos troyanos.

3.7. Objetivo de Control "Gestión de la vulnerabilidad técnica".

3.7.1. Primer control "Control de las vulnerabilidades técnicas".

Se debe conocer a tiempo la información sobre las vulnerabilidades técnicas de los sistemas información utilizadas, dar a conocer las vulnerabilidades y las medidas para minimizar dichos riesgos.

Se necesita realizar un inventario actual y completo de los sistemas de información la cual debe incluir: número de versión, el estado actual de la aplicación y las personas dentro de la organización responsables del software.

Las siguientes pautas deben seguirse para establecer un proceso de gestión de vulnerabilidades técnicas efectivas:

a) Se debe definir y establecer los roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas, incluyendo el monitoreo de vulnerabilidades, la evaluación de la vulnerabilidad de riesgo, el parchado, el seguimiento de activos y cualquier otra responsabilidades coordinadas.

b) Los recursos de información que se utilizaran para identificar las vulnerabilidades técnicas relevantes y para mantener precaución sobre ellos se deben identificar para el software y otras tecnologías; estos recursos de información deben ser actualizados basados en cambios de inventario o cuando un recurso nuevo o más útil se encuentre.

c) Definir una linea de tiempo para reaccionar ante notificaciones de vulnerabilidades técnicas potenciales y relevantes.

d) Una vez identificada las vulnerabilidades técnicas potenciales, la organización debe identificar los riesgos asociados y las acciones a ser tomadas en cuenta. Esta acción puede implicar el parchado de sistemas vulnerables y/o la aplicación de otros controles.

e) Dependiendo en que tan urgente sea necesario tratar una vulnerabilidad técnica, la acción a ser tomada en cuenta debe ser llevada a cabo de acuerdo a controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante incidentes en la seguridad de información.

f) Si un parche se encuentra disponible, se deben tratar los riesgos asociados con la instalación.

g) Los parches deben ser probados y evaluados antes de que sean instalados con el fin de asegurar que sean efectivos y que no resulten en efectos secundarios que no puedan ser tolerados; si no existe ningún parche disponible, se considera otros controles como:

Apagar los servicios y capacidades relacionadas con la vulnerabilidad.

Monitoreo creciente para detectar o prevenir ataques actuales.

Aumento en la precaución de la vulnerabilidad.

h) Se debe realizar un registro de ingreso para todos los procedimientos emprendidos.

i) Se debe monitorear y evaluar la gestión de procesos en la vulnerabilidad técnica con el fin de asegurar su efectividad y eficiencia.

j) Los sistemas en alto riego deben ser tratados primero por prioridad urgente/importante.

CAPÍTULO 4.

MATRIZ DE RIESGO Y PLAN DE MITIGACIÓN DE RIESGO

Capítulo 4.

Matriz de Riesgo y Plan de Mitigación de Riesgo

4.1. Inventario de Activos de Información.

Actualmente el Banco CoopNacional S.A. tiene a disposición su Departamento de Sistemas y su Centro Alterno en el cual tiene un servidor StandBy que almacena toda la información de la institución el cual puede ser habilitado para que funcione en el caso de que el Servidor principal presente alguna eventualidad.

Entre los equipos que consta en el Inventario de Activos de Información son: Servidores de Base de Datos, Servidores de Dominio y Equipos de Trabajo que son necesarios e indispensables para la continuidad del negocio:

El Banco CoopNacional S.A. tiene a disposición 2 Servidores de Base de Datos el cual tiene las siguientes características tanto del Servidor como del Storage.

Servidor Sun Enterprise T5140/2 Proc/4 core 1.2GHz/16GB	
Descripción	**Cantidad**
Sun SPARC Enterprise T5140 Server Base, 2 * 4 Core 1.2 GHz UltraSPARC T2 Plus processors, no memory, no disk backplane, no disks, no DVD, 4 10/100/1000 Ethernet ports, 1 serial port, 4 USB ports, 1 dedicated PCI-E low profile slot, 2 PCI-E low profile or XAUI (10 Gb Ethernet) slots, no power supplies, RoHS-6 compliant. (For Factory Integration Only)	1

4 GB Memory Expansion (2 * 2 GB) low-profile FBDIMMs, 1.5 V, for Sun SPARC Enterprise T5140, T5240 and Netra T5440, RoHS 6. (For Factory Integration Only)	4
4 disk capacity disk backplane. For use with Sun SPARC Enterprise T5140. RoHS 6. (For Factory Integration Only)	1
146 GB 10 K PRM 2.5'' SAS disk drive with bracket (Qty1). For use with Sun SPARC Enterprise T5120, T5220, T5140 & T5240. RoHS 6 For Factory Integration Only	4
SATA DVD drive assembly with 8x DVD+/-RW, slot load, slimline. For use with Sun SPARC Enterprise T5xx0. RoHS 6. ATO option.	1
AC power supply unit, 760W, for use with Sun SPARC Enterprise T5140. RoHS-6. (for Factory Integration Only)	2
Screw mounted slide rail kit for rack mounting of the Sun SPARC Enterprise T5120, T5220, T5140 & T5240. RoHS-6. For Factory Integration Only	1
Standard agency label for SUN SPARC Enterprise T5140 servers. (For Factory Integration Only)	1
Two memory slot filler panels for Sun SPARC Enterprise T5x40 servers and Netra T5220. (For Factory Integration Only)	4
XVR-300 2D Graphics Frame Buffer. 24-bit color, high resolution 2D graphics accelerator PCI Express x8 interface and dual DVI-I. RoHS-6.	1
Localized Power Cord Kit North American/Asin, RoHS-6 compliant.	2

Sun SPARC Enterprise T5120, T5220, T5140 and T5240 server software pre-install, including Solares 10 10/09 (update 8) plus required patches, Sun Studio 12, LDoms MGR) including MIB 1.3, GCC Version [4.3.2] CMT Developer Tools Version [1.0], and LIVE UPGRADE ABE. (For Factory Integration Only)	1
Expanded Solaris 10 10/08 Media kit, DVD only. No license. Contains additional software. SPARC/x86. Multilingual. Pricing per kit.	1

Sun StorageTek 2530/ 12*300 GB 15K RPM	
Descripción	**Cantidad**
Sun Storage Tek(TM) 2530 SAS Array, Rack-Ready Controller Tray, 3600GB, 12 * 300 GB 15 Krpm SAS drives, 2 * 512 MB cache SAS HW RAID controllers, 2 * redundant AC power supplies, 2 * redundant cooling fans; Includes Sun Storage Tek(TM) Common Array Manager software and 2 * storage domains using Sun Storage Domains software; RoHS-5.	1
Sun StorEdge(TM) 2500 2U universal rack, adjustable depth rail kit; RoHS-5	1
Sun Storage Tek(TM) 1 GB memory Cartridge for 2500 Raid Controllers Only. RoHS-5	2
Localized Power Cord Kit North American/Asian, RoHS-6 compliant.	2
Sun Storage Tek(TM) 8-port external SAS PCI-Express Host Bus Adapter. RoHS 6. X-option	2

Sun Storage 6.0m, mini, shielded, SAS cable; For connection between array and host; RoHS-6	2

Servicio de Soporte de HW por 1 año Gold 7x24	
Descripción	**Cantidad**
SOPORTE DE HW para T5140 2 PROC 4 CORE, 1 YR GOLD 7X24	1
SOPORTE DE HW PARA SUN STORAGE TEK 2530 12 * 300 GB, 1 YR GOLD 7x24	1

Precio de los Servidores	USD. 79,480.86
Garantía	1 año
Ubicación	• Centro de cómputo de la Oficina Matriz • Centro de cómputo alterno (Backup)

Tabla 4.1. Características del Servidor de Base de Datos

Se cuenta con 3 Servidores cuyo precio y característica se detalla a continuación:

Servidor DELL POWER EDGE 2950 2P/QC XEON 2.66GHz/8GB UY582	
Tipo	**Descripción**
Base Unit	Dell Power Edge 2950 2P/QC XEON
Processor	Quad Core Xeon E5430 Processor 2x6MB Cache, 2.66 GHz, 1333 MHz FSB, PE2950 (223-4489)
Memory	8GB 667MHz (4x2GB), Dual Ranked Fully Buffered DIMMs (311-6197)
Video Card	LOM NICs are TOE Ready (430-2968)
Video Memory	Riser with 2 PCI-X-Slots (3 Volts) and 1 PCIe Slot for PowerEdge 2950 (320-4608)
Hard Drive	1TB 7.2K RPM Universal SATA 3Gbps 3.5-in HotPlug Hard Drive (341-5887)
Hard Drive Controller	PERC6i SAS RAID Controller, 2x4 Connectors, Int, PCIe, 256MB cache, x6 Bkpl(341-5734)
Floppy Disk Drive	No Floppy Drive for x6 Backplane (341-3685)
Operating System	No Operating System (420-6320)
NIC	ONBOARD BROADCOM 5708 1 DBE NETWORKING (430-1764)

Modem	Dell Remote Access Card, 5th Generation for PowerEdge Remote Management (313-3923)
CD-ROM or DVD-ROM	8x DVD-ROM for PowerEdge 2950 (313-3920)
Sound Card	Bezel for PE 2950 (313-3920)
Speakers	1x6 Backplane for 3.5-inch Hard Drives (311-7936)
Documentation Diskette	Electronic Documentation and OpenManage DVD Kit (310-7415)
Additional Storage Products	1 TB 7.2 RPM Universal SATA 3Gbps 3.5-in HotPlug Hard Drive (341-5887)
Feature	Integrated STA/SATA RAID 6, PERC 6/i Integrated (341-5729)
Feature	Universal Sliding Rapid/Versa Rails, includes Cable Management Arm (310-7412)
Service	Dell Hardware Limited Warranty Plus On Site Servide Initial YR (911-9457)
Service	DECLINED CRITICAL BUSINESS SERVER OR STORAGE SOFTWARE SUPPOER PACKAGE-CALL YOUR DELL SALES REP IF UPGRADE NEEDED (911-9519)
Service	Dell Hardware Limited Warranty Plus On Site Service Extended YR (911-9538)

Service	Basic: Business Hours (5x10) Next Business Day On Site Hardware Limited Warranty Repair Init YR (913-6250)
Service	Basic: Business Hours (5x10) Next Business Day On Site Hardware Limited Warranty Repair Init YR (913-6792)
Installation	On-Site Installation Declined (910-9997)
Misc	Redundant Power Supply with Dual Cords (310-9905)
Misc	1TB 7.2 RPM Universal SATA 3Gbps 3.5-in HotPlug Hard Drive (341-5887)
Misc	Power Cord, 250 vol, C13 to C14, PDU Style, 10 amps, 2 feet (310-9862)
Misc	1TB 7.2K RPM Universal SATA 3 Gbps 3.5-in HotPlug Hard Drive (341-5887)
Misc	1TB 7.2K RPM Universal SATA 3 Gbps 3.5-in HotPlug Hard Drive (341-5887)

Precio por cada Servidor	USD. 4,653.00
Garantía	1 año
Ubicación	Todos los servidores se encuentran en el Centro de Cómputo de la Matriz

Uso de Cada Servidor	• Servidor de Correo • Servidor de Intranet e Internet • Servidor de Digitalización de Documentos

Tabla 4.2. Características del Servidor de Dominio

El Desarrollador de Aplicaciones tiene a su cargo dos equipos cuyas características se detallan a continuación:

DELL POWER EDGE 2950 2P/QC XEON 2.66GHz/8GB UY582	
Tipo	**Descripción**
Base Unit	Dell Precision T7500 Workstation (224-4856)
Processor	Quad Core Processor E5504, 2.0 GHz, 4M, 4.8GT/s. Dell Precision TX500 (317-0293)
Memory	6GB DDR3 ECC SDRAM Memory, 1066MHz, 3X2GB. Dell Precision TX500 (317-0335)
Keyboard	Dell, USB Quiet KYBD, Spanish Opti, Black (330-1992)
Monitor	Dell Ultra Sharp 2007FP, Standard, 20in Viewable Image Size, HASS. VGA/DVI, CLIENT (320 4683)
Video Card	256MB ATI FireMV 2260, Dual Monitor 2DP to DVI Aapter Dell Precision T1500, T5500 and T7500 (320-1321)
Hard Drive	1TB SATA 3.0Gb/s 7200 RPM HardDrive with 16MB

	DataBurst Cache Dell Precision TX500 (341-9025)
	C1 All SATA Hard Drives Non-RAID for 1 Hard Drive Dell Precision T7500 (341-8813)
Floppy Disk Drive	Internal USB Media Card Reader19:1, Dell Precision TX500 (341-8560)
Operating System	EMRP, Windows 7 Professional, Media, 64-bit Fixed Precision, Spanish (421-1945)
Operating System	Windows 7 Label, Optiplex, Fixed Precision, Vostro Desktop (330-6228)
Mouse	New Dell USB 2 Button Optical Mouse with Scroll Black Precision (310-9602)
CD-ROM or DVD-ROM	16X DVD+/-RW Data Only Dell Precision TX500 (313-7457)
CD-ROM or DVD-ROM	Cyberlink Power DVD 8.3 with Media, dell Relationship LOB (421-1189)
Speakers	Internal Chassis Speaker Dell Precision (313-3417)
Cable	Precision T7500 Power Supply (330-3555)
Documentation Diskette	Spanish Dell Precision (330-3159)
Documentation Diskette	Power Cord 125V 2M C13 Dell Precision (330-3159)
Controller Option	Integrated L SI1068e SAS/SATA 3.0Gb/s controller Dell

Cable	Precision T7500 Power Supply (330-3555)
Documentation Diskette	Documentation Spanish Dell Precision (330-3159)
Documentation Diskette	Power Cord 125V, 2M, C13, Dell Precision (330-3157)
Controller Option	Integrated L SI 1068e SAS/SATA 3.0Gb/s controller Dell Precision T750 (341-9290)
Software Disk Two	Display Port to VGA Adapter Dell Precision (330-4087)
Feature	Resource DVD contains Diagnistics and Drivers for Dell Precision T7500 (330-3571)
Service	Dell Hardware Limited Warranty Extended (916-9208)
Service	Dell Hardware Limited Warranty Plus On Site Service Initial Year (948-0067)
Service	NBD On-Site Service 2 Years Extended (948-0700)
Service	NBD On-Site Service Initial Year (948-0700)
Extended Service	International Processing (499-9997)
Misc	Chassis Intrusion Swith Dell Precision T5500 (330-3559)
Misc	Quick Reference Set-up Guide Dell Precision T5400, Factory tied (310-9578)

Misc	Shipping Material for System Dell Precision T7500 (330-3569)

Precio de cada equipo	USD. 2,435.00
Garantía	1 año
Ubicación	• Centro de cómputo de la Oficina Matriz • Centro de cómputo alterno (Backup)

Tabla 4.3. Características del Equipo de Desarrollo de Aplicación

4.2. Factores de Riesgo.

Actualmente el Banco CoopNacional S.A. consciente de su responsabilidad social y su compromiso hacia sus clientes y socios, ha mantenido una filosofía de innovación y mejoramiento tecnológico que permita afrontar de manera sustentable su crecimiento operativo y financiero, garantizando la seguridad de su información y asegurar la continuidad del negocio.

El Banco debe contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones

Para considerar la existencia de un apropiado ambiente de gestión de riesgo tecnológico, el Banco deberá cumplir con las políticas, procesos y procedimientos, formalmente establecidos por el Directorio del Banco, que aseguren una adecuada planificación y administración de la tecnología de información.

4.3. Identificación de Eventos, Fallas o Insuficiencias y Factores del Riesgo Tecnológico.

Una vez analizado los factores de riesgo el Banco debe considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio, el cual se da a conocer en la siguiente tabla:

IDENTIFICACIÓN DE EVENTOS, FALLAS O INSUFICIENCIAS Y FACTORES DEL RIESGO OPERATIVO		
Tipo de Evento	**Fallas o insuficiencias.**	**Factores de Riesgo Operativo**
Daños a los activos físicos provocados por:		
iños o fallas de equipos r desastres naturales.	Corresponde a daños de activos fijos como los servidores y equipos de comunicación.	Eventos Externos
iños o fallas de activos icos por terrorismo	Corresponde a daños o destrucción de activos fijos como equipo de cómputo siendo éstos servidores y equipos de comunicación.	Eventos Externos
años o fallas de activos icos por vandalismo	Corresponde a daños o destrucción de activos fijos siendo éstos equipos de computación tales como los servidores de dominio, servidores de base de datos y comunicaciones.	Eventos Externos
Interrupción del negocio por fallas en los sistemas		
allas en el software	Deficiencia en el proceso de ciclo de vida del sistema de información tanto en el desarrollo y/o implantación.	Tecnología de Información
allas en el hardware	Falta de previsión en la capacidad de los recursos para el volumen de las operaciones. Falta de mantenimiento	Tecnología de Información

	preventivo de los servidores centrales para prevenir eventualidades.	
blemas de comunicación	Caida en los enlaces de comunicación al comento del envío y recepción de información desde la terminal del usuario a la base de datos	Tecnologia de Información
te en los servicios licos	Falta de planes de contingencia para preveer prolongados cortes de energia	Eventos Externos
eño de aplicativos que tan a otros módulos.	Corresponde a la incapacidad de operar en otros aplicativos por la puesta en marcha de uno nuevo.	Tecnología de Información
nipulación de rmación por terceros.	Corresponde a la falta de validación, restricciones o bloqueos por perfil de usuario.	Tecnología de Información

eficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y otros externos

ores en el ingreso de os	Falta de controles de ingreso de datos en las aplicaciones.	Tecnología de Información
a en la administración colaterales	Inadecuada segregación de funciones.	Procesos
cumentación legal ompleta	Falta de verificación del área legal	Procesos
ceso restringidos a las ntas de clientes	El proceso se definió para el control de información de los clientes que manejan un volumen alto de transaccionabilidad en sus cuentas.	Procesos
puta con proveedores	Deficiencia en la contratación.	Procesos
umplimiento en la rega de la información ia terceros	Falta de controles en el envío de la información, siendo éstas las estructuras de información a los organismos de control.	Tecnología de Información
umplimiento de veedores	Corresponde a una mala selección del proveedor o pedidos	Procesos

	realizados con poca anticipación.	

Tabla 4.4. Identificación de Eventos, Fallas o Insuficiencias y Factores del Riesgo Operativo

4.4. Esquema representativo del Proceso de Gestión de Riesgo.

Las metodologías aplicadas a la gestión de riesgo tecnológico contempla un enfoque estructurado de tres elementos para una efectiva gestión de riesgos que son: principios de gestión de riesgo, estructura para la gestión de riesgo y proceso de gestión de riesgo, el cual se observa en el siguiente gráfico:

Figura 4.1. Esquema representativo del Proceso de Gestión de Riesgo

Las principales ventajas del proceso de Gestión de Riesgo son:

a) Crea y protege valor
b) Es una parte integral de los procesos de la organización
c) Forma parte de la toma de decisiones
d) Explícitamente atiende la incertidumbre
e) Es sistemática, estructurada y oportuna
f) Está basada en la mejor información disponible
g) Está adaptada a la organización
h) Toma en cuenta factores humanos y culturales
i) Es transparente e inclusiva
j) Es dinámica, iterativa y responde al cambio

k) Facilita la mejora continua

A continuación se detalla cada una de las etapas del esquema representativo del proceso de Gestión de Riesgo.

4.4.1. Comunicación y consulta.

En esta fase se define y utiliza mecanismos para comunicar y consultar con los interesados internos y externos, según resulte apropiado en cada etapa del Proceso de Gestión de Riesgos. Dichos mecanismos deben permitir a las autoridades tomar decisiones en forma oportuna respecto de los riesgos con mayores desviaciones en relación a los niveles aceptado.

En esta fase se realiza las consultas y comunicaciones con:

a) Las partes involucradas en todas las etapas del proceso, para lo cual se realiza:

Identificación de los procesos
Identificación de las partes involucradas en el proceso.

b) Se procede a realizar planes para la comunicación y consulta, con el fin de:

Abordar aspectos relacionados con el propio riesgo, sus causas y consecuencias
Establecer medidas que se requieran para tratarlo.

c) Se realizan comunicaciones y consultas externas e internas, con el fin de:

Entender la base sobre las cuales se toman las decisiones
Acciones por las cuales se requiere acciones particulares

4.4.2. Establecimiento del Contexto.

En esta fase se establecen los contextos estratégico, organizacional y de gestión en los cuales tendrá lugar el Proceso de Gestión de Riesgos. Se debe establecer los criterios contra los cuales se evaluarán los riesgos y definirse la estructura de análisis, los roles y responsabilidades.

A través de la estructura organizacional del Banco, se procederá a identificar la estructura de Buen Gobierno Corporativo, la estructura orgánica de cada área, las funciones y responsabilidades de los funcionarios.

Figura 4.2. Organigrama Estructural

4.4.3. Identificación de Riesgos y Oportunidades.

El Banco deberá identificar y evaluar el riesgo operativo inherente a todos sus productos, actividades, procesos y sistemas relevantes.

Además, también deberá comprobar que antes de lanzar o presentar nuevos productos, actividades, procesos o sistemas, se evalúa adecuadamente su riesgo operativo inherente.

La identificación del riesgo es fundamental para el posterior desarrollo de un sistema de control y seguimiento del mismo. Para ello, se tienen en cuenta tanto factores internos (la estructura del banco, la naturaleza de sus actividades, la calidad de su capital humano, cambios organizativos) como externos (cambios en el sector y avances tecnológicos) que pudieran obstaculizar el logro de los objetivos del banco.

Para implementar una metodología de identificación de eventos de riesgo operativo, se analiza la incorporación de las siguientes herramientas:

a) Autoevaluación
b) Mapas de Riesgos
c) Indicadores
d) Tablas de Control (Scorecards)
e) Bases de Datos, u otras.

4.4.3.1. Autoevaluación.

La autoevaluación se realiza mediante muestreos a través de instrumentos de medición, utilizando para ello cuestionarios estandarizados los cuales están dirigidos a los responsables del proceso o al personal idóneamente potencial para identificar el riesgo, en donde se incluye preguntas determinando si los controles de los procesos a su cargo impiden o bloquean los eventos de riesgo a suscitarse. Una vez completado los cuestionarios son compilados por la unidad de riesgos. El cuestionario estará categorizado por tipos de eventos de riesgos

por cada factor y las respuestas tendrán una valoración de 1 a 5 y determinará una matriz de escala.

A través de la autoevaluación el banco comprueba la vulnerabilidad de sus operaciones y actividades ante el riesgo operativo (Anexo 1).

El Banco realizará por lo menos una vez al año, autoevaluaciones que detecten las fortalezas y debilidades del entorno de control en las operaciones y actividades de servicios, según el listado de potenciales riesgos operativos identificados a los que está expuesto.

Otra herramienta para la identificación de riesgos operativos consiste en la realización de reuniones grupales guiadas en donde se observa e identifica los eventos de riesgo operativo que se han suscitado y otros que posiblemente ocurran en la institución.

Se utilizan también listas de control o grupos de trabajo para identificar los puntos fuertes o débiles del entorno del riesgo operativo.

La autoevaluación también incluye los eventos de riesgo operativo que los responsables de cada proceso han notificado a la unidad de riesgos (Anexo 1).

a) Los responsables de cada proceso o a través de un funcionario con mayor conocimiento del proceso, serán responsables de notificar los eventos de pérdida suscitados de acuerdo al formato de notificación establecido para el efecto.

b) Todos los eventos de riesgo serán notificados en un hasta el día siguiente después de suscitado el evento. En caso de tratarse de un evento de impacto mayor o catastrófico este será reportado de manera inmediata.

La autoevaluación es un componente critico del marco de gestión del Riesgo Operativo en el Banco, pues en base a este proceso la entidad financiera puede comprobar la vulnerabilidad de sus operaciones y actividades ante el mismo.

a) El analista de riesgo será responsabilidad de validar la información entregada y comunicar de cualquier cambio o actualización de los riesgos debido a modificaciones en los procedimientos o efectividad destacada en la aplicación de los controles.

4.4.3.2. Mapas de Riesgos.

En este proceso, se agrupan por tipo de riesgo las diferentes líneas de negocio y procesos lo que puede dejar al descubierto ámbitos que presenten deficiencias debido a la ocurrencia del evento, por lo que ayudan a determinar cuáles son las prioridades que el Banco deberá gestionar. La representación de la asignación de riesgos es a través de una figura bidimensional cuyas dimensiones son probabilidad y el impacto. Los colores representan en función de la tolerancia al riesgo de la entidad y el resultado es una herramienta gráfica que permite resaltar aquellos riesgos que requerirán ser rápidamente mitigados.

Figura 4.3. Perfil de Riesgo – Mapa de Riesgos

Las matrices de riesgo serán revisadas por el área de auditoria anualmente.

4.4.3.3. Indicadores.

Los indicadores de riesgo representan estadísticas o parámetros, que pueden revelar qué riesgos asume el Banco. Estos indicadores son revisados periódicamente (mensual o trimestralmente) para alertar sobre cambios que puedan ser reveladores de problemas con el riesgo. Se utilizan parámetros como el número de operaciones fallidas, las tasas de rotación de asalariados y la frecuencia de los errores u omisiones

4.4.3.4. Bases de Datos, u otras.

Se utilizan para registrar historiales de pérdida del Banco y poder monitorear los problemas que se materialicen para su respectiva revisión. Se realizan a fin de establecer un marco para registrar sistemáticamente la frecuencia, gravedad y otros aspectos importantes de cada caso de pérdida.

Para realizar alguna de estas metodologías es importante considerar los siguientes criterios:

a) Se debe entender el entorno del negocio del Banco y desarrollarlo a nivel de toda la Organización, proceso, subproceso, unidad organizacional (área o agencia), producto (existente o propuesto) o proyecto específico, se debe conocer mediante la lectura de los manuales de procedimientos, cómo se realiza el proceso del cual identificaremos los eventos de riesgo, para ir identificando las deficiencias, faltas o incumplimientos de políticas y procedimientos.
b) Identificar los riesgos ocasionados por factores definidos (personas, tecnología de la información, procesos, eventos externos) en el inventario de procesos críticos principalmente y las causas que originan que estos eventos afectan al Banco en sus procesos, subprocesos, unidades organizacionales, productos, o los proyectos que emprenda el Banco.
c) Determinar en cada proceso el tipo de evento de riesgo encontrado, eventos que puedan afectar al Banco y actualizarlos periódicamente.

4.4.3.5. Parámetros para calificación de riesgo mediante Autoevaluación.

Para esta fase se debe elaborar Fichas de Entrevistas para estimar el perfil de riesgo operacional de un proceso.

Las fichas de entrevistas, permitirá determinar fallas en los procesos a través de preguntas abiertas, cada una de ellas representa la frecuencia en que se produce un error o falla y el impacto en el proceso analizado.

Se realizan 9 preguntas a los responsables del proceso sobre los siguientes aspectos:

a) Descripción del riesgo.
b) Causa del riesgo.
c) Fallas por tipo de riesgo.
d) Clase de eventos de riesgo.
e) Determinar el efecto o consecuencia del riesgo
f) Determinar los controles para el riesgo identificado
g) Determinar la frecuencia e impacto en la que ocurre la falla
h) Determinar los costos incurridos
i) Controles

De acuerdo a la descripción del evento de riesgo, se asignará una ponderación cuyo total será de 5 puntos para cada grupo (probabilidad e impacto). Posteriormente se registrarán los datos para cada proceso a través de tabulaciones que permitirán la aplicación de la siguiente representación:

Se utilizará 4 niveles de escala que permitirán:

a) Manejar cuadrantes de riesgo: Inferior, Moderado, Alto y Extremo;
b) El Riesgo de los factores se determinará por su probabilidad e impacto de ocurrencia.

Al graficar los resultados de los cuestionarios en los cuadrantes, tendremos como resultados los riesgos extremos, que serán aquellos que se ubiquen en la sección sombreada de rojo, mientras que los riesgos se ubiquen en el área de color naranja, amarillo y verde corresponderán a eventos de riesgo alto, moderado e inferior respectivamente. Una vez obtenida la concentración por perfiles de riesgo se procede a realizar el análisis.

4.4.4. Análisis de Riesgos.

El análisis del riesgo se puede realizar con diversos grados de detalle, dependiendo del riesgo, el propósito del análisis y la información, datos y recursos disponibles. El análisis puede ser cualitativo, cuantitativo, o una combinación de ellos, dependiendo de las circunstancias.

Las consecuencias y su posibilidad se pueden determinar modelando los resultados de un evento o grupo de eventos. Las consecuencias se pueden expresar en términos de impactos tangibles e intangibles.

Para realizar el análisis de los riesgos en el Banco, se considerarán las siguientes causas posibles y consecuencias o efectos de los eventos de riesgo identificados:

a) Causas:

Inadecuada asignación de funciones
Insuficiente entrenamiento
Debilidad en supervisión de gestión
Procesos de auditoria inadecuados
Medidas seguridad inadecuadas
Pobre diseño de sistemas
Débiles políticas de RRHH

b) Consecuencias (Pérdidas Operacionales)

Responsabilidad Legal
Penalidades regulatorias, cumplimiento e impuestos
Pérdida o daño en activos
Devoluciones

Pérdida de recursos

Castigo

Reputación

Negocio/Estratégico

4.4.5. Evaluación de Riesgos.

La evaluación consiste en determinar la consecuencia e impacto que originaría posibles pérdidas financieras al Banco en menor o mayor proporción.

Una vez identificados los eventos en la matriz de riesgos por factores se procede a llenar la matriz de Riesgos basándonos en una evaluación cuantitativa de riesgos en base a la probabilidad de ocurrencia y el impacto que podría ocasionar en donde:

El Impacto se refiere a la magnitud de la consecuencia si se materializa el riesgo.

La probabilidad se refiere a la frecuencia con que se puede presentar el evento de riesgo.

El Impacto y probabilidad definen el nivel de riesgo del Banco. El nivel de riesgo se puede estimar bajo tres escenarios:

a) Riesgo Inherente (sin controles)
b) Riesgo Residual (con controles existentes)
c) Riesgo Residual deseado (con controles propuestos)

Para realizar la metodología de identificación de riesgo a través de talleres, se debe calificar la probabilidad e impacto determinando si el nivel de riesgo o evento es inherente; en un siguiente nivel de análisis se puede evaluar el nivel de riesgo residual y luego con los controles propuestos resultando el riesgo deseado.

Se realiza un análisis previo al taller identificando eventos suscitados y contemplados en informes de auditoria, cumplimiento o que hayan sido identificados en talleres anteriores. Se realiza una revisión a los manuales de procedimientos que corresponden al proceso y se organiza a los responsables del mismo.

Durante el taller se manifiesta la evaluación del impacto y probabilidad en cada evento de riesgo aplicando un puntaje de acuerdo a criterios definidos.

Los criterios cualitativos de probabilidad e impacto a considerarse para realizar la evaluación cualitativa, se definen a continuación.

MEDIDAS CUALITATIVOS DE PROBABILIDAD			
al	Descriptor	Descripción detallada	Rango de Probabilidad
A	Casi Cierto	Ocurrirá en la mayoria de las veces; todos los dias o varias veces al mes	95%
B	Probable	Probablemente ocurrirá en la mayoria de las circunstancias; cuando menos una	75%
C	Posible	Puede ocurrir en algún momento; cuando menos una vez por semestre.	50%
D	Improbable	Podria Ocurrir en algun momento; cuando menso una vez cada dos años.	25%
E	Raro	Puede ocurrir en circunstancias excepcionales; una vez en diez años o más	5%

Tabla 4.5. Medidas Cualitativos de Probabilidad

Los rangos de probabilidad son establecidos de acuerdo a su frecuencia en el periodo de un año.

MEDIDAS CUALITATIVOS DE CONSECUENCIAS			
Nivel	Descriptor	Descripción detallada	Impacto económico ($)
	Insignificante	Pérdida menor; riesgo aceptable en el sector; no hay daño a la reputación, no hay cobertura en los medios, no aumentan las quejas de los clientes	0-5,000
	Menor	Pérdida moderada, cobertura de medios local; aumento en los reclamos de los clientes; riesgo aceptable en el sector; posible cierre de cuentas; no hay impacto negativo en el valor de las acciones.	5,001-50,000
	Moderada	Pérdida o daño significativo; riesgo inusual en el sector; cobertura de medios nacionales limitada; reclamos de clientes a gran escala; pérdida de algunos clientes; indagaciones informales del regulador; efecto negativo potencial en el valor de las acciones; posible involucramiento de la alta gerencia	50,001-200,000
	Mayor	Pérdida o daño mayor, pérdida de valor de las acciones; riesgo inusual o inaceptable en el sector; cobertura de medios nacionales sostenida, de algunos clientes; indagaciones informales del regulador; efecto negativo potencial en el valor de las acciones; posible involucramiento de la alta gerencia	200,001-500,000
	Catastrófica	Pérdida o daño catastrófico; pérdida importante del valor de las acciones; inaceptable en el sector; cobertura de medios nacionales sostenida; de algunos clientes; indagaciones informales del regulador; efecto negativo potencial en el valor de las acciones; posible involucramiento de la alta gerencia.	> 500,000

Tabla 4.6. Medidas Cualitativos de Consecuencias

Se ejecuta un proceso de votación por cada riesgo o evento de riesgo a ser evaluado a nivel de talleres por los responsables de los procesos. Los "votos" son compilados, obteniendo un valor promedio de probabilidad e impacto por cada riesgo o evento de riesgo.

La combinación de ambos criterios define el nivel de riesgo (X,Y) en función de la apreciación subjetiva del grupo, y muestra finalmente la prioridad de los riesgos:

1	PROCESO	(Nombre del Proceso)										
	Evento de RO	(Descripción del Evento a evaluar)										
	Número de votantes	1	2	3	4	5	6	7	8	9	10	Promedio
A	Probabilidad											X
	Impacto											Y
B	Probabilidad											X1
	Impacto											Y1
C	Probabilidad											X2
	Impacto											Y2

	Riesgo Inherente	(X, Y)
	Riesgo Residual	(X1,Y1)
	Riesgo Residual Deseado	(X2,Y2)

Tabla 4.7. Análisis de Probabilidad - Impacto

Una vez realizada la votación por cada evento de riesgo se consolida la información en matrices de:

4.4.5.1. Matriz de Riesgos por Factores:

En esta matriz se detalla el evento de riesgo por la categoria del factor de riesgo establecido por la Superintendencia de Bancos y Seguros:

Campo	Descripción
No.-	Número de Evento identificado en Taller
Código del Proceso	Código del Proceso correspondiente al evento de riesgo
Proceso	Proceso al cual pertenence el evento de riesgo identificado
Código del Subproceso	Código del Sub-Proceso correspondiente al evento de riesgo
Subproceso	Subproceso al cual pertenece el evento identificado
Linea de Negocio	La Banca a la cual está dirigido el mercado objetivo del Banco
Tipo de Pérdida	Tipo de pérdida que se podría generar si ocurre el evento de pérdida
Evento	Descripción del evento identificado
Control Actual	Control actual existente identificado
Tipo de Evento	Tipo de evento en el cual se identifica el evento de riesgo
Linea de Negocio	Linea de negocio que podria ser afectada si ocurre el evento
Fallas o Insuficiencias	Falla o insuficiencia que existe para que se identifique el evento de riesgo
Factores de Riesgo Operativo	Factor causante del evento de riesgo

Tabla 4.8. Matriz de Riesgos por Factores

4.4.5.2. Matriz de Riesgos y Controles Empleados:

En esta matriz se realiza la evaluación consolidada de los eventos de riesgo identificados y sus controles.

Campo	Descripción
No.	Número de Evento, viene de Matriz de Riesgo por Factores
Subproceso	Nombre del Proceso o Subproceso, viene de Matriz de Riesgo por Factores
Tipo de Evento	Tipo de evento, viene de MRF
Evento de Riesgo	Descripción del evento de pérdida, se compone de el tipo de pérdida mas el evento de riesgo identificado, viene de MRF
Riesgo Inherente - P	Promedio ponderado de la calificación de los participantes del taller de la Probabilidad basada en los criterios de la Matriz de Análisis Cualitativo de Riesgos considerando el Riesgo sin controles existentes
Riesgo Inherente - I	Promedio ponderado de la calificación de los participantes del taller del Impacto basado en los criterios de la Matriz de Análisis Cualitativo de Riesgos considerando el Riesgo sin controles existentes
Riesgo Inherente - Z	Es la combinación de Probabilidad e Impacto para determinar el Nivel de Riesgo Inherente
Riesgo Inherente - N	Nivel de Riesgo Inherente basado en la Matriz de Analisis Cualitativo de Riesgos
Controles Actuales	Controles existentes en el proceso por donde pasa el riesgo identificado
Tipo de Control	Tipos de Categoria (RP reduce la prob de ocurrencia del evento y RC reduce el impacto, Tipo Preventivo o Detectivo, Tipo Manual o Automático y Situación de la implementación
Eficiencia en la ejecución de los Controles	Eficiencia identificada tanto en el diseño del control y en la operatividad del mismo, si este está siendo aplicado y ejecutado
Riesgo Residual - P	Promedio ponderado de la calificación de los participantes del taller de la Probabilidad basada en los criterios de la Matriz de Análisis Cualitativo de Riesgos considerando el Riesgo con los controles actuales y basado en su eficiencia.
Riesgo Residual - I	Promedio ponderado de la calificación de los participantes del taller del Impacto basado en los criterios de la Matriz de Análisis Cualitativo de Riesgos considerando el Riesgo con los controles actuales y basado en su eficiencia.
Riesgo Residual - Z	Es la combinación de Probabilidad e Impacto para determinar el Nivel de Riesgo Residual
Riesgo Residual - N	Nivel de Riesgo Residual basado en la Matriz de Analisis Cualitativo de Riesgos
Respuesta al Riesgo	Respuesta que se quiere dar al Riesgo, puede ser: Asumir, Evitar,Transferir o Compartir
Sugerencia de acción (Plan de Tratamiento de Riesgos)	La Matriz sugiere la acción a realizarse, para poder enfocar el Control necesario ya sea: disminuir la probabilidad o disminuir el impacto
Controles deseados	Se registra los Controles se sugieren para minimizar el nivel de riesgo, a todos aquellos riesgos cuyo nivel de riesgo sea mayor al aceptado por el Banco
Riesgo Residual Deseado - P	Promedio ponderado de la calificación de los participantes del taller de la Probabilidad basada en los criterios de la Matriz de Análisis Cualitativo de Riesgos considerando el Riesgo con los controles actuales, basado en su eficiencia y los Nuevos controles que se están proponiendo
Riesgo Residual Deseado - I	Promedio ponderado de la calificación de los participantes del taller del Impacto basado en los criterios de la Matriz de Análisis Cualitativo de Riesgos considerando el Riesgo con los controles actuales, basado en su eficiencia y los Nuevos controles que se están proponiendo
Riesgo Residual Deseado - Z	Es la combinación de Probabilidad e Impacto para determinar el Nivel de Riesgo Residual Deseado
Riesgo Residual Deseado - N	Nivel de Riesgo Residual Deseado basado en la Matriz de Analisis Cualitativo de Riesgos

Tabla 4.9. Matriz de Riesgos y Controles Empleados

Los eventos de bajo impacto y probabilidad no ameritan por la unidad de riesgos una mayor atención, mientras que los eventos de alto impacto y alta probabilidad ameritan atención y un análisis considerable respecto a la implementación de los controles que lo mitigan.

Los niveles o parámetros a evaluar serán: INFERIOR, MODERADO, ALTO y EXTREMO al igual que la evaluación de los controles

4.4.5.3. Matriz de análisis cualitativo de Riesgos – Nivel de Riesgos.

Matriz de análisis cualitativo de riesgos - Nivel de riesgos					
Impacto (5) Catastrófico	ALTO	ALTO	EXTREMO	EXTREMO	EXTREMO
(4) Mayor	MODERADO	ALTO	ALTO	EXTREMO	EXTREMO
(3) Medio	INFERIOR	MODERADO	ALTO	EXTREMO	EXTREMO
(2) Bajo	INFERIOR	INFERIOR	MODERADO	ALTO	EXTREMO
(1) Insignificante	INFERIOR	INFERIOR	MODERADO	ALTO	ALTO
	(1) Bajo	(2) Bajo-Medio	(3) Medio	(4) Medio-Alto	(5) Alto
	PROBABILIDAD				

Tabla 4.10. Matriz de análisis cualitativo de riesgos

La matriz de análisis cualitativo de riesgos es una matriz de 5X5 que relaciona las variables de probabilidad e impacto, las cuales al combinarse resultan en veinticinco áreas de riesgo agrupadas por niveles según el siguiente cuadro:

Niveles de Riesgo	Definición
INFERIOR	RIESGO INFERIOR: El riesgo considerado como mínimo basado en los procesos y controles actuales. Son gestionados bajo procedimientos de rutina. Baja probabilidad e impacto.
MODERADO	RIESGO MODERADO: Son riesgos de los cuales existen procedimientos implementados para el control del riesgo.
ALTO	ALTO RIESGO: Estos riesgos podrían ser de un impacto importante para el Banco. Se necesita un monitoreo de los mismos así como la definición del personal responsable por estas tareas. Adicionalmente se deberían hacer reportes frecuentes al Comité de Administración Integral de Riesgos.
EXTREMO	RIESGO EXTREMO: En estos riesgos no se dispone de controles que impidan el evento o los controles son ineficientes, provocando pérdidas financieras a la Institución. Adicionalmente se deberían hacer reportes frecuentes al Comité de Administración Integral de Riesgos. Se requiere de acción inmediata

Tabla 4.11. Niveles de Riesgo

Los parámetros a considerar más detalladamente son los siguientes:

a) Frecuencia: Enfocada a la probabilidad de ocurrencia de las fallas o contingencias.
b) Impacto: En base a la severidad del riesgo en caso de contingencias externas como fallas internas.
c) La severidad es el resultado de multiplicar el valor de probabilidad por el valor de impacto.

Al identificar el impacto de los eventos de riesgos operativo a los que el Banco está expuesto, se podrán dimensionar las medidas de prevención y recuperación de acuerdo a las necesidades que presenta.

Una vez realizada la relación probabilidad e impacto por cada evento de riesgos, se determina si el riesgo resultante responde a la calificación agrupada por niveles.

Se realiza una priorización de los eventos de riesgo identificados de acuerdo a los niveles de riesgo resultantes

Extremos y Altos, en donde se requiere una acción inmediata por el Comité de Administración de Riesgos para su control y monitoreo. No serán aceptados riesgos superiores al nivel residual "Moderado", por tanto se dará prioridad en la efectividad de los controles a aquellos que no cumplan este nivel.

4.4.5.4. Cuantificación en la eficiencia de la ejecución de controles.

Una vez identificados los riesgos, se realiza la determinación para establecer la efectividad de los controles que han sido incorporados a efectos de mitigar los riesgos, los cuales estarán clasificados de acuerdo a la siguiente escala:

CALIFICACIÓN DE EFECTIVIDAD DE CONTROLES	
1	NINGUNO
2	BAJO
3	MEDIO
4	ALTO
5	DESTACADO

Tabla 4.12. Calificación de Efectividad de Controles

4.4.6. Tratamiento de Riesgos.

Una vez definidos los controles existentes para cada evento de riesgo encontrado se determina un plan de acción o tratamiento de brechas o llamado también plan de mitigación para evitar, transferir, compartir o asumir el riesgo, reduciendo sus consecuencias y efectos.

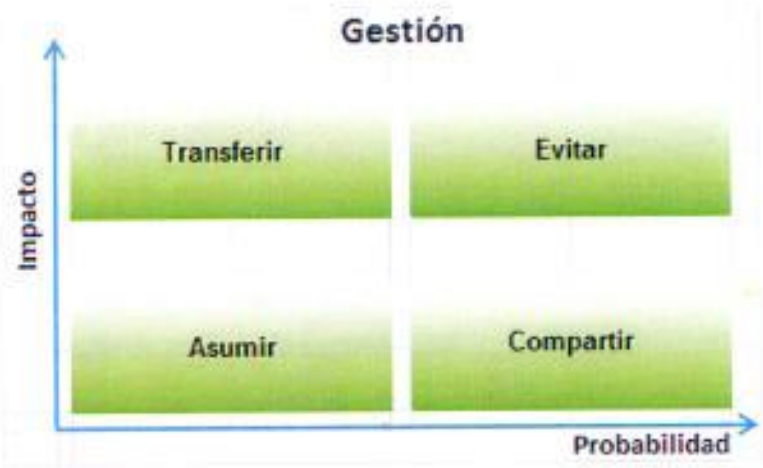


Figura 4.5. Tratamiento de Riesgos

Los responsables de área conjunto con la Alta Gerencia, propondrán la respuesta al riesgo por evento y las acciones a tomar para cerrar las brechas de control, debiendo registrar estas acciones en una matriz de riesgos y controles que deberá ser aprobado por el Comité de Administración Integral de Riesgos y Directorio. Para realizar el seguimiento de los controles, se realizarán las plantillas de tratamiento de riesgos.

a) Evitar: No se identifican opciones de respuesta que lleven el riego residual a un nivel aceptable. Eliminar la fuente del riesgo: unidad del negocio, línea de productos, segmento geográfico, etc. Decidir no comprometerse en nuevas iniciativas/actividades que aumentarían el riesgo.

b) Compartir: Reducir impacto y/o probabilidad compartiendo el riesgo con un tercero. Asegurar pérdidas significativas inesperadas y realizar alianzas estratégicas. Tercerizar procesos de negocios. La tercerización puede constituir una amenaza en la relación costo/riesgo. Evaluar si es correcta la observación. Acuerdos contractuales con clientes, proveedores u otros socios de negocios.

c) Asumir: El riesgo residual está dentro de las tolerancias deseadas. No se toma acción para reducir impacto y probabilidad. Auto asegurarse contra pérdidas.

d) Transferir: Transferir aquellos riesgos que no se está dispuesto a gestionar. Cubrir riesgos a través de Instrumentos financieros. Contratación de pólizas de seguros.

Preparación e implementación de los planes para el tratamiento del riesgo (fichas):

La información suministrada en los planes de tratamiento incluye:

a) Las razones para la selección de las opciones de tratamiento, que incluyan los beneficios que se espera obtener;
b) Los responsables de aprobar el plan y los responsables de implementarlo
c) Acciones propuestas
d) Requisitos de recursos, incluyendo las contingencias
e) Tiempo y cronograma.(Ficha de Inicio y fecha final)

Los controles pueden involucrar políticas efectivas, procedimientos o cambios físicos. La selección de la opción más apropiada involucra la comparación del costo de la realización versus el beneficio esperado, La institución evalúa las opciones que reducen el riesgo a un bajo costo y se implementa, pero las que tienen una incidencia económica considerada media alta debe ser evaluada por el área afectada con el Comité de Administración Integral de Riesgos en la medida de que se justifica o no dicha implementación.

Así también cuando se considera la implementación de una nueva tecnología o desarrollo o mejora de alguna aplicación se considerará una priorización de requerimientos los cuales estarán basados en análisis de riesgos y controles, tiempo de desarrollo, costo beneficio dado por las

áreas afectadas para su respectiva implementación y prioridad organizacional.

Deberá asignarse responsables los cuales velaran por la implementación correcta, si luego de efectuarse el tratamiento existiera algún riesgo residual que no se había detectado o que sea de nivel Moderado, se debe tomar nuevamente la decisión de repetir el proceso de tratamiento de los riesgos.

BANCO COOPNACIONAL

PLANTILLA DE TRATAMIENTO DE RIESGOS

Taller No:

Fecha: dd/mm/aaaa

Evento de Riesgo:

Descripción del Riesgo:

Nivel de Riesgo Inherente:

Descripción:

Control Actual	Responsable del Control	Tipo de Control	Frecuencia

Nivel de Riesgo Residual

Descripción:

Respuesta (Evitar,Compartir, Asumir o Rechazar):

Razones la elaboración de un plan de tratamiento de riesgos:

Plan de Tratamiento o Sugerencias de acción:

Responsable	Area	Acciones	Fecha Inicio	Fecha Final	Requisitos o Req.	Estatus	Desempeño

Nivel de Riesgo Deseado u Objetivo:

Descripción:

Figura 4.6. Plantilla de Tratamiento de Riesgos

4.4.6.1. Base de Datos de Eventos de Riesgo Operativo.

En razón de que la administración del riesgo operativo constituye un proceso continuo y permanente, será necesario que el Banco conforme bases de datos centralizadas, suficientes y de calidad, que permitan registrar, ordenar, clasificar y disponer de información sobre los eventos de riesgo operativo; fallas o insuficiencias incluidas las de orden legal; y, factores de riesgo operativo clasificados por línea de negocio, determinando la frecuencia con que se repite cada evento y el efecto cuantitativo de pérdida producida y otra información que el Banco considere necesaria y oportuna, para que a futuro se pueda estimar las pérdidas esperadas e inesperadas atribuibles a este riesgo.

Se debe tomar en cuenta los tipos de pérdidas como se detalla a continuación:

Pérdidas Directas vs. Pérdidas indirectas.

a) **Directas:** Impacto visible sobre el Estado de Pérdidas y Ganancias; ej. Multas pagadas a organismos de control, intereses por cancelaciones tardías de operaciones, contra-cargos no presentados a tiempo.

b) **Indirectas:** Impacto no directamente visible en el Estado de Pérdidas y Ganancias; ej. Operaciones no realizadas por fallas en sistemas, comunicaciones, etc. Negocios no concretados por falta de conocimiento, capacidad o entrenamiento. Operaciones no realizadas por falta de documentación, Horas hombre gastadas en resolver fallas diarias, hacer procesos ineficientes, costos de oportunidad en general.

La información a ingresar será la siguiente:

a) Proceso
b) Sub-Proceso
c) Evento
d) Causa de Evento
e) Factores de Riesgo Operativo
f) Tipo de Evento Operativo
g) Producto o Servicio Asociado
h) Efecto o Consecuencia
i) Pérdidas Monetarias (Directas o Indirectas)
j) Falla o Insuficiencia
k) Frecuencia del Evento
l) Nivel de Riesgo Inherente (Probabilidad, Impacto, Nivel de Riesgo)
m) Control Actual
n) Eficiencia en los Controles
o) Nivel de riesgo residual (Probabilidad, Impacto, Nivel de Riesgo)
p) Respuesta al Riesgo
q) Plan de Contingencia o Mitigación/Acciones de control
r) Nivel de Riesgo Residual Deseado u Objetivo (Probabilidad, Impacto, Nivel de Riesgo)
s) Residual Neto Calculado

4.4.6.2. Control.

Un aspecto importante de la administración del riesgo operativo es el control, por tal motivo el Banco deberá contar con sistemas de control interno adecuados, esto es, políticas, procesos, procedimientos y niveles de control formalmente establecidos y validados periódicamente. Los controles deben formar parte integral de las actividades regulares de la entidad para generar respuestas oportunas ante diversos eventos de riesgo operativo y las fallas o insuficiencias que los ocasionaron.

El control de los eventos de riesgo operativo del Banco estará dado por las revisiones periódicas por parte de Auditoría Interna, debiendo esta unidad incorporar en su plan de auditoría anual las revisiones relacionadas con el riesgo operativo de la institución.

Todos los eventos de riesgo operativo identificados a través de cuestionarios, talleres y reportes de notificación de eventos por parte de los responsables de los procesos, deberán ser registrados en la Base de Datos de Eventos de Riesgo.

Producto de los eventos de riesgos identificados y los suscitados, se generarán nuevos controles que derivarán en actividades y proyectos cuyo seguimiento mensual estará a cargo del Analista de Riesgo Operativo y su implementación a cargo de los responsables de proceso. Los responsables de la implementación de los Controles establecidos en las fichas de tratamiento de riesgos enviarán a la Unidad de Riesgos los informes sobre los avances hasta la tercera semana de cada mes.

Si la implementación de un control implica la actualización de políticas o procedimientos, se notificará al responsable del proceso para que se encargue de la actualización del respectivo manual, su aprobación e implementación.

La Unidad de Riesgos se encargará de verificar y monitorear que los controles identificados para minimizar los riesgos operativos estén debidamente implementados y formalizados al incorporarlos en la normativa interna (políticas, procedimientos, planes y reglamentos), en los sistemas aplicativos y en la infraestructura tecnológica cuando se disponga.

4.4.7. Monitoreo y Revisión.

El Banco debe contar permanentemente con un esquema organizado de reportes que permitan disponer de información suficiente y adecuada para gestionar el riesgo operativo en forma continua y oportuna.

CAPÍTULO 5.

IMPLEMENTACIÓN DE UN SISTEMA DE INFORMACIÓN PARA LA ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO EN LA BANCA

Capítulo 5.

Implementación de un Sistema de Información para la Administración del Riesgo Tecnológico en la Banca.

5.1. Características del Sistema de Información

Una vez establecido la matriz de riesgo a nivel de tecnología, se ve la necesidad de automatizar dicha información, en el cual se puede recuperar la información ingresada por el usuario en un período de tiempo óptimo, con la ayuda de la herramienta informática se puede tener un mejor control en el análisis de riesgo.

Figura 5.1. Ingreso al Sistema de Administración de Riesgo Operativo

Para poder ingresar al Sistema de Administración de Riesgo Operativo se necesita tener un usuario y una clave; la información ingresada se validará con las seguridades a nivel del Sistema.

Figura 5.2. Pantalla Principal del Sistema de Administración de Riesgo Operativo

Una vez que el usuario ha ingresado correctamente el usuario y la clave; nos muestra la pantalla principal del Sistema con las diferentes opciones:

- **Archivo.-** Maneja información de configuración del Sistema
- **Maestro.-** Contiene información básica que se va a utilizar en los procesos Transaccionales.
- **Procesos.-** Se ingresa los procesos relacionados a la Administración de Riesgos.
- **Consulta – Reporte.-** Se visualiza a través de una opción la información ingresada.
- **Ayuda.-** Muestra la versión del Sistema de Administración de Riesgo Operativo.

5.2. Maestro

5.2.1. Monitoreo y Revisión.

Figura 5.3. Ingreso de los Procesos de Riesgo

La opción de Proceso de Riesgo se ingresa todas las actividades relacionadas a un producto o servicio al cliente, siendo un complemento para el ingreso de la transacción de Riesgo.

5.2.2. Sub-Proceso

Figura 5.4. Ingreso del Sub-Proceso de Riesgo

La opción de Sub-Proceso de Riesgo se ingresa todas las actividades relacionadas al Proceso inicial de un producto o servicio al cliente, siendo un complemento para el ingreso de la transacción de Riesgo.

5.2.3. Evento.

Figura 5.5. Ingreso de los Eventos de Riesgo

La opción de Evento de Riesgo se ingresa todas las actividades relacionadas al Proceso y Subproceso enfocado a un producto o servicio al cliente, siendo un complemento para el ingreso de la transacción de Riesgo.

5.2.4. Causa.

Figura 5.6. Ingreso de la Causa de Riesgo

La opción de Ingreso de Causa de Riesgo es un parámetro de almacenamiento el cual se complementa a los procesos de Riesgos.

5.2.5. Factores.

Figura 5.7. Ingreso de los Factores de Riesgo

La opción de Factores de Riesgo es la causa primaria o el origen de un evento de riesgo operativo que se complementa en el proceso de Matriz de Riesgo.

5.2.6. Tipo de Evento.

Figura 5.8. Ingreso de los Tipos de Eventos de Riesgo

La opción de Tipo de Evento es un complemento de acuerdo a la Gestión de Riesgo Operativo para la creación de la Matriz de Riesgo.

5.2.7. Producto.

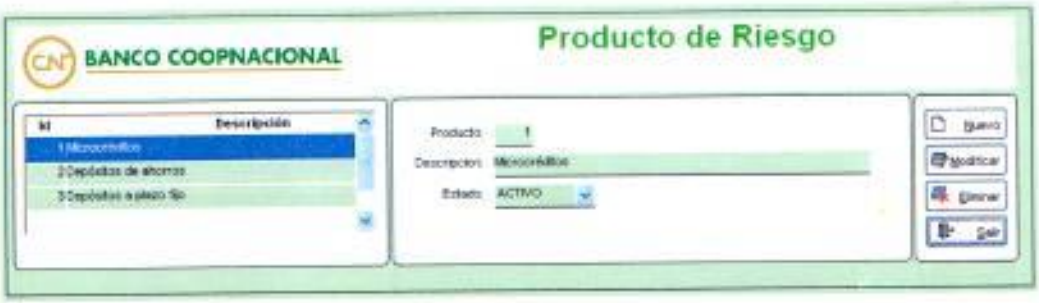


Figura 5.9. Ingreso de los Productos o Servicios

La opción de Ingreso de Productos o Servicios tiene como objetivo a nivel de productos que generen valor para la institución, esta información servirá como complemento para la creación de la Matriz de Riesgo.

5.2.8. Efecto.

Figura 5.10. Ingreso de los Efectos de Riesgo

La opción de Efectos de Riesgo tiene como objetivo indicar las consecuencias que pueden darse al momento de presentarse un incidente que afecte el rendimiento de la institución, esta información servirá como complemento para la creación de la Matriz de Riesgo.

5.2.9. Pérdidas Monetarias.

Figura 5.11. Ingreso de las Pérdidas Monetarias

La opción de Pérdidas Monetarias tiene como objetivo indicar las consecuencias a nivel económico que pueden darse al momento de presentarse un incidente que afecte el rendimiento de la institución, esta información servirá como complemento para la creación de la Matriz de Riesgo.

5.2.10. Frecuencia.

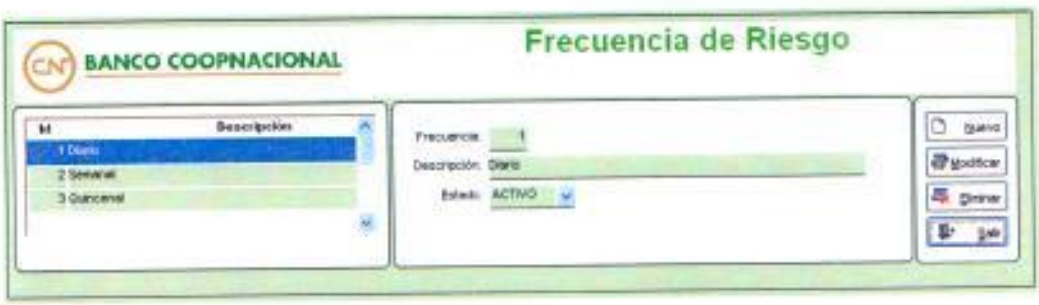


Figura 5.12. Ingreso de la Frecuencia

La opción de ingreso de Frecuencia se puede determinar el tiempo en el cual se presentan las novedades, esta información servirá como complemento para la creación de la Matriz de Riesgo.

5.2.11. Probabilidad

Figura 5.13. Ingreso de las Probabilidad de Riesgo

La opción de ingreso de Probabilidad se refiere a la frecuencia con la que se puede representar el evento de riesgo, esta información servirá como complemento para la creación de la Matriz de Riesgo.

5.2.12. Impacto.

Figura 5.14. Ingreso del Impacto de Riesgo

La opción de Impacto de Riesgo se puede determinar la magnitud de la consecuencia si se llega a presentar el evento, esta información servirá como complemento para la creación de la Matriz de Riesgo.

5.2.13. Eficiencia.

Figura 5.15. Ingreso de la Eficiencia en los Controles

La opción de eficiencia se puede determinar el grado de validez del control implementado, esta información servirá como complemento para la creación de la Matriz de Riesgo.

5.2.14. Respuesta al Riesgo.

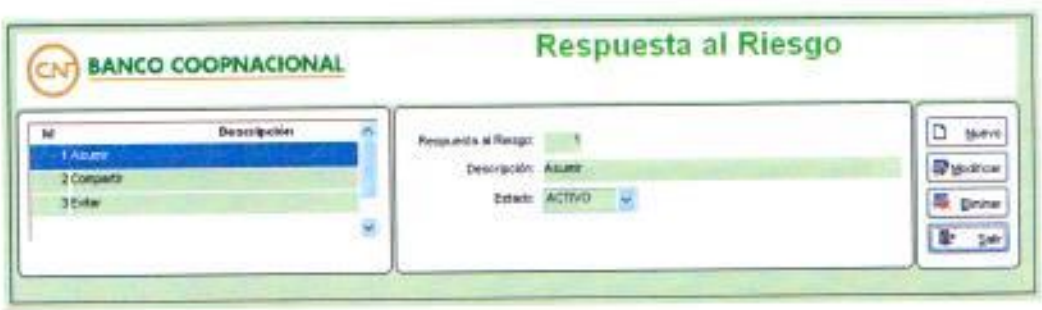


Figura 5.16. Ingreso de la Respuesta al Riesgo

La opción de ingreso de Respuesta al Riesgo es el grado de responsabilidad que se le va a dar a un evento de riesgo, pudiendo asumir, compartir o evitar el grado de peligro a la entidad.

5.2.15. Persona.

Figura 5.17. Ingreso de la Persona

La opción de ingreso de persona se especifica a los elementos que van a estar incluidos en la gestión de riesgo, esta información servirá como complemento para la creación de la Matriz de Riesgo.

5.2.16. Tipo de Manual.

Figura 5.18. Ingreso del Tipo de Manual

La opción de Tipo de Manual se especifica la documentación a usar en el Plan de Acción de Medición de Riesgo.

5.2.17. Efectividad del Control.

Figura 5.19. Ingreso de la Efectividad del Control

La opción de efectividad de control se especifica el grado de certeza que se le da a un control, esta información servirá como complemento para la creación de la Matriz de Riesgo.

5.3. Procesos

5.3.1. Matriz de Riesgo.

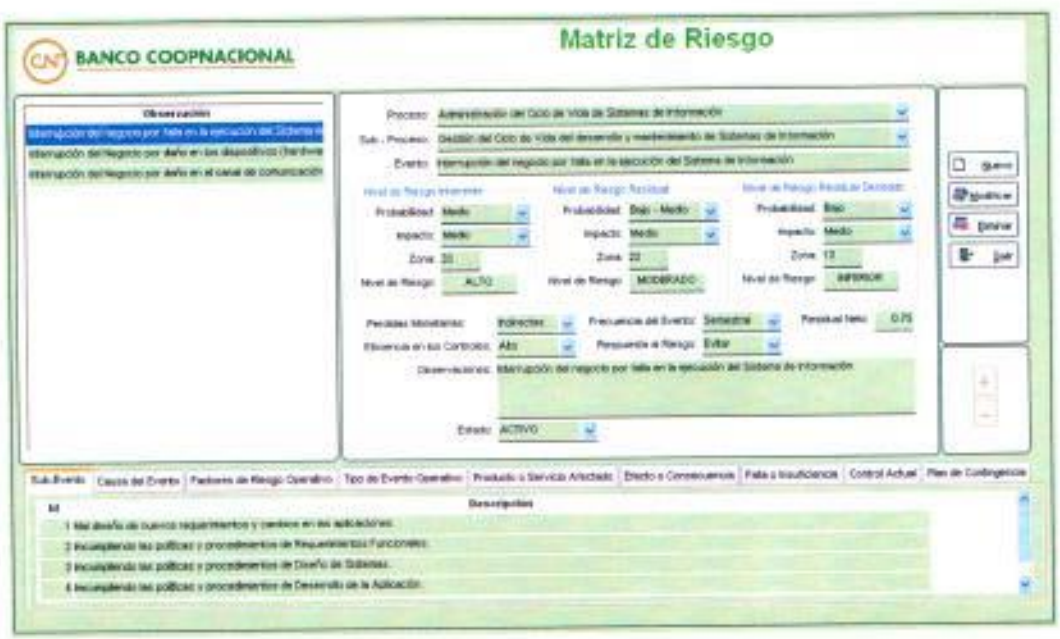


Figura 5.20. Ingreso de la Matriz de Riesgo – Sub-Evento

El proceso de Matriz de riesgo se detallan todos los Eventos que se presentan en la institución indicando el nivel de riesgo inherente, riesgo residual y el riesgo deseado, especificando el grado de sensibilidad y el nivel de importancia que se debe brindar para minimizar los eventos criticos de la entidad.

Figura 5.21. Ingreso de la Matriz de Riesgo – Causa del Evento

En el Proceso de Matriz de Riesgo se puede ingresar más de una causa de evento pudiendo determinar el grado de responsabilidad de las personas que involucran en el proceso de controlar la eventualidad.

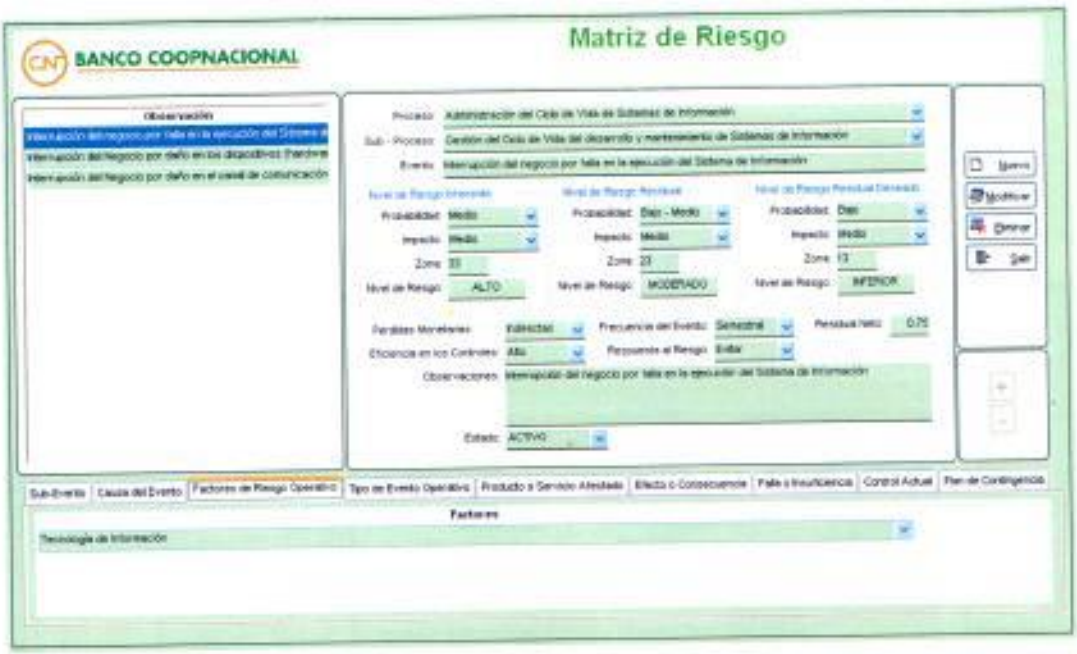


Figura 5.21. Ingreso de la Matriz de Riesgo – Factores de Riesgo Operativo

La opción de Factores de Riesgo Operativo en la Matriz de Riesgo son los diferentes escenarios que se presentan y se debe minimizar.

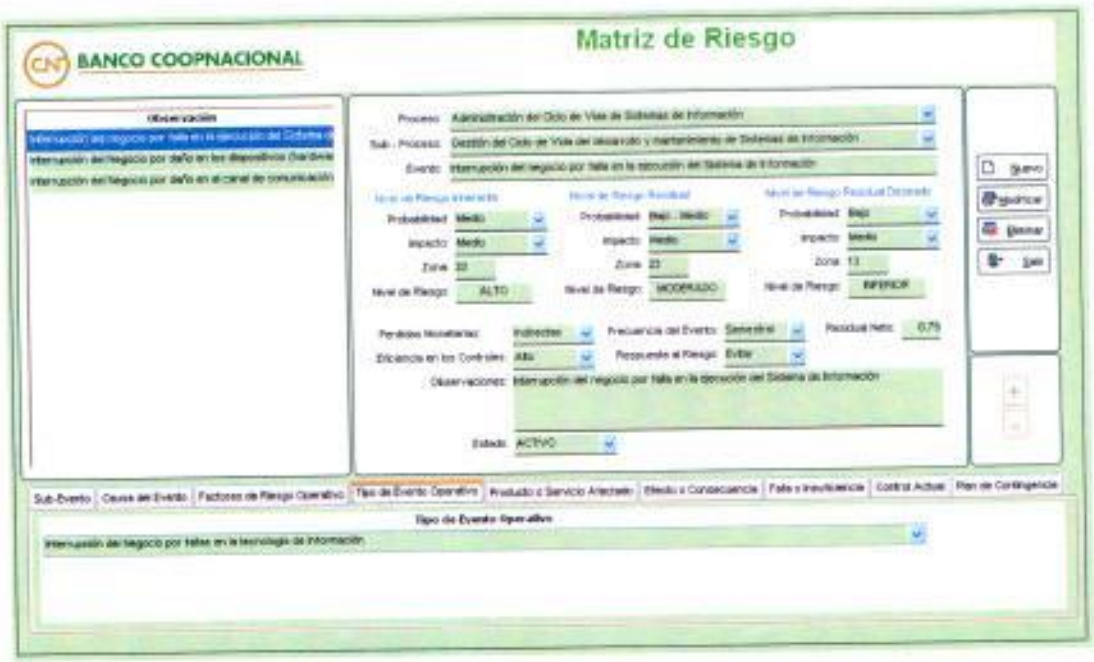


Figura 5.22. Ingreso de la Matriz de Riesgo – Tipo de Evento Operativo

La opción de Tipo de Evento es un complemento de acuerdo a la Gestión de Riesgo Operativo para la creación de la Matriz de Riesgo, se determina cuáles son los motivos que pueden originar algún incidente de seguridad en la institución.

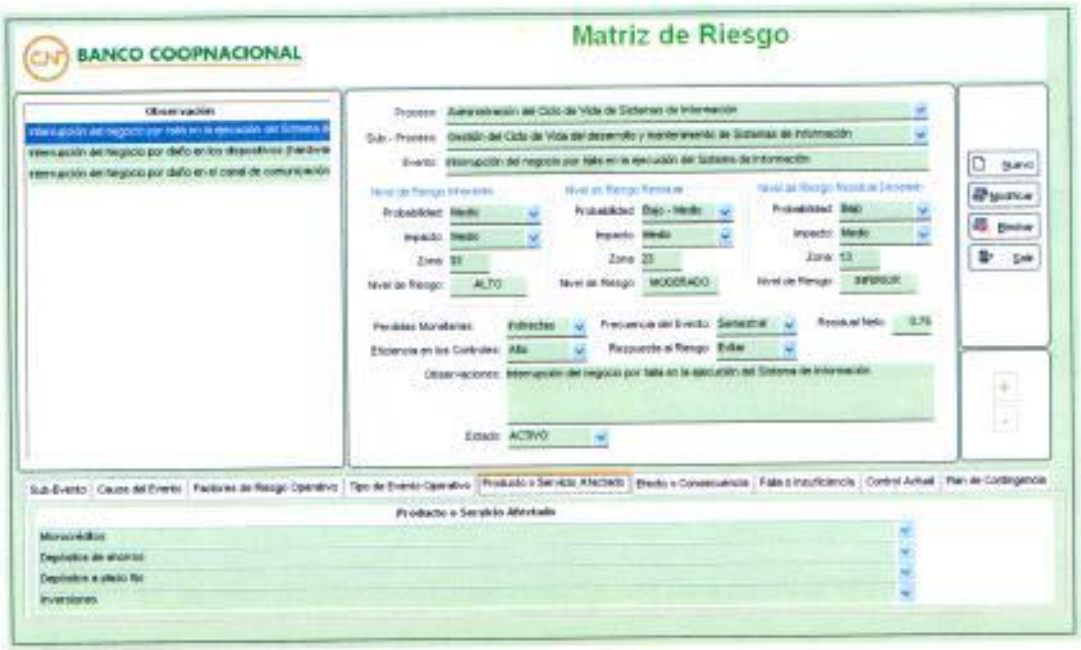


Figura 5.23. Ingreso de la Matriz de Riesgo – Producto o Servicio Afectado

El ingreso del producto o servicio afectado nos da a conocer que Servicios de la Institución son afectados en el caso de presentarse un incidente semejante en la entidad.

Figura 5.24. Ingreso de la Matriz de Riesgo – Efecto o Consecuencia

El ingreso de Efecto o Consecuencia nos da a conocer el resultado del Evento que se presenta en la entidad.

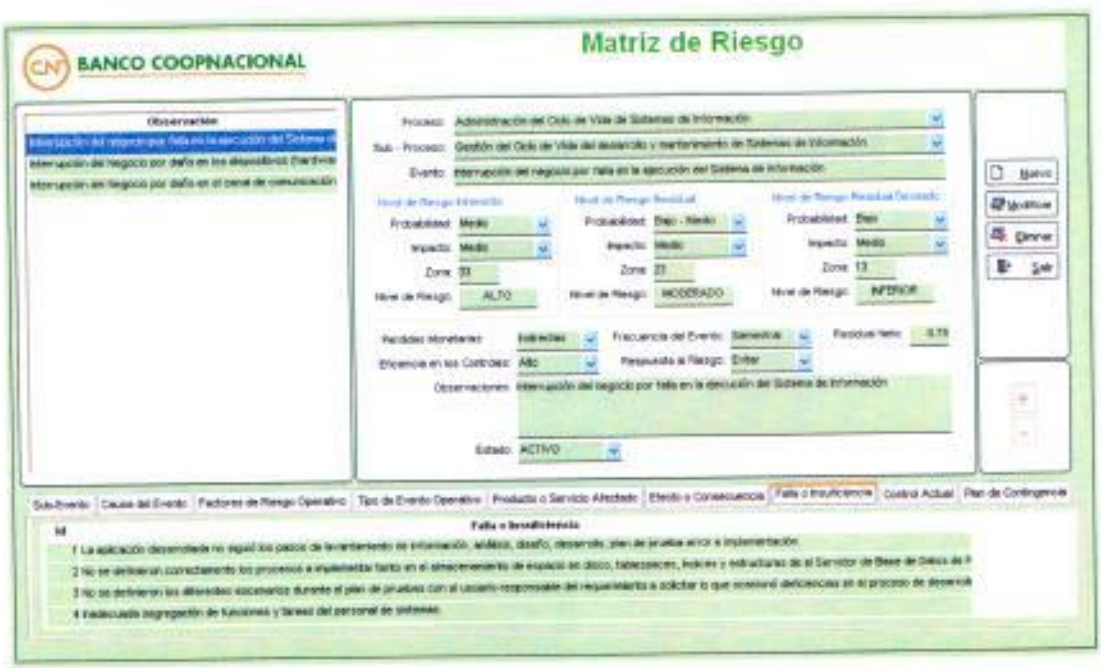


Figura 5.25. Ingreso de la Matriz de Riesgo – Falla o Insuficiencia

El ingreso de Falla o Insuficiencia nos da a conocer a nivel de personal en donde se originó el incidente, determinando responsabilidad por falta de control de previsión por parte del grupo departamental.

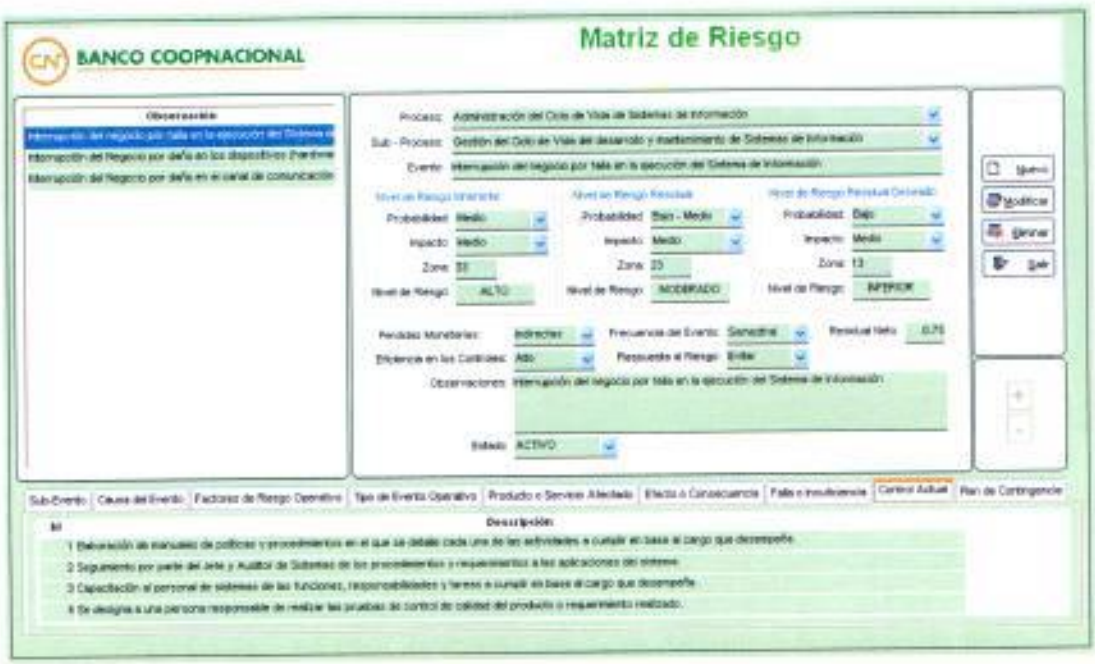


Figura 5.26. Ingreso de la Matriz de Riesgo – Control Actual

El ingreso de los Controles que se tiene actualmente en para minimizar el Riesgo, se determina las observaciones generales que se realizan para controlar que el Evento que se presente no tenga un impacto de gran consecuencia para la entidad sino minimizar y mejorar su control.

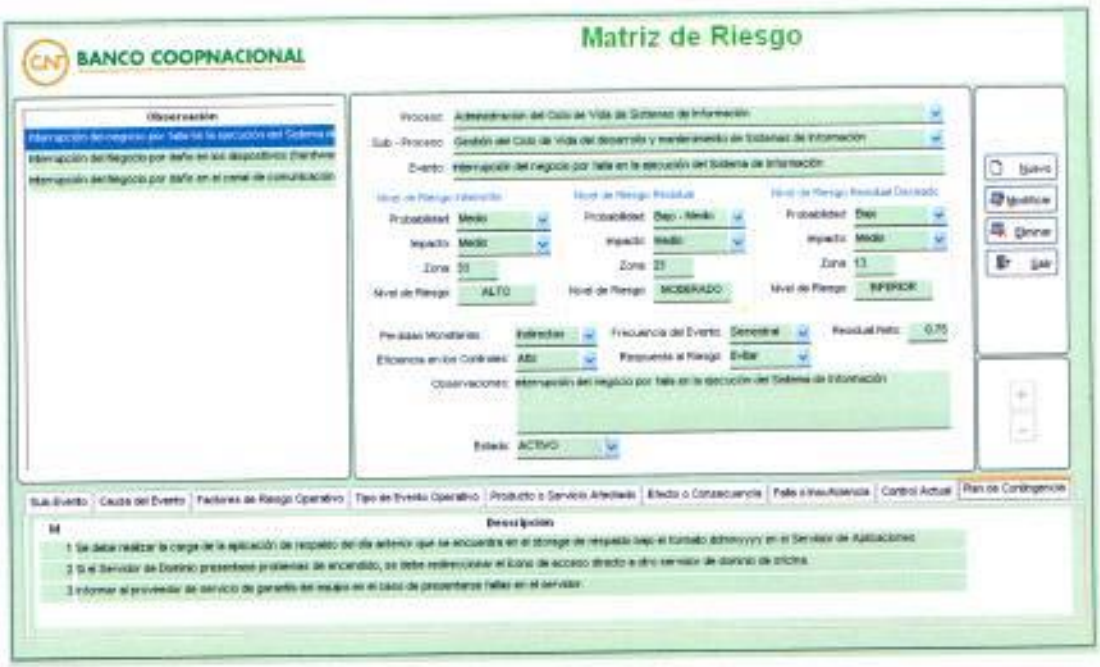


Figura 5.27. Ingreso de la Matriz de Riesgo – Plan de Contingencia

El ingreso del Plan de Contingencia se determina la secuencia de pasos a seguir en el caso de presentarse algún Incidente que afecte el rendimiento de la Entidad.

5.3.2. Plan de Acción.

Figura 5.28. Plan de Acción – Manuales

El ingreso del Plan de Acción se determina la secuencia de pasos a seguir en el caso de presentarse el Evento en la Entidad, a su vez se indica los manuales que se deben conocer para lograr que el impacto no afecte a la institución.

Figura 5.29. Plan de Acción – Asigna Responsables

El ingreso de Asignación de Responsables nos da a conocer la segregación de funciones por cada tipo de evento que se presenta y la función que debe cumplir el mismo.

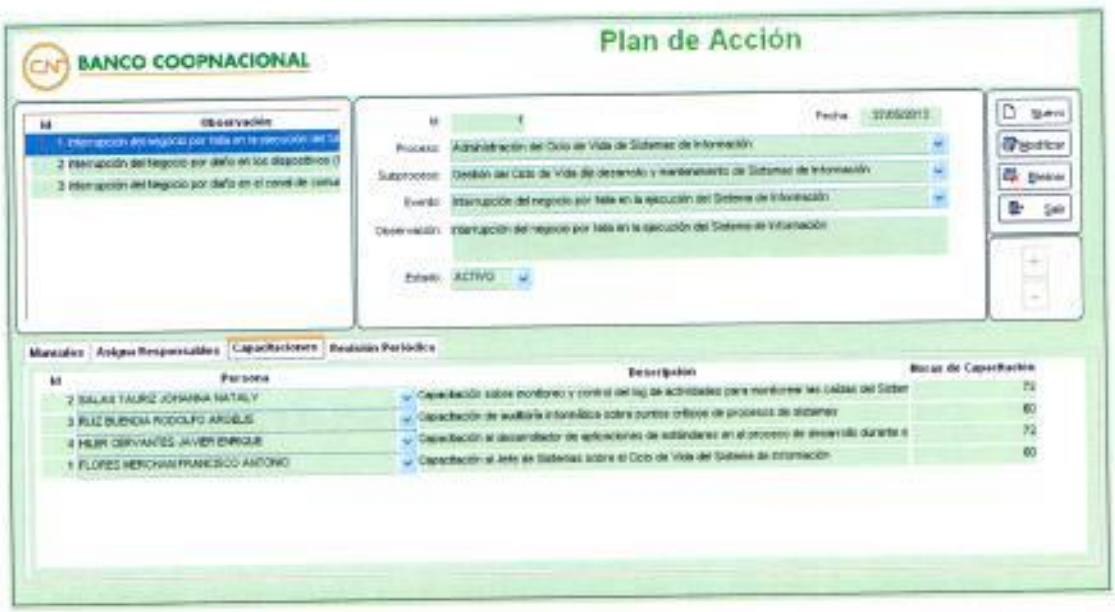


Figura 5.30. Plan de Acción – Capacitaciones

El ingreso de Capacitaciones se da a conocer la preparación que se le ha dado al personal para mejorar la eficiencia del departamento.

Figura 5.31. Plan de Acción – Revisión Periódica

El ingreso de la Revisión Periódica se establece el seguimiento en un tiempo determinado para verificar que los manuales, las personas responsables y las capacitaciones se han brindado en el tiempo necesario para actuar en el caso de presentarse un incidente en la institución.

5.3.3. Control de Eventualidad.

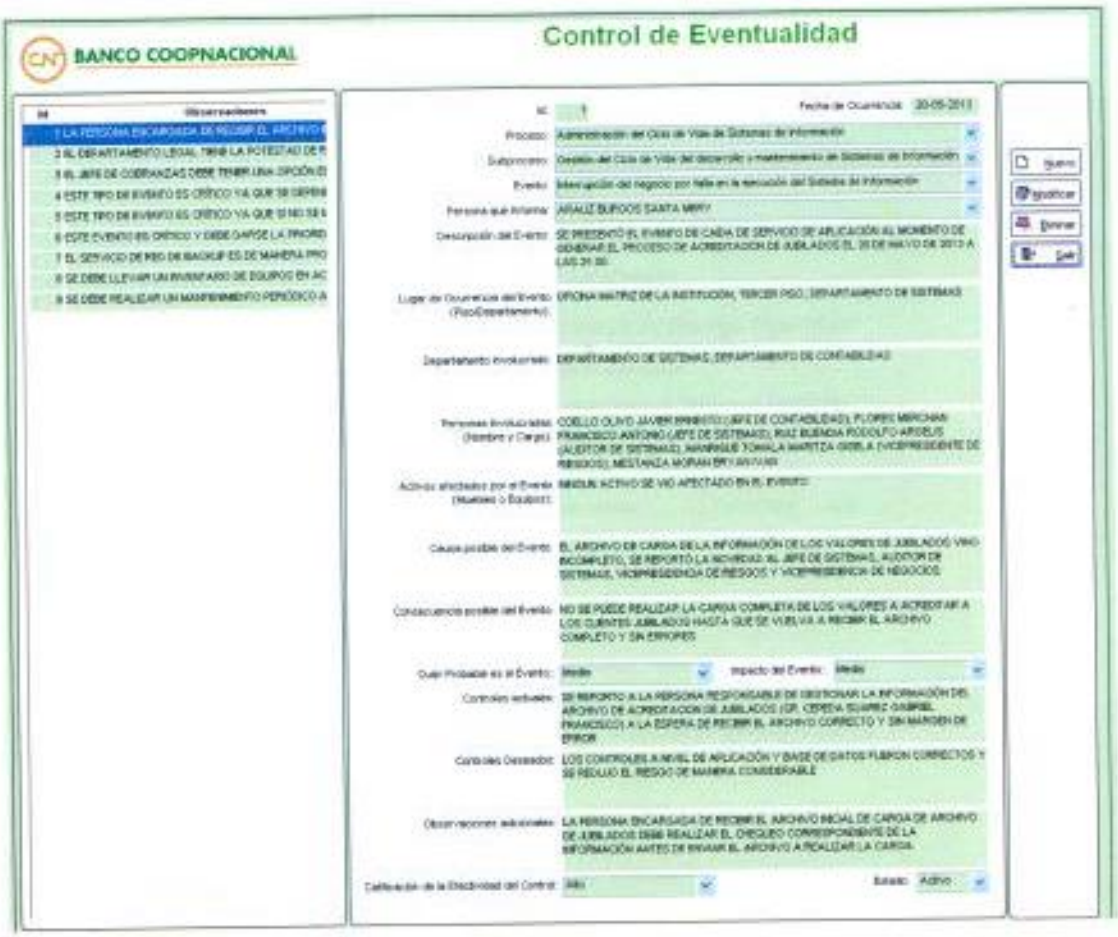


Figura 5.32. Control de Eventualidad

El Control de Eventualidad determina los lineamientos, pasos y procedimientos que se ejecutaron en el momento de presentar el evento, indicando la fecha y hora presentada del evento indicando si el plan de acción se ejecutó correctamente.

5.4. Consulta - Reportes

5.4.1. Notificación Formal de Eventos de Riesgo Operativo.

Figura 5.33. Notificación Formal de Eventos de Riesgo Operativo

El reporte de Notificación formal de Eventos de Riesgo Operativo nos da a conocer los eventos que maneja la entidad con el nivel de riesgo que presenta aplicando los controles necesarios para minimizar el riesgo en cada uno de los eventos.

5.4.2. Control de Eventualidad de Eventos de Riesgo Operativo.

Figura 5.34. Control de Eventualidad de Eventos de Riesgo Operativo

El reporte de Control de Eventualidad determina los lineamientos, pasos y procedimientos que se ejecutaron en el momento de presentar el evento, indicando la fecha y hora presentada del evento indicando si el plan de acción que se realizó y el resultado de haber ejecutado todos los lineamientos del Plan de Acción.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones y Recomendaciones

Conclusiones:

- Las Instituciones Bancarias en el Ecuador en los últimos años han tenido un crecimiento muy importante a nivel financiero y operacional, lo que se ve reflejado en el aumento de los depósitos a la vista y las operaciones de crédito; convirtiéndose después de los bancos, en el principal subsector financiero del país.
- El uso de la tecnología y los sistemas de información en las Instituciones Bancarias es un aspecto fundamental dentro de la planificación estratégica, la realización de sus operaciones, el control interno y financiero y el mejoramiento de los productos y servicios ofrecidos a sus clientes.
- El Control Interno es una herramienta fundamental para lograr una eficiencia, eficacia, productividad y el desarrollo operativo y administrativo de las Instituciones Bancarias bajo un ambiente de prevención de riesgos y pro actividad en el logro de los objetivos institucionales.
- Las Instituciones Bancarias tienen la necesidad de adaptar su gestión hacia una cultura de prevención y administración de los diferentes riesgos a los cuales se enfrenta su giro de negocio; entre los que según el Acuerdo de Basilea se componen en riesgo de mercado, riesgo de liquidez y riesgo operacional.
- La Superintendencia de Bancos y Seguros del Ecuador consciente de la necesidad de que las Instituciones Bancarias incorporen a sus procesos de negocio la administración integral de sus riesgos de acuerdo a los lineamientos del Acuerdo de Basilea, ha emitido un conjunto de resoluciones y normativas orientadas hacia una administración de los riesgos, responsable y eficaz en las Entidades Financieras que se encuentran bajo su control.
- La resolución conocida como 834 emitida por la Superintendencia de Bancos incorpora los lineamientos y mejores prácticas de control interno para la administración del riesgo operacional para las Entidades Financieras

del Ecuador e identifica 4 aspectos de la administración del riesgo operaciones que deben ser administrados en forma adecuada: los procesos, las personas, la tecnología de información y los eventos externos.

- La administración del riesgo tecnológico es un aspecto fundamental control de la gestión de riesgo operativo y es una de las responsabilidades y desafíos más importantes a las que se enfrentan las Instituciones Bancarias en el Ecuador, debido a que involucra el uso de recursos organizacionales, humanos, financieros y tecnológicos.
- El rol de auditoría ha evolucionado en los últimos años de tal forma que se ha convertido en un factor importante dentro de la evaluación del riesgo tecnológico y en la mejora continua de los procesos de TI, a través del uso de herramientas tecnológicas para el análisis de las operaciones, la evaluación de riesgos y la planificación de la auditoría.

Recomendaciones

- Las Instituciones Bancarias debe incorporar a sus procesos de negocio la administración de riesgo operacional y del control interno como una oportunidad para lograr los objetivos institucionales, para agregar valor a sus líneas de negocio y alcanzar una ventaja competitiva frente a la competencia; garantizando su desarrollo administrativo, operativo, financiero y tecnológico.
- La Gerencia General debe participar continuamente en la Administración del riesgo, manejando los eventos y escenarios que afectan a la continuidad operativa del negocio con la ayuda de herramientas tecnológicas que nos permita minimizar los factores de riesgo tecnológico en la institución.

ANEXO 1

FICHA DE ENTREVISTA A LOS RESPONSABLES DEL PROCESO PARA LA IDENTIFICACIÓN DE LOS RIESGOS TECNOLÓGICOS

OBJETIVO.-

Se examinará la frecuencia e impacto de los eventos de riesgo posibles a darse en el análisis de los procesos gobernantes, habilitantes y productivos.

DEFINICIONES.-

- ✓ **Eventos de Riesgo.-** es el hecho que puede derivar en pérdidas financieras a la Institución.

- ✓ **Factores de Riesgo.-** Es la causa primario o el origen de un evento de riesgo operativo. Los factores son los ***procesos, personas, tecnología de información y eventos externos.***

El siguiente cuestionario será administrado por el Departamento de Riesgo, el cual ne experiencia en el manejo de la información que se va a recabar por parte del usuario anejando las diferentes variables de asociación entre el riesgo inherente, la probabilidad y el ıpacto que representa dicho evento.

Evento de Riesgo (Operacional/Legal)

Causas del Riesgo

¿Qué tipos de fallas ocurren por factor de riesgo? Describa.

Personal

Sistemas

Proceso

Eventos Externos

¿Qué clase de eventos de riesgo pueden ocurrir?

raude Interno _____

_____

_____

raude Externo _____

_____

_____

rácticas Laborales –Ambiente de Trabajo _____

_____

_____

rácticas con clientes, productos y negocio _____

_____

_____

)año a los Activos Físicos _____

_____

_____

'allas en Sistemas _____

_____

)eficiencias en Ejecución de Procesos _____

_____

_____

Determine el efecto (consecuencia) del riesgo

_____

_____

Determine los controles actuales para el riesgo identificado

¿Cuál es la frecuencia e impacto en la que ocurre cada falla?

FALLAS	Frecuencia o Probabilidad	Impacto	Controles Eficientes	Causa de la falla
Fraude Interno				
Fraude Externo				
Prácticas Laborales Ambiente de Trabajo				
Prácticas con clientes, productos y negocio				
Daño a los Activos Físicos				
Fallas en Sistemas				
Deficiencias en Ejecución de Procesos				

Otros				

Planes de mitigación/contingencia

_____

_____

_____

echa: _____

_____

esponsable del Proceso/Área Responsable

BANCO COOPNACIONAL

NOTIFICACION FORMAL DE EVENTOS DE RIESGO OPERATIVO

NOMBRE:	
FECHA DE OCURRENCIA:	
PERSONA QUE INFORMA:	
TIPO EVENTO DE RIESGO (Fraude Interno, Fraude Externo, Practicas Laborales - Ambiente de Trabajo, Prácticas con clientes, producto y negocio, Daños a los activos físicos, Fallas en Sistemas, Deficiencias en ejecución de procesos)	
DESCRIPCIÓN DEL EVENTO:	
LUGAR DE OCURRENCIA DEL EVENTO (PISO/DEPARTAMENTO):	
DEPARTAMENTO INVOLUCRADO:	
PERSONAS INVOLUCRADAS (NOMBRE Y CARGO):	
PERDIDA ESTIMADA O REAL (EFECTIVO/DOCUMENTOS):	
PERSONAS AFECTADAS POR EL EVENTO (INTERNAS O EXTERNAS):	
ACTIVOS AFECTADOS POR EL EVENTO (MUEBLES O EQUIPOS):	
CAUSA POSIBLE DEL DEL EVENTO:	
CONSECUENCIA POSIBLE DEL EVENTO:	
CUÁN PROBABLE ES EL EVENTO: (Casi cierto, probable, posible, improbable, raro)	
IMPACTO DEL EVENTO:	
CONTROLES ACTUALES:	
CONTROLES DESEADOS:	
OBSERVACIONES ADICIONALES:	

Fecha de Notificación:

Firma del Responsable de Notificar

GLOSARIO DE TÉRMINOS

GLOSARIO DE TÉRMINOS

Actividad: Es el conjunto de tareas

Activos de Información: Se refiere a los datos de la Institución e incluye a los equipos, las aplicaciones, las personas, que se utilizan para crear, gestionar, transmitir y destruir la información y que tienen un valor para la Institución.

Administración de la información: Es el proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito en papel, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes.

Alta gerencia: La integran los presidentes y vicepresidentes ejecutivos, gerentes generales, vicepresidentes o gerentes departamentales, entre otros, responsables de ejecutar las disposiciones del directorio u organismo que haga sus veces, quienes tomarán decisiones de alto nivel, de acuerdo con las funciones asignadas y la estructura organizacional definida en El Banco.

Administrador Base de Datos: Persona que trabaja con los usuarios para crear,

mantener, y salvaguardar los datos que se encuentran en una Base de Datos.

Análisis de Riesgos: Proceso sistemático para estimar la magnitud de los riesgos a la que está expuesta la Institución.

Aplicación: Programa que se utiliza para realizar un determinado tipo de trabajo, como por ejemplo el procesamiento de texto. También suele utilizarse, indistintamente, el término "programa".

Archivo (File): Colección de Datos o programas que sirve para un único propósito. Se almacenan con el objetivo de recuperarlos más adelante.

Auditoría: Seguimiento de las actividades de los usuarios, mediante el registro de tipos de sucesos seleccionados en el registro de seguridad de un servidor o estación de trabajo.

Base de Datos: Conjunto de Datos relacionados con un tipo de aplicación especifico.

Calidad de la información: Es el resultado de la aplicación de los mecanismos implantados que garantizan la efectividad, eficiencia y confiabilidad de la información y los recursos relacionados con ella.

Confiabilidad: Es la garantía de que la información es la apropiada para la administración de la entidad, ejecución de transacciones y para el cumplimiento de sus obligaciones.

Confidencialidad: Es la garantía de que sólo el personal autorizado accede a la información preestablecida.

Ciclo de vida de un sistema: Etapas que intervienen al desarrollar un Sistema. Técnicamente son 4 Análisis, Diseño, Desarrollo e Implementación.

Cumplimiento: Se refiere a la observancia de las leyes, regulaciones y acuerdos contractuales a los que los procesos de El Banco están sujetos.

D

Datos: Es cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido.

Disponibilidad: La información está lista para acceder a ella o utilizarse cuando se necesita.

G

Gestión de la Continuidad del Negocio (BCM): Proceso de gestión integral que identifica las amenazas potenciales para la Institución y los impactos en las operaciones comerciales.

Gestión de Riesgos: Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

P

Pista de auditoría: Es el registro de datos lógicos de las acciones o sucesos ocurridos

en los sistemas aplicativos u operativos, con el propósito de mantener información histórica para fines de control, supervisión y auditoria.

Plan de contingencia: Es el conjunto de procedimientos alternativos a la operatividad normal de la entidad cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto financiero que pueda ocasionar cualquier evento inesperado especifico. El plan de contingencia se ejecuta el momento en que se produce dicho evento.

Plan de Continuidad del Negocio (BCP): Colección documentada de procedimientos y de información que es desarrollada, compilada y mantenida; y, que se encuentra lista para su uso ante un incidente, con la finalidad de que la Institución pueda continuar prestando sus actividades críticas en un nivel aceptable predefinido.

Plan de Manejo de Incidentes: Plan de acción claramente definido y documentado para su uso en el momento de un incidente, por lo general cubre el personal clave, recursos, servicios y acciones necesarias para aplicar el proceso de manejo de incidentes.

Plan de reanudación: Especifica los procesos y recursos para mantener la continuidad de las operaciones en la misma ubicación del problema.

Plan de recuperación: Especifica los procesos y recursos para recuperar las funciones del negocio en una ubicación alterna dentro o fuera de la institución.

Procedimiento: Es el método que especifica los pasos a seguir para cumplir un propósito determinado.

Proceso crítico: Es el indispensable para la continuidad del negocio y las operaciones de El Banco, y cuya falta de identificación o aplicación deficiente puede generarle un impacto financiero negativo.

Proceso: Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente, sea interno o externo.

Planes de Emergencia: Desarrollo y mantenimiento de los procedimientos acordados para prevenir, reducir, controlar, mitigar y tomar otras acciones en el caso de una emergencia civil.

Programa de Gestión de la Continuidad del Negocio: Comprende la gestión continua y el proceso de gobernabilidad con el apoyo de la alta dirección para disponer de los recursos adecuados que garanticen el cumplimiento de los pasos necesarios que permitan identificar el impacto de las pérdida potenciales; y, mantener estrategias y planes viables de recuperación que aseguren, a través de su ejecución, pruebas, mantenimiento y revisión, la continuidad de los productos y servicios del negocio.

Seguridad de la Información: Consiste en la protección de la confidencialidad, integridad y disponibilidad de los activos de información según sea necesario para alcanzar los objetivos de negocio de la institución y abarca la seguridad informática.

Seguridades lógicas: Se refieren a la seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

BIBLIOGRAFÍA

Bibliografía

Asociación de Auditoría y Control de Sistemas de Información – http://www.isaca.org

Organización Internacional de Estándares – http://www.iso.org

Information Technology Infrastructure Library – http://www.itil-oficialsite.com/

Software Engineering Institute – http://www.sei.cmu.edu/cmmi

Ingeniería de Seguridad de Sistemas – Modelo de Madurez de Capacidades.- http://www.sse-cmm.org

Comité de Estándares del Instituto de Administración de Proyectos – http://www.pmi.org

CGAP. Resumen de los Principios Clave de las Microfinanzas: Resumen informativo. Recuperado de http://cgap.org

Barnier Brian G. Seven Hurdles to IT & Physical Risk Management. Symantec. Recuperado de http://www.symantec.com/business/resources/articles/article.jsp?aid=managing_it_risk

Institute IT Governance. COBIT Mapping: Mapping of ITIL With COBIT, sf.

Basel II: Aprovechamiento de las soluciones de gestión de los servicios empresariales para una excelente administración del riesgo. Recuperado de http://www.bmc.com

IT Governance Institute. IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance, sf.

Superintendencia de Bancos y Seguros. Estadísticas del Sistema Financiero. Recuperado de www.sbs.gob.ec

Institute IT Governance. COBIT Mapping: Overview of International IT Guidance.

Institute IT Governance. COBIT Mapping: Mapping of ISO/IEC 17799:2005 With COBIT