Elaboración de un Plan de Implementación de la ISO/IEC 27001:2005

Andrea Ariza Díaz

TRABAJO FINAL DE MASTER - Elaboración de un Plan de Implementación de la ISO/IEC 27001:2005 en **Banco ABC**

DIRECTOR: Antonio Jose Segovia Henares

FECHA FINALIZACIÓN: Junio 7 de 2013

Máster Interuniversitario en Seguridad de las TIC (MISTIC)

UAB Universitat Autònoma de Barcelona

UOC www.uoc.edu Universitat Rovira i Virgili

Abstract

Information is an asset that, like other major assets of value requires adequate protection. It should adequately protect information whatever form it takes or the means by which it is shared or stored, against threats that may endanger the continuity of levels of competitiveness, profitability and legal compliance necessary to achieve the objectives of the organization.

Why implementing an ISMS? It is possible to significantly reduce the impact of risk information assets identified for each process of the organization without the need for large investments. Therefore, the Information Security Management System (ISMS) set policies, procedures and controls in relation to the business objectives of the organization, in order to always keep the risk of information assets below the level assumed by the organization. This tool provides an overview of the state of resources and information assets, security measures applied and the results from that application.

In this way with the implementation of ISMS an organization can know the risks they are subjected to give information assets management systematically defined, documented and known to all, is monitored and continually improved.

This paper explains the process of implementation of a Information Security Management System ISMS in an organization belonging to the financial sector and the results associated with the implementation.

Resumen del trabajo

La información es un activo que como otros activos importantes tiene valor y requiere en consecuencia una protección adecuada. Se debe proteger adecuadamente la información cualquiera que sea la forma que tome o los medios por los que se comparte o almacene, frente a amenazas que puedan poner en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal necesarias para alcanzar los objetivos de la organización.

¿Por qué implantar un SGSI? Es posible disminuir de forma significativa el impacto de los riesgos de los activos de información identificados para cada proceso de la organización sin necesidad de realizar grandes inversiones. Por lo tanto, el Sistema de Gestión de Seguridad de la información (SGSI) permite establecer políticas, procedimientos y controles en relación a los objetivos de negocio de la organización, con el objeto de mantener siempre el riesgo de los activos de información debajo del nivel asumible por la organización. Es una herramienta que ofrece una visión global sobre el estado de los recursos y activos de información, las medidas de seguridad que se aplican y los resultados a partir de dicha aplicación.

De esta manera con la implantación de SGSI una organización puede conocer los riesgos a los que están sometidos los activos de información para darles gestión de manera sistemática definida, documentada y conocida por todos, que se monitorea y mejora continuamente.

El presente trabajo permite conocer el proceso de implantación de un Sistema de Gestión de Seguridad de la información SGSI en una organización perteneciente al sector financiero y los resultados asociados a dicha implantación.

Contenido

Abstract 2
Resumen del trabajo 2
1. Introducción trabajo final de máster 9
1.1. Objetivo 9
1.2. Enfoque y método 9

2. SITUACIÓN ACTUAL: Contextualización, objetivos y análisis diferencial 10
2.1. Introducción 10
2.2. Objetivos 11
2.3. Alcance 13
2.4. Metodología 16
2.5. Análisis Diferencial 17
2.5.1. Objetivo 17
2.5.2. Alcance 17
2.6. Resultados del Análisis Diferencial 18

3. SISTEMA DE GESTIÓN DOCUMENTAL 19
3.1. Política de Seguridad de la Información 19
3.1.1. Propósito 19
3.1.2. Alcance 19
3.1.3. Cumplimiento 19
3.1.4. Definición de Términos 19
3.1.5. Principios y Fundamentos 21
3.2. Procedimiento de Auditorías Internas 22
3.2.1. Plan de Auditoría 22
3.2.2. Información General 22
3.2.3. Procedimientos de Control de las Pruebas 24
3.2.4. Definición de las Pruebas 25
3.3. Procedimiento Revisión por Dirección 26
3.4. Gestión de Roles y Responsabilidades 27
3.4.1. Introducción 27

3.5. Metodología de Análisis de Riesgos 30
3.5.1. Factores Críticos de Éxito para la Administración de Riesgos 30
3.5.2. Metodología 30
3.5.2.1. Determinación del Contexto Estratégico 30
3.5.2.2. Identificación de Riesgos 31
3.5.2.3. Análisis y Evaluación de Riesgos 31
3.5.2.4. Tratamiento y Monitoreo de Riesgos 32
3.5.2.5. Elaboración Matriz de Riesgos 34
3.6. Declaración de Aplicabilidad 35

4. ANÁLISIS DE RIESGOS 36
4.1. Introducción 36
4.1.1. Propósito 36
4.1.2. Alcance 36
4.2. Inventario de Activos 37
4.2.1. Inventario por proceso 37
4.2.2. Inventario por grupos 38
4.3. Valoración de los Activos 39
4.4. Dimensiones de Seguridad 40
4.5. Tabla Resumen de Valoración 40
4.6. Análisis de Amenazas 42
4.7. Impacto Potencial 45
4.8. Nivel de Riesgo Aceptable y Riesgo Residual 49

5. PROPUESTAS DE PROYECTOS 51
5.1. Introducción 51
5.2. Propuestas de proyectos 51
5.3. Resultados 57

6. AUDITORÍA DE CUMPLIMIENTO 59
6.1. Introducción 59
6.2. Evaluación de la madurez 60

6.3. Resultados 61

7. Conclusiones 63

Referencias Bibliográficas 64

ANEXO 1 – Resultado Análisis Diferencial 65
Resumen Ejecutivo 65
Resultados 66
Cubrimiento de controles 68
Nivel de madurez 68
Resultados por dominio 71
Dominio 5 – Política de Seguridad de la información 71
Observaciones 71
Oportunidades de mejora 71
Dominio 6 – Organización de la Seguridad de la Información 71
Observaciones 72
Oportunidades de mejora 72
Dominio 7 – Gestión de Activos 73
Observaciones 73
Oportunidades de mejora 73
Dominio 8 – Seguridad de los Recursos Humanos 74
Observaciones 74
Oportunidades de mejora 74
Dominio 9 – Seguridad Física y del Entorno 75
Observaciones 75
Oportunidades de mejora 75
Dominio 10 – Gestión de Comunicaciones y Operaciones 76
Observaciones 76
Oportunidades de mejora 78
Dominio 11 – Control de Acceso 78
Observaciones 79

Oportunidades de mejora 80
Dominio 12 – Adquisición, Desarrollo y Mantenimiento de Sistemas de información 80
Observaciones 81
Oportunidades de mejora 82
Dominio 13 – Gestión de los Incidentes de Seguridad de la Información 82
Observaciones 82
Oportunidades de mejora 83
Dominio 14 – Gestión de la Continuidad del Negocio 83
Observaciones 83
Oportunidades de mejora 84
Dominio 15 – Cumplimiento 84
Observaciones 84
Oportunidades de mejora 85
Dominio – Estrategia de Seguridad de la Información 85
Observaciones 85
Oportunidades de mejora 85
Dominio – Gobierno de la Función Responsable por la Seguridad de la Información 86
Observaciones 86
Oportunidades de mejora 86
Dominio 6 – Arquitectura de la Seguridad de la Información 86
Observaciones 87
Oportunidades de mejora 87
ANEXO 2 – Declaración de Aplicabilidad 88
Políticas de Control y Seguridad 88
Clasificación de la Información 88
Personal 91
Seguridad Física 95
Internet y Correo Electrónico 100
Ambiente de Usuario Final 102
Uso Autorizado de Software 105

Plan de Contingencias **106**

ANEXO 3 – MAI_ComercioExterior **108**
ANEXO 4 – MAI_AdministracionPortafolios **108**
ANEXO 5 – MAI_AdministracionLiquidez **108**
ANEXO 6 – MAI_Reportes **108**
ANEXO 7 – Riesgo_Inherente **108**
ANEXO 8 – Formato SGSI Auditoría **108**

1. Introducción trabajo final de máster

Los sistemas de información y los datos almacenados son uno de los recursos más valiosos con los que puede contar cualquier organización. El constante flujo de información y el traslado de recursos de un sitio a otro permite el desarrollo y generación de vulnerabilidades y/o debilidades que ponen en riesgo la seguridad de la infraestructura de la organización, esta seguridad puede ser tanto lógica como física.

Proteger la información y aquellos recursos tecnológicos informáticos que los contienen es una tarea continua y de vital importancia. Las amenazas que se pueden presentar provienen tanto de agentes externos como de agentes internos a la organización. Para ellos es primordial desarrollar una estrategia de seguridad fundamentada en políticas que estén respaldadas por todos los miembros de la organización y respaldada por la alta dirección.

Se debe considerar que la violación de la seguridad en un sistema podría llegar a afectar gravemente las operaciones críticas de la empresa y dejarla expuesta a daños que incluyen pérdidas monetaria y de imagen, según en el sector que operen.

En este trabajo se fundamenta la implantación de un sistema de gestión de seguridad de la información en una organización definida donde se presenta todo el proceso de creación de una estrategia de seguridad basada en políticas, seguimiento y auditoría de la misma.

1.1. Objetivo

Establecer, desarrollar e implementar un enfoque sistemático de la seguridad en una organización perteneciente al sector financiero, planteado desde un análisis inicial de riesgos y alineado con la estrategia y objetivos del negocio, y entendido como un proceso independiente.

1.2. Enfoque y método

Las normas ISO 27001 e ISO 27002 son las que actualmente tienen mayor difusión y aceptación a nivel internacional, por lo cual se utilizarán para trabajar sobre la implantación de los sistemas de gestión de la seguridad de la información (SGSI).

2. SITUACIÓN ACTUAL: Contextualización, objetivos y análisis diferencial

2.1. Introducción

La empresa objeto de nuestro análisis es un Banco en Colombia, al que denominaremos Banco ABC. El Banco ABC tiene como objeto social la celebración y ejecución de todas las operaciones legalmente permitidas a los bancos comerciales, con sujeción a los requisitos, restricciones y limitaciones impuestos por las leyes.

Consultores XYZ seremos los encargados de realizar la implantación del Sistema de Gestión de Seguridad de la Información para el Banco.

Desde el año 2002 la entidad ha experimentado cambios en los distintos frentes de su actividad, consolidando su vocación bancaria a través del lanzamiento de nuevos productos, tales como cuenta corriente, operaciones de divisas, créditos de consumo, de libre inversión, de tesorería y empresariales, sin abandonar las tradicionales líneas de depósitos de ahorro (cuentas y CDT), entre otros.

El Banco ABC se encuentra en un período creativo y de consolidación, que apunta al objetivo estratégico de lograr su crecimiento, para lo cual se ha preparado; cuenta con una red de oficinas competitiva, su fuerza de ventas ha sido formada y tiene a su disposición la mejor tecnología y un eficiente soporte administrativo. La filosofía que se encuentra en la base de la actividad actual del Banco se sintetiza en los siguientes postulados, difundidos y compartidos por sus funcionarios.

La entidad cuenta con un estado inicial de seguridad donde La Gerencia de Seguridad de la Información con el apoyo de la Alta Dirección de Banco ABC desarrollará e implementará el Sistema de Gestión de Seguridad de la Información, con el cual se brindará el apoyo necesario para proteger sus activos de información de acuerdo con las metas y objetivos contemplados en el plan estratégico de seguridad de la información de la Compañía. Para cumplir con este objetivo se deberá tener en cuenta los siguientes aspectos:

- La documentación, aprobación y publicación de políticas de seguridad de la información.
- La gestión de riesgo de tecnologías de la información.
- La organización de seguridad de la información.
- La gestión de activos de la información.
- La seguridad de los recursos humanos.
- La seguridad física y ambiental de los sistemas de información.
- La gestión de comunicaciones y operaciones de sistemas de información.
- El control de acceso de tecnologías de información.
- La adquisición, desarrollo y mantenimiento de los sistemas de información.

- La continuidad del negocio en caso de fallas en sus sistemas de información.
- La gestión de incidentes de tecnologías de información.
- El cumplimiento de los requisitos legales.

La asignación de responsabilidades se realiza conforme a los requerimientos de seguridad de la información. Protegiendo de esta manera los activos de la información.

El Propietario del activo de información puede delegar las tareas de seguridad; sin embargo, no lo exime de su responsabilidad, teniendo la obligación de supervisar y determinar el cumplimiento de las tareas delegadas con los requerimientos de seguridad.

Las responsabilidades en las áreas serán definidas así:

- Identificar claramente los activos de información y procesos de seguridad asociados a este.

- El área responsable de cada activo de información o proceso de seguridad será notificada de esta responsabilidad, las cuales deben estar descritas en un documento.

- Los niveles de autorización deben estar claramente definidos y documentados.

2.2. Objetivos

La necesidad para el Banco ABC de implantar un SGSI es:

- **Factores Externos:**

    - Cumplimiento de las circulares externas exigidas por la Superintendencia Financiera de Colombia:

        - *Circular externa 038*

          Teniendo en cuenta que la operación de una entidad depende en gran medida de sus sistemas de información, es necesario adoptar controles que garanticen la seguridad, calidad y cumplimiento de la información generada.

          Los sistemas de información y comunicación son la base para identificar, capturar e intercambiar información en una forma y período de tiempo que permita al personal cumplir con sus

responsabilidades y a los usuarios externos contar oportunamente con elementos de juicio suficientes para la adopción de las decisiones que les corresponde en relación con la respectiva entidad.

La tecnología es imprescindible para el cumplimiento de los objetivos y la prestación de servicios de las entidades a sus diferentes grupos de interés, en condiciones de seguridad, calidad y cumplimiento. Por lo tanto, se tendrá que velar porque el diseño del SCI para la gestión de la tecnología responda a las políticas, necesidades y expectativas de la entidad, así como a las exigencias normativas sobre la materia.

- *Circular externa 052*

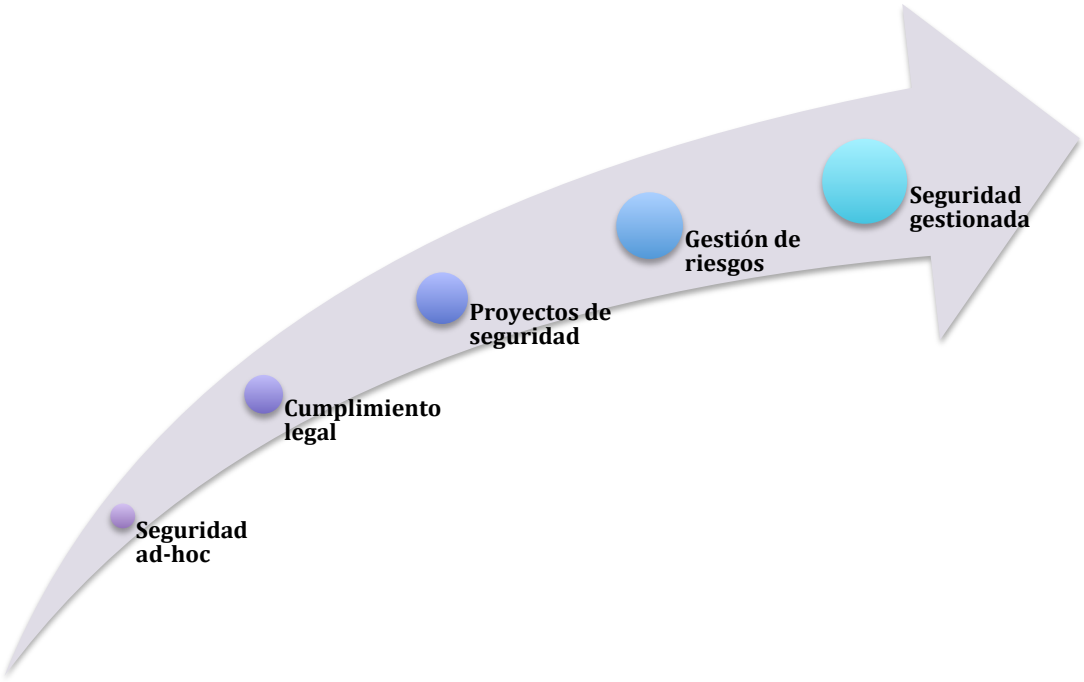
  Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios

- Cumplimiento de la Directiva Presidencial No. 01 de 1999, Directiva Presidencial No. 02 de 2002, Circular No. 04 de 2006 y la Circular No. 12 de 2007, referente al cumplimiento de normas de uso de software de acuerdo por lo establecido con la Dirección Nacional de Derechos de Autor.

- **Factores Internos:**

  - Confianza frente a clientes
  - Diferenciación en el sector financiero

Se pretende obtener alcanzar este nivel de madurez en el sistema de gestión de seguridad de la información:



2.3. Alcance

El banco opera bajo procesos definidos y categorizados de tres maneras: Procesos estratégicos, Procesos Misionales y Procesos Habilitantes como se presenta en la siguiente ilustración.

Procesos Estratégicos	**Sistemas de Administración de Riesgos**	Algunos procesos de esta línea de negocio son: ▪ SARO ▪ Monitoreo SARC ▪ Modelación SARC
Procesos Misionales	**Captaciones**	Algunos procesos de esta línea de negocio son: ▪ Administración de Efectivo ▪ Embargos y Desembargos de Productos ▪ Vinculación del Cliente
	Colocaciones	Algunos procesos de esta línea de negocio son: ▪ Otorgamiento ▪ Normalización ▪ Cobranzas
	Comercio Exterior	▪ Comercio Exterior
	Gestión de Tesorería	Algunos procesos de esta línea de negocio son: ▪ Administración de Liquidez ▪ Reportes de cartera a entes externos ▪ Administración de Portafolios
	Servicios Canales Electrónicos	Algunos procesos de esta línea de negocio son: ▪ Operación Servilínea ▪ Utilización de Tarjeta Débito y Crédito ▪ Operación Portal Banca Personal
	Servicios Oficinas	Algunos procesos de esta línea de negocio son: ▪ Recaudo ISS ▪ Paz y Salvos, Referencias, Certificaciones

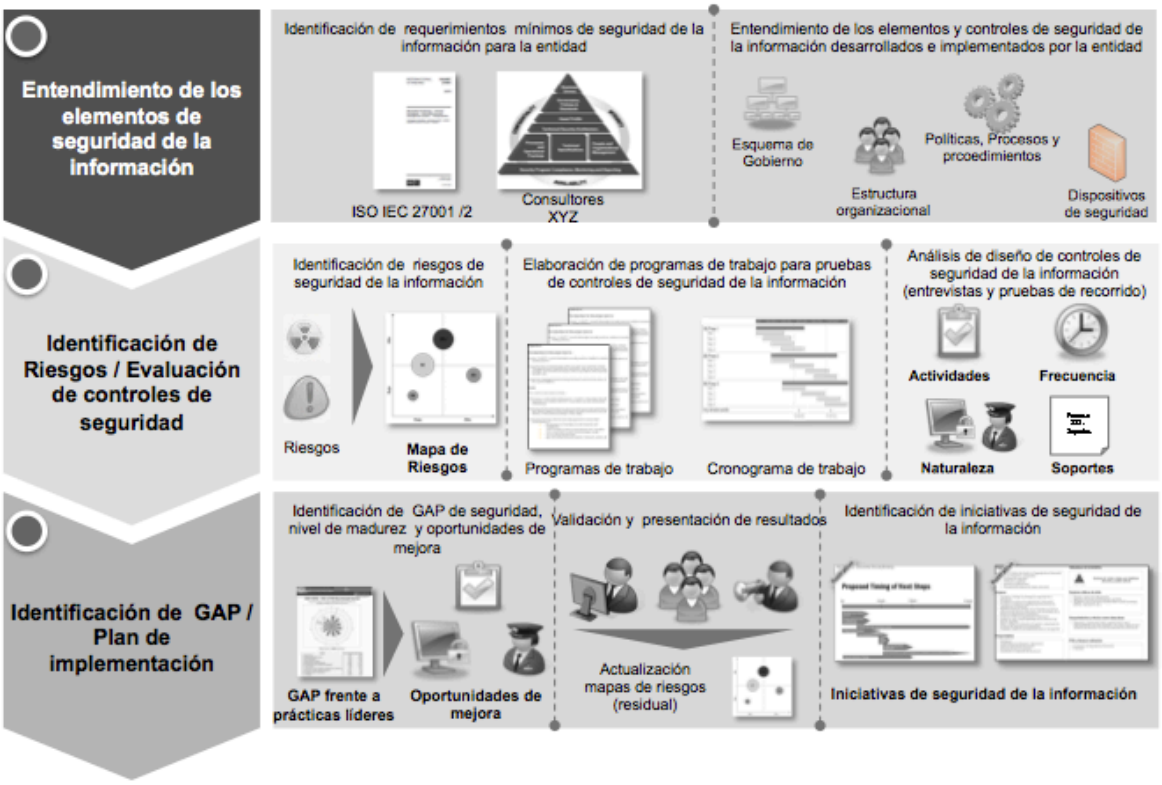
Procesos Habilitantes	**Gestión Financiera**	Algunos procesos de esta línea de negocio son: ▪ Generación de Informes y Reportes ▪ Valoración del Banco ▪ Planeación Financiera
	Gestión Jurídica	Algunos procesos de esta línea de negocio son: ▪ Crédito Público ▪ Procesos Concursales ▪ Defensa y Representación Judicial
	Gestión Tributaria	Algunos procesos de esta línea de negocio son: ▪ Devolución de Impuestos y Retenciones a Clientes ▪ Planeación Tributaria
	Gestión de IT	Algunos procesos de esta línea de negocio son: ▪ Administración de Cambios ▪ Adquisición de Tecnología ▪ Continuidad de Negocio
	Gestión de Seguridad	Algunos procesos de esta línea de negocio son: ▪ Procesos Penales ▪ Modelo del Sistema de Gestión de Seguridad de la Información

A partir de lo anterior y viendo la complejidad de procesos que maneja el Banco ABC, inicialmente el alcance del Sistema de Gestión de Seguridad de la Información que se implantará en el Banco ABC contemplará cuatro (4) procesos críticos de la operación:

- Comercio Exterior
- Administración de Liquidez
- Reportes de cartera a entes externos
- Administración de Portafolios

2.4. Metodología

A continuación se describe la metodología utilizada por Consultores XYZ para el desarrollo del trabajo en el Banco ABC:



2.5. Análisis Diferencial

A continuación se describen los resultados obtenidos de la evaluación de seguridad de la información realizada al Banco ABC, la cual se realizó determinando el nivel de madurez[1] de los controles existentes en la norma ISO/IEC 27001:2005[2] y algunos propuestos por el marco de referencia de seguridad de la información de la empresa Consultores XYZ[3]. A continuación se mencionan los dominios evaluados:

- Política de Seguridad de la Información
- Organización de la Seguridad de la Información
- Gestión de Activos
- Seguridad de los Recursos Humanos
- Seguridad Física y del entorno
- Gestión de Comunicaciones y Operaciones
- Control de Acceso
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Gestión de los Incidentes de Seguridad de la Información
- Gestión de la Continuidad del Negocio
- Cumplimiento
- Estrategia de Seguridad de la Información
- Gobierno de la función responsable por la Seguridad de la Información
- Arquitectura de Seguridad de la Información

2.5.1. Objetivo

Presentar los resultados obtenidos en el análisis y evaluación de los controles de seguridad de la información definidos e implementados por el Banco ABC, como parte de su modelo de seguridad, frente al Estándar ISO/IEC 27001:2005 y al Marco de Referencia de Seguridad de la Información de Consultores XYZ.

2.5.2. Alcance

El análisis diferencial presenta los resultados obtenidos por cada uno de los dominios y controles evaluados, y las oportunidades de mejora correspondientes, con respecto a las practicas líderes aceptadas por la industria y al marco de referencia desarrollado por Consultores XYZ.

[1] El Modelo de Madurez de Capacidades o CMM (Capability Maturity Model), es un modelo de

[2] Estándar para la seguridad de la información ISO/IEC 27001 (Information technology – Security techniques – Information security management – Requirements

[3] Marco de referencia de seguridad de la información definido por Consultores XYZ

A continuación se mencionan los dominios de seguridad de la información evaluados:

- Política de Seguridad de la Información
- Organización de la Seguridad de la Información
- Gestión de Activos
- Seguridad de los Recursos Humanos
- Seguridad Física y del entorno
- Gestión de Comunicaciones y Operaciones
- Control de Acceso
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Gestión de los Incidentes de Seguridad de la Información
- Gestión de la Continuidad del Negocio
- Cumplimiento
- Estrategia de Seguridad de la Información
- Gobierno de la función responsable por la Seguridad de la Información
- Arquitectura de Seguridad de la Información

2.6. Resultados del Análisis Diferencial

Para ver en detalle los resultados del análisis diferencial ver ANEXO 1 – Resultados de Análisis Diferencial.

3. SISTEMA DE GESTIÓN DOCUMENTAL

3.1. Política de Seguridad de la Información

3.1.1. Propósito

El presente documento establece las directrices que permitan facilitar el cumplimiento de la misión y objetivos del Banco ABC a través de la prevención y administración de los riesgos asociados a los activos de información, sensibilizando sobre la existencia de estos y la necesidad de mitigarlos ofreciendo un método sistemático para su identificación, análisis y evaluación.

3.1.2. Alcance

Esta Política Corporativa de Seguridad de la Información aplica a todos los activos de información propiedad del Banco ABC durante su ciclo de vida, incluyendo creación, distribución, transmisión, almacenamiento y eliminación; así como en todas sus formas: digital, física y hablada.

Activos de información son datos o información propietaria en medios electrónicos, impreso u otros medios, considerados sensitivos o críticos para los objetivos de negocio del Banco ABC.

3.1.3. Cumplimiento

El Banco ABC a través de sus canales formales se reserva el derecho de tomar las medidas correspondientes para los casos de incumplimiento de la presente política.

El grupo Seguridad de la Información perteneciente a la Gerencia Corporativa de Riesgos, como responsable de monitorear del cumplimiento de la presente política, debe mantener informadas a las Gerencias de las unidades estratégicas de negocio y la presidencia de la Organización, y al mismo tiempo, debe informarle sobre los incumplimientos registrados.

3.1.4. Definición de Términos

Administración de riesgos: Una rama de administración que aborda las consecuencias del riesgo. Consta de dos etapas: a. El diagnóstico o valoración, mediante Identificación, análisis y determinación del Nivel, b. El manejo o la administración propiamente dicha, en que se elabora, ejecuta y hace seguimiento al

Plan de manejo que contiene las Técnicas de Administración del Riesgo propuestas por el grupo de trabajo, evaluadas y aceptadas por la alta dirección.

Análisis de riesgos: Determinar el Impacto y la Probabilidad del riesgo. Dependiendo de la información disponible pueden emplearse desde modelos de simulación, hasta técnicas colaborativas.

Control: Es toda acción que tiende a minimizar los riesgos, significa analizar el desempeño de las operaciones, evidenciando posibles desviaciones frente al resultado esperado para la adopción de medidas preventivas. Los controles proporcionan un modelo operacional de seguridad razonable en el logro de los objetivos.

Custodio activo de información: Es una parte designada de la organización, un cargo, proceso o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad (Toma de copias de seguridad, asignar privilegios de: Acceso, Modificaciones, Borrado) que el propietario de la información haya definido, con base en los controles de seguridad disponibles en la organización.

Evaluación del riesgo: Es el resultado de confrontar la valoración del riesgo con los controles existentes.

Factores de riesgo: Manifestaciones o características medibles u observables de un proceso que indican la presencia de Riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Identificación del Riesgo: Establecer la estructura del riesgo; fuentes o factores, internos o externos, generadores de riesgos; puede hacerse a cualquier nivel: total entidad, por áreas, por procesos, incluso, por funciones; desde el nivel estratégico hasta el operativo.

Impacto: Consecuencias que puede ocasionar a la organización la materialización del riesgo.

Matriz de riesgos: Herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, definiéndolos, haciendo la descripción de cada uno de estos y las posibles consecuencias.

Mapa de riesgo: Representación gráfica que indica el nivel de exposición al riesgo luego de la medición de los factores de riesgo presentes en cada actividad.

Probabilidad: Una medida (expresada como porcentaje o razón) para estimar la posibilidad de que ocurra un incidente o evento. Contando con registros, puede estimarse a partir de su frecuencia histórica mediante modelos estadísticos de mayor o menor complejidad.

Propietario del activo de la información: Es una parte designada de la organización, un cargo, proceso o grupo de trabajo que tiene la responsabilidad de definir quienes tienen acceso y que pueden hacer con la información y de determinar cuales son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de confidencialidad o destrucción deliberada, y al mismo tiempo de definir que se hace con la información una vez ya no sea requerida.

Responsables: Son las dependencias o áreas encargadas de adelantar las acciones propuestas.

Riesgo: posibilidad de ocurrencia de toda aquella situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.

Riesgo inherente: el máximo riesgo sin los efectos mitigantes de la administración del riesgo.

Riesgo residual: es el riesgo que queda cuando las técnicas de la administración del riesgo han sido aplicadas.
Seguimiento: Recolección regular y sistemática sobre la ejecución del plan, que sirven para actualizar y mejorar la planeación futura.

Sistema: Conjunto de cosas o partes coordinadas, ordenadamente relacionadas entre sí, que contribuyen a un determinado objetivo.

3.1.5. Principios y Fundamentos

La Política Corporativa para la Administración de Riesgos de Activos de Información describe el conjunto de componentes de control, que al interrelacionarse, permiten al Banco ABC, estudiar y evaluar aquellos eventos, que pueden afectar o impedir el cumplimiento de su misión y objetivos, habilitándola para emprender las acciones necesarias de protección y aseguramiento contra los efectos ocasionados por la ocurrencia de estos eventos.

La Política Corporativa para la Administración de Riesgos de Activos de Información reconoce la presencia de la incertidumbre en todas las actividades organizacionales, requerida para dar cumplimiento a su misión constitucional y legal, permitiendo garantizar la coordinación de las actuaciones necesarias a su manejo.

El adecuado tratamiento de los riesgos asociados a los activos de información propicia el crecimiento y desarrollo de la Organización y favorece el cumplimiento de su función constitucional. Para ello es necesaria la definición de su entorno, su

reconocimiento, análisis, evaluación y definición de las alternativas de manejo bajo la siguiente estructura de Elementos:

Contexto Estratégico: Metodología de Gestión Estratégica que permite la identificación y análisis de las Fortalezas, Debilidades, Oportunidades y Amenazas a las cuales se encuentra expuesta la Organización. La consolidación de los resultados del Contexto Estratégico es empleada como elemento de entrada para la Administración de Riesgos de Activos de Información.

Identificación de Riesgos: Proceso de análisis cualitativo que tiene por objeto identificar todos aquellos eventos que pueden afectar el cumplimiento de los objetivos de la Organización. Las Debilidades y Amenazas, identificadas como parte del Contexto Estratégico, proporcionan una fuente de entrada para la identificación de los riesgos.

Análisis de Riesgos: Consiste en la determinación de la frecuencia de ocurrencia del riesgo y la gravedad que presenta en caso de que llegue a ocurrir.

Evaluación de Riesgos: Se determina a partir del análisis y cuantificación del mismo. La evaluación del riesgo es el producto de confrontar los resultados de la valoración del riesgo con los controles, con el objetivo de establecer prioridades para su manejo y fijación de políticas.

Tratamiento de Riesgos: Son las directrices establecidas por la Alta Dirección para minimizar el impacto de los riesgos más críticos identificados para cada uno de los procesos.

Monitoreo de Riesgos: Los riesgos asociados a los activos de información y las medidas de control necesitan ser monitoreadas para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos. Pocos riesgos permanecen estáticos.

3.2. Procedimiento de Auditorías Internas

3.2.1. Plan de Auditoría

El equipo auditor, una vez firmados los acuerdos de confidencialidad y la Carta de Auditoría materializada en la oferta de servicios profesionales, facilita a la dirección del auditado un Plan de Auditoría con el siguiente contenido.

3.2.2. Información General

a. Objetivo del plan

El objetivo general de la auditoría a realizar será identificar fallas los control es definidos para los activos de información correspondientes a los desarrollos de nuevos productos de la organización. El objeto del presente documento es recopilar los distintos aspectos a revisar dentro de los procedimientos bajo auditoría. Se describirán todos los aspectos relevantes que serán revisados.

Además, este documento constituirá la guía a emplear para la coordinación entre equipo- auditor (interno) y la organización a la hora de planificar, programar las pruebas a realizar y gestionar las autorizaciones que sean necesarias para la realización de la auditoría. Este plan no pretende recopilar el detalle de todas y cada una de las pruebas que se realizarán sino que su objetivo es describir en detalle la estrategia de prueba que se seguirá.

Seguidamente, se busca principalmente:

- Velar por el cumplimiento de los controles internos establecidos.
- Revisar y evaluar la efectividad, propiedad y aplicación de los controles internos.
- Cerciorarse del grado de cumplimiento de las normas, políticas y procedimientos vigentes.
- Comprobar el grado de confiabilidad de la información que produzca la organización.
- Evaluar la calidad del desempeño en el cumplimiento de las responsabilidades asignadas.
- Promover la eficiencia operacional

b. Alcance

La auditoría se ceñirá a la revisión de controles de seguridad aplicados para el control de acceso lógico y físico a los activos de información correspondientes a los desarrollos de nuevos productos de la organización.

Los apartados a auditar, son lo siguientes:

- Seguridad de cumplimiento de normas y estándares.
- Gestión de activos
- Seguridad del personal
- Seguridad de Sistema Operativo.
- Seguridad de Software.
- Seguridad de Comunicaciones.
- Seguridad de Base de Datos.

- Seguridad de Proceso.
- Seguridad de Aplicaciones.
- Seguridad Física
- Control de acceso
- Gestión de la Continuidad de negocio
- Conformidad

c. Documentación de referencia

El tipo de auditoría elegido para esta evaluación es "Revisión de los mecanismos de control de acceso a la información y revisión de la gestión del ciclo de vida de los sistemas" que está basada en la metodología de controles ISO/IEC 17799. Específicamente, se hizo la revisión de los capítulos relacionados con los mecanismos de control de acceso a la información y la verificación de la clasificación y controles de activos según la norma mencionada. Además, se utilizarán las normas NIST para la elaboración de las encuestas y para la revisión de los controles específicos de las aplicaciones en desarrollo. Se utilizarán las metodologías NIST y OWASP dado lo particular de la auditoría.

3.2.3. Procedimientos de Control de las Pruebas

a. Entorno de pruebas requerido

La Auditoría de la seguridad en la informática abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan.

b. Gestión de incidentes

En el caso que durante la ejecución del Plan de Auditoría se detectara una vulnerabilidad grave que pudiera comprometer la seguridad (confidencialidad, disponibilidad o integridad) de la aplicación se comunicará a la organización la incidencia y circunstancias que la provocaron.

Con anterioridad al inicio de la ejecución de las pruebas se tendrá que determinar con exactitud los procedimientos a emplear, los POC (Point of Contact) adecuados y los periodos en los que se encontrarán disponibles y los medios a emplear en cada caso. En el caso que el Banco tuviera ya definido un modo de proceder, se procederá de la manera que se tenga prevista en estos procedimientos. En caso contrario, se procederá del siguiente modo:

- El procedimiento de comunicación urgente de las incidencias se activará cuando un auditor de EQUIPO-AUDITOR detecte, ya sea mediante la realización de una prueba o bien por cualquier otra circunstancia, una vulnerabilidad grave. Se entiende por vulnerabilidad grave cualquier aspecto del funcionamiento de la aplicación que cause:

    - Una filtración de información confidencial
    - Una modificación no autorizada de información
    - Un malfuncionamiento de la aplicación que cause, o pudiera causar si fuera explotada de manera adecuada, una denegación de servicio
    - En general, cualquier incidente que pudiera situar al sistema a un estado inoperable.

  En este caso y una vez comprobada la existencia de la vulnerabilidad, el auditor se pondrá en contacto con el POC mediante los cauces previstos para informar de la situación y las circunstancias que lo provocan.

3.2.4. Definición de las Pruebas

1. **Estrategia de prueba**

El presente plan de auditoría se centra en la revisión de controles de seguridad aplicados a los activos de información correspondientes. A partir de ello se verificara la implementación de mecanismos de control de acceso a la información y realizará la verificación de la clasificación y controles de activos. Además, se utilizarán las normas NIST para la elaboración de las encuestas y para la revisión de los controles específicos de las aplicaciones en desarrollo. Se utilizarán las metodologías NIST y OWASP dado lo particular de la auditoría.

2. **Recogida de información**

Los siguientes estados serán empleados durante la ejecución del plan de pruebas para mantener el control de la situación en la que se encuentra la auditoría.

- Tipo de prueba
- Requerimiento a probar
- Descripción de la prueba
- Resultados esperados de la prueba

3. **Tipos de pruebas**

A continuación se describen y especifican el tipo de prueban tanto técnicas como no técnicas que se llevarán a cabo durante la ejecución de la auditoría:

- Revisión de los mecanismos de control
- Revisión de documentación: se revisan los controles propuestos por la norma para ver si están implementados y si estos son idóneos
- Realización de entrevistas
- Ejecución de pruebas técnicas
- Realización de visitas físicas

3.3. Procedimiento Revisión por Dirección

Este manual de Políticas de Seguridad de la Información, identifica responsabilidades y establece requerimientos mínimos para una protección apropiada y consistente de la información del Banco y la de sus clientes. La implementación de estas políticas reduce el riesgo de divulgar, modificar, destruir, retardar o dar mal uso a la información del Banco y la de sus clientes de una forma accidental o intencional. Estas políticas suministran las bases para las auditorías y autoevaluaciones a todos los niveles dentro del Banco.

Para el cumplimiento de estas políticas, los Directores deben ser responsables por el establecimiento y mantenimiento de controles sobre la información del Banco. Estos controles deben cumplir con las políticas contenidas en este manual.

Las Políticas de Seguridad de la Información contenidas en este manual aplican a toda la información a través de su ciclo de vida, incluyendo creación, distribución, almacenamiento y disponibilidad.

Las políticas cubren la información en todas sus formas: escrita, hablada, telefónica o electrónica. Los mismos riesgos que comprometen la información en su forma impresa también existen para la información hablada o electrónica.

Estas políticas están dirigidas a proteger la información del Banco en todos los ambientes donde reside. La información que reside en clientes o agentes externos también debe estar sujeta a los mismos controles usados para proteger la información procesada internamente.

Todos los empleados, clientes y agentes externos que usen, tengan acceso o sean responsables de la información y todo el personal que diseñe, opere o sea responsable por sistemas manuales y computarizados que contengan información del Banco deben cumplir con estas políticas.

El cumplimiento de las Políticas y Procedimientos de Seguridad de la Información es obligatorio. Los Directores son responsables de asegurar su cumplimiento y tomar las acciones correctivas cuando los controles de seguridad no sean acordes con estas políticas.

La Auditoría incorpora la revisión del cumplimiento de las Políticas de Seguridad de la Información dentro de sus estándares de revisión en cada una de las áreas del Banco.

Si el cumplimiento de estas políticas se debe hacer por fases, las prioridades que se den a cada una de las fases debe estar basada en una evaluación de la exposición al riesgo.

3.4. Gestión de Roles y Responsabilidades

3.4.1. Introducción

Para proteger la información del Banco ABC, se requiere del esfuerzo y compromiso de todos los usuarios de sus sistemas de información. Las responsabilidades específicas asociadas con estos roles se describen en las siguientes páginas.

a. Responsable de SGSI

Es el encargado de mantener el Sistema de Gestión de Seguridad de la Información para la organización.

Sus responsabilidades incluyen:

- Actualizar el SGSI de forma periódica
- Ejecutar monitoreo sobre el cumplimiento de políticas y procedimientos de seguridad.

b. Directores

Los Directores son los responsables por el cumplimiento y aprobación de las políticas y procedimientos de seguridad.

Sus responsabilidades incluyen:

- Aprobar y vigilar el cumplimiento con las políticas y procedimientos de seguridad de la información.
- Establecer sanciones por el incumplimiento de las políticas y procedimientos de seguridad de la información.

c. Gerentes

Los Gerentes son responsables de dirigir las actividades del personal subalterno. Sus responsabilidades incluyen:

- Aceptar la responsabilidad por toda la información que está bajo su control.
- Asegurar el acatamiento de los requerimientos para proteger la información, estableciendo controles que permitan cumplir con las políticas.
- Asegurar que las políticas y procedimientos de seguridad de la información sean comunicados a todos los usuarios bajo su supervisión.
- Asignar responsables de la información. Cuando se presentan cambios de personal en sus equipos de trabajo, nombrar un nuevo usuario dueño de la información y asegurarse que el es consciente de sus responsabilidades.
- Velar por la existencia de recursos suficientes para las actividades de protección de información.
- Tomar medidas para minimizar el riesgo por pérdida o exposición de la seguridad de la información bajo su responsabilidad.
- Asegurar que el personal asignado cumple con las responsabilidades por la seguridad de la información.

d. Gerencia de Tecnología de la Información

La función de la Gerencia de Tecnología de la Información es establecer, mantener y administrar una arquitectura de seguridad para el Banco y facilitar la incorporación de prácticas de seguridad de la información en todas las dependencias.

Sus responsabilidades incluyen:

- Establecer un plan general de estrategias, políticas y estándares de seguridad para el Banco, bajo la dirección y aprobación de los Directores.
- Orientar, recomendar y aconsejar a todos los usuarios de los sistemas de información del Banco en cuanto a la seguridad de la información.
- Representar al Banco ante organizaciones externas sobre temas de seguridad de la información.
- Revisar los planes estratégicos y de operaciones y asegurar la integración con las estrategias de seguridad.
- Ayudar a resolver problemas de seguridad.
- Dar un entrenamiento adecuado a los usuarios en cuanto a los requerimientos y responsabilidades sobre la seguridad de la información.
- Monitorear las actividades de seguridad de la información para determinar la eficacia del programa.

- Desarrollar métodos y técnicas para monitorear efectivamente los sistemas de seguridad de la información y reportar periódicamente su efectividad a los Socios.
- Realizar investigaciones de incidentes de seguridad de la información.
- Asegurar que el Banco es consciente del estado del arte de la tecnología de seguridad en computadores y adoptar esta tecnología cuando sea factible.
- Evaluar, recomendar y desarrollar especificaciones técnicas para la seguridad de los sistemas de información.
- Coordinar el desarrollo, mantenimiento y prueba del plan de Contingencias del Banco.

e. Auditores

Los auditores serán responsables de evaluar y medir la efectividad del sistema de control interno. Sus responsabilidades incluyen:

- Evaluar el cumplimiento de las políticas y procedimientos de seguridad de la información.
- Recomendar políticas y procedimientos de seguridad.
- Evaluar los riesgos sobre los controles propuestos.
- Asistir al Banco en la investigación y revisión del cumplimiento de los controles.

f. Usuarios

Un usuario es cualquier persona que está autorizada por la Gerencia de Conocimiento para acceder a la información del Banco. Dependiendo de su categoría y niveles de acceso, podrá crear, consultar, modificar y eliminar información. Todas las personas que utilizan los sistemas de información del Banco son considerados usuarios de los sistemas de información, aunque difiera el alcance de sus accesos.

Todos los usuarios son responsables de proteger y usar apropiadamente la información a la cual tengan acceso.

Sus responsabilidades incluyen:

- Usar solamente la información para propósitos autorizados por el Banco.
- Cumplir con los requerimientos de seguridad y confidencialidad establecidos por el Banco..
- Informar a los Directores y/o la Gerencia de Conocimiento cualquier exposición de riesgo de la seguridad ya sea real o potencial.
- Cumplir con los requerimientos en caso de recuperación de desastres.

3.5. Metodología de Análisis de Riesgos

3.5.1. Factores Críticos de Éxito para la Administración de Riesgos

El manejo exitoso de riesgos de los activos de información del Banco ABC debe considerar que:

- La Administración de Riesgos sea una parte integral del proceso de planeación, de proyectos, operativo de las actividades desarrolladas para todos los niveles del Banco ABC.

- La Administración de Riesgos sea abiertamente aceptada y soportada por el Banco ABC, direccionada como una buena herramienta que provee valor a la Organización, y reforzada a través de su incorporación a otros mecanismos de la Organización.

- La Administración de Riesgos sea una herramienta fácil de incorporar dentro de las actividades diarias y se empiece a ver como una ayuda completa que permite lograr nuestra Visión y Objetivos.

3.5.2. Metodología

El Banco ABC, en cumplimiento de su propósito con la prevención y administración de los riesgos asociados a los activos de información que puedan entorpecer el normal desarrollo de sus funciones y afectar el cumplimiento de su misión y objetivos, establece el siguiente proceso metodológico para la administración de riesgos de activos de información:

3.5.2.1. Determinación del Contexto Estratégico

A partir del análisis y la planeación estratégico de la Organización, se construye la Matriz de Identificación de Factores Generadores de Riesgos de Activos de Información, que representa las situaciones desfavorables que para la misma tiene el entorno político, social, económico, cultural, tecnológico y ambiental. Frente a las debilidades y amenazas detectadas.

Responsable(s): Grupo Corporativo de Seguridad de la Información
Instrumento de Análisis: Matriz de Identificación de Vulnerabilidades en los Activos de Información

3.5.2.2. Identificación de Riesgos

La identificación de riesgos en los activos de información posibilita el reconocimiento de los eventos particulares que presentan algún grado de amenaza al cumplimiento de las funciones del Banco. Los pasos que deben seguirse corresponden a:

- **a.** Identificación de las vulnerabilidades asociadas a los activos de información para cada una de las actividades de los diferentes procesos. Es importante que la asignación de las vulnerabilidades se realice con el mayor grado de objetividad posible, para ello se debe considerar los resultados del análisis del contexto estratégico realizado.
- **b.** Identificación de las amenazas que pueden aprovechar las vulnerabilidades identificadas.
- **c.** Documentación los hallazgos encontrados en la visita de reconocimiento del proceso.
- **d.** Identificación del Responsable del Riesgo, es decir la UEN, grupo o personas encargadas de administrar la actividad asociada a la situación de riesgo.

Responsable(s): Grupo Corporativo de Seguridad de la Información - líderes proceso – propietario activo de información – custodio activo de información
Instrumento de Análisis: Formato Matriz de Riesgos de Activos de Información (Sección "Identificación")

3.5.2.3. Análisis y Evaluación de Riesgos

El análisis de riesgos permite evaluar la probabilidad de ocurrencia de los Riesgos de activos de información y el impacto de su materialización. El análisis de riesgos puede hacerse tomando como sustento datos históricos existentes en la Organización, o bien, a partir del conocimiento y experiencia de los funcionarios que participan en el análisis. Las etapas que deben seguirse como parte del Análisis de Riesgos corresponden a:

1. Tome como base la información hallada en la etapa de Identificación de Riesgos (Descripción actividades, vulnerabilidades, amenazas y hallazgos).
2. Asigne la valoración del riesgo inherente en término de su probabilidad e impacto, considerando la matriz de evaluación y respuesta a los riesgos.

La evaluación permite determinar el nivel o grado de exposición del Banco al impacto del riesgo de activos de información inherente, permitiendo estimar las prioridades para su tratamiento. Evaluación del riesgo es el producto de confrontar los resultados de la valoración del riesgo con los controles, con el objetivo de establecer prioridades para su manejo y fijación de políticas. En la valoración de los controles se deben considerar las siguientes cuestiones:

a. Existencia del control
b. El control debe estar documentado
c. El control debe ser efectivo

Situación	Guía de Valoración
No existen controles	Se mantiene el resultado de la evaluación.
Los controles existentes no son efectivos	Se mantiene el resultado de la evaluación.
Los controles existentes son efectivos y están documentados	Cambia el resultado a una casilla inferior de la matriz de evaluación (el desplazamiento depende de sí el control afecta el impacto o la probabilidad).

Una vez determinada la efectividad del control, se debe identificar si el mismo contribuye a reducir el Impacto, la Probabilidad, o ambos componentes, y en que medida, obteniendo una nueva medida que corresponde a la Valoración del Riesgo Residual.

Responsable(s): Grupo Corporativo de Seguridad de la Información – líderes de Proceso - propietario activo de información – custodio activo de información.
Instrumentos de Análisis: Formato Matriz de Riesgos de Activos de Información (Secciones "Análisis y Evaluación", "Guía de Evaluación y Respuesta" y "Programa a la medida").

3.5.2.4. Tratamiento y Monitoreo de Riesgos

Partiendo del reconocimiento de la valoración para el Riesgo de activo de información bajo análisis, la Matriz de Evaluación y Respuesta a los Riesgos indica las siguientes acciones a considerar:

- **Evitar el riesgo:** Es siempre la primera alternativa a considerar. Se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño, ejecución o eliminación de actividades.

- **Reducir el riesgo:** Si el riesgo de activos de información no puede ser evitado porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al más bajo nivel posible. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.

La Matriz de Identificación de Vulnerabilidades posee un listado de controles sugeridos para implementación, de acuerdo a la vulnerabilidad y amenaza

identificada. La implementación de estos controles no es mandatorio, puede ser sustituida por controles complementarios que cumplan con el mismo objetivo.

Para asignar los recursos y aplicar controles efectivos de costos, la Organización, después de identificar todos los controles posibles y evaluar su viabilidad y eficacia, deben llevar a cabo un análisis costo-beneficio para cada control propuesto a fin de determinar qué controles son necesarios y apropiados para sus circunstancias.

El análisis costo-beneficio puede ser cualitativo o cuantitativo. Su propósito es demostrar que el gasto de ejecución de controles puede ser justificado por la reducción del nivel de riesgo.

Un análisis de costo-beneficio para una propuesta de nuevos controles o mejoras a los mismos debe abarcar lo siguiente:

- Determinar el impacto de la aplicación de los nuevos controles o mejoras de los mismos.
- Determinar el impacto de no implementar los nuevos controles o mejoras de los mismos.
- Estimación de los costos de la aplicación. Estos pueden incluir:
- Equipamiento técnico y las compras de software
- Reducción de la eficacia operativa si el rendimiento del sistema o la funcionalidad es reducido para una mayor seguridad
- Costo de la aplicación de las políticas y procedimientos adicionales
- Costo de la contratación de personal adicional para implementar las políticas propuestas, procedimientos o servicios
- Los gastos de formación
- Los costos de mantenimiento
- Evaluar los costos de ejecución, los beneficios y la importancia crítica contra el sistema de datos para determinar la importancia para la Organización de la aplicación de los nuevos controles, dado sus costos y el impacto relativo.

La Organización tendrá que evaluar los beneficios de los controles en cuanto al mantenimiento de una postura aceptable para la misión de la misma. Así como hay un costo para la aplicación de control necesario, hay un costo por no ponerlo en práctica. Al relacionar el resultado de no la aplicación con la aplicación del control, la Organización puede determinar si es factible renunciar a su aplicación.

- **Transferir el riesgo:** Hace referencia a buscar respaldo y compartir con otro parte del riesgo como por ejemplo tomar pólizas de seguros; se traslada el riesgo a otra parte o físicamente se traslada a otro lugar. Esta técnica es usada para eliminar el riesgo de un lugar y pasarlo a otro o de un grupo a otro. Así mismo, el riesgo puede ser minimizado compartiéndolo con otro grupo o dependencia.

- **Asumir el riesgo:** Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Una vez diseñado y validado el plan de tratamiento de riesgo, en la Matriz de Riesgos de Activos de Información, es necesario monitorearlo teniendo en cuenta que estos nunca dejan de representar una amenaza para la Organización.

El monitoreo es esencial para asegurar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas.

El monitoreo debe estar a cargo de los líderes de Proceso y del Grupo Corporativo de Seguridad de la Información, su finalidad principal será la de aplicar y sugerir los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo. El Grupo Corporativo de Seguridad de la Información dentro de su función asesora comunicará y presentará luego del seguimiento y evaluación sus resultados y propuestas de mejoramiento y tratamiento a las situaciones detectadas.

Responsable(s): Grupo Corporativo de Seguridad de la Información – líderes de proceso – propietario activo de información – custodio activo de información.
Instrumento de Análisis: - Formato Matriz de Riesgos de Activos de Información (Sección "Tratamiento y Monitoreo")

3.5.2.5. Elaboración Matriz de Riesgos

Todo lo anterior, el proceso de identificación, análisis, evaluación y tratamiento del riesgo de activos de información, así como los programas a la medida ejecutados, los controles implementados y los planes de acción desarrollados deben considerarse como la matriz de riesgo.

La Matriz de Riesgos facilita la visualización y entendimiento de los riesgos de activos de información que se presentan en la Organización en los diferentes niveles de su modelo de operación, facilitando la definición de medidas de respuesta o tratamiento.

A partir de la matriz es generado el mapa de riesgo que consiste en una representación gráfica que permite a la alta dirección observar el nivel de exposición al riesgo que se encuentra su proceso o producto, visualizando rápidamente los aspectos en los que hay situaciones de alarma, aquellos con

situaciones de advertencia y los que satisfacen lo establecido por la Organización, facilitando el diagnóstico, monitoreo y la toma de decisiones.

Responsable(s): Grupo Corporativo de Seguridad de la Información
Instrumento de Análisis: Formato Matriz de Riesgos de Activos de Información (Secciones "Matriz de riesgo" y "Mapa de riesgo").

3.6. Declaración de Aplicabilidad

Para ver en detalle los la Declaración de Aplicabilidad ver ANEXO 2 – Declaración de Aplicabilidad.

4. ANÁLISIS DE RIESGOS

4.1. Introducción

4.1.1. Propósito

El principal objetivo de un análisis de riesgos, tal y como su nombre indica, es poner de manifiesto cuáles son los riesgos a los que el negocio está expuesto, para que la Dirección de la compañía pueda analizar, para cada uno de ellos, cuáles son las acciones a acometer, sin perder en ningún momento de vista el principio de proporcionalidad, ya que el costo de la implantación de un control no deberá nunca superar el posible impacto de la materialización de una amenaza.

Las posibles posturas ante un riesgo son:

a. **Aceptarlo**: no emprender acciones. El negocio asume un posible impacto en caso de materialización de la amenaza. De producirse el incidente, se procederá a la recuperación.

b. **Mitigarlo:** aplicar controles (técnicos u organizativos) para reducir el nivel de riesgo intrínseco a un nivel de riesgo aceptable para la compañía.

c. **Transferirlo**: Cambiar un riesgo por otro.

d. **Evitarlo o eliminarlo:** Suprimir las causas del riesgo, es decir, eliminar el activo, la amenaza o la vulnerabilidad.

En definitiva, el análisis de riesgos nos permitirá responder a las preguntas:

- ¿Qué hay que proteger?
- ¿De qué o de quién y, por qué?
- ¿Cómo proteger?

4.1.2. Alcance

Como bien se indicó en la Contextualización, objetivos y análisis diferencial inicial el Sistema de Gestión de Seguridad de la Información enmarcará inicialmente parte de la organización, es decir, se evaluarán cuatro procesos críticos lo cuales se listan a continuación:

- Comercio exterior
- Administración de portafolios de la tesorería

- Administración de liquidez
- Reporte de cartera a entes externos

4.2. Inventario de Activos

4.2.1. Inventario por proceso

A continuación se adjuntan los archivos con cada una de las matrices de activos de información clasificadas por proceso. En cada una de ellas se identifican los siguientes aspectos divididos en tres etapas:

Etapa 1 – Identificación del inventario de activos de información:

- Proceso
- Dueño del proceso
- Oficina/Dependencia
- Consecutivo
- Nombre del activo de información
- Tipo de activo de información

Etapa 2 – Características básicas de los activos de información:

- Origen del activo de información
- Contenedor
- Custodios de los contenedores

Etapa 3 - Análisis de impacto en el negocio – Clasificación de activos de información

- Clasificación por:
    - Confidencialidad
    - Integridad
    - Disponibilidad

Inventario:

Proceso	Clasificación de activos de información
Comercio exterior	Ver ANEXO 3 – MAI_ComercioExterior
Administración de portafolios de la tesorería	Ver ANEXO 4 – MAI_AdministracionPortafolios
Administración de liquidez	Ver ANEXO 5 – MAI_AdministracionLiquidez
Reporte de cartera a entes externos	Ver ANEXO 6 – MAI_Reportes

4.2.2. Inventario por grupos

De acuerdo al inventario anterior, se realizó la clasificación de activos por grupos para cada uno de los procesos anteriormente nombrados:

Comercio exterior		
Ámbito	**Consecutivo**	**Activo**
Instalaciones	CE1	Edificio Dirección General Piso 6
Hardware	CE2	Servidor CE
Aplicación	CE3	OnBase
Datos/Información	CE4	Avales y garantías recibidas en moneda extranjera
Personal	CE5	Analista cambiario

Administración de portafolios de la tesorería		
Ámbito	**Consecutivo**	**Activo**
Instalaciones	AP1	Edificio Dirección General Piso 13
Hardware	AP2	Bloomberg
Aplicación	AP3	Dialogo
Personal	AP4	Analista mesa renta fija

Administración de liquidez		
Ámbito	**Consecutivo**	**Activo**
Instalaciones	AL1	Edificio Dirección General Piso 10
Hardware	AL2	Servidor Swift
Aplicación	AL3	Summit
Datos/Información	AL4	Informe de posición de liquidez en dólares
Personal	AL5	Gerente tesorería

Reporte de cartera a entes externos		
Ámbito	**Consecutivo**	**Activo**
Instalaciones	RC1	Edificio Dirección General Piso 9
Hardware	RC2	Servidor Iris09
Aplicación	RC3	Sistema central de endeudamiento

Reporte de cartera a entes externos		
Ámbito	**Consecutivo**	**Activo**
Datos/Información	RC4	Reporte de endeudamiento de clientes
Personal	RC5	Gerente control de crédito

4.3. Valoración de los Activos

La valoración de un activo es la determinación del coste que supondría salir de una incidencia que destrozara dicho activo. Hay muchos factores a considerar:

a. Coste de reposición, que debe incluir tanto la adquisición como la instalación

b. Coste de mano de obra especializada invertida en recuperar el valor del activo

c. Pérdida de ingresos

d. Capacidad de operar: una pérdida de confianza de los usuarios o proveedores se traduce en una pérdida de contratos o en peores condiciones económicas

e. Sanciones por incumplimiento legal u obligaciones contractuales

f. Daños a otros activos, propios o ajenos.

g. Daños a personas.

h. Daños medioambientales.

Esta valoración se puede realizar de forma cuantitativa (valor numérico) o cualitativa (en una escala de valores). En este caso, se realizará una valoración cuantitativa, concretamente una valoración económica. Para ello, se utilizará la siguiente escala:

Valoración	Siglas	Rango (Eur)	Valor estimado para el cálculo (Eur)
Muy alto	MA	Vr.>200.000	300.000
Alto	A	100.000 < Vr. < 200.000	150.000
Medio	M	50.000 < Vr. < 100.000	75.000
Bajo	B	100.000 < Vr. <200.000	30.000
Muy bajo	MB	Vr. < 10.000	10.000

El valor estimado para el cálculo, será el que utilizaremos como valoración económica de los activos que caigan dentro del correspondiente rango.

Generalmente el activo que tiene mayor valoración es el de la información, que es la razón de ser de todo el sistema de información que lo soporta.

4.4. Dimensiones de Seguridad

De un activo puede interesar calibrar diferentes dimensiones:

- **Confidencialidad**: ¿qué daño causaría que lo conociera quien no debe?
- **Integridad**: ¿qué perjuicio causaría que estuviera dañado o corrupto?
- **Disponibilidad**: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?

En los activos esenciales, frecuentemente es útil valorar:

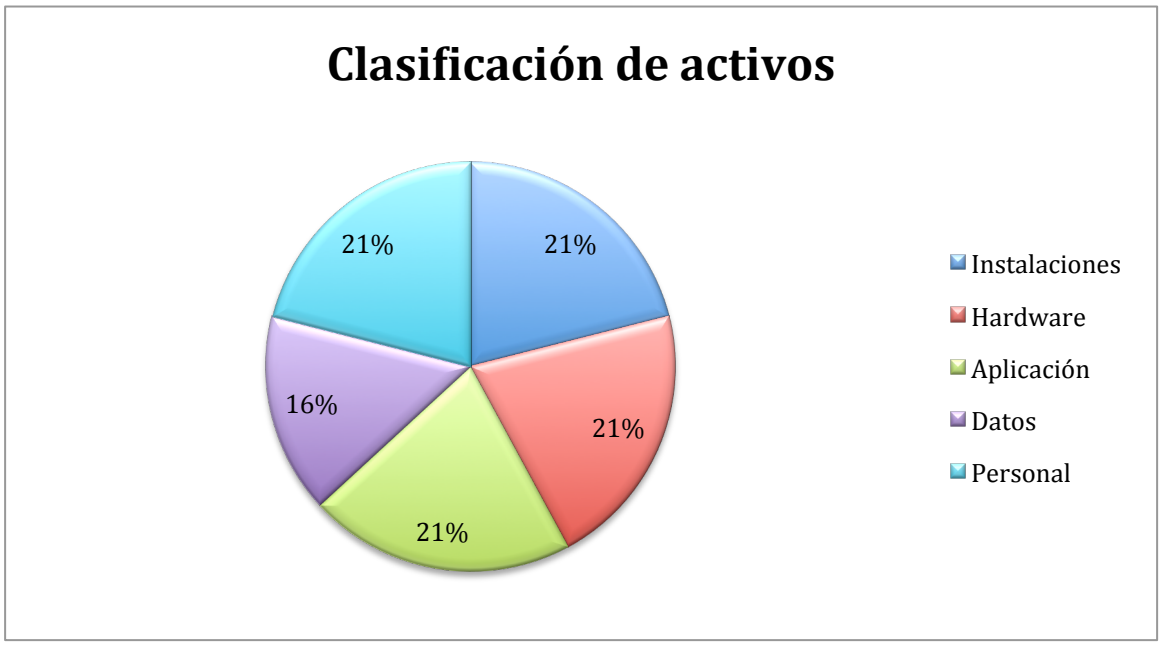
- **Autenticidad**: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
- **Trazabilidad del uso del servicio**: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?
- **Trazabilidad del acceso a los datos**: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

4.5. Tabla Resumen de Valoración

Ámbito	Proceso	Activo	Valor	Aspectos críticos				
				A	C	I	D	T
Instalaciones	Comercio exterior	Edificio Dirección General Piso 6	MA	3	5	7	10	3
	Administración de portafolios de la tesorería	Edificio Dirección General Piso 13	MA	3	5	7	10	3
	Administración de liquidez	Edificio Dirección General Piso 10	MA	3	5	7	10	3
	Generación y divulgación de informes	Edificio Dirección General Piso 9	MA	3	5	7	10	3
Hardware	Comercio exterior	Servidor CE	A	10	10	10	10	10

Ámbito	Proceso	Activo	Valor	Aspectos críticos				
				A	C	I	D	T
	Administración de portafolios de la tesorería	Bloomberg	A	10	10	10	10	10
	Administración de liquidez	Servidor Swift	A	10	10	10	10	10
	Generación y divulgación de informes	Servidor Iris09	M	10	10	10	10	10
Aplicación	Comercio exterior	OnBase	A	10	10	10	10	10
	Administración de portafolios de la tesorería	Dialogo	A	10	10	10	10	10
	Administración de liquidez	Summit	A	10	10	10	10	10
	Generación y divulgación de informes	Sistema central de endeudamiento	A	10	10	10	10	10
Datos	Comercio exterior	Avales y garantías recibidas en moneda extranjera	M	10	3	10	6	6
	Administración de liquidez	Informe de posición de liquidez en dólares	A	10	3	10	6	6
	Generación y divulgación de informes	Reporte de endeudamiento de clientes	M	10	3	10	6	6
Personal	Comercio exterior	Analista cambiario	M	3	5	7	10	3

Ámbito	Proceso	Activo	Valor	Aspectos críticos				
				A	C	I	D	T
	Administración de portafolios de la tesorería	Analista mesa renta fija	M	3	5	7	10	3
	Administración de liquidez	Gerente tesorería	A	3	5	7	10	3
	Generación y divulgación de informes	Gerente control de crédito	A	3	5	7	10	3



4.6. Análisis de Amenazas

El siguiente paso consiste en identificar amenazas para cada activo y en cada una de las dimensiones.

Para la identificación de amenazas es bueno tener en cuenta la experiencia pasada, ya sea propia o de organizaciones similares. Habitualmente este análisis se basa en los catálogos de amenazas que algunas metodologías u organizaciones especializadas proporcionan, tal y como ocurre en Magerit.

Analicemos brevemente las amenazas propuestas y realicemos algunas hipótesis, para intentar acotar cuál será su afectación sobre los activos definidos por cada proceso:

- **Acceso no autorizado:** Es una amenaza contra la confidencialidad de los datos. Puede tratarse del acceso por parte de personal interno, o bien por parte de personal externo (un hacker por ejemplo, la competencia, entre otros). En este ejercicio se considera un acceso no autorizado a la información y a las aplicaciones, pero no al Hardware.

- **Ataque malintencionado:** Podría ser una amenaza a la confidencialidad, la integridad e incluso la disponibilidad, de ser por ejemplo un ataque de denegación de servicio. En este caso, y para simplificar, se considera que se trata de una amenaza a la integridad de la información, por ejemplo, un caso de manipulación de código o de datos.

- **Incumplimiento de requerimientos legales:** Dependería del tipo de incumplimiento, pero un caso típico sería el de la ley orgánica de protección de datos, en que típicamente se produciría una amenaza a la confidencialidad de la información mediante un acceso no autorizado.

- **Errores de diseño:** se considera una amenaza a la disponibilidad de la aplicación.

- **Fallo del suministro eléctrico:** amenaza típica a la disponibilidad, aunque podría provocar también problemas de integridad de datos.

- **Errores de los usuarios:** si se considera un usuario administrador, por ejemplo, se trataría de una amenaza típica a la disponibilidad, aunque podría provocar también problemas de integridad de datos.

- **Inundación:** amenaza a la disponibilidad de los sistemas de información y las comunicaciones, y de las instalaciones en general, dependiendo de la gravedad de dicha inundación.

- **Fallo de equipos de aire acondicionado:** amenaza a la disponibilidad de las máquinas o equipos de cómputo.

- **Marcha de personal crítico:** podría suponer amenaza a la confidencialidad de la información y en según que circunstancias, dependiendo de cómo se produjera la salida, en caso de un despido por ejemplo, a la integridad y la disponibilidad.

El siguiente paso consiste en efectuar un Análisis de vulnerabilidades. Para Magerit, la vulnerabilidad se entiende como la frecuencia de ocurrencia de una amenaza; concretamente como una tasa anual de ocurrencia. Así, se modela la vulnerabilidad como el cociente entre la frecuencia estimada de ocurrencia y el número de días del año.

Se utilizará una escala de cinco rangos, en que una ocurrencia diaria se considera extremadamente frecuente y una ocurrencia anual, muy poco frecuente.

Vulnerabilidad	Siglas	Rango	Valor estimado para el cálculo
Extremadamente frecuente	EF	1 vez al día	365/365=1
Muy frecuente	MF	1 vez por semana	52/365=0.142
Frecuente	F	1 vez por mes	12/365=0.033
Poco frecuente	PF	1 vez al trimestre	4/365=0.011
Muy poco frecuente	MPF	1 vez al año	1/365-0.003

La estimación se realizará tomando en consideración:

- La capacidad: conocimientos necesarios para ejecutar la amenaza o recursos necesarios para ejecutarla (número de atacantes, de máquinas, entre otras). Cuanto más complejo es el ataque, menor capacidad.

- La motivación, o interés que puede existir por ejecutar la amenaza.

- La frecuencia estadística de ocurrencia de la amenaza, que se obtendrá de la propia experiencia del pasado, y de fuentes externas.

- La existencia de salvaguardas que minimizarían dicha frecuencia de ocurrencia. Es en este punto donde interviene el concepto de vulnerabilidad. Cuantas más vulnerabilidades existan sobre nuestros activos no cubiertas por salvaguardas, mayor probabilidad de materialización de la amenaza.

De acuerdo a lo anterior, se establece la vulnerabilidad (entendida como frecuencia de ocurrencia), para cada una de las amenazas y se hace a partir de un conjunto de hipótesis:

Amenaza	Vulnerabilidad	Comentarios
Acceso no autorizado	F	Mucha capacidad, poca motivación, frecuencia histórica media, ausencia de controles
Ataque	F	Poca capacidad, poca motivación,

Amenaza	Vulnerabilidad	Comentarios
malintencionado		frecuencia histórica baja y ausencia de controles
Suplantación de la identidad del usuario	PF	Mucha capacidad, poca motivación, frecuencia histórica baja, ausencia de controles
Errores de diseño	PF	Poca capacidad, poca motivación, frecuencia histórica alta y existencia de controles (alta disponibilidad *de Servidores)*
Fallo del suministro eléctrico	F	Poca capacidad, poca motivación, frecuencia histórica muy alta y ausencia de salvaguardas.
Errores de usuario	F	Poca capacidad, poca motivación, frecuencia histórica muy alta y ausencia de salvaguardas.
Inundación	MPF	Poca capacidad, poca motivación, frecuencia histórica muy baja y ausencia de salvaguardas.
Fallo de equipos de aire acondicionado	PF	Poca capacidad, poca motivación, frecuencia histórica baja y ausencia de salvaguardas
Marcha de personal crítico	MPF	Frecuencia histórica baja y ausencia de salvaguardas

4.7. Impacto Potencial

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Cuantificaremos el impacto como el "porcentaje de degradación del activo" de forma que se puede perder entre un 0% y un 100%.

Impacto	Siglas	Valor
Total (catastrófico)	T	100%
Alto	A	90%
Medio	M	50%
Bajo	B	10%
Nulo	N	0%

El valor del impacto dependerá del tipo de amenaza y del activo amenazado. Así pues, un acceso no autorizado sobre información muy confidencial tendrá un impacto muy alto, mientras que si la información es pública o de uso interno, quizás no sea necesario ni considerar la amenaza por el bajo impacto que implica.

Para analizar el impacto, es importante realizar un paso previo, que nos permita relacionar activos y amenazas, dado que cada activo, dependiendo de su naturaleza, estará expuesto a amenazas distintas. Magerit nos proporciona esta información, relacionando amenazas con tipos de activo

Amenaza	Activos																		
	CE1	CE2	CE3	CE4	CE5	AP1	AP2	AP3	AP4	AL1	AL2	AL3	AL4	AL5	RC1	RC2	RC3	RC4	RC5
Acceso no autorizado	X					X				X					X				
Ataque malintencionado		X	X				X	X			X	X				X	X		
Suplantación de la identidad del usuario			X					X				X					X		
Errores de diseño			X					X				X					X		
Fallo del suministro eléctrico		X					X				X					X			
Errores de usuario			X	X				X				X	X				X	X	
Inundación	X					X				X					X				
Fallo de equipos de aire acondicionado		X					X				X					X			
Marcha de personal crítico					X				X					X					X

Cálculo del impacto potencial:

Amenaza	Frecuencia	Valor	A	C	I	D	T	Comentarios
Acceso no autorizado	F	0.033	50%	50%	50%	50%	50%	El nivel de confidencialidad es alto, pero se asume que se trata de un acceso interno de la organización, y que por tanto el riesgo está algo controlado.
Ataque malintencionado	F	0.033	90%	90%	90%	90%	90%	Afecta totalmente la integridad
Suplantación de la identidad del usuario	PF	0.011	50%	50%	50%	50%	50%	El similar a un acceso no autorizado
Errores de diseño	PF	0.011	10%	10%	10%	10%	10%	Los servidores se encuentran en alta disponibilidad por lo tanto el impacto es bajo
Fallo del suministro eléctrico	F	0.033	100%	100%	100%	100%	100%	Al no existir salvaguardas, independientemente de la alta disponibilidad implementada, la caída del suministro eléctrico arrastrará a todos los sistemas. El impacto es del 100%.
Errores de usuario	F	0.033	90%	90%	90%	90%	90%	Como pueden afectar a la disponibilidad y a la integridad, el impacto será muy alto en cada uno de los procesos críticos.
Inundación	MPF	0.003	100%	100%	100%	100%	100%	Se considera un impacto del 100% por destrucción del Hardware
Fallo de equipos de aire acondicionado	PF	0.011	50%	50%	50%	50%	50%	Se presupone una degradación del rendimiento, pero no la discontinuidad, por lo que se estima un impacto del 50%.
Marcha de personal crítico	MPF	0.003	50%	50%	50%	50%	50%	El personal tiene el know-how, pero se considera que hay cierta documentación para la transferencia de ese know-how. Por este motivo, consideramos un impacto del 50%.

4.8. Nivel de Riesgo Aceptable y Riesgo Residual

A continuación se relaciona un archivo en donde se efectúa el cálculo del riesgo aceptable, seguidamente se establecen algunos controles o salvaguardas de acuerdo al resultado que se obtuvo para obtener el riesgo residual.

Para ver en detalle los la Declaración de Aplicabilidad ver ANEXO 7 – Riesgo Inherente

- **Primera salvaguarda:**

  Un ataque malintencionado sobre algún servidor de los 4 procesos críticos tiene un impacto del 90%. Tal y como se ha comentado un ataque que permitiera alterar la integridad de la información sería catastrófico, puesto que el impacto sobre el proceso de distribución sería altísimo.

  Una salvaguarda eficiente al respecto, sería realizar auditorías periódicas de código y OWASP antes del paso a producción de versiones, para minimizar la probabilidad de existencia de vulnerabilidades en esta línea.

- **Segunda salvaguarda**

  Se observa que otra fuente de riesgo son los fallos de suministro eléctrico y picos de tensión (generalmente se engloban en un único concepto). Como salvaguarda se propone la instalación de un SAI, Sistema de Alimentación Ininterrumpida que, por un lado es un estabilizador de corriente, que neutraliza picos de corriente y por otro, permite mantener el sistema funcionando durante un determinado tiempo, que como mínimo debiera ser el tiempo necesario para realizar un cierre ordenado del sistema. Si el sistema es muy crítico, en ocasiones se contrata un segundo ramal de suministro a otra compañía eléctrica o bien se dispone de un generador eléctrico, con el consiguiente suministro de combustible, que garantizará el servicio durante el tiempo de recuperación de la incidencia.

Cálculo del riesgo residual:

Auditorías:

La realización de auditorías de código y auditorías OWASP periódicas supondría una reducción de la vulnerabilidad (salvaguarda preventiva), que podría pasar a ser poco frecuente, es decir, 0.011.

Dicha salvaguarda no supone ninguna variación sobre el impacto, puesto que de materializarse la amenaza, el impacto sería el mismo.

El riesgo residual sería en este caso:

Riesgo residual = Valor (XX) x Nueva vulnerabilidad (0.011) x Impacto (XX)

En este caso, se trata de una salvaguarda que actúa sobre el impacto, puesto que los cortes y caídas de corriente seguirán produciéndose al mismo ritmo (no depende de nosotros, sino de la compañía eléctrica), mientras que el impacto se minimizará enormemente, al permitir mantener el servicio en marcha hasta la recuperación de la incidencia. Por no considerar que el impacto es nulo, pasaremos a considerarlo Bajo.

El cálculo del riesgo residual sería:
Riesgo residual = Valor (XX) x Vulnerabilidad (0.033) x Nuevo impacto (10%)

5. PROPUESTAS DE PROYECTOS

5.1. Introducción

De acuerdo a los resultados obtenidos durante toda la implantación del SGSI en el Banco ABC, se determinaron las siguientes propuestas de proyectos para cada uno de los 11 dominios definidos en el marco de referencia.

5.2. Propuestas de proyectos

Dominio	**Política de Seguridad de la Información**
Proyecto	Revisión de política de seguridad de la información
Descripción	Establecer un proceso formal y continuo de revisión a la política de seguridad de la información, que tenga en cuenta los resultados de los indicadores del sistema, los informes de auditorías y revisiones al SGSI, el estado de madurez de los controles definidos en el sistema, las vulnerabilidades y amenazas identificadas en las evaluaciones de riesgo que no están siendo tratadas adecuadamente, incidentes de seguridad presentados, acciones de seguimiento de revisiones anteriores y cambios generados sobre las plataformas tecnológicas o sobre el negocio que impacten el modelo de seguridad definido.
Plazos de consecución	Este proceso se debe ejecutar con una periodicidad no mayor a un año y se debe empezar a ejecutar en el corto plazo (Menos de tres meses)
Puntos de control	Se debe realizar un mantenimiento de la documentación soporte de las revisiones realizadas a la misma por el periodo definido.
Análisis de impacto	Como resultado se debe obtener: • Acciones de mejoramiento a la política de seguridad y al SGSI. • Orientación de las acciones de gestión del riesgo de la información. • Estrategias de alineación del sistema con los objetivos de negocio y generación de valor hacia el negocio.

Dominio	**Organización de la Seguridad de la Información**
Proyecto	Seguridad para terceros y proveedores
Descripción	Refuerzo del análisis de riesgos realizado a los proveedores/terceros críticos con acceso a información y soluciones de procesamiento de información del Banco,

	considerando en el mismo los aspectos relacionados con seguridad de la información (actualmente sólo se consideran riesgos de disponibilidad). En este caso se deben ejecutar las siguientes actividades: • Realizar un inventario de los proveedores con acceso a los activos de información del Banco. • Determinar el tipo de acceso de los proveedores sobre los activos de información del Banco (v.gr. acceso físico a las oficinas, acceso lógico a bases de datos, sistemas de información, red de datos, etc.). • Establecer la clasificación de los activos de información accedidos por los proveedores del Banco. • Identificar las posibles situaciones de riesgos que pueden comprometer la confidencialidad e integridad de la información. • Definir los controles que deben ser implementados por el Banco y los proveedores para proteger los activos de información.
Plazos de consecución	Este proceso se debe ejecutar con una periodicidad no mayor a un año y se debe empezar a ejecutar en el corto plazo (Menos de tres meses)
Puntos de control	Se debe mantener registro de la actualización del inventario de proveedores de forma periódica por el tiempo definido.
Análisis de impacto	Como resultado se debe obtener: • Acciones de mejoramiento a la política de seguridad y al SGSI. • Orientación de las acciones de gestión del riesgo de la información enfocadas a agentes externos a la organización. • Estrategias de alineación del sistema con los objetivos de negocio y generación de valor hacia el negocio.

Dominio	**Gestión de activos**
Proyecto	Política de actualización de inventario de activos de información
Descripción	• Documentar, formalizar y poner en operación una política para la actualización del inventario de activos de información y verificar su cumplimiento (v. gr. definir una función centralizada, responsable de la consolidación del proceso de identificación, inventario y clasificación de activos de información, o utilizar una herramienta tecnológica que

	soporte el proceso). • Definir indicadores sobre el proceso de clasificación de activos de información, que permita establecer el estado de ejecución del proceso, los resultados del mismo y priorizar los esfuerzos o acciones a seguir para su protección. (v. gr. % de activos de información físicos con clasificación Confidencial Restringida / Confidencial en el Banco, etc.)
Plazos de consecución	Este proceso se debe ejecutar con una periodicidad no mayor a un año y se debe empezar a ejecutar en el corto plazo (Menos de tres meses)
Puntos de control	Se debe proteger de manera adecuada de los activos de información organizacionales y asegurar que la información recibe el nivel de control adecuado.
Análisis de impacto	Como resultado se debe obtener: • Acciones de mejoramiento a la política de seguridad y al SGSI. • Definición del grado de seguridad de cada unos de los activos identificados • Análisis de dependencia de activos por cada proceso crítico de la organización

Dominio	**Seguridad de los recursos humanos**
Proyecto	Monitoreo de controles
Descripción	Monitorear y medir el cumplimiento de los controles, y establecer mecanismos para detectar que los mismos se apliquen de manera consistente en todos los casos (v. gr. eliminación oportuna de cuentas y perfiles de acceso asignados a los empleados retirados, etc.).
Plazos de consecución	Este proceso se debe ejecutar con una periodicidad no mayor a un año y se debe empezar a ejecutar en el mediano plazo (Menos de 1 año)
Puntos de control	Indicadores de cumplimiento
Análisis de impacto	Como resultado se debe obtener: • Acciones de mejoramiento a la política de seguridad y al SGSI.

Dominio	**Seguridad física y del entorno**
Proyecto	Mejoramiento del esquema de control físico y del entorno
Descripción	Mejorar el esquema de control actual, mediante elaboración, formalización y divulgación de la documentación relacionada a los requerimientos de cableado de energía y datos, así como áreas de carga, despacho y acceso público, con el fin de que no haya dependencia en personal clave sobre la ejecución de los controles relacionados a éstos temas (v.gr. Estándar de cableado utilizados actualmente, etc.). Fortalecer el cumplimiento de los controles de éste dominio, mediante las siguientes acciones: • Actualizar y divulgar el procedimiento de borrado seguro, considerando las herramientas utilizadas actualmente, y los responsables de su ejecución. • Poner en operación el control de borrado seguro sobre equipos que se reasignan para uso dentro del Banco, debido a que actualmente sólo se realiza sobre aquellos que no se utilizarán más en la Organización. Así mismo, actualizar y divulgar el procedimiento de borrado seguro, considerando las herramientas utilizadas actualmente, y los responsables de su ejecución. • Monitorear y medir el cumplimiento de los controles del dominio, con el fin de detectar desviaciones de los mismos (v.gr. control de borrado seguro para los equipos reasignados y marcados para donación, etc.).
Plazos de consecución	Este proceso se debe ejecutar con una periodicidad no mayor a un año y se debe empezar a ejecutar en el mediano plazo (Menos de 1 año)
Puntos de control	Indicadores de cumplimiento de controles Registros de ejecución de borrado seguro
Análisis de impacto	Como resultado se debe obtener: • Acciones de mejoramiento a la política de seguridad y al SGSI.

Dominio	**Gestión de Comunicaciones y Operaciones**
Proyecto	Administración de la capacidad
Descripción	Fortalecer la puesta en operación del proceso de administración de la capacidad, mediante la implementación de las siguientes actividades específicas:

	• Establecer un proceso para la revisión de la capacidad de los recursos de tecnología, alineado a los acuerdos de nivel de servicios establecidos, que considere información actual y pronosticada de requerimientos, prioridades y objetivos del negocio e impacto en el presupuesto. • Evaluar regularmente los niveles de desempeño y capacidad frente a los requerimientos (demanda) del negocio, la capacidad de los recursos, tendencias identificadas y ANS. • Elaborar pronósticos de desempeño y capacidad de los recursos de tecnología y monitorear constantemente, para evitar interrupción o degradación de los servicios. Utilizar técnicas de generación de modelos para la elaboración de los pronósticos. • Monitorear la capacidad de los recursos de tecnología, considerando cargas de trabajo, priorización de procesos, etc.
Plazos de consecución	Este proceso se debe ejecutar con una periodicidad no mayor a un año y se debe empezar a ejecutar en el mediano plazo (Menos de 1 año)
Puntos de control	Registros de revisión de niveles de desempeño y capacidad
Análisis de impacto	Como resultado se debe obtener: • Acciones de mejoramiento a la política de seguridad y al SGSI.

Dominio	**Control de acceso**
Proyecto	Segregación de red
Descripción	Los controles de control de acceso a las redes, se deben reforzar mediante la implementación de la segregación de red para los ambientes de pruebas y desarrollo.
Plazos de consecución	Este proceso se debe ejecutar con una periodicidad no mayor a un año y se debe empezar a ejecutar en el corto plazo (Menos de tres meses)
Puntos de control	Pruebas de intrusión que verifique que se segregó la red
Análisis de impacto	Como resultado se debe obtener: • Acciones de mejoramiento a la política de seguridad y al SGSI.

Dominio	**Adquisición, Desarrollo y Mantenimiento de Sistemas de Información**
Proyecto	Mantenimiento de sistemas
Descripción	Definir e implementar los siguientes controles: • Ofuscamiento/enmascaramiento de la data de pruebas extraída de los ambientes de producción. • Imágenes para el alistamiento de máquinas (estaciones y servidores), considerando el software base requerido por plataforma. • Prevención de fuga de información (DLP).
Plazos de consecución	Este proceso se debe ejecutar con una periodicidad no mayor a un año y se debe empezar a ejecutar en el mediano plazo (Menos de 1 año)
Puntos de control	Registros de revisión y mantenimiento de sistemas
Análisis de impacto	Como resultado se debe obtener: • Acciones de mejoramiento a la política de seguridad y al SGSI.

Dominio	**Gestión de los Incidentes de Seguridad de la Información**
Proyecto	Monitoreo de incidentes
Descripción	Implementación de los mecanismos de control que permiten monitorear la gestión que se realiza sobre los diferentes tipos de incidentes, así como también volúmenes de ocurrencia y costos de los mismos.
Plazos de consecución	Este proceso se debe ejecutar con una periodicidad no mayor a un año y se debe empezar a ejecutar en el corto plazo (Menos de tres meses)
Puntos de control	Reportes de incidentes de forma periódica (Mensual)
Análisis de impacto	Como resultado se debe obtener: • Acciones de mejoramiento a la política de seguridad y al SGSI.

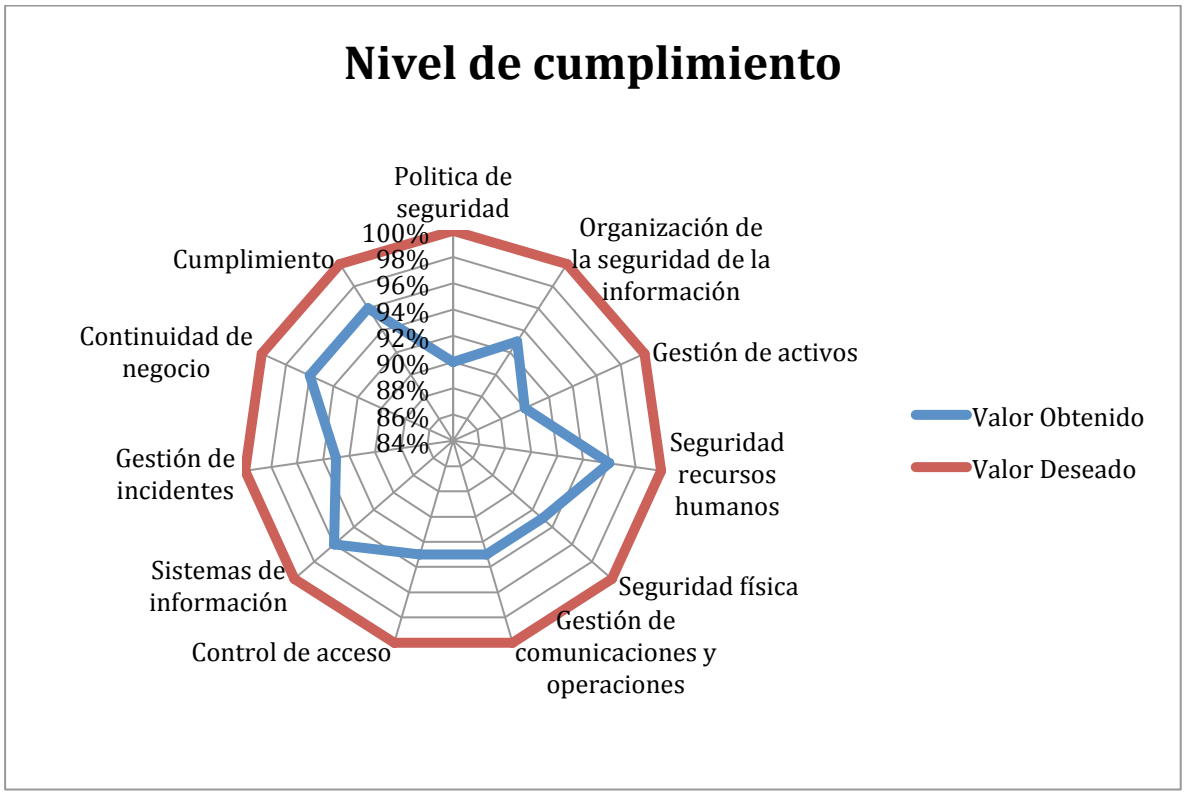
Dominio	**Gestión de la Continuidad del Negocio**
Proyecto	Medición de efectividad de PCN
Descripción	Definir y establecer indicadores para medir la efectividad del

	proceso de continuidad del negocio (v. gr. # de procedimientos operativos definidos para el plan de continuidad del negocio, # de revisiones periódicas de los planes de continuidad del negocio, recuperación ante desastres y de emergencias.).
Plazos de consecución	Este proceso se debe ejecutar con una periodicidad no mayor a un año y se debe empezar a ejecutar en el corto plazo (Menos de tres meses)
Puntos de control	Indicadores de efectividad de continuidad de negocio
Análisis de impacto	Como resultado se debe obtener: • Acciones de mejoramiento a la política de seguridad y al SGSI.

Dominio	**Cumplimiento**
Proyecto	Verificación de cumplimiento de políticas de seguridad
Descripción	Implementación de herramientas que permitan verificar el cumplimiento de las políticas de seguridad establecidas por el Banco (v. gr. agentes colectores de información), y monitorear las posibles alertas que se generen de las mismas.
Plazos de consecución	Este proceso se debe ejecutar con una periodicidad no mayor a un año y se debe empezar a ejecutar en el mediano plazo (Menos de 1 año)
Puntos de control	Reportes de monitoreo de cumplimiento de políticas
Análisis de impacto	Como resultado se debe obtener: • Acciones de mejoramiento a la política de seguridad y al SGSI.

5.3. Resultados

De acuerdo a las iniciativas planteadas anteriormente se indica cómo evoluciona el riesgo y el impacto de materialización de cada una de ellas, así como el nivel de cumplimiento de los diferentes dominios de la norma ISO/IEC 27002. A continuación se indica de forma gráfica en un diagrama de radar la evolución de los diferentes dominios y su cumplimiento antes y después de la realización de los diferentes proyectos.


Nivel de cumplimiento
Politica de seguridad
Organización de la seguridad de la información
Gestión de activos
Seguridad recursos humanos
Seguridad física
Gestión de comunicaciones y operaciones
Control de acceso
Sistemas de información
Gestión de incidentes
Continuidad de negocio
Cumplimiento
100%
98%
96%
94%
92%
90%
88%
86%
84%
Valor Obtenido
Valor Deseado

6. AUDITORÍA DE CUMPLIMIENTO

6.1. Introducción

En la evaluación realizada se observó que la Seguridad de la Información hace parte de la cultura organizacional del Banco ABC, pues se evidencia la adopción de prácticas líderes, tales como ISO/IEC 27001-2, BS 259995, ITIL V36, CobiT7 y PCI DSS8 (en curso), entre otras, así como el compromiso de la alta dirección con la seguridad de la información, a través del Comité de Seguridad de la Información, tanto a nivel de la entidad, como a nivel corporativo.

La estructura de gobierno de la función de Seguridad de la Información, se encuentra liderada por el Director de Seguridad de la Información, y cuenta con roles de Oficial de Seguridad de la Información –CISO"9. Actualmente, la Dirección de Seguridad de la Información hace parte de la Contraloría, la cual a su vez reporta a Presidencia. El seguimiento y reporte de la función de Seguridad de la Información, lo realiza el Comité de Seguridad de la Información.

Con respecto a la existencia de los controles evaluados, observamos iniciativas de implementación y documentación sobre el 95% de los mismos, con oportunidades de mejora que se presentan a lo largo de todo el documento.

En cuanto al diagnóstico realizado sobre los controles descritos en la norma ISO/IEC 27001:2005 (ISO 27002), éste muestra que en el Banco ABC, los dominios en los que se identificaron oportunidades de mejora importantes son:

- Gestión de Activos de Información
- Control de acceso
- Adquisición, desarrollo y mantenimiento
- Gestión de Incidentes de la Seguridad de la Información

Por otra parte, se identificaron oportunidades de mejora en los siguientes dominios:

- Gestión de comunicaciones y operaciones

Por último, los dominios de seguridad de la información que presentan un mayor desarrollo son:

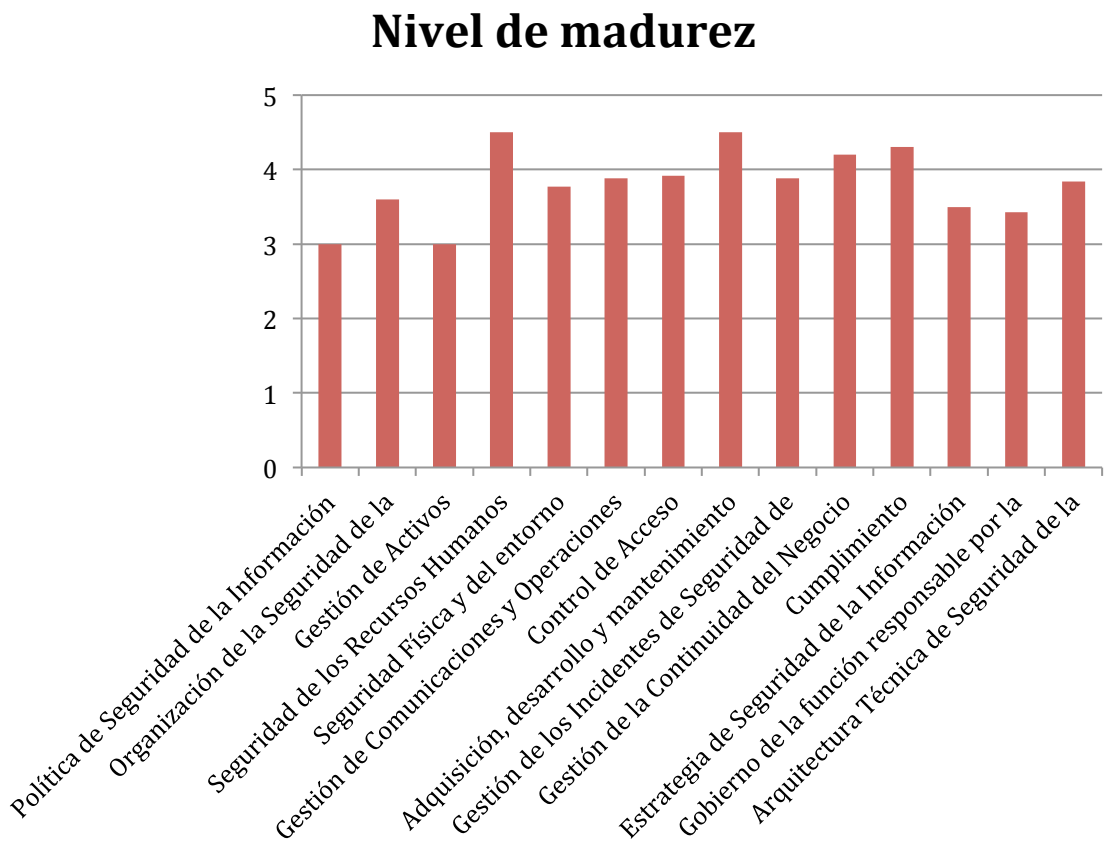
- Política de seguridad de la información
- Organización de seguridad de la información
- Seguridad del recurso humano
- Seguridad física y del entorno
- Gestión de la continuidad del negocio

Con respecto a los controles de los 11 dominios, el nivel de madurez promedio de los controles se encuentra en *Definido.*

6.2. Evaluación de la madurez

Para establecer el nivel de madurez de la seguridad de la información en el Banco ABC nos apoyamos en la escala definida por el CMMI, la cual presentamos de manera general a continuación. Los resultados detallados de la auditoría se reflejan en el documento el ANEXO 8 – Formato SGSI Auditoría.

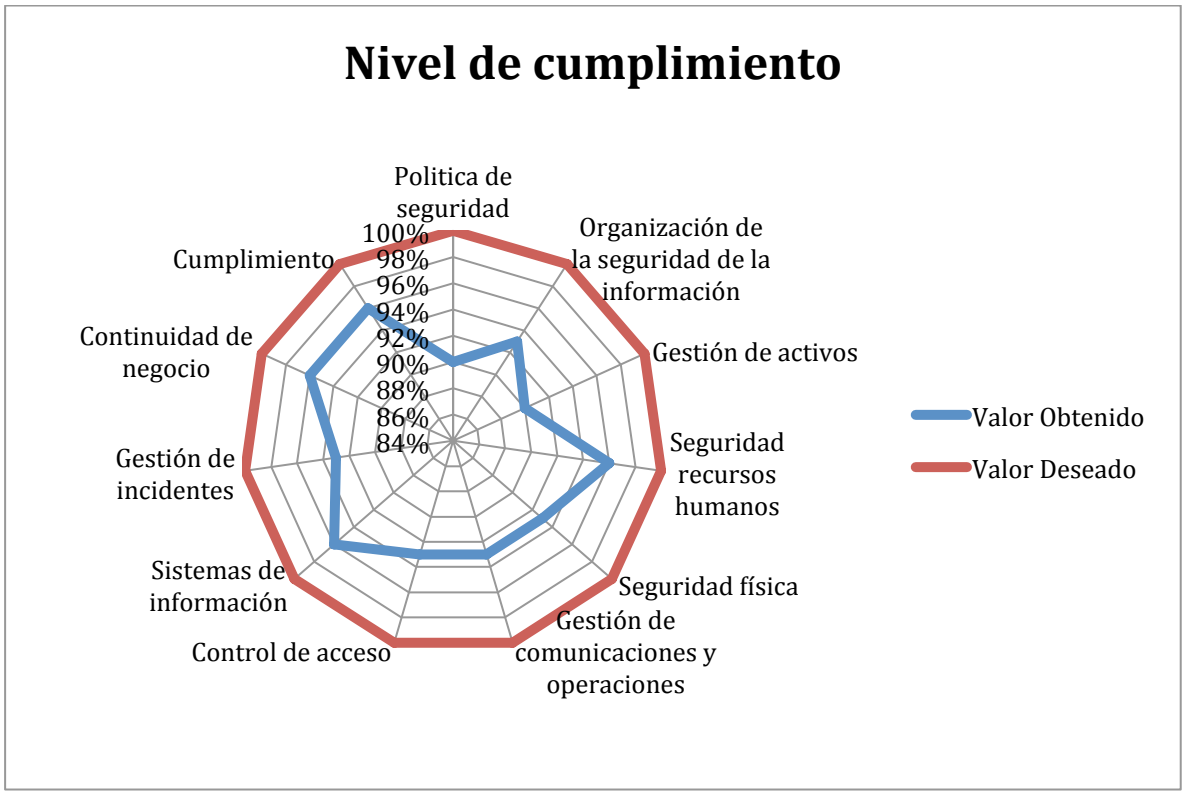
Estos resultados se pueden apreciar en la siguiente figura:



6.3. Resultados

La evaluación del Modelo de Seguridad de la Información del Banco ABC se realizó considerando el estado de desarrollo actual del mismo, frente el estándar ISO/IEC 27001:2005 (ISO 27002). Para determinar el nivel de madurez de los 11 dominios, se evaluó el diseño de cada uno de los controles propuestos, teniendo en cuenta atributos tales como; documentación, formalización, divulgación, asignación, indicadores, monitoreo, entre otros.

A continuación se presenta el resultado y el nivel de cumplimiento del Banco ABC.


Nivel de cumplimiento
Politica de seguridad
Organización de la seguridad de la información
Gestión de activos
Seguridad recursos humanos
Seguridad física
Gestión de comunicaciones y operaciones
Control de acceso
Sistemas de información
Gestión de incidentes
Continuidad de negocio
Cumplimiento
100%
98%
96%
94%
92%
90%
88%
86%
84%
Valor Obtenido
Valor Deseado

7. Conclusiones

En lo que respecta a la seguridad de la información, uno de los aspectos más importantes es comprender que esta debe ser gestionada, especialmente cuando se trata de proteger redes corporativas. Sobre este aspecto, aprovechamos la oportunidad para compartir con ustedes un concepto muy importante: Sistema de Gestión de la Seguridad de la Información (SGSI).

Por lo general es posible disminuir el impacto de los riesgos potenciales sin necesidad de grandes cambios, pero a la vez es necesaria la planificación e implantación de ciertos controles basados en un cuidadoso análisis de riesgo. Un SGSI ayuda a mantener este riesgo por debajo del nivel aceptable que se haya determinado a nivel directivo.

En conclusión, un SGSI debe ser considerado a la hora de administrar la seguridad en una organización, en especial cuando la estructura cuenta con un alto nivel de complejidad, para conseguir así una mayor eficiencia y garantía en la protección de sus activos de información.

Referencias Bibliográficas

[1].ISO/IEC27001 – Especificaciones para los sistemas de gestión de la seguridad de la información (SGSI).

[2].ISO/IEC27002 – Código de buenas prácticas para la gestión de la seguridad de la información.

[3].ISOGuide72 – Guía para la justificación y desarrollo de sistemas de gestión.

[4].Instituto Argentino de Normalización, "Código de práctica para la administración de la seguridad de la información", IRAM-ISO IEC 17799, Buenos Aires, febrero 2002.

ANEXO 1 – Resultado Análisis Diferencial

Resumen Ejecutivo

En la evaluación se observó que la Seguridad de la Información hace parte de la cultura organizacional del Banco ABC, pues se evidencia la adopción de prácticas líderes, tales como; ISO/IEC 27001-2 y CobiT[4], entre otras, así como el compromiso de la alta dirección con la seguridad de la información, a través del Comité de Seguridad de la Información.

En cuanto a la estructura de gobierno de la función de Seguridad de la Información, existe un Líder de Seguridad de la Información, el cual reporta directamente a la Contraloría.

Existe una política de seguridad de la información formalizada, en la cual se definen las políticas y normas a cumplir. Esta política se encuentra aprobada por las directivas de la entidad, y está publicada para su consulta por parte del personal del Banco.

Con respecto a la existencia de los controles evaluados, observamos iniciativas de implementación y documentación sobre el 99% de los mismos, con oportunidades de mejora que se presentan a lo largo de todo el documento.

En cuanto al diagnóstico realizado sobre los controles descritos en la norma ISO/IEC 27001:2005 (ISO 27002) y en el Marco de Referencia de Seguridad de la Información de Consultores XYZ, éste muestra que en el Banco ABC, los dominios en los que se identificaron oportunidades de mejora son:

- Política de seguridad de la información
- Gestión de activos
- Gobierno de seguridad de la información

Por otra parte, los dominios de seguridad de la información que presentan un mayor desarrollo son:

- Organización de la seguridad de la información
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de acceso

[4] Es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA) y el Instituto de Administración de las Tecnologías de la Información (ITGI) en 1992

- Adquisición, desarrollo y mantenimiento de sistemas de información
- Gestión de los incidentes de la seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento
- Estrategia de Seguridad de la información
- Arquitectura de seguridad de la información

Con respecto a los controles de los 14 dominios, el nivel de madurez promedio de los controles se encuentra en **Definido.**

Resultados

La evaluación del Modelo de Seguridad de la Información del Banco ABC se realizó considerando el estado de desarrollo actual del mismo, frente el estándar ISO/IEC 27001:2005 (ISO 27002), y en el Marco de Referencia de Seguridad de la Información de Consultores XYZ. Para determinar el nivel de madurez de los 14 dominios, se evaluó el diseño de cada uno de los controles propuestos, teniendo en cuenta atributos tales como; documentación, formalización, divulgación, asignación, indicadores, monitoreo, entre otros.

Los controles evaluados están enmarcados en los siguientes dominios:

- **Política de seguridad de la información**. Considera las políticas, normas y procedimientos relacionados con la posición de la entidad en cuanto a seguridad de la información.

- **Organización de la seguridad de la información.** Contempla aspectos como la estructura organizacional, la asignación de responsabilidades y consideraciones de los riesgos relacionados con partes externas.

- **Gestión de activos de información.** Hace referencia al inventario, clasificación y uso aceptable de los activos de información.

- **Gestión de los Recursos Humanos.** Incluye el proceso de selección, los términos y condiciones laborales (manuales de funciones y responsabilidades de los empleados y usuarios), la educación y formación en seguridad, el proceso disciplinario (leyes, resoluciones, reglamentos, etc.) y la terminación de la relación laboral.

- **Seguridad física.** Hace referencia al acceso físico, la seguridad de las oficinas, la protección contra amenazas ambientales y disturbios de orden público, la seguridad y mantenimiento de los equipos y del cableado, el servicio de suministro y la reutilización y destrucción de equipos.

- **Gestión de comunicaciones y operaciones.** Contempla los procedimientos operacionales (gestión del cambio, documentación, copias de respaldo, planificación y criterios de aceptación de los sistemas, manejo de los medios de almacenamiento removibles, etc.), la prestación del servicio por terceras partes, la seguridad en redes y el seguimiento (monitoreo) de los sistemas de información y la seguridad en el intercambio de información.

- **Control de acceso.** Incluye aspectos como la gestión de usuarios (registro, privilegios, contraseñas), las responsabilidades de los usuarios (uso de contraseñas) y la computación móvil y el trabajo remoto.

- **Adquisición, desarrollo y mantenimiento de sistemas.** Hace referencia a los requisitos de seguridad y validación del sistema (datos de entrada y salida, procesamiento, integridad), cifrado, protección de los datos de prueba y del código fuente, en los procesos de adquisición y desarrollo de sistemas de información.

- **Gestión de incidentes de seguridad de la información.** Concierne lo referente a los incidentes de seguridad de la información, como la identificación, las responsabilidades y procedimientos y el manejo de evidencia, entre otros.

- **Gestión de la continuidad del negocio.** Relacionado con los aspectos de seguridad de la información en los planes de continuidad, contingencia y de recuperación de desastres.

- **Cumplimiento.** Contempla la revisión del cumplimiento de la normatividad interna y los requisitos legales aplicables (legislación aplicable, derechos de propiedad intelectual, etc.).

- **Estrategia de Seguridad de la Información.** Hace referencia a la manera en que la entidad alinea las iniciativas de seguridad de la información con respecto al cumplimiento de sus objetivos.

- **Gobierno de la función responsable por la Seguridad de la Información.** Contempla las prácticas que se deben tener en cuenta para la alineación estratégica, gestión de los riesgos, entrega de valor de las inversiones en seguridad, gestión de los recursos, medición del desempeño e integración de actividades de seguridad.

- **Arquitectura de seguridad de la información.** Hace referencia a la manera en que la entidad protege su infraestructura tecnológica a través de la implementación de controles de seguridad.

Cubrimiento de controles

Con respecto a la existencia de los controles evaluados, observamos iniciativas de documentación e implementación sobre el 61% de los mismos (134 controles), con oportunidades de mejora que se presentan a lo largo del documento.

A continuación se presenta la gráfica de cubrimiento de controles:

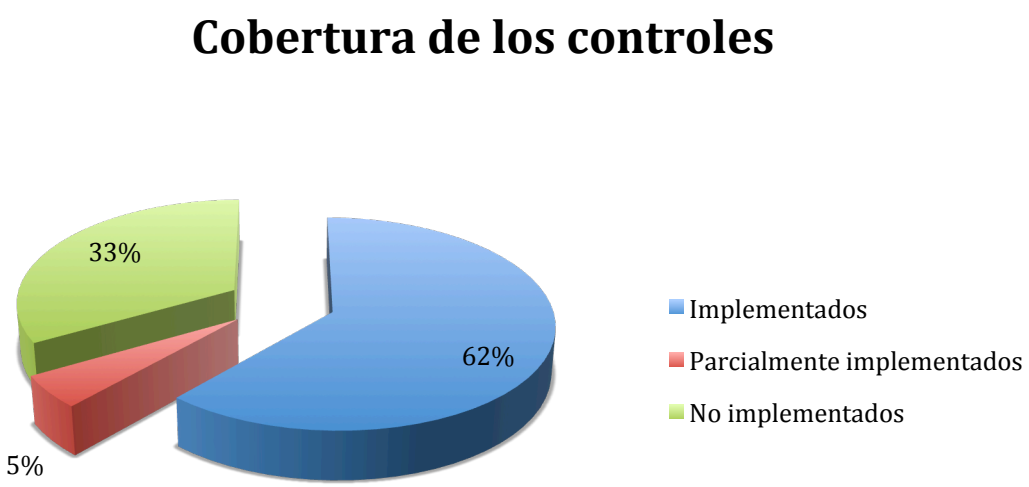


Ilustración 1. Cobertura de los Controles

Nivel de madurez

Para establecer el nivel de madurez de la seguridad de la información en el Banco ABC se utilizó en la escala definida por el CMMI, la cual se presenta a continuación de manera general:

En cuanto a los resultados generales del diagnóstico realizado sobre los controles descritos en la norma ISO 27002 (Anexo A de ISO/IEC 27001:2005)[5], — éste muestra que en el Banco ABC, los dominios en los que se identificaron oportunidades de mejora son:

- Política de seguridad de la información
- Gestión de activos
- Gobierno de seguridad de la información

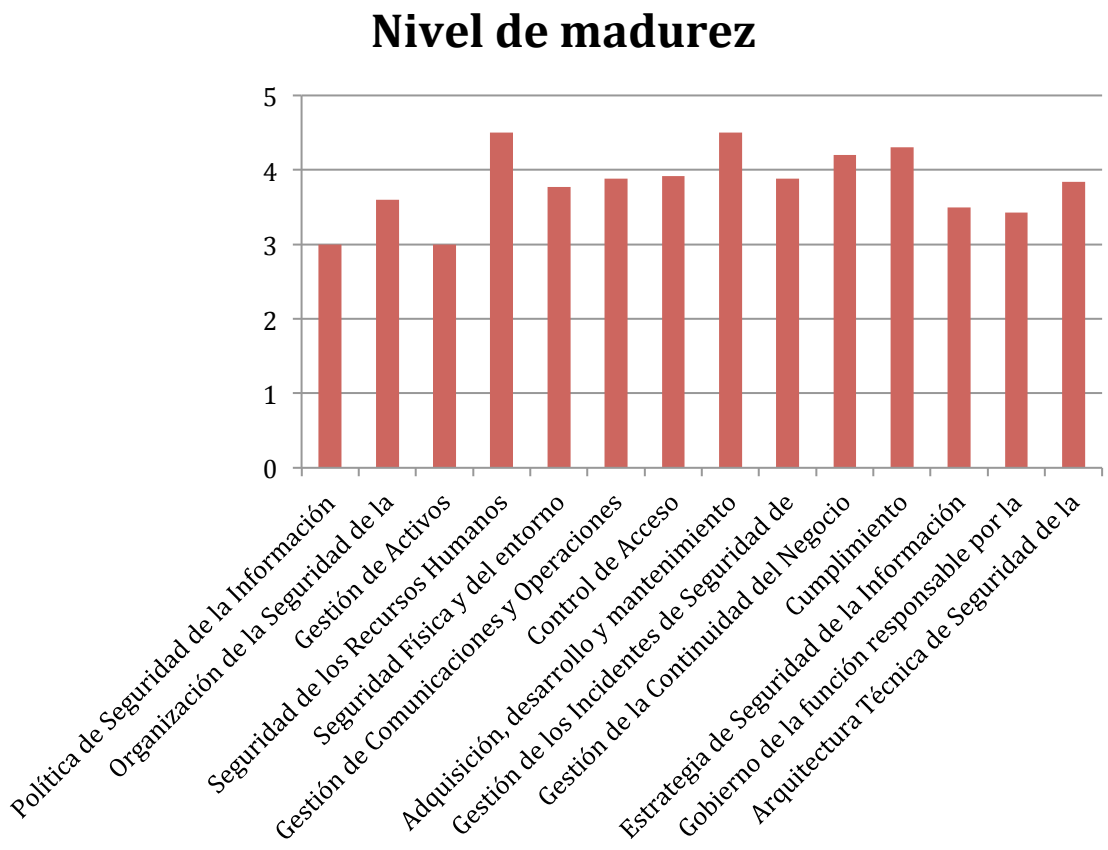
Así mismo, los dominios de seguridad de la información que presentan un mayor desarrollo son:

- Organización de la seguridad de la información

[5] Estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International Organization for Standardization y por la Comisión Electrotécnica Internacional en el año 2000, con el título de Information technology - Security techniques - Code of practice for information security management.

- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Gestión de los incidentes de la seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento
- Estrategia de Seguridad de la información
- Arquitectura de seguridad de la información

Estos resultados se pueden apreciar en la siguiente figura:



En términos generales, los controles establecidos en la norma ISO/IEC 27001:2005 (ISO 27002) y en el Marco de Referencia de Consultores XYZ — aplicados en Banco ABC —, se encuentran en un nivel de madurez **Definido**.

Resultados por dominio

A continuación se describen los resultados obtenidos por cada uno de los dominios evaluados, así como las oportunidades de mejora correspondientes.

Dominio 5 – Política de Seguridad de la información

Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.

Observaciones

En la evaluación se observó la existencia y adopción de un documento de Política de Seguridad de la Información, el cual se encuentra a los usuarios del Banco a través de el Manual de Calidad público de en la Intranet de la compañía. Esta política se encuentra alineada con la norma ISO IEC 27001.

Oportunidades de mejora

Formalizar los procedimientos para efectuar la revisión de la política de seguridad de la información del Banco, en el cual se establezca:

- La frecuencia de revisión (v.gr. anual o cuando se requiera, etc.)
- Los niveles jerárquicos involucrados (v.gr. Comité de seguridad de la información, etc.)
- Las posibles entradas que serán consideradas en el proceso de revisión y actualización de las políticas de seguridad de la información (v.gr. resultados de las revisiones independientes, resultados de las revisiones realizadas por la entidad, cambios en el entorno de la organización, circunstancias del negocio, aspectos contractuales, regulatorios y legales, condiciones del ambiente técnico, tendencias relacionadas con las amenazas y vulnerabilidades, incidentes de seguridad de la información, entre otros).
- Documentación soporte de la revisión.

Dominio 6 – Organización de la Seguridad de la Información

Objetivo: Gestionar la seguridad de la información dentro de la entidad y mantener la seguridad de la información y de los servicios de procesamiento a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.

Observaciones

La Gerencia de Auditoría de Riesgo Tecnológico y Seguridad de la Información participa activamente en los siguientes comités tanto a nivel interno, como a nivel corporativo:

- Comité de Auditoría de Junta Directiva
- Comité de Contralores
- Comité de Presidencia

En los cuales se presentan temas actuales de la función de seguridad de la información en el Banco, se definen las iniciativas de seguridad y se realiza seguimiento a los planes propuestos según la estrategia y las necesidades del Banco.

Actualmente, la Gerencia de Auditoría de Riesgo Tecnológico y Seguridad de la Información, cuenta con los recursos humanos adecuados y suficientes para la gestión y operación de las diferentes actividades del modelo de seguridad de la información definido e implementado. Los roles y responsabilidades de la función de seguridad de la información están definidos, documentados y asignados a los diferentes integrantes del área, y demás interesados clave del Banco (v.gr. comité de seguridad, etc.).

Por otra parte, se observó que la función de seguridad de la información participa activamente en las iniciativas y proyectos que consideran la captura y procesamiento de información del Banco.

Adicionalmente, se observó que existen acuerdos de confidencialidad con funcionarios, proveedores y clientes del Banco para determinar la responsabilidad ante situaciones que comprometan la seguridad de la información.

Por último se observó que el área de Seguridad Bancaria y Prevención de Fraudes mantiene contacto con grupos especiales, para la cual cuenta con un listado confidencial de contactos con las principales autoridades del país.

Oportunidades de mejora

Definir e implementar indicadores para medir el desempeño y cumplimiento de los controles del dominio, así como las actividades de monitoreo y gestión de los mismos. A continuación se relacionan los indicadores sugeridos son:

- Porcentaje de proyectos en los que participa seguridad de la información
- Porcentaje de la población de usuarios con acceso recursos de información con acuerdo de confidencialidad firmado (v.gr. funcionarios del Banco, terceros, etc.)

- Porcentaje de Terceros para los cuales se ha efectuado análisis de riesgos de seguridad de la información
- Porcentaje de riesgos de seguridad de la información generados por terceros que son gestionados
- Porcentaje de cumplimiento de requisitos de seguridad por parte de terceros

Dominio 7 – Gestión de Activos

Objetivo: Lograr y mantener la protección adecuada de los activos de información organizacionales y asegurar que la información recibe el nivel de control adecuado.

Observaciones

La Gestión de Activos de Información está soportada desde la Política de Seguridad de la Información, y la definición de la organización de seguridad de la información, para lo cual existe el cargo "Analista de Seguridad de la Información - Inventario de Activos".

Durante la ejecución del trabajo se observó la existencia de una metodología y procedimiento formal para la Gestión de Activos de Información del Banco, mediante el cual se clasifican los mismos con base en su confidencialidad e integridad. Así mismo, evidenciamos la existencia de un inventario de los activos de información del Banco, en el cual se encuentran identificados y relacionados los propietarios de los mismos (el inventario de activos de información se encuentra publicado en la solución SHAREPOINT).

Según la información suministrada por la función de seguridad de la información, las áreas usuarias responsable de las operaciones del Banco participan activamente en la identificación y clasificación de los activos de información.

Adicionalmente, la función de seguridad de la información ha desarrollado un manual para el uso adecuado de activos de información, en el cual se incluye las responsabilidades en cuanto a la gestión de los activos, posibles conflictos, prevenciones, prohibiciones, ética y confidencialidad. Así mismo, existen lineamientos de etiquetado y protección de los activos de información, tanto físicos y lógicos.

Oportunidades de mejora

Clasificar los activos de información, teniendo en cuenta la importancia del mismo, frente a su disponibilidad para soportar las operaciones del Banco (v.gr. Misión critica, crítica o no critica).

Dominio 8 – Seguridad de los Recursos Humanos

Objetivos:

- Asegurar que los funcionarios, contratistas y usuarios de terceras partes entienden sus responsabilidades y son adecuados para los roles para los que se considera.
- Reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.
- Asegurar que todos los funcionarios, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes y que estén equipados para apoyar la política de seguridad de la entidad en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.
- Asegurar que los funcionarios, los contratistas y los usuarios de terceras partes salen de la entidad o cambian su contrato laboral de forma ordenada.

Observaciones

En la ejecución de la evaluación se observó que en el proceso de Gestión Humana existen controles para el manejo de la seguridad del personal, desde el ingreso, en donde se siguen procedimientos para la selección de personas idóneas (v.gr. análisis de antecedentes penales, laborales, académicos y visita Domiciliaria), durante la relación laboral (capacitaciones y sensibilizaciones en temas de seguridad de la información), hasta el retiro de las mismas (v.gr. retiro de derechos de acceso, entrega formal de activos tecnológicos, procesos disciplinarios, etc.).

Las responsabilidades relacionadas con la seguridad de la información son incluidas en el contrato laboral, lo cual se constituye como una condición para la aceptación de los cargos.

El Banco cuenta con programas de sensibilización en seguridad de la información para sus funcionarios, el cual desarrolla a través de campañas, que incluyen la inducción de los nuevos empleados y la plataforma e-Learning. Así mismo, hace seguimiento y evaluación de la ejecución y efectividad de los programas verificando que los empleados hayan atendido a los cursos y las actualizaciones de los mismos.

El Banco cuenta con proceso disciplinario para la aplicación de sanciones relacionadas con incumplimiento de las políticas de seguridad de la información.

Oportunidades de mejora

Solicitar a las empresas contratistas de servicios generales (v.gr. Servicios de Aseo, Cafetería, etc.) la verificación de antecedentes de los funcionarios dispuestos para el Banco, considerando los aspectos revisados actualmente por la entidad.

Dominio 9 – Seguridad Física y del Entorno

Objetivos:

- Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la Banco.
- Evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la Banco

Observaciones

Se observó la existencia de controles de acceso físico para las distintas instalaciones de la entidad (v.gr. Sedes administrativas, sucursales etc.), en especial para las áreas criticas y de procesamiento de información (v.gr. Centros de cómputos, cuartos de cableado, etc.), tales como; autenticación por huella, CCTV, máquina de rayos "X", recepcionistas, vigilantes, etc. Las áreas seguras del Banco están claramente identificadas y cuentan con controles de acceso físico para la protección de los activos que se resguardan en éstas (v.gr. Centros de cómputo, garantía de tenencias, etc.).

El Banco cuenta con un proceso definido de retiro de activos informáticos de las instalaciones.

El centro de cómputo cuenta con controles, tanto de acceso, como de seguridad ambiental, tales como; acceso biométrico, CCTV, sistemas de detección y extinción de incendios, aire acondicionado, UPS, etc. Actualmente, se cuenta con planes de mantenimiento periódico sobre los equipos, tales como UPS, sistemas de aire acondicionado, servidores, etc. Se cuentan con planes de evacuación, controles ante inundaciones, terremoto y malestar civil (vandalismo y asonada). En general, se evidencia la existencia de controles apropiados para la protección de los activos de información.

Oportunidades de mejora

Fortalecer campañas de divulgación a los colaboradores del Banco para no permitir el ingreso a personas no autorizadas a áreas seguras del mismo.

- Una vez finalicen las obras de adecuación del Datacenter es necesario realizar un mantenimiento preventivo a los equipos de apoyo y actualización de la documentación.
- Implementar auditorias para verificar el cumplimiento de normatividad de instalación de cableado estructurado.
- Definir e implementar indicadores para medir el desempeño y cumplimiento de los controles del dominio, así como las actividades de monitoreo y gestión de los mismos:

    - Porcentaje de áreas críticas aseguradas
    - Porcentaje de incidentes de seguridad de la información generados por acceso física no autorizado

Dominio 10 – Gestión de Comunicaciones y Operaciones

Objetivos:

- Asegurar la operación correcta y segura de los servicios de procesamiento de información.
- Implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes
- Minimizar el riesgo de fallas en los sistemas
- Proteger la integridad del software y de la información.
- Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.
- Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.
- Evitar la divulgación, modificación, retiro o destrucción de activos no autorizada y la interrupción en las actividades de negocio.
- Mantener la seguridad de la información y del software que se intercambian dentro de la entidad y con cualquier entidad externa.
- Garantizar la seguridad de los servicios de comercio electrónico y su utilización segura.
- Detectar actividades de procesamiento de información no autorizadas.

Observaciones

En general se observaron procedimientos para la operación segura de la infraestructura de procesamiento de información de la entidad. Los procedimientos técnicos de operación y manuales de administración se encuentran documentados, aprobados y divulgados.

Se cuenta con un proceso formal de Gestión de Cambios a nivel de equipos de redes, sistemas operativos y bases de datos el cual está en proceso de automatización en la herramienta ClearQuest de IBM. En el marco del proceso de Gestión de Cambios se determinan los criterios para la aceptación de los sistemas que ingresan al ambiente de producción, entre los cuales se incluyen requisitos de seguridad de la información, entre otros.

A nivel de servidores se implementó la separación de los ambientes de desarrollo, pruebas y producción, lo que reduce el riesgo de acceso y de modificaciones no autorizadas sobre la información de cada ambiente.

El Banco tiene definido los acuerdos de niveles de servicio (ANS) en los contratos de TI con terceros (v.gr. Telmex, IBM, etc.), y monitorea periódicamente su cumplimiento.

Se implementó la herramienta Symantec EndPoint como solución integral para el control de código malicioso (v.gr. virus, gusanos, spyware, etc.) y restricción de acceso a puertos y servicios, la cual es gestionada y monitoreada para garantizar la seguridad de los equipos y la información.

La entidad cuenta con herramientas automáticas y procedimientos formales para el respaldo de la información almacenada y administrada en las diferentes plataformas (v.gr. As400, OS390, Open, etc.), los cuales incluyen: bitácora de respaldos, notificaciones y alertas por respaldos exitosos y/o fallidos, cintotéca interna, contrato de custodia externa de medios con un proveedor confiable, prueba de medios, entre otros.

La arquitectura técnica de seguridad se encuentra claramente documentada y estructurada por audiencia (v.gr. clientes, terceros, empleados, etc.), e incluye los mecanismos de seguridad y control para el intercambio de información entre los recursos del Banco, teniendo en cuenta su valor. Entre dichos controles se encuentran los siguientes: firewalls, IDS/IPS, VPN, NAC, certificados y firmas digitales, tokens, entre otros.
Las características de registros de auditorías se han definido en la política de log para las distintas plataformas y servicios de tecnología existentes en la infraestructura de la entidad (v.gr. sistemas operativos, dispositivos de red, dispositivos criptográficos, etc.).

Se cuenta con una solución integral para el monitoreo constante de los recursos informáticos, desde la cual se reportan y gestionan las fallas, a nivel de hardware y datos.

Oportunidades de mejora

- Continuar con la implementación de la solución IBM InfoSphere Guardium para controlar y monitorear las actividades realizadas por los administradores de las bases de datos.
- Establecer un plan formal para el monitoreo periódico de las actividades realizadas por los administradores de la infraestructura, sobre las diferentes plataformas de TI que soportan las operaciones del negocio.
- Verificar que los dispositivos de control y seguridad de las redes (v.gr. Firewall, IPS y DLP, entre otros,) se encuentren sincronizados con el servidor NTP.
- Definir mecanismos de control para restringir que los administradores de plataforma almacenen contraseñas de acceso a las mismas en archivos de Excel. Durante nuestra revisión observamos que en la intranet de seguridad de la información existe un archivo denominado "A-vpns%20abc(1).xls", el cual contiene las contraseñas de las VPNs Site to Site del Banco.
- Definir e implementar un proceso de gestión de capacidad de la plataforma de TI que soporta las operaciones del Banco, el cual permita estimar capacidad requerida de la misma para garantizar el normal desarrollo de las operaciones del negocio (disponibilidad y eficiencia).
- Definir e implementar un proceso para la realización de pruebas al software libre que se autoriza a instalar en las estaciones de trabajo de los usuarios, para mitigar posibles riesgos de seguridad (v.gr. código malicioso).
- Definir e implementar indicadores para medir el desempeño y cumplimiento de los controles del dominio, así como las actividades de monitoreo y gestión de los mismos:

    - Porcentaje de SLA cumplidos
    - Porcentaje de OLA cumplidos
    - Porcentaje de servicios que se acercan a los umbrales
    - Porcentaje de recursos de procesamiento de información con esquemas de respaldo
    - Porcentaje de recursos de procesamiento de información que son monitoreados
    - Porcentaje de incidentes de seguridad de la información generados por tareas de administración / operación no autorizadas

Dominio 11 – Control de Acceso

Objetivos:

- Controlar el acceso a la información.

- Asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.
- Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.
- Evitar el acceso no autorizado a servicios en red.
- Evitar el acceso no autorizado a los sistemas operativos.
- Evitar el acceso no autorizado a la información contenida en los sistemas de información.
- Garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.

Observaciones

En la ejecución de la evaluación se observó que el Banco cuenta con políticas y procedimientos para el control de acceso de los usuarios a los recursos de información, las cuales se encuentran alineadas con el Estándar ISO/IEC 27001:2005.

Por otra parte, observamos que el Banco cuenta con un procedimiento para la creación, modificación y eliminación de matrices de roles por cada cargo del Banco. Adicionalmente, evidenciamos que se realiza un análisis de riesgos, para los eventos en los que se requiere otorgar / asignar privilegios de acceso sobre los recursos de información del negocio.

Se cuenta con un procedimiento para monitorear y validar periódicamente (cada 3 meses) en la herramienta IDM de Novell, que los privilegios definidos en las matrices de roles de los usuarios correspondan a las funciones que los mismo desempeñan en el negocio.

Las contraseñas y privilegios de acceso son gestionados a través de la herramienta IDM de Novell, lo cual permite una administración centralizada de las diferentes plataformas de TI que soportan las operaciones del negocio (v.gr. servidores y sistemas de información, etc.).

El Banco ha establecido e implementado un procedimiento de catalogación de software para la gestión del mismo en las estaciones de trabajo y servidores.

Actualmente se cuenta con soluciones especializadas para la gestión del acceso a las redes (v.gr. firewalls, VPN, Network Access Control –NAC, entre otros.), lo cual incrementa y fortalece el nivel de seguridad de los equipos que conectados en los diferentes segmentos de red de la entidad. Así mismo, observamos que se utilizan servicios de comunicación y conexión seguros tanto a nivel de redes como servidores (v.gr. ssh, https, acls, etc.).

Oportunidades de mejora

- Formalizar el proceso de revisión y detección de riesgos en la asignación de privilegios de acceso a los usuarios de procesos sensibles del Banco (v.gr. usuarios que evalúan y aprueban una línea de crédito fuera de su rango de aprobación, etc.).
- Continuar con el proyecto de separación de redes en las áreas del banco (Proyecto Zonas Seguras), según la clasificación de la información que transmite a través de la misma.
- Formalizar el proceso de revisión y detección de usuarios retirados con permisos activos. Así mismo, sugerimos fortalecer el proceso de eliminación de privilegios de acceso de los usuarios que se retiran del Banco, para lo cual se debe trabajar conjuntamente con el área de Recursos Humanos y las áreas de negocio, de manera tal que notifique oportunamente el retiro de funcionarios y terceros, y se eliminen los accesos privilegios de acceso actuales (v.gr. bloqueo o eliminación de las cuentas de acceso). En caso que por necesidades operativas sea requerido mantener por un tiempo la cuenta activa, se debe asignar de manera formal un responsable a cargo de la misma.
- Adicionalmente, sugerimos establecer un procedimiento para la validación periódica de la última fecha de ingreso de las cuentas de acceso asignadas al personal retirado de la compañía, y en caso que ésta sea posterior a la fecha en que debieron ser retiradas de los sistemas de información, determinar si se registraron transacciones no autorizadas en los mismos. Los resultados y las excepciones presentadas en estas revisiones deben ser formalmente documentados y analizados para determinar situaciones anómalas.
- Evaluar la posibilidad para establecer horarios de trabajo autorizados para el acceso a los servidores críticos del Banco.
- Formalizar las plantillas de configuración segura para switch y router, el proceso de asignación de privilegios de acceso sobre los equipos de red.
- Definir e implementar indicadores para medir el desempeño y cumplimiento de los controles del dominio, así como las actividades de monitoreo y gestión de los mismos:

    - Porcentaje de usuarios con asignación errada de privilegios
    - Porcentaje de utilidades de procesamiento de información con esquema de autenticación y gestión de contraseñas

Dominio 12 – Adquisición, Desarrollo y Mantenimiento de Sistemas de información

Objetivos:

- Garantizar que la seguridad es parte integral de los sistemas de información.

- Evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.
- Proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos.
- Garantizar la seguridad de los archivos del sistema.
- Mantener la seguridad del software y la información del sistema de aplicaciones.
- Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

Observaciones

En el desarrollo de la evaluación se observó que la función de Seguridad de la Información participa activamente en los diferentes proyectos de desarrollo e implementación de soluciones relevantes y con alto impacto las operaciones del Banco.

Adicionalmente, se han definido políticas de desarrollo seguro, arquitectura y estándares de seguridad a tener en cuenta en el desarrollo de aplicaciones. Lo anterior facilita la consideración de requerimientos de seguridad de la información en el desarrollo e implementación de aplicaciones, y permite incrementar el nivel de seguridad de las mismas antes de su puesta en producción.

El proceso de desarrollo se software definido e implementado en el Banco se automatizó través de la Herramienta Clear Quest, optimizando el mismo y llevando una trazabilidad de las diferentes actividades realizadas por los interesados clave que participan en éste.

El Banco cuenta con ambientes de desarrollo, pruebas y producción separados para las diferentes aplicaciones que soportan las operaciones de negocio, lo cual reduce el riesgo de acceso y modificaciones no autorizadas sobre la información de cada ambiente.

Los sistemas de información incluyen controles y mecanismo de seguridad para proteger la información administrada por éstas, tales como: certificados y firmas digitales, protocolos seguros (v.gr. HTTPS , RSA-SHA1 , SSL, etc.), entre otros.

El Banco implementó la herramienta DSS WebSense para la protección, detección y generación de alertas ante situaciones de fuga de información.
Por último, observamos que la seguridad de los sistemas de información se revisa periódicamente a través de pruebas de análisis de vulnerabilidades contratadas por el Banco.

Oportunidades de mejora

Definir e implementar un proceso para la realización de pruebas al software libre que se autoriza a instalar en las estaciones de trabajo de los usuarios, para mitigar posibles riesgos de seguridad (v.gr. código malicioso).

Dominio 13 – Gestión de los Incidentes de Seguridad de la Información

Objetivos:

- Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.
- Asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

Observaciones

El Banco ha definido un proceso formal para la gestión de incidentes de seguridad de la información, tanto internos como externos, los cuales dependiendo de su origen pueden ser reportados a la Central Única de Reclamo (externos), o Help Desk (internos). Estos eventos se replican y centralizan en la herramienta HP Service Manager, en la cual se priorizan y se da solución. Adicionalmente, el Banco ha creado tipificaciones formales para la atención de incidentes.

Como parte de la centralización y atención de los incidentes de seguridad de la información, se ha definido un procedimiento que indica los roles de cada actor del proceso. Esto considera la participación de especialistas encargado de su solución (en caso de ser necesario).

A partir de la información de incidentes de seguridad de la información, se generan reportes periódicos cuantificados con la cantidad de incidentes atendidos y pendientes.

Por otra parte, observamos que el área de seguridad de la información realiza escaneo de vulnerabilidades trimestralmente y a demanda sobre los equipos del Banco, a través de la herramienta SiteProtector, con el fin de identificar debilidades de seguridad en los sistemas de información recursos de TI que soportan las operaciones del negocio.

El Banco cuenta con un repositorio (base de datos de conocimiento) para la publicación de los resultados, los cuales son considerados en caso ocurran incidentes similares.

Oportunidades de mejora

- Definir e implementar indicadores de desempeño (KPI) para medir el desempeño en relación a la cantidad de incidentes de seguridad ocurridos, atendidos y la efectividad de la respuesta.
- Continuar con la implementación del sistema SIEM para correlacionar los eventos y facilitar el registro y atención de posibles incidentes de seguridad.

Dominio 14 – Gestión de la Continuidad del Negocio

Objetivo: Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y asegurar su recuperación oportuna.

Observaciones

El proceso para la Gestión de la Continuidad del Negocio (BCP) y Recuperación de Desastres (DRP) se encuentra definido y alineado con prácticas líderes, tales como BS 25999 y DRII (Disaster Recovery Institute International).

El Banco cuenta actualmente con un plan de continuidad de negocio que se fundamenta en un Análisis de Impacto al Negocio (BIA) y la definición de tiempos objetivos de recuperación (RTO), que permiten identificar los posibles impactos sobre los activos críticos y establecer las prioridades de las actividades a ejecutar ante un evento que comprometa el normal desarrollo de las operaciones del negocio (v.gr. estrategias de recuperación, etc.).

Actualmente la entidad cuenta con estrategias de continuidad documentadas, formalizadas y divulgadas en la intranet del Banco, las cuales se incluyen en las pruebas generales que se realizan periódicamente sobre el plan de continuidad del negocio.

Existen recursos tecnológicos (v.gr. replicación en línea) para garantizar la disponibilidad y continuidad de las operaciones críticas, los cuales se han implementado para dar cumplimiento a los Tiempos Objetivos de Recuperación (RTO). El centro de cómputo alterno cuenta controles adecuados de seguridad físico (TIAR 3).

Los planes de continuidad del negocio se prueban regularmente para validar su operatividad y eficacia.

Por otra parte, se observó que se realiza capacitación y transferencia de conocimiento al personal clave que participa en el proceso, sobre las actividades de Gestión de la Continuidad del Negocio.

Oportunidades de mejora

Durante el desarrollo del trabajo no se identificaron oportunidades de mejora relevantes que llamaran nuestra atención, en relación con los controles asociados a este dominio.

Dominio 15 – Cumplimiento

Objetivos:

- Evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.
- Asegurar que los sistemas cumplen con las normas y políticas de seguridad de la entidad.
- Maximizar la eficacia de los procesos de auditoría de los sistemas de información y maximizar su interferencia

Observaciones

El modelo de seguridad de la información definido e implementado por el Banco ABC, considera el cumplimiento con normas, estándares y regulaciones, tales como ISO/IEC 27001:2005, CobiT, PCI DSS, Circulares 052 y 038 de la Superintendencia Financiera de Colombia, entre otras.

El Modelo de Seguridad de la Información es revisado de forma periódica e independiente, ya sea por la función de auditoría interna o por un tercero especializado, lo cual permite a la entidad contar con retroalimentación sobre la efectividad del mismo.

El área Jurídica revisa periódicamente la normatividad que impacta cualquier área del Banco, para lo cual monitorea las páginas de los entes reguladores (v.gr. Superintendencia Financiera de Colombia, Banco de la República, Ministerios, página Notinet, etc.). Tan pronto se identifican novedades normativas o regulatorias relacionadas con seguridad de la información, se notifica a la Gerencia de Auditoría de Riesgo Tecnológico y Seguridad de la Información, para que ésta la revise y defina las acciones a seguir para darle cumplimiento a la misma.

En el Banco existen políticas y procedimientos relacionados con los Derechos de Propiedad Intelectual (DPI), los cuales son monitoreados de forma automática, a través de herramientas informáticas.

Oportunidades de mejora

Durante el desarrollo del trabajo no se identificaron oportunidades de mejora relevantes que llamaran nuestra atención, en relación con los controles asociados a este dominio.

Dominio – Estrategia de Seguridad de la Información

Objetivos:

- Desarrollar una estrategia de seguridad de la información que esté alineada con las metas y objetivos del negocio.
- Alinear la estrategia de seguridad de la información con el gobierno corporativo.

Observaciones

El Banco cuenta con una estrategia de seguridad de la información formalizada y divulgada a las áreas interesadas, la cual contiene los aspectos necesarios para guiar la función de esta área dentro del Banco.

La estrategia de seguridad de la información incluye aspectos de la entrega de valor, los cuales se monitorean por cada uno de los proyectos e iniciativas del área. Esta revisión es efectuada periódicamente por la Contraloría y el Comité de Presidencia.

Los objetivos de la Alta Dirección son considerados para estrategia de seguridad de la información anualmente.

Oportunidades de mejora

Durante el desarrollo de nuestro trabajo no identificamos oportunidades de mejora relevantes que llamaran nuestra atención, en relación con los controles asociados a este dominio.

Dominio – Gobierno de la Función Responsable por la Seguridad de la Información

Objetivos:

- Alinear la seguridad de la información con la estrategia de negocio para apoyar los objetivos organizacionales.
- Ejecutar medidas apropiadas para mitigar los riesgos y reducir el posible impacto que tendrían en los recursos de información a un nivel aceptable.
- Optimizar las inversiones en la seguridad en apoyo a los objetivos del negocio.
- Utilizar el conocimiento y la infraestructura de seguridad de la información con eficiencia y eficacia.
- Monitorear y reportar procesos de seguridad de la información para garantizar que se alcancen los objetivos.
- Integrar todos los factores de aseguramiento relevantes para garantizar que los procesos operan de acuerdo con lo planeado de principio a fin.

Observaciones

Como parte de la gestión operativa del área, el Gerente de Auditoría de Riesgo Tecnológico y Seguridad de la Información realiza un seguimiento a las actividades realizadas, y reporta cualquier necesidad del incremento de la capacidad de Seguridad de la Información para el desarrollo de sus responsabilidades.

El Banco cuenta con una metodología para la administración de riesgos (SARO), la cual se aplica en para los riesgos de seguridad de la información, y dentro de la cual se considera la generación de planes de acción de los riesgos calificados como altos y extremos.

Se cuenta con procesos formales de auditoría para la identificación de brechas de seguridad e incumplimientos de las políticas establecidas, lo cual es reportado a las áreas correspondientes para su corrección.

Oportunidades de mejora

Las prácticas líderes establecen que la función de seguridad de la información debe ser independiente de la función de auditoría (Nivel de dependencia).

Dominio 6 – Arquitectura de la Seguridad de la Información

Objetivo: Desarrollar arquitecturas de seguridad para definir y utilizar los recursos de la infraestructura de manera eficiente.

Observaciones

La arquitectura técnica de seguridad de la información del Banco cuenta con controles para proteger los activos de información.

Existe un Comité Adjunto de Seguridad de la Información, en el cual se analiza las tendencias técnicas / legales que puedan impactar la seguridad de la información.

El Banco cuenta con un repositorio formal de líneas base de configuración segura para los componentes de plataforma de TI (v.gr. servidores, bases de datos, etc.).
Así mismo, se cuenta con un plan para la adquisición e implementación de tecnologías de seguridad de la información.

Existe un proceso para la identificación, evaluación y seguimiento de las vulnerabilidades de seguridad de la información.

Oportunidades de mejora

Formalizar el proceso de reunión del Comité de Arquitectura de Seguridad de la Información, considerando su frecuencia, integrantes, temas a tratar, evidencias y seguimiento a los acuerdos realizados.

ANEXO 2 – Declaración de Aplicabilidad

Políticas de Control y Seguridad

Clasificación de la Información

El propósito de estas políticas es presentar los lineamientos para la clasificación de la información. Esta clasificación nos permite establecer los niveles apropiados de seguridad en cuanto a los requerimientos de integridad, confidencialidad y disponibilidad de la información.

Los usuarios dueños deben basar sus decisiones entendiendo el impacto que puede tener para el Banco si se presenta un riesgo que afecte la confidencialidad, integridad y disponibilidad de la información. La clasificación también debe ser aplicada en forma consistente.

Definición de Clasificación

La clasificación de información es un proceso que sistemáticamente categoriza la información indicando el nivel de seguridad requerido.

Asignación de Clasificación

Los Directores y la Gerencia de Conocimiento son responsables por la clasificación de su información. Periódicamente debe reconfirmar la asignación para verificar su aplicabilidad.

Categorías

Las categorías de clasificación son:

- Confidencialidad - Se refiere a la necesidad de mantener la información privada. Su divulgación presentaría riesgos.
- Integridad - Se refiere a la necesidad de mantener la información exacta y completa.
- Disponibilidad - Se refiere a la necesidad de mantener acceso continuo y oportuno a la información.

Dentro de cada categoría existen valores que se asignan a la información. Para la categoría de confidencialidad se asignan los siguientes valores:

1. **General** - Información dirigida al público. Tiene muy poco o ningún impacto para el Banco si es divulgada, modificada o utilizada de una manera inapropiada.

   Impacto del Uso Inapropiado: Ningún impacto.
   Ejemplos: La información presentada en las páginas WEB del Banco, divulgación de noticias y literatura de productos o servicios.

2. **Uso Interno** - Este valor se asigna a la información que se debe mantener interna. Información dirigida al uso dentro del Banco y normalmente no compartida con personas que no son empleados del mismo. Pueden existir necesidades del negocio que requieran distribuir esta información fuera del Banco. Tiene el potencial de causar mínimo daño al Banco si se divulga.

   Impacto del Uso Inapropiado: Podría causar daños a la imagen del Banco.
   Ejemplos: Directorio telefónico, listas de correo, manual de empleados y algunos manuales de entrenamiento.

3. **Confidencial** - Información de uso selectivo. Su acceso se basa en la necesidad de conocerla o usarla para cumplir con su función. Esta información es compartida solamente bajo condiciones predefinidas. Se considera confidencial la información del cliente cuando no está disponible públicamente o cuando no es ampliamente conocida. Los clientes protegen tal información contra revelación a terceros a fin de mantener una ventaja competitiva.

   Impacto del Uso Inapropiado: Podría tener un impacto adverso al Banco, directores, empleados, proveedores o clientes.
   Ejemplos: Información de clientes, información personal, plan de operaciones a corto plazo, y estrategias de mercadeo y operaciones.

4. **Altamente Sensible** - Información de la más alta confidencialidad. Se autoriza el acceso a personas que tengan una necesidad específica de conocerla o usarla para cumplir con sus funciones; no debe ser compartida a menos que exista aprobación de los Directores. Información de la más alta confidencialidad del cliente que difundirla fuera del equipo del compromiso no sirve ningún propósito de negocios y presenta un riesgo de revelación inadecuada.

   Impacto del Uso Inapropiado: Podría causar daños financieros, legales, regulatorios o de imagen graves para el Banco, sus Directores, clientes, proveedores y empleados.
   Ejemplos: contraseñas, claves de cifrado, planes de inversión, resultados financieros previos a su liberación, planes estratégicos a largo plazo y estrategias de negocios.

La mayoría de los activos de información del Banco están en la segunda y tercera clasificación: **Uso Interno** y **Confidencial**.

Desde el punto de vista de su **disponibilidad**, la información se puede clasificar en:

1. **Muy crítica** - Información que si no está disponible en el momento que se requiere puede causar consecuencias serias para el Banco. Esta categoría puede abarcar el 20% o menos de su información.

2. **Crítica** - Información necesaria para la continuidad de operaciones del Banco. Si no está disponible en el término de uno a dos días o durante los períodos de cierre, puede causar consecuencias sobre el negocio. Esta categoría también incluye aquellas aplicaciones y archivos que se tornan críticos periódicamente, tales como al final del mes, trimestre o año. Esta categoría de información incluye el 50% de la información del negocio.

3. **Importante** - La falta de disponibilidad de esta información implica que el Banco puede operar por un término de cinco días sin estos recursos de información en particular o puede encontrar modos de procesamiento alternos (a menudo manuales) para trabajar fuera de línea.

Desde el punto de vista de su **integridad**, la información se puede clasificar en:

1. **Modificación Altamente Restringida** - La modificación de esta información sin autorización puede causar daño significativo al Banco, sus clientes, vendedores, asociados o al público. Este tipo de información requiere autorización individual por el usuario dueño de la información para actividades específicas sobre archivos de datos específicos y requiere revisión y aprobación por parte de la Auditoría.

2. **Modificación Restringida** - Información potencial para cambios moderados a través de fraudes, robo electrónico u otras formas para obtener beneficio personal. Esta clasificación aplica a información para la cual el Banco está dispuesto a otorgar derechos de modificación sobre una base Altamente Sensible.

3. **Modificación Controlada** - Recursos de información que se le pueden dar a cualquier usuario para efectuar modificaciones bajo circunstancias debidamente controladas. Los usuarios pueden modificar directorios internos y programas relacionados. Terceros pueden tener acceso bajo esta categoría.

Pautas para la Clasificación

Los siguientes factores ayudarán a determinar la clasificación apropiada de la información.

1. La consideración más importante en la clasificación de la información es el impacto probable de su divulgación, compromiso, o destrucción no autorizada. Algunos aspectos para tener en cuenta son:

   e. Costos de reemplazarla o reconstruirla
   f. Interrupción del negocio
   g. Pérdida de la confidencialidad del cliente
   h. Usurpación de la privacidad
   i. Valor para un intruso
   j. Pérdida de ventaja competitiva
   k. Oportunidad para actividades fraudulentas
   l. Cumplimientos regulatorios

2. Si es posible, a cada uno de estos factores se les debería asignar un monto. Si la divulgación, compromiso o destrucción no autorizada de la información resulta en un alto riesgo para el Banc, en cualquiera de los aspectos anteriores, la información probablemente deberá ser considerada sensible.

3. La clasificación apropiada debe ser basada en la magnitud del impacto:

   - Ningún impacto **General**
   - Impacto insignificante **Uso Interno**
   - Impacto adverso **Confidencial Reservada**
   - Daños severos o sanciones **Altamente Sensible**

4. Si una información contiene datos de valor y sensibilidad variables, la clasificación asignada debe reflejar los datos con valor y sensibilidad más altos dentro de la misma.

5. La clasificación dada por un tercero a su información debe ser respetada y mantenida por los usuarios del Banco.

Reclasificación

Solamente un nivel superior al usuario puede autorizar un cambio de clasificación. Una clasificación puede cambiar cuando la edad cambia el valor de la información.

Personal

El propósito de las políticas de personal del Banco es describir los controles de seguridad sobre la información que debe observar el personal que usa o tiene en

custodia información del Banco. Estas políticas están organizadas de acuerdo con las relaciones de los usuarios con el Banco.

Alcance

Estas políticas detalladas aplican sin excepción a todo el personal que custodie o tenga acceso a información del Banco.

Responsables

Consulte la sección *Roles y Responsabilidades* de este manual para mayor información. Los responsables de las políticas de personal son:

m. **Directores**: Deben asegurar que los empleados se adhieran y cumplan con las políticas que controlan el acceso y el uso de información y proveer entrenamiento sobre la seguridad de la información.
n. **Empleados**: Deben usar apropiadamente la información del Banco.
o. **Clientes, Agentes Externos y Empleados Temporales**: Deben cumplir con las reglas del Banco y con las políticas de seguridad sobre la información establecidas.

Requerimientos Mínimos Generales

Deberes **individuales**:

1. Usar la información del Banco únicamente para propósitos de trabajos contratados por el Banco y en cumplimiento de su labor.
2. Respetar la confidencialidad de la información del Banco.
3. No compartir perfiles de usuario ni contraseñas.
4. Ajustarse a las políticas de clasificación de la información.
5. Desconectar, apagar o cerrar con llave la Terminal cuando no esté en su puesto de trabajo.
6. Respaldar periódicamente la información importante que almacene en el computador asignado, utilizando el mecanismo definido para tal fin.

Deberes de los **Directores y la Gerencia de Conocimiento**:

- Autorizar el acceso a la información acorde con las funciones.
- Asegurar que los privilegios de acceso individuales reflejen una adecuada segregación de funciones. Un usuario no debe tener la habilidad de modificar las bases de datos u otra información del Banco sin una revisión independiente por un superior autorizado.
- Restringir el acceso del personal en horas hábiles a áreas que hayan sido adicionalmente Altamente Sensibles por razones de seguridad.

- Asegurar que todo el personal al momento de ingresar al Banco o con asignación de trabajos específicos, esté lo suficientemente capacitado en el manejo de la información y los controles que debe tener.
- Conservar los registros de los empleados con privilegios de acceso a la información. Adicionalmente, la Gerencia de Conocimiento, debe mantener actualizadas las autorizaciones y perfiles de los usuarios basándose en los archivos de Recursos Humanos donde se encuentran todos los empleados y las áreas a las que pertenecen.

Nuevos Empleados

1. Los nuevos empleados deben recibir una copia del Manual de Políticas de Seguridad de la Información como parte de la orientación que brinda el Banco.

2. Los nuevos empleados deben:

   a. Recibir una copia del folleto de seguridades que le dé el conocimiento apropiado como parte de la orientación del Banco.
   b. Confirmar por escrito el recibo de sus privilegios de acceso tanto a los recursos físicos como a la información.
   c. Recibir capacitación en seguridades y dejar constancia de dicha capacitación.

3. Los Directores son responsables por:

   a. Proveer a la Gerencia de Tecnología de la Información una notificación por escrito de:

      - Requerimientos de acceso a la plataforma donde se encuentra la información e indicación de la necesidad de accederla.
      - Fecha de inicio

   b. Suministrar, a través de la Gerencia de Tecnología de la Información, capacitación en Seguridad de la Información a los nuevos empleados en el manejo de la información bajo su cargo.

Promociones

1. Los Directores son responsables por:

   a. Informar al Departamento de Tecnología de la Información, a través de un memorando o un correo electrónico, la fecha de cambio de los privilegios de acceso del empleado que ha sido promovido.

b. Si dichos empleados deben tener acceso a áreas Altamente Sensibles, también se deben indicar estos permisos.
c. Asegurar que dichos empleados tengan una copia del manual de seguridad de la información de acuerdo a sus nuevas funciones.
d. Asegurar que los empleados promovidos reciban capacitación sobre Seguridad de la Información relacionada con sus nuevas funciones.

2. Los empleados promovidos deben confirmar el recibo de la capacitación en seguridades y de los privilegios de acceso para el desempeño de sus nuevas funciones tanto a los recursos físicos como a la información.

Temporales

1. La Gerencia de Conocimiento es responsable de asegurar que los empleados temporales:

   - Reciban el folleto de conocimiento de las Seguridades de la Información.
   - Firmen, a través de su contrato de trabajo, un acuerdo de confidencialidad de la información.

2. Los empleados temporales deben confirmar el recibo de los privilegios de acceso tanto a los recursos físicos como a la información.

3. El jefe del empleado temporal es el responsable por:

   a. Determinar, con la aprobación de un Director, los niveles de acceso del empleado temporal tanto a la áreas Altamente Sensibles del Banco como a los sistemas de información.

   b. Enviar por escrito a la Gerencia de Conocimiento lo siguiente:

      - Requerimientos de acceso a la información e indicación de la necesidad de accederla.
      - Fecha de inicio de la autorización.
      - Tiempo de duración de dichas autorizaciones.

   c. Capacitar a los empleados temporales en seguridad de la información para las funciones específicas a desempeñar.

   d. Supervisar el acceso y uso de la información a la que está autorizado el empleado temporal.

e. Recoger los equipos y revocar las autorizaciones que tengan los empleados temporales una vez hayan completado su período de trabajo en el Banco

Ausencias Temporales

Cuando un empleado se ausenta de su trabajo por un período de tiempo, su superior inmediato debe:

1. Determinar si los accesos a los recursos físicos y a la información deben ser suspendidos.
2. Notificar al Departamento de Tecnología de la Información, la fecha en que el acceso debe ser suspendido, de ser necesario.
3. Recoger los equipos de seguridad como por ejemplo llaves, claves, computadoras, etc.

Retiros

1. Cuando un empleado es suspendido, el acceso a los recursos físicos y a la información debe ser inmediatamente suspendido por su jefe inmediato.

2. Cuando un empleado es retirado (voluntaria o involuntariamente), su jefe inmediato es responsable por:

   a. Solicitar la revocación de las autorizaciones.
   b. Revocar o restringir los privilegios de acceso antes de notificarle la terminación del contrato, si es apropiado.
   c. Recoger los equipos, los dispositivos físicos y la revocación de las autorizaciones a los sistemas de información.

Seguridad Física

El Banco depende de la continua disponibilidad e integridad de la información que procesa y almacena. La seguridad física de la información, incluyendo la protección de los métodos utilizados para manejarla y procesarla, es la primera línea de defensa contra riesgos potenciales que puedan interrumpirla, dañarla o destruirla.

Alcance

Estos estándares cubren todos los sitios donde la información del Banco es almacenada o procesada.

Los estándares de seguridad física son diseñados para asegurar que la información sea almacenada y procesada en un ambiente adecuadamente controlado.

Responsabilidades

Véase la sección *Roles y Responsabilidades* de este manual para más información sobre responsabilidades.

Control de Acceso

1. El acceso a todas las áreas donde se procesa y almacena información del Banco debe ser limitado a aquellos empleados que de acuerdo con sus funciones requieran accederla. Esto incluye tanto información sensitiva mostrada por pantalla como información guardada en el escritorio.
2. Visitantes y personal de servicio que no estén autorizados a entrar regularmente, deben ser escoltados en las áreas de acceso restringido.
3. Las puertas exteriores debe ser cerradas con llave o estar aseguradas de otra forma durante las horas no hábiles.
4. Áreas diseñadas como Altamente Sensibles deben también tener controles de acceso especiales. El acceso a estas áreas debe ser únicamente para personal autorizado.
5. El personal del Departamento de Tecnología de la Información y de áreas de acceso restringido, son los responsables de asegurar el acceso únicamente a personal autorizado.
6. Los jefes de áreas de acceso restringido deben asegurarse que los controles de acceso como llaves o cerraduras con claves maestras sean cambiadas periódicamente. (No cuando el control haya sido comprometido).
7. Se debe usar un sistema de control que deje registro individual de las salidas de las instalaciones de las oficinas, de equipos u otros recursos tecnológicos.
8. Todos los paquetes, computadores, impresoras, etc., sacados de las instalaciones del Banco, deben estar sujetos a inspección por parte del Personal de Seguridad.
9. Todas las rutas de acceso físico a las instalaciones de computador como puertas, ventanas, aire acondicionado, escape de gases, etc. deben ser considerados como puntos potenciales de acceso no autorizado y como tal deben ser protegidos.
10. Dispositivos magnéticos, imanes, equipos eléctricos personales, comidas y bebidas son prohibidos en áreas de procesamiento electrónico de datos.
11. Los sistemas de control de acceso deben ser monitoreados permanentemente.

Ambiente de Oficina

El propósito de esta sección es describir como debe ser protegida la información en el lugar de trabajo. Estas políticas están organizadas por el ciclo de vida de la información. Si un medio o clasificación específica requiere controles especiales, esos controles son descritos.

Alcance
Estas políticas aplican a todos los ambientes donde la información del Banco está presente. Esto incluye, oficinas, lugares de trabajo en el cliente, agentes externos, y cualquier otro lugar donde la información del Banco sea guardada o procesada. Estas políticas aplican a toda la información sin tener en cuenta su medio: forma escrita, telefónica, electrónica y verbal.

Creación

General

- Documentos que contienen información clasificada como **Altamente Sensible** o **Confidencial** no pueden ser dejados desatendidos o inseguros.
- Cualquier documento que contenga información clasificada como **Altamente Sensible** o **Confidencial** debe ser apropiadamente autorizado para la divulgación de acuerdo con los estándares de clasificación de la información por parte del Banco.
- La divulgación de información clasificada como **Altamente Sensible** o **Confidencial**, cualquiera que fuere su medio, verbal, escrita, telefónica o electrónica, debe ser efectuada sobre la base de la necesidad de conocerla.
- Reuniones relacionadas con el manejo de información clasificada como **Altamente Sensible** o **Confidencial** deben llevarse a cabo en áreas de oficinas cerradas.
- Información clasificada como **Altamente Sensible** o **Confidencial** no debe ser accedida o enviada a través de cualquier tecnología de fácil acceso, tales como teléfonos celulares o inalámbricos. Para información sobre si una tecnología específica es apropiada para información clasificada como **Altamente Sensible** o **Confidencial**, comuníquese con el Departamento de Tecnología de la Información.

Copias de Respaldo

1. La información crítica de las operaciones del Banco debe ser respaldada regularmente. El Banco determina qué información debe ser respaldada, con qué frecuencia, en qué forma, y quién debe efectuar la copia. El Banco también es responsable por asegurar que las copias sean enviadas a un lugar externo, si es apropiado.

2. Una nueva copia de respaldo debe ser efectuada si la información contenida en el original cambia.

Distribución

- El acceso a o distribución de información de **Uso Interno** debe ser limitado a empleados u otros con la necesidad de conocerla o usarla para cumplir con sus funciones.
- Los documentos que contengan información **Altamente Sensible** o **Confidencial** deben ser impresos en un área segura o con la supervisión adecuada.
- La distribución de información **Altamente Sensible** o **Confidencial** debe ser limitada a individuos o grupos que la necesiten para cumplir con sus funciones.
- Los registros sobre la distribución de información **Altamente Sensible** deben ser guardados, incluyendo el número de copias de los documentos y los individuos en posesión de cada copia. Estos registros deben ser guardados por el Banco hasta que el documento sea eliminado o su clasificación sea cambiada.
- Para documentos **Altamente Sensibles** o **Confidenciales** se deben usar mecanismos que aseguren una entrega completa y confidencial. Ejemplos: sobres lacrados, correo registrado, correos de confianza y mecanismos de identificación.
- La información **Altamente Sensible** debe ser entregada personalmente al destinatario o su delegado si está en forma de documento. Correo de voz, correo electrónico o fax no deben ser usados para información **Altamente Sensible** a menos que existan controles específicos que aseguren su seguridad. Si la información es físicamente entregada y el destinatario no está presente para recibirla, el delegado debe firmar el recibo del documento y guardarlo bajo control hasta que éste sea entregado al destinatario.
- Los mecanismos de entrega utilizados para información **Altamente Sensible**, deben contemplar confirmación de recibo.
- Toda clasificación dada por un tercero a su información debe seguir las políticas internas del Banco para ese tipo de clasificación.

Almacenamiento

Estas políticas aplican tanto a los originales como a todas las copias de la información.

1. El acceso a información **Altamente Sensible** o **Confidencial** que se encuentre almacenada debe ser adecuadamente controlado. Esto incluye información **Altamente Sensible** o **Confidencial** almacenada externamente o copias de respaldo.
2. Las copias de respaldo de información **Altamente Sensible** o **Confidencial** deben ser protegidas de destrucción intencionada o accidental.
3. La información almacenada por períodos prolongados debe ser revisada regularmente (mínimo cada tres meses) para verificar su legibilidad.

4. Los individuos que tienen acceso remoto a la información del Banco son responsables por la seguridad de la información con los mismos niveles de control requeridos dentro del Banco.

Período de Almacenamiento

- Toda la **información debe** tener un período de almacenamiento asignado.
- Cuando sea almacenada por requerimientos legales o del Banco, la información debe ser protegida durante el período de almacenamiento que cumpla con este requerimiento. Este período debe ser indicado al frente del documento o en el medio que los contenga. Las copias de respaldo de los documentos también deben tener fechas de almacenamiento.
- A la expiración de su período de almacenamiento, todas las copias de los documentos deben ser destruidas de acuerdo con las disposiciones internas o su clasificación.
- La reclasificación de información durante su período de almacenamiento debe ser efectuada por el usuario responsable de acuerdo con las políticas de reclasificación en la sección de *Clasificación de la Información* de este manual.

Copiado

1. Obtención de copias de información clasificada de **Uso Interno** debe ser con autorización escrita de personal del Banco.
2. Se debe tener cuidado en la reproducción de información **Altamente Sensible** , **Confidencial** o de **Uso Interno** para evitar divulgación de partes no autorizadas.
3. Las copias de la información clasificada como **Altamente Sensible** deben ser numeradas y registradas.

Destrucción

1. La información clasificada como **Altamente Sensible** o **Confidencial** debe ser destruida de tal forma que quede ilegible.
2. Los medios electrónicos que contengan información clasificada como **Altamente Sensible** o **Confidencial** deben ser borrados o sobre-escritos antes de que sean reusados o destruidos.
3. Cualquier medio que se encuentre dañado o que contenga información incompleta está sujeto a todos los controles de destrucción aplicables.
4. La destrucción de información **Altamente Sensible** o **Confidencial** debe ser efectuada por empleados o por un servicio de fianza.
5. Los listados que ya no se requieran se deben destruir. No se deben botar a la papelera ni se deben sacar del Banco.

Internet y Correo Electrónico

El Banco suministra a los usuarios el acceso al INTERNET y al correo electrónico como herramientas para el uso exclusivo de sus funciones dentro del Banco. Además, se estimula el uso del INTERNET y del correo electrónico porque ellos hacen que las comunicaciones sean más eficientes y efectivas. Sin embargo, los servicios de INTERNET y del correo electrónico son propiedad del Banco y el propósito de uso de ellos es facilitar sus negocios.

Políticas de Uso

1. Cada usuario tiene la responsabilidad de utilizar el INTERNET y el correo electrónico de una manera productiva para el Banco.
2. Los servicios de INTERNET y correo electrónico no deben ser usados para transmitir, recibir o almacenar comunicaciones de naturaleza discriminatoria u ofensiva o material obsceno.
3. Los servicios de INTERNET y correo electrónico no deben ser usados para la persecución de cualquier especie.
4. No se permite la transmisión de mensajes despectivos, difamatorios, comentarios acerca de raza, edad, incapacidad, religión, nacionalidad, atributos físicos o preferencias sexuales de individuos, a través de los servicios de INTERNET o correo electrónico.
5. No se permite el uso de lenguaje ofensivo para transmisiones a través del INTERNET o del correo del Banco.
6. Estos medios electrónicos no deben ser usados para propósitos ilegales, en contra de las políticas o de los intereses del Banco.
7. Los servicios de INTERNET y del correo electrónico no deben ser usados para negocios que no son del Banco o para ganancias personales.
8. Los servicios de INTERNET y del correo electrónico no deben ser usados para atacar desde el Banco sitios externos.
9. Información clasificada como Altamente Sensible, Confidencial o de Uso Interno, no debe estar disponible para el dominio público.
10. El uso personal está permitido siempre y cuando no interfiera con las obligaciones laborales y no atente contra las políticas del Banco ni las regulaciones locales.
11. Ningún usuario debe intentar deshabilitar, romper o evadir los dispositivos de seguridad como firewalls.
12. Las conexiones directas a Internet por cuentas dial-up solo son permitidas cuando no está conectada la computadora a la red del Banco.
13. Los empleados no están autorizados para hablar o escribir en nombre del Banco en grupos de Chat o de correo.

14. Está estrictamente prohibido desarrollar, ejecutar y distribuir deliberadamente virus, troyanos, gusanos, o cualquier otro tipo de código nocivo para los sistemas del Banco, clientes o sitios externos.
15. No se deben evadir o deshabilitar los sistemas de auditoría automáticos (logs, controles de seguridad, autenticación, etc.) instalados en las redes del Banco, redes de clientes ni de las conexiones remotas de usuarios y clientes.

Comunicaciones

1. Todos los usuarios que generan un mensaje a través de los servicios de INTERNET y correo electrónico del Banco son responsables por su contenido.
2. Todos los mensajes comunicados por los servicios de INTERNET o correo electrónico del Banco, deben identificar el remitente.
3. Todo mensaje o información enviada por un usuario del Banco se debe considerar como una declaración que puede reflejar la opinión del Banco. Cualquier declaración personal debe explícitamente indicarse para que no se comprometa el nombre del Banco o se asuma como una opinión general del Banco.
4. Debe evitarse al máximo la transmisión de información o archivos confidenciales. En caso de requerirse de debe utilizar el mecanismo de cifrado estándar del Banco.
1. No está permitido activar el reenvío automático de mensajes de cuentas de correo del Banco hacia cuentas externas. Esto atenta contra la confidencialidad.

Software

Las políticas para descargar software del INTERNET son:

1. Necesidad del software para cumplir con sus funciones.
2. Al descargar o recibir software el usuario debe chequearlo a través de un software antivirus.
3. El usuario debe cumplir con los requerimientos de licenciamiento del proveedor. No debe hacer copias ilegales del software.
4. El software debe ser bajado de empresas conocidas y en caso de desconocimiento se debe contactar al Departamento de Tecnología de la Información.
5. El software descargado de INTERNET debe ser eliminado cuando no haya necesidad del usuario para su uso.
6. Está prohibido instalar y usar software que permite compartir archivos a través de internet corporativo, sobre cualquiera de los activos del Banco, clientes o afiliados.

Derechos de Autor

No se debe transmitir información a través de los servicios de INTERNET o correo electrónico que viole los derechos de autor.

Seguridad

Usuarios de la red del Banco que requieran de los servicios de INTERNET, deben utilizar la infraestructura que posee el Banco para esto y no utilizar medios alternos mientras estén conectados a la red.

Los empleados del Banco no deben compartir con terceros (incluyendo familiares) los recursos de Internet que le han sido otorgados.

Monitoreo

No es política del Banco monitorear permanentemente el contenido de los mensajes transmitidos por el sistema de correo. Sin embargo, el contenido de las comunicaciones electrónicas puede ser monitoreado para propósitos de la operación, mantenimiento, soporte, auditoría y para actividades de investigación.

Los usuarios deben dar el mejor uso a este recurso propiedad del Banco, reconociendo en hecho que el Banco hará revisiones esporádicas del contenido de las comunicaciones electrónicas para verificar el cumplimiento de las políticas.

Violaciones

Cualquier empleado que abuse de los privilegios concedidos por el Banco para acceder el correo electrónico o a INTERNET está sujeto a sanciones.

Estas políticas se pueden comunicar de varias formas:

- Una línea de mensajes que aparece cuando el usuario se registra en el correo electrónico o en INTERNET.
- Incluir en el manual de empleados un enunciado corto de las políticas recordando el uso aceptable del correo electrónico e INTERNET.
- Orientar y notificar a los empleados nuevos sobre las políticas de uso del correo electrónico e INTERNET.
- Sesiones de entrenamiento sobre las políticas de uso de computadoras, correo electrónico e INTERNET. Un empleado a quien se le diga que se puede monitorear el uso del correo electrónico y de INTERNET puede ser cuidadoso en el uso de estos sistemas. Sesiones de entrenamiento donde se explican detalladamente las políticas pueden aliviar el temor de los usuarios.

Ambiente de Usuario Final

Las actividades del usuario final involucran manipulación de datos y el uso de la información del Banco y del Cliente para propósitos del negocio.

El objetivo de estas políticas es minimizar la probabilidad que la información sea modificada, revelada, perdida o retenida accidental o intencionalmente en el ambiente de trabajo del usuario final. Estas políticas también están dirigidas a asegurar la exactitud de la información procesada en el computador del usuario final.

Alcance

A través de este manual un *Usuario Final* es definido como cualquier persona que ha sido autorizada por el Banco para utilizar los sistemas de información del Banco. Esta definición no solamente incluye personas en las áreas del negocio del Banco sino también personal de sistemas que tiene acceso a los programas o quienes pueden efectuar funciones de reportaje eventuales.

General

Estas políticas aplican a todos los sistemas y equipos del ambiente de trabajo del usuario final.

- Cada usuario es responsable por el buen uso de la información del Banco, sea que la obtenga de documentos, listados, medios magnéticos o electrónicos.
- Cada usuario es responsable por la seguridad de sus datos, por lo tanto no debe dejar información **Altamente Sensible** o **Confidencial** en directorios públicos de red y en discos duros a disposición de los demás usuarios.
- Los computadores portátiles deben ser marcados con el nombre del propietario.
- Los computadores portátiles deben tener clave de arranque.
- Todos los datos en los computadores portátiles deben estar cifrados.
- Los computadores portátiles deben estar protegidos por una póliza de seguros.
- En los computadores personales que son compartidos, no se debe almacenar permanentemente información clasificada como Altamente Sensible o Confidencial. Es decir, la información una vez respaldada debe ser borrada.
- La entrega y recibo de equipos portátiles compartidos debe ser efectuada mediante una revisión previa por parte de la persona responsable de administrar la rotación de los mismos. Esta rotación de equipos debe quedar documentada.
- Las políticas en el uso de equipos portátiles forman parte de este documento.

Respaldo

Metas de Respaldo

El objetivo de la ejecución de copias respaldos de los diferentes sistemas de información del Banco debe ser la recuperación de la información en caso de desastre parcial o total, con el fin de garantizar la continuidad del negocio. Todos los sistemas de información del Banco deben tener respaldo, independiente del medio en el cual se encuentre la información. Es la responsabilidad del usuario final determinar los requerimientos de respaldo de su información y definir su frecuencia, rotación y destrucción. Es responsabilidad del Gerente del Compromiso determinar los requerimientos de respaldo de la información del cliente, definir su frecuencia y controlar la entrega de los archivos magnéticos al Pool, al finalizar el compromiso.

Período de Almacenamiento

Es el usuario final de la información quien debe definir por cuanto tiempo se debe tener el respaldo de su información y seleccionar el medio. Cuando existan requerimientos legales relacionados con el período de almacenamiento, estos se deben cumplir.

Seguridad y Acceso al Almacenamiento

Los respaldos de los diferentes sistemas de información del Banco deben guardarse en lugares seguros y deben poseer controles de acceso bien definidos con el fin de garantizar que sólo las personas autorizadas tienen acceso a dicha información. El control de acceso para el respaldo de información debe tener las mismas restricciones y controles que posee la información en el medio original.

Los respaldos de la información deben ser guardados en áreas seguras y bajo condiciones ambientales adecuadas.

Almacenamiento Externo

El usuario final es responsable por determinar cuales copias de respaldo de la información bajo su cargo requieren de almacenamiento externo. Para soporte adicional en el cumplimiento de esta política, consultar a la Gerencia de Tecnología de la Información.

Solicitudes para Restauración

Los usuarios de las diferentes dependencias que requieran restaurar información de otros usuarios, deben hacer esta solicitud a través del usuario dueño.

Uso Autorizado de Software

En los computadores del Banco sólo se puede instalar software desarrollado o adquirido legalmente y cuya licencia de uso esté a nombre del Banco.

La única área del Banco que puede coordinar el mantenimiento de programas o aplicaciones es el Departamento de Tecnología de la Información.

Está prohibido en los computadores del Banco:

- Copiar el software desarrollado o adquirido por el Banco.
- Utilizar software diferente al adquirido legalmente por el Banco y para propósitos distintos a los señalados cuando se instala.

Los usuarios deben cumplir con la Legislación Colombiana que regula los derechos de autor.

Control de Virus

Se entiende por virus, un programa con la capacidad de reproducirse por medio de la modificación de otros archivos o programas.

- Los computadores personales deben mantener activo un software antivirus.
- Los servidores de archivos y programas y correo electrónico deben mantener activo un software antivirus.
- Los computadores personales y servidores deben ser chequeados contra virus periódica y automáticamente.
- Cualquier información que venga por medio electrónico o magnético como disquetes, correo electrónico o información de INTERNET, debe ser revisada por un software antivirus antes de ser utilizada.
- El Departamento de Tecnología de la Información es responsable por la actualización oportuna del software antivirus.
- Los usuarios deben evitar arrancar los computadores desde la unidad de disquete. Si se requiere de iniciar el sistema desde un disquete, éste debe ser previamente chequeado por un software antivirus.
- Es responsabilidad de los usuarios reportar todos los incidentes de infección de virus al Departamento de Tecnología de la Información.
- Es responsabilidad de los usuarios tomar copias de la información y verificar que el respaldo esté libre de cualquier infección de virus.
- El usuario debe asegurar que toda la información provenga de fuentes conocidas.
- Ningún usuario puede escribir, distribuir o introducir software que conozca o sospeche que tiene virus.

Plan de Contingencias

Para que el Banco pueda continuar operando durante una contingencia es importante tener los procedimientos documentados que le ayudarán a recuperar sus operaciones con el mínimo impacto posible a sus clientes y empleados. Si ocurre una interrupción que afecte las operaciones, el Banco necesita restaurarlas en un tiempo razonable manteniendo un nivel apropiado de control que durante la contingencia pueda asegurar razonablemente la confidencialidad e integridad de la información.

La existencia de numerosas amenazas contra la continuidad de operaciones del Banco y la dificultad para determinar su ocurrencia, requieren de un análisis formal en el cual se identifique el nivel de riesgo y el impacto al negocio si se pierde una función de servicio.

Alcance

Estas políticas aplican para todas las áreas del Banco que ejecutan o soportan funciones del negocio. Aunque los sistemas de información y continuidad de operaciones son críticos, la principal consideración para el Banco es la seguridad de sus empleados.

General

1. El plan de contingencias debe estar basado en un análisis de riesgo e impacto al negocio si se presenta una consistencia.
2. El plan de contingencias debe identificar responsables para el desarrollo, mantenimiento y prueba del plan.
3. El plan de contingencias debe identificar los roles y responsabilidades de implementar, ejecutar y mantener el plan.
4. **El plan de contingencias debe ser probado periódicamente dejando documentación de cada una de sus pruebas.**
5. La documentación de las pruebas efectuadas al plan de contingencias debe reflejar los resultados obtenidos en cada una de ellas.
6. El plan de contingencias debe adaptarse a una variedad de interrupciones, incluyendo fallas operacionales, emergencias y desastres.
7. El plan debe cubrir todas las instalaciones críticas del Banco para reducir la probabilidad de que una falla operacional o emergencia en una de ellas conlleve a un desastre mayor.
8. El usuario dueño del plan de contingencias debe mantener informados a los Socios del estado general del plan.
9. El plan de contingencias debe ser documentado y almacenado en copia impresa y medio magnético en un sitio remoto.

Desarrollo y Mantenimiento del Plan

1. **Todos los planes de contingencia** deben:
   - **a.** Como mínimo, adaptarse a los estándares y guías establecidos por el Banco en caso de una emergencia.
   - **b.** Incluir procedimientos de seguridad física y seguridad lógica. El nivel de seguridad requerido durante un desastre debe ser como mínimo el mismo nivel usado durante la operación normal. Solamente los Directores pueden aprobar un nivel de seguridad inferior.

2. **El plan de contingencias debe**:
   - **a.** Identificar uno o más sitios de procesamiento y redes de telecomunicaciones alternos que sean capaz de procesar todas las aplicaciones importantes del Banco.
   - **b.** Incluir el desarrollo, prueba y mantenimiento de planes que puedan ser usados para procesar todas las aplicaciones del Banco en un sitio alterno.

3. Se debe firmar un acuerdo formal con todos los sitios externos alternos y redes. Este acuerdo debe ser revisado y renovado periódicamente.

Seguridad Física

1. El Departamento de Tecnología del Banco es responsable de establecer la seguridad física y los planes de evacuación en caso de emergencia para todos sus recursos. Estos planes deben cumplir con todas las reglamentaciones aplicables y de ley.
2. El Departamento de Tecnología, debe asegurar que periódicamente se revisen las seguridades físicas y los planes de evacuación de emergencias mediante simulacros de desastres en todas las dependencias del Banco.

ANEXO 3 – MAI_ComercioExterior

Ver archivo ../3 Fase/Activos/MAI_ComercioExterior.xlsx

ANEXO 4 – MAI_AdministracionPortafolios

Ver archivo ../3 Fase/Activos/MAI_AdministracionPortafolios.xlsx

ANEXO 5 – MAI_AdministracionLiquidez

Ver archivo ../3 Fase/Activos/MAI_AdministracionLiquidez.xlsx

ANEXO 6 – MAI_Reportes

Ver archivo ../3 Fase/Activos/MAI_Reportes.xlsx

ANEXO 7 – Riesgo_Inherente

Ver archivo ../3 Fase/Riesgo_Inherente.xlsx

ANEXO 8 – Formato SGSI Auditoría

Ver archivo ../5 Fase/FORMATO_SGSI_AUDITORIA.xlsx