Elaboración de un plan de implementación de la ISO/IEC 27001:2013

Nombre Estudiante: Luz Dary Méndez Uribe

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área: Sistemas de Gestión de la Seguridad de la Información

Consultor: Antonio Jose Segovia Henares
Profesor responsable de la asignatura: Carles Garrigues Olivella
Centro: Universitat Oberta de Catalunya

Fecha entrega: 30/12/2016

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Licencias alternativas (elegir alguna de las siguientes y sustituir la de la página anterior)

A) Creative Commons:

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento 3.0 España de Creative Commons

B) GNU Free Documentation License (GNU FDL)

Copyright © AÑO TU-NOMBRE.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free

Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU Free Documentation License".

C) Copyright

© (el autor/a)
Reservados todos los derechos. Está prohibido la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la impresión, la reprografía, el microfilme, el tratamiento informático o cualquier otro sistema, así como la distribución de ejemplares mediante alquiler y préstamo, sin la autorización escrita del autor o de los límites que autorice la Ley de Propiedad Intelectual.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013*
Nombre del autor:	*Luz Dary Méndez Uribe*
Nombre del consultor/a:	Antonio Jose Segovia Henares
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	12/2016
Titulación::	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	*Español*
Palabras clave	*SGSI, MAGERITH,ISO*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

Como trabajo final del Máster, se ha realizado el presente proyecto aplicando gran parte del conocimiento adquirido en un caso de estudio para el cual se ha seleccionado un BANCO (ficticio) en el cual se quiere implementar un SGSI y para ello se crea un plan de implementación basado principalmente en la norma ISO/IEC 27001:2013. Se ha limitado el alcance tratando de conservar aspectos relevantes afines a buena parte de las empresas que pudieran estar interesadas en implementar un SGSI. El proyecto se ha llevado a cabo en 6 fases obteniendo en cada una de ellas entregables que sirven de apoyo importante en la ejecución de la siguiente fase. Cada fase tiene unos objetivos especiales en relación al SGSI conocer la normatividad a utilizar, definir el estado inicial, validar los niveles de implementación de los controles, completar el esquema documental, identificar activos de información, realizar análisis de riesgos y en consideración de resultados proponer proyectos que incluyan acciones de mejora y salvaguardas. Como resultado de la ejecución de estos proyectos se evidencia en la auditoría un impacto positivo tanto en la implementación de controles como en la reducción de riesgos residuales, la evolución en los niveles de madurez no se ha completado y por tanto se requiere el apoyo de los directivos y áreas involucradas para dar curso a la mejora continua.

Abstract (in English, 250 words or less):

As a final project of the Master, the present project has been applied applying much of the knowledge acquired in a case study for which a BANK (fictitious)

has been selected in which it is wanted to implement an ISMS and for this a plan of Implementation based mainly on ISO / IEC 27001: 2013. The scope has been limited by trying to preserve relevant aspects related to many of the companies that might be interested in implementing an ISMS. The project has been carried out in 6 phases, obtaining in each one of them deliverables that serve as important support in the execution of the next phase. Each phase has special objectives in relation to the ISMS to know the normativity to be used, to define the initial state, to validate the levels of implementation of the controls, to complete the documentary scheme, to identify information assets, to carry out risk analysis and to consider the results proposed Projects that include improvement actions and safeguards. As a result of the execution of these projects, a positive impact on the implementation of controls and on the reduction of residual risks is evidenced in the audit, the evolution in maturity levels has not been completed and therefore the support of the Managers and areas involved to give direction to continuous improvement.

Índice

1. Introducción 2
1.1 Contexto y justificación del Trabajo 2
1.1.1 Contexto 2
1.1.2 Justificación 3
1.2 Objetivos del Trabajo 3
1.2.1 Objetivo Principal 3
1.2.2 Objetivos Específicos SGSI 3
1.3 Enfoque y método seguido 4
1.3.1 Marco normativo utilizado 4
1.3.2 Fases del proyecto 5
1.4 Planificación del Trabajo 6
2. Sistema de Gestión de Seguridad de la Información 1
2.1 Alcance del SGSI 1
2.1.1 Áreas involucradas 1
2.1.2 Procesos involucrados 2
2.1.3 Aplicativos involucrados 3
2.2 Resumen de análisis diferencial 5
2.3 Sistema de Gestión documental 7
2.3.1 Política de seguridad 7
2.3.2 Procedimiento de Auditorías Internas 7
2.3.3 Gestión de Indicadores 7
2.3.4 Procedimiento Revisión por Dirección 7
2.3.5 Gestión de Roles y Responsabilidades 7
2.3.6 Metodología de riesgos 7
2.4 Análisis de riesgos 8
2.5 Proyectos planteados a la dirección para el futuro 1
2.6 Auditoría de cumplimiento 5
3. Conclusiones 6
4. Glosario 7
5. Bibliografía 14
6. Anexos 15
ANEXO 1: POLÍTICA DE SEGURIDAD 15
ANEXO 2: PROCEDIMIENTO DE AUDITORÍAS INTERNAS 39
ANEXO 3: GESTIÓN DE INDICADORES 42
ANEXO 4: PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN 50
ANEXO 5: GESTIÓN DE ROLES Y RESPONSABILIDADES 53
ANEXO 6: INFORME AUDITORÍA INTERNA 55

Lista de figuras

Figura 1: Cronograma de proyecto 1
Figura 2: Cronograma de proyecto 2 2
Figura 3: Áreas involucradas parte 1 2
Figura 4: Áreas involucradas parte 2 2
Figura 5: Procesos involucrados 3
Figura 6: Estructura del aplicativo 4
Figura 7: Diagrama de arquitectura 4
Figura 8: Análisis diferencial ISO/IEC27001 6
Figura 9: Análisis diferencial ISO/IEC27002 7
Figura 10: Metodología de análisis de riesgos 8

Lista de tablas

Tabla 2: Aplicativos relacionados con SAAG 5
Tabla 3: Resumen Análisis diferencial ISO/IEC 27001:2013..... 5
Tabla 4: Resumen Análisis diferencial ISO/IEC 27002:2013..... 6
Tabla 5: Análisis de riesgos inicial con riesgos no aceptables 2
Tabla 6: Riesgos calculados después de la ejecución de los proyectos propuestos de la fase 4 3
Tabla 7: Proyecto | Política de seguridad 1
Tabla 8: Proyecto |Organización de la seguridad de la información..... 1
Tabla 9: Proyecto | Seguridad en los recursos humanos 2
Tabla 10: Proyecto | Gestión de activos 2
Tabla 11: Proyecto | Control de acceso..... 3
Tabla 12: Proyecto | Seguridad física y ambiental 3
Tabla 13: Proyecto | Gestión de comunicaciones y operaciones 4
Tabla 14: Proyecto | Adquisición, desarrollo y mantenimiento de Sistemas de Información..... 5
Tabla 15: Proyecto | Gestión de incidentes 5
Tabla 16: Proyecto | Gestión de continuidad de negocio 5

1. Introducción

Toda compañía tiene en su poder activos de información de diversos tipos, los cuales son de gran importancia para su funcionamiento, preservarlos y administrarlos eficientemente es uno de los propósitos implícitos dentro de toda actividad de negocio y de allí, surge la necesidad de utilizar diversos mecanismos para hacerlo de la mejor forma posible. Para facilitar ésta tarea existen normas, metodologías y compendios de buenas prácticas que han generado resultados de éxito a muchas compañías y con el ánimo de hacer uso de algunos de estos recursos y aplicar buena parte del conocimiento adquirido durante el Máster en un caso de estudio se realiza el presente trabajo final.

Como resultado se tendrá un plan de implementación de un SGSI de la ISO/IEC 27001:2013 asociado a un compañía, en éste caso un BANCO (ficticio) y para su elaboración se manejarán 6 fases resumidas a continuación:

FASE 1: se dan a conocer las normas ISO/IEC 27001:2013 y ISO/IEC 27002:2013, que servirán de guía y se realiza un análisis diferencial incluyendo procesos, áreas, personal y aplicativos definidos en el alcance, para definir una línea base de cumplimiento de requisitos e implementación de controles requeridos.

FASE 2: recopila documentación existente para agregar al esquema documental y se generan algunos documentos faltantes.

FASE 3: se realiza el proceso completo de análisis de riesgos teniendo en cuenta la metodología documentada previamente, la descripción de la metodología utilizada para el análisis de riesgos relacionados con seguridad, está basada en MAGERITH.

FASE 4: Se proponen proyectos que incluyen diversas mejoras en consideración de los resultados de las fases anteriores

FASE 5: se realiza la auditoría interna para validar el estado actual del SGSI.

FASE 6: Se consolidan los resultados para mostrar a los directivos

1.1 Contexto y justificación del Trabajo

1.1.1 Contexto

La compañía seleccionada como caso de estudio corresponde a un BANCO (ficticio) se encuentra ubicada en Colombia con sedes administrativas en la ciudad de Bogotá, lleva más de 50 años de constituida, se encuentra vigilada por la SFC (Superintendencia Financiera de Colombia) en cumplimiento de su normatividad y cuenta con certificación ISO9001 (versión 2008) en algunos de los procesos más importantes, lo cual servirá de gran ayuda con respecto a la

familiarización preliminar en cuanto a procesos, mejora continua y auditorías.

Adicional a esto, pese a no tener de momento un Sistema de Gestión de la seguridad de la información la entidad cuenta con un Modelo de seguridad de la información genérico y aplicable a muchos de los procesos manejados por la empresa. Para la gestión de riesgo operativo se utiliza el sistema SARO (Sistema de Administración de Riesgo Operativo) incorporando todo un esquema para la definición, identificación, análisis, evaluación, mitigación, monitoreo, comunicación y consulta de riesgos operativos. Otro de los sistemas que generan gran impacto en el manejo de seguridad corporativa es SARLAFT (Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo) requerido como mecanismo de control para la SFC. Dado el gran tamaño de la compañía, se limitó el alcance del SGSI a "Los sistemas de información que dan soporte al aplicativo de administración de garantías", fue elegido de ésta forma con el objetivo de involucrar una buena parte de aspectos que pueden ser afines a muchas empresas que pudieran estar interesadas en implementar un SGSI.

1.1.2 Justificación

Si bien es cierto, la compañía contaba inicialmente con varios sistemas implementados para apoyar la seguridad de la información esto no era suficiente, puesto que se presentaban inconvenientes en todas las dimensiones de seguridad, por tal motivo se espera que con el plan propuesto se vean reflejados resultados positivos y una evolución considerable en cuanto a niveles de madurez de implementación de controles y requisitos que se encuentren relacionados con el alcance (procesos, áreas, aplicaciones, etc.). Adicional a esto se esperan beneficios competitivos, una mejora en la imagen de la compañía puesto que se involucra en el alcance parte del manejo de información confidencial de clientes.

1.2 Objetivos del Trabajo

1.2.1 Objetivo Principal

Elaborar un "Plan de Seguridad de la información" teniendo en cuenta el cumplimiento de los requisitos necesarios para su implementación los cuales están definidos en la norma ISO/IEC 27001: 2013 y a su vez, utilizando los controles y buenas prácticas que ofrece la norma ISO/IEC 27002:2013.

1.2.2 Objetivos Específicos SGSI

- Teniendo en cuenta el alcance, proteger la información de la compañía en cada una de sus dimensiones (confidencialidad, integridad, disponibilidad, eficiencia, efectividad y confiabilidad de la información)
- Realizar el análisis diferencial acorde con los requisitos de la ISO/IEC27001 y los controles propuestos en el estándar ISO/IEC 27002 de manera regular para validar el estado de implementación de requisitos y controles

- Definir procedimientos y tareas complementarias que permitan dar cumplimiento a los objetivos del sistema de seguridad de la información dentro de los procesos involucrados en los sistemas de información definidos en el alcance
- Realizar la clasificación de activos con asignación de responsables que sirva de base en el tratamiento de riesgos
- Diseñar un plan de gestión de riesgos que se ajuste a las necesidades corporativas y los objetivos misionales
- Proponer proyectos o acciones de mejora que promuevan la mejora continua del SGSI, en consideración de los resultados que arrojen los análisis de riesgos, auditorías y demás procesos que informen sobre hallazgos, incidentes o problemas
- Comunicar a los participantes sobre las novedades generadas para involucrarlos y comprometerlos en el cambio
- Promover el cumplimiento de las leyes y normas vigentes que apliquen en el país para entidades bancarias
- Promover una cultura de seguridad de la información en función del cumplimiento de las políticas y normas de la política de seguridad

1.3 Enfoque y método seguido

El método utilizado principalmente consiste en realizar validación explicita de controles relacionados con la norma ISO/IEC27002:2013 y los requisitos establecidos por la norma ISO/IEC27001:2013, a su vez se hace uso del documento de declaración de aplicabilidad donde se indican los documentos que pueden servir como evidencia de implementación de controles. Para tal validación fue necesario revisar cada ítem de cumplimiento propuesto en consideración de los elementos incluidos en el alcance (procesos, áreas, aplicaciones, etc.). También se involucró como metodología de análisis de riesgos de seguridad a MAGERITH que cuenta con suficiente respaldo y puede aplicar a prácticamente cualquier tipo de compañía.

1.3.1 Marco normativo utilizado

Como fundamento normativo para la realización del proyecto se utilizaron las normas ISO/IEC27001:2013 e ISO/IEC27002:2013. Por un lado, la ISO/IEC27001 corresponde a un estándar publicado en octubre del año 2005 por la ISO(International Organization for Standardization) y la IEC(International Electrotechnical Commission), el cual define cuales son los requisitos básicos para establecer, implantar, mantener y mejorar un SGSI (Sistema de Gestión de Seguridad de la Información). Actualmente es el único estándar que a nivel internacional es aceptado para la gestión de la seguridad de la información, además es certificable y relaciona de forma específica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la información, en función del ciclo PDCA (Plan, Do, Check, Act).
Éste norma corresponde al resultado de la evolución de varios estándares relacionados también con la seguridad de la información tales como:

- 1901 – Normas “BS”: La British Standards Institution publica normas con el prefijo “BS” con carácter internacional
- 1995- BS 7799-1:1995: Mejores prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información
- 1998 – BS 7799-2:1999: (Revisión de la anterior norma) Define los requisitos para implementar una SGSIE certificable
- .1999 – BS 7799-1:1999: Revisión de la norma anterior
- 2000 – ISO/IEC 17799:2000: Corresponde a una adaptación sin grandes cambios que realizó la ISO de la norma británica BS 7799-1
- 2002 – BS 7799-2:2002: Se publica la nueva versión que permitió acreditar empresas por parte de una entidad certificadora en Reino Unido y en otros países.
- 2005 – ISO/IEC 27001:2005 e ISO/IEC17799:2005: Se da a conocer el estándar ISO 27001 como norma internacional certificable y se revisa la ISO 17799 dando lugar a la ISO 27001:2005.
- 2007 – ISO 17799: Cambia de nombre para convertirse en la ISO 27002:2005
- 2007 – ISO/IEC 27001:2007: Se publica la nueva versión.
- 2009 – Se publica un documento adicional de modificaciones llamado ISO 27001:2007/1M:2009.
- 2013 - ISO/IEC 27001 Se publica la nueva versión de la ISO27001 incluyendo cambios significativos en cuanto a estructura, evaluación y tratamiento de los riesgos.

De otro lado, la ISO/IEC 27002 corresponde al estándar original ISO 17799(2007) que en el 2007 cambió de nombre a ISO 27002:2005 y fue publicado por la ISO(International Organization for Standardization) y la IEC(International Electrotechnical Commission) reuniendo una serie de buenas prácticas y controles sugeridos que se pueden adaptar a casi cualquier organización. Comparte su historia de evolución de estándares con la ISO/IEC 27001 hasta el momento de su nacimiento y al igual que la ISO/IEC 27001 su última versión corresponde al año 2013.

1.3.2 Fases del proyecto

FASE 1: Se presentaron aspectos importantes de la compañía utilizada como caso de estudio con el objetivo de entrar en contexto, se definió el alcance del SGSI y a partir de ésta definición se realizó una valoración del estado de la compañía evaluando los procesos, áreas y políticas relacionados a éste, obteniendo como resultado el análisis diferencial tanto para los requisitos de la norma ISO/IEC27001 como los controles que integran la norma ISO/IEC/27002. Pese a que la compañía contaba en su momento con un Plan de seguridad de la información a modo general en la compañía, se detectaron varias falencias a partir del análisis diferencial realizado así como mejoras considerables por realizar.

FASE 2: Se recopilan política, procedimientos y documentos existentes, así como documentos creados para dar cumplimiento a requisitos establecidos como punto de partida.

FASE 3: Ésta fase toma especial significado, puesto que corresponde al análisis de riesgos asociado a los activos de información, utilizando la metodología propuesta en la etapa anterior la cual se encuentra basada especialmente en la metodología MAGERITH.

FASE 4: Como resultado del análisis de riesgos realizado en la fase anterior, se define una serie de proyectos propuestos para reducir los niveles de riesgo que sobrepasan el límite de riesgo aceptable definido por la empresa que corresponde a un valor de 3.

FASE 5: La quinta fase consiste en la realización de una auditoría interna para evaluar los niveles de cumplimiento y para ello nos apoyaremos en la documentación obtenida en la fase 2, en función de la declaración de aplicabilidad se validarán los documentos que permiten corroborar la implementación de controles, teniendo en cuenta el análisis diferencial definido en la primera fase podemos validar la evolución del cumplimiento con la ejecución de proyectos y por último se obtendrán un informe como resultado que permitirá dar un diagnóstico más adecuado y cuyas recomendaciones permitirán que el SGSI se fortalezca.

FASE 6: Por último, la fase de entrega de resultados que arrojará información notable que será utilizada en el informe que será comunicado a los directivos de la compañía.

1.4 Planificación del Trabajo

En la Figura 1 y la Figura 2, se muestran las actividades que componen cada fase y su duración

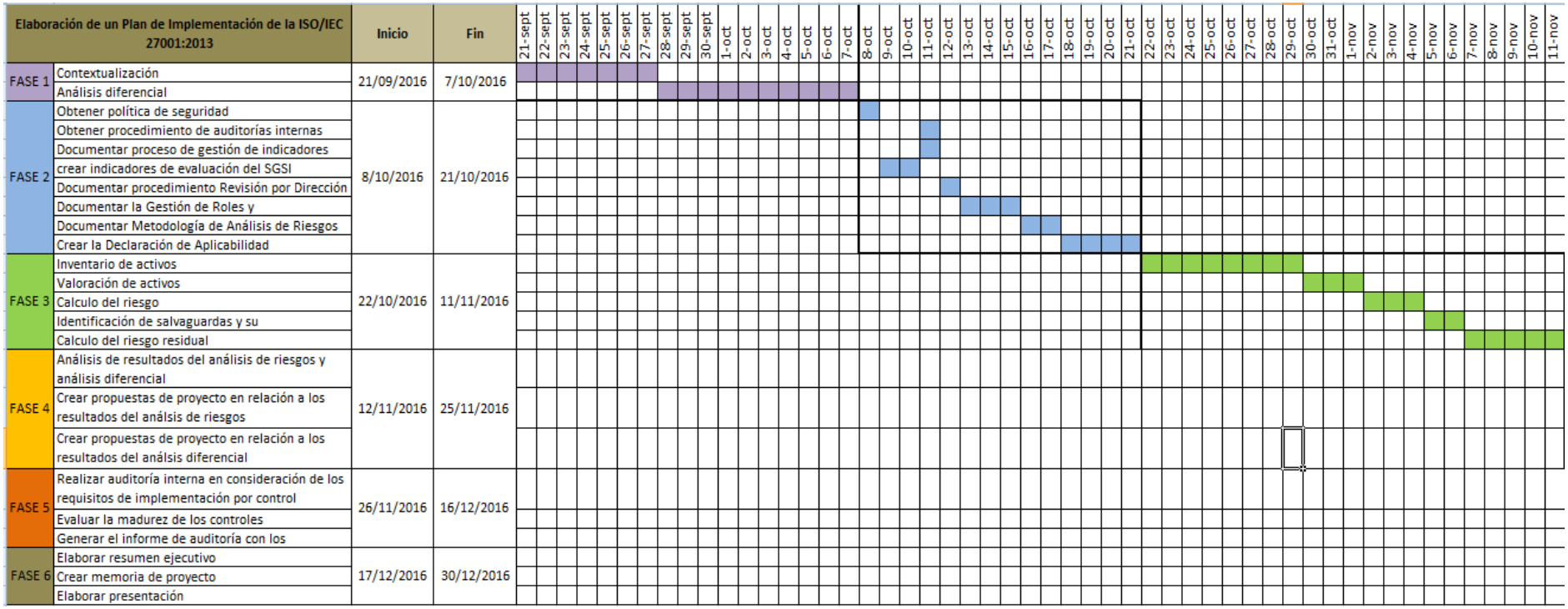

Figura 1: Cronograma de proyecto

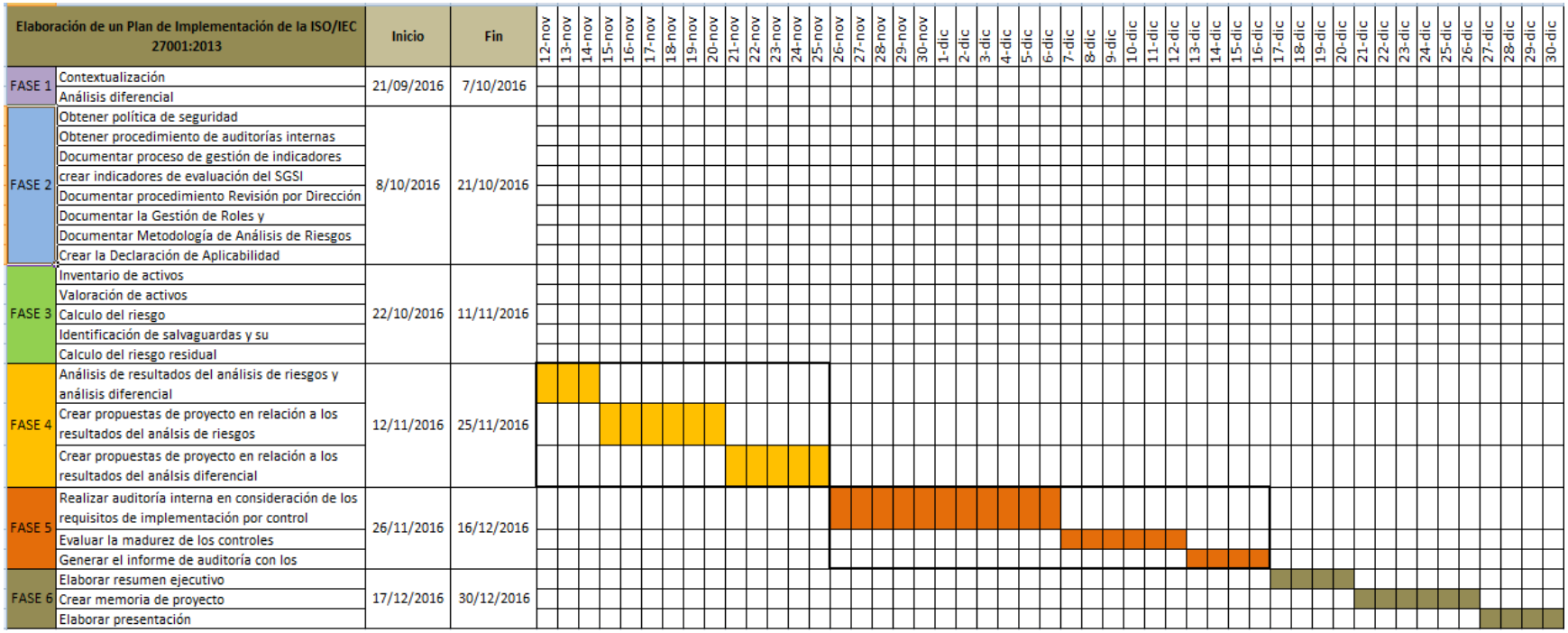

Figura 2: Cronograma de proyecto 2

2. Sistema de Gestión de Seguridad de la Información

2.1 Alcance del SGSI

2.1.1 Áreas involucradas

- *Área de administración documental:* Encargada de la administración y control de las garantías
- *Área de control de riesgos:* Encargada de consolidar y revisar los resultados de las auditorías realizadas, para informar a los responsables sobre problemas encontrados con posibles soluciones.
- *Área de auditoría:* Realizar y documentar auditorías
- *Área de seguridad de la información:* Encargada de crear políticas de seguridad para el modelo de seguridad existente
- *Área de Tecnología:* Se encarga de la administración, asignación y mantenimiento de los recursos tecnológicos de la compañía, también de realizar instalación de artefactos y de realizar las configuraciones necesarias.
- *Área de desarrollo:* Se encarga de diseñar, crear, hacer mantenimiento y dar soporte a los aplicativos de la compañía.
- *Área de pruebas:* Se encuentra encargado de realizar los planes de pruebas y las pruebas necesarias para aprobar el paso a producción de cambios realizados en los sistemas
- *Área de procesos:* Se encarga de crear, actualizar y documentar los diversos procesos de la compañía, así como de crear formatos para su gestión

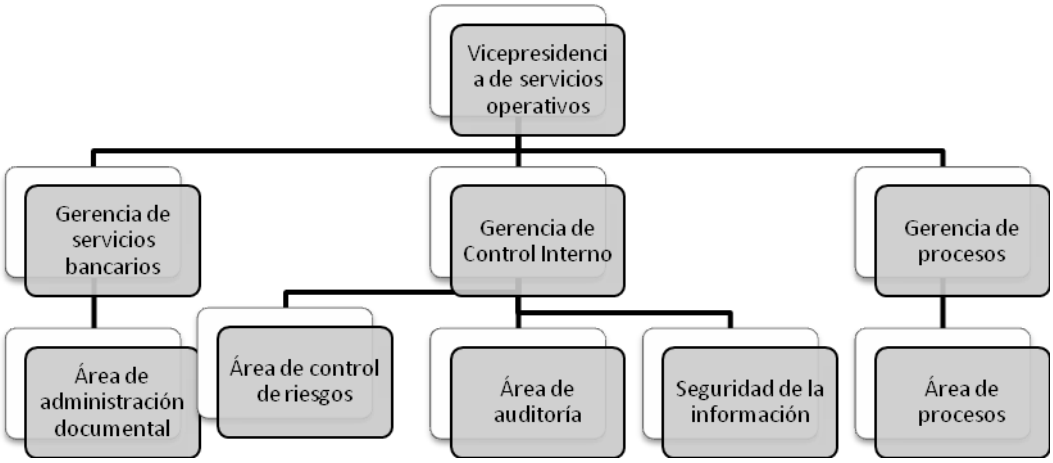

Figura 3: Áreas involucradas parte 1

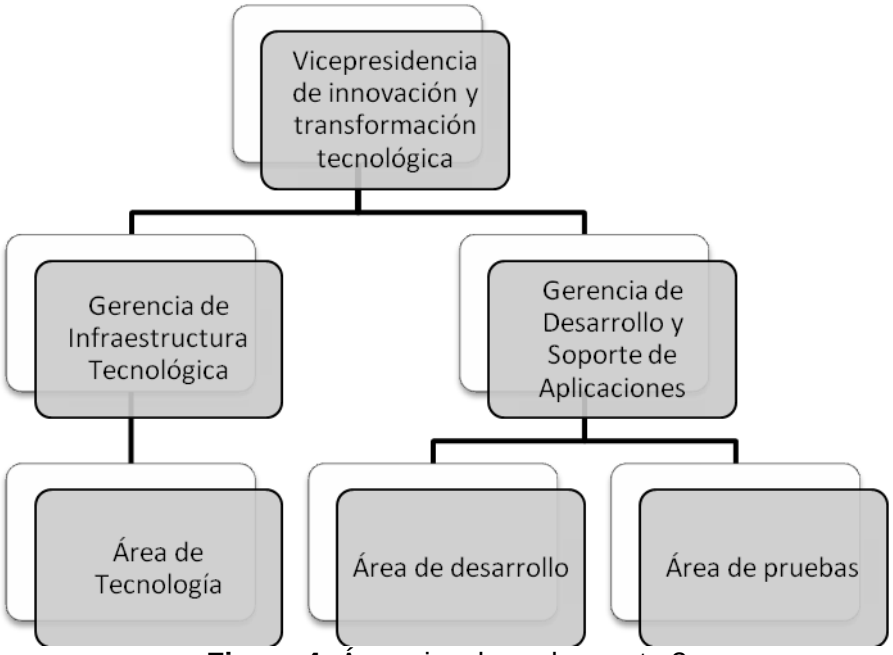

Figura 4: Áreas involucradas parte 2

2.1.2 Procesos involucrados

Mantenimiento de SW: Corresponde a un grupo de tareas que se llevan a cabo para crear, mejorar y/o ajustar funcionalidades que requiere la herramienta ya sea por motivos de negocio, inconsistencias o falencias del sistema.

Administración, disponibilidad y capacidad de la infraestructura tecnológica: Encargado de realizar las actividades administrativas necesarias para garantizar la disponibilidad y capacidad de los recursos y servicios tecnológicos utilizados.

Administración de operaciones: Se encuentra relacionado a las tareas operativas que realiza personal calificado para correr procesos no automatizados.

Seguridad de los sistemas: Orientado a una protección de sistemas mediante el uso de herramientas tales como IMPERVA, ARCIGHT, entre otros y el análisis de los resultados obtenidos para informar a los responsables sobre la detección de problemas y vulnerabilidades en busca de soluciones. NOTA: De momento no existe una protección como tal de activos de información basado en riesgos específicamente

Seguridad de la información: Su misión es la creación de políticas de seguridad

Auditoría interna: Es un proceso a cargo de la contraloría interna para auditar tanto los procesos de sistemas como el proceso de administración y gestión documental

Administración de instalaciones: Enfocado en la adecuación de instalaciones físicas donde se encuentran ubicados los servidores, equipos de computo, entre otros.

Gestión de procesos: Enfocado en la creación, actualización y documentación de procesos según las necesidades de la compañía.

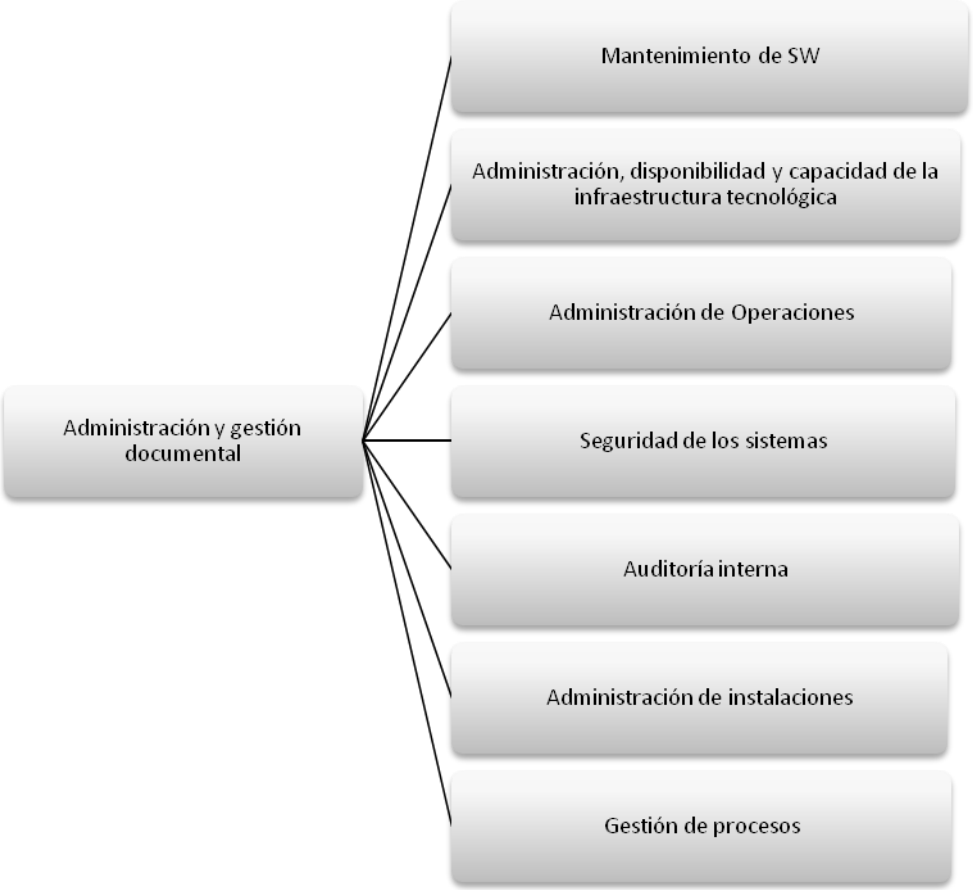

Figura 5: Procesos involucrados

2.1.3 Aplicativos involucrados

El aplicativo SAAG (Sistema de Administración de Avales y Garantías) consta de un modelo de tres capas, la primera de ellas es la capa de presentación (Interfaz gráfica) cuyo desarrollo es llevado a cabo en páginas WEB que están Instaladas en el servidor de aplicaciones para tal fin, el acceso principal es Invocado a través de la intranet por los usuarios; la segunda capa es el servidor de aplicaciones en sí, que además de alojar las páginas se encarga de la lógica, el procesamiento de las

transacciones, la concurrencia, y el acceso a usuarios; por último se encuentra la tercera capa que consiste en el soporte de datos.

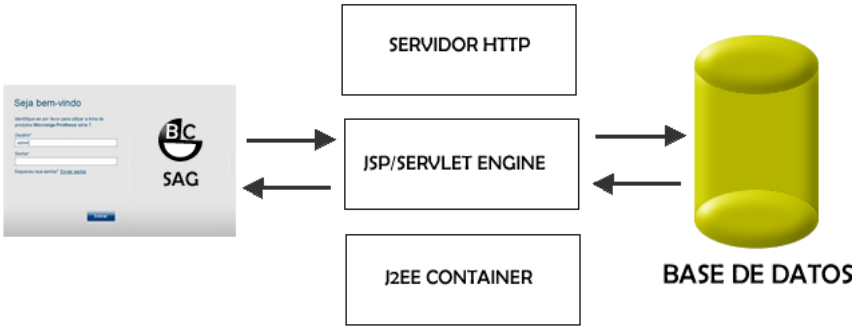

Figura 6: Estructura del aplicativo

Usuarios de oficinas: Consultan información sobre el estado de las garantías de los clientes y solicitan garantías o documentos en préstamos
Usuarios CAG: Son los usuarios que hacen parte del Centro de Administración de garantías con perfiles asociados como el creador de garantías, verificador de garantías, generador de reportes, custodio de garantías, perfil de inventarios, entre otros.
Usuarios de cartera-cobranzas: Validan información asociada a clientes que presentan mora en sus créditos
Usuarios encargados de hacer desembolsos: Validar información específica al realizar su tareas

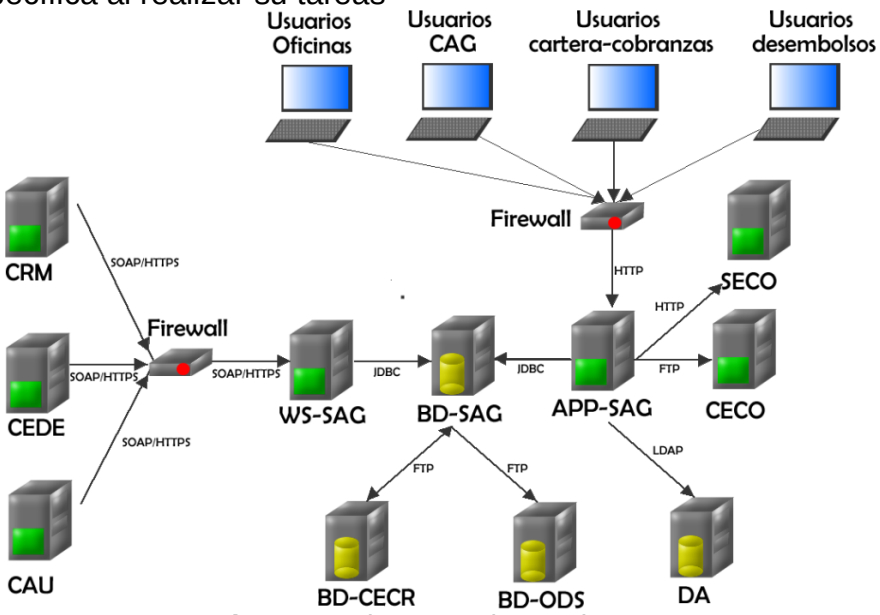

Figura 7: Diagrama de arquitectura

N°	APLICATIVO RELACIONADOS		RELACIÓN
1	CRM	Software para la administración de la relación con los clientes	Consultas y ejecución de tareas específicas mediante el consumo de servicios web
2	CEDE	Central de desembolsos	
3	CAU	Central de administración de usuarios	

4	CECR	Central de créditos	Una de las interacciones más importantes que tiene el aplicativo, corresponde a cartera consolidada aplicación en la cual se centraliza la información de los créditos y genera una interfaz mediante la cual se carga información de los créditos y las garantías a las cuales se encuentran asociados.
5	DA	Directorio activo	Al momento de ingresar al aplicativo se consume un servicio para autenticación de usuarios en uso de LDAP hacia el directorio activo (DA).
6	ODS	Almacén de datos operacionales	Existen procesos manuales que se ejecutan en un orden específico mediante .bats, los cuales corren procesos de base de datos que permiten el cargue de información, procesamiento de datos, generación y transmisión de archivos planos para aplicaciones tales como: ODS, CECR y CECO
7	CECO	Central contable	Para el envío de correos el aplicativo se conecta con un servidor que centraliza el envío de correos
8	SECO	Servidor de correos	

Tabla 1: Aplicativos relacionados con SAAG

2.2 Resumen de análisis diferencial

Al realizar el análisis diferencial inicial

Resumen Análisis diferencial ISO/IEC 27001:2013 Inicial Vs Actual

Dominio	Inicial	Actual
CONTEXTO DE LA ORGANIZACIÓN	38%	80%
LIDERAZGO	55%	85%
PLANIFICACIÓN	40%	80%
SOPORTE	60%	83%
OPERACIÓN	40%	78%
EVALUACIÓN DEL DESEMPEÑO	55%	75%
MEJORA	34,50%	70%

Tabla 2: Resumen Análisis diferencial ISO/IEC 27001:2013

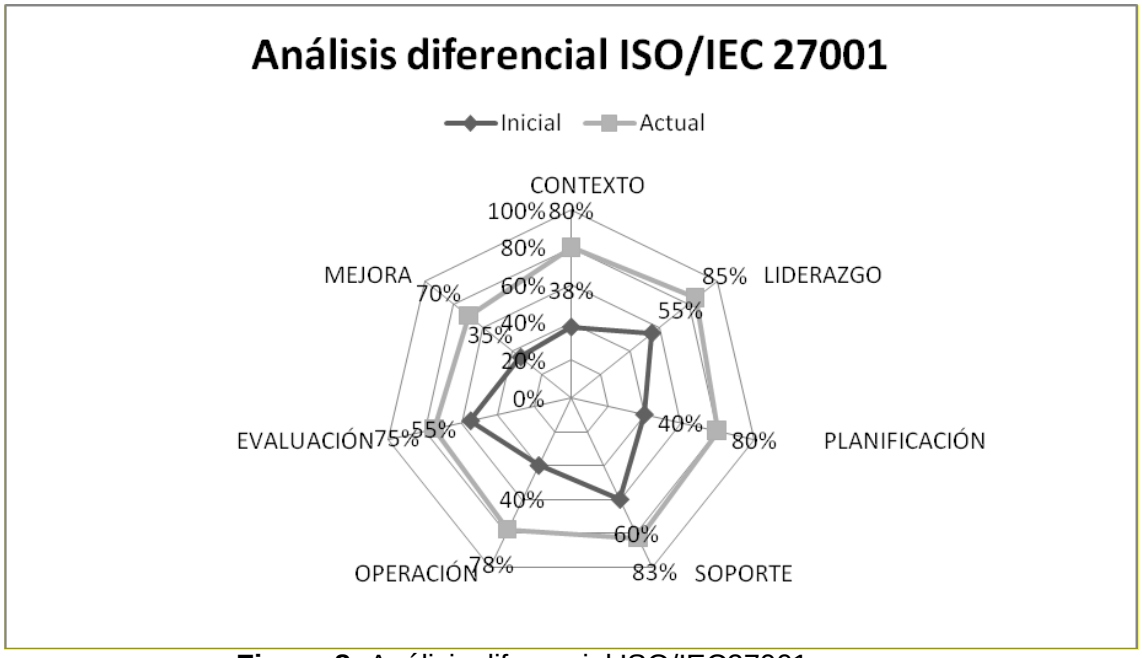

Figura 8: Análisis diferencial ISO/IEC27001

Resumen Análisis diferencial ISO/IEC 27002:2013 Inicial Vs Actual

Dominio	Inicial	Actual
Política de seguridad	65%	90%
Organización de la seguridad de la información	69%	85%
Seguridad en los recursos humanos	73%	92%
Gestión de activos	65,40%	90%
Control de acceso	63%	90%
Seguridad física y ambiental	62,00%	90%
Gestión de comunicaciones y operaciones	52,50%	90%
Adquisición, desarrollo y mantenimiento de Sistemas de Información	10%	90%
Gestión de incidentes	45,71%	91%
Gestión de continuidad de negocio	68%	88%
Cumplimiento	36,25%	90%

Tabla 3: Resumen Análisis diferencial ISO/IEC 27002:2013

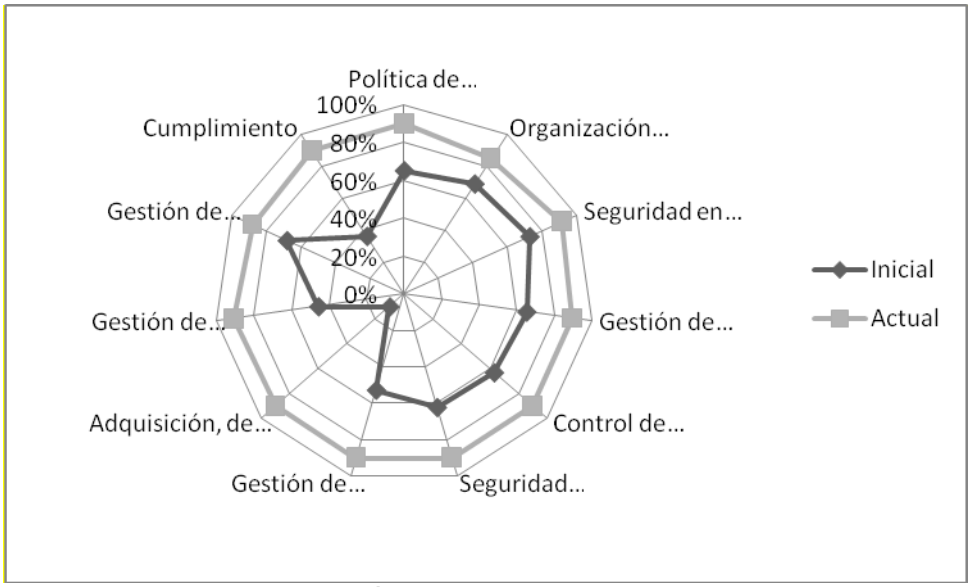

Figura 9: Análisis diferencial ISO/IEC27002

2.3 Sistema de Gestión documental

2.3.1 Política de seguridad

Anexo 1: Política de seguridad

2.3.2 Procedimiento de Auditorías Internas

Anexo 2: Procedimiento de auditorías internas

2.3.3 Gestión de Indicadores

Anexo 3: Procedimiento de Gestión de Indicadores

2.3.4 Procedimiento Revisión por Dirección

Anexo 4: Procedimiento Revisión por dirección

2.3.5 Gestión de Roles y Responsabilidades

Anexo 5: Gestión de Roles y Responsabilidades

2.3.6 Metodología de riesgos

Se adopta una metodología de riesgos basada en MAGERITH para analizar los riesgos de seguridad, inicialmente se definen los activos de información existentes en la organización e involucrados con el alcance, se realiza la respectiva valorización, se identifican las amenazas que pudieran afectar a cada activo, se define la frecuencia de amenaza y por último calculamos el riesgo. En consideración de los resultados obtenidos, la empresa define un umbral de riesgo aceptable que corresponde al valor 3. En consideración de las amenazas se identifican medidas preventivas (para evitar o reducir el riesgo) o reactivas (para reducir el impacto) que se denominan salvaguardas.

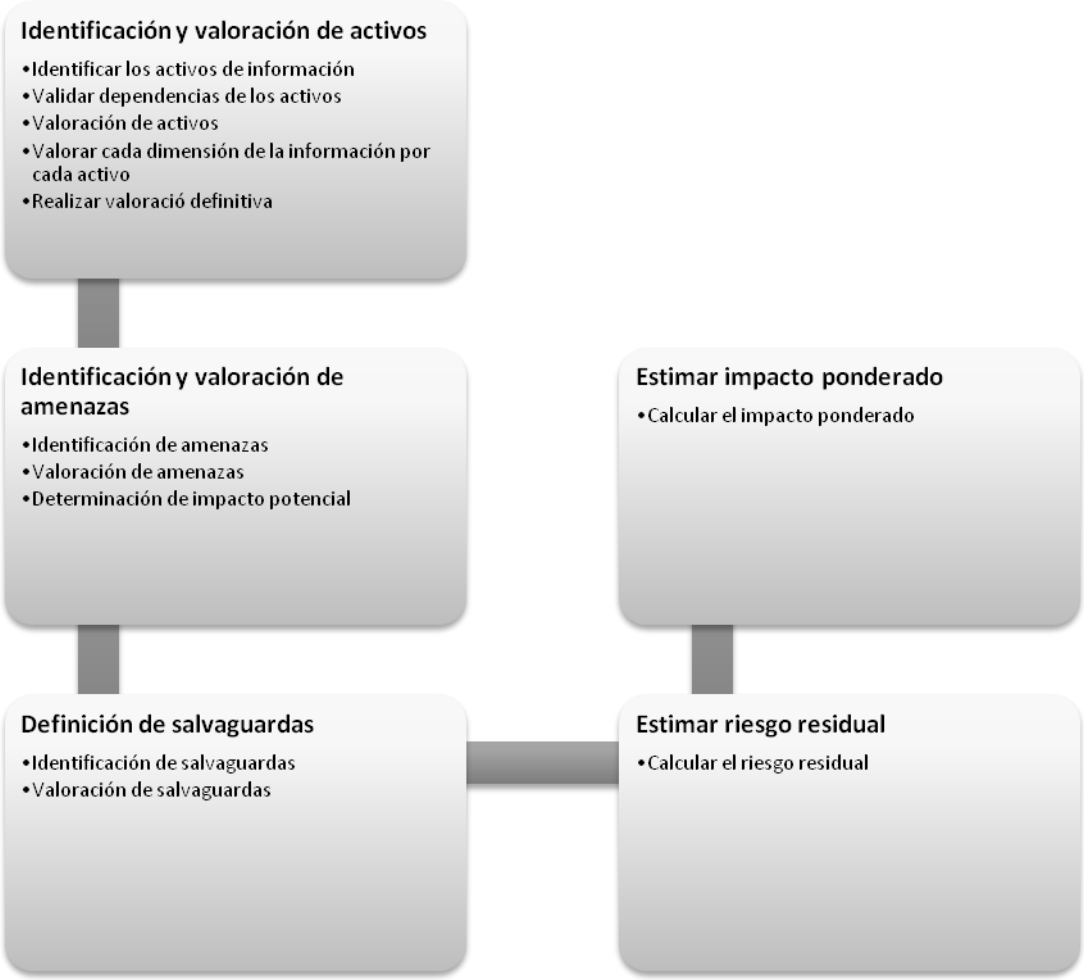

Figura 10: Metodología de análisis de riesgos

2.4 Análisis de riesgos

Para presentar los resultados del último análisis de riesgos realizado, centraremos nuestra atención en los riesgos que en un análisis preliminar superaron el nivel de riesgo aceptable que fue definido por la compañía, en otras palabras aquellos cuyo riesgo potencial es superior a 3, éste resumen se encuentra incluido en la Tabla 36 del presente documento. Los proyectos y las salvaguardas propuestas se enfocaron precisamente en mitigar estos riesgos, en la Tabla 37 se han resaltado los cambios presentados en los valores se muestra el cambio en las frecuencias cuya reducción ha permitido también la reducción del riesgo y de otro lado vemos que también han variado las cifras relacionadas al impacto. También se evidencia que no se presentaron cambios en algunas de las amenazas, puesto que algunos proyectos tenían por objetivo la planeación y viabilidad de soluciones definitivas que harán parte de futuros proyectos.

Activo	Amenaza	F	Valor					Impacto					Impacto potencial					Riesgo Residual				
			A	C	I	D	A	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
HW2	Fallos de servicios de comunicación	1	4	6	6	6	4				75%		0	0	0	4,5	0	0	0	0	4,5	0
	Caída del sistema por agotamiento de recursos	10	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	60	0
HW3	Caída del sistema por agotamiento de recursos	1	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	9	0
HW7	Denegación del servicio	1	6	4	6	4	4				100%		0	0	0	4	0	0	0	0	4	0
HW10	Caída del sistema por agotamiento de recursos	1	7	6	7	6	6				100%		0	0	0	6	0	0	0	0	6	0
HW12	Avería de origen Físico o lógico	1	1	9	9	7	1				100%		0	0	0	7	0	0	0	0	7	0
	Fallos de servicios de comunicación	1	1	9	9	7	1				75%		0	0	0	5,25	0	0	0	0	5,25	0
HW13	Corte del suministro eléctrico	1	1	6	3	4	1				100%		0	0	0	4	0	0	0	0	4	0
SW7	Errores de mantenimiento / actualización de programas (software)	1	3	7	7	7	2		60%		60%		0	4,2	0	4,2	0	0	4,2	0	4,2	0
SW8	Errores de mantenimiento / actualización de programas (software)	1	3	7	7	7	2		60%		60%		0	4,2	0	4,2	0	0	4,2	0	4,2	0
SW9	Errores de mantenimiento / actualización de programas (software)	1	7	7	7	7	7		80%		80%		0	5,6	0	5,6	0	0	5,6	0	5,6	0
A3	Introducción de información incorrecta	1	7	9	9	9	7			60%			0	0	5,4	0	0	0	0	5,4	0	0
	Denegación de servicio	1	7	9	9	9	7				60%		0	0	0	5,4	0	0	0	0	5,4	0
	Vulnerabilidades de los programas (software)	1	7	9	9	9	7		60%	60%		60%	0	5,4	5,4	0	4,2	0	5,4	5,4	0	4,2
D1	Escapes de información	1	7	9	9	9	7		50%				0	4,5	0	0	0	0	4,5	0	0	0
	Degradación de la información	1	7	9	9	9	7		80%	80%			0	7,2	7,2	0	0	0	7,2	7,2	0	0
D4	Introducción de información incorrecta	1	4	4	4	4	4			80%			0	0	3,2	0	0	0	0	3,2	0	0
D5	Introducción de información incorrecta	1	4	4	4	4	4			80%			0	0	3,2	0	0	0	0	3,2	0	0
D6	Introducción de información incorrecta	1	9	9	9	9	9			80%			0	0	7,2	0	0	0	0	7,2	0	0
D12	Fallos de servicios de comunicación	1	10	7	10	10	7				80%		0	0	0	8	0	0	0	0	8	0
	Acceso de personal no autorizado	1	10	7	10	10	7		80%				0	5,6	0	0	0	0	5,6	0	0	0
D13	Fallos de servicios de comunicación	0,1	9	4	9	9	4			100%	100%		0	0	9	9	0	0	0	0,9	0,9	0

	Encaminamiento de mensajes	1	7	7	7	7	7		100%				0	7	0	0	0	0	7	0	0	0
D15	Degradación de los soportes de almacenamiento de la información	1	7	7	9	9	4			50%	50%		0	0	4,5	4,5	0	0	0	4,5	4,5	0
	Alteración de la información	1	7	7	9	9	4	50%	100%	50%			3,5	7	4,5	0	0	3,5	7	4,5	0	0
D16	Errores de los usuarios	1	4	3	4	4	3			100%	100%		0	0	4	4	0	0	0	4	4	0
D17	Errores de los usuarios	1	4	3	4	4	3			100%	100%		0	0	4	4	0	0	0	4	4	0
D18	Errores de secuencia	1	10	7	10	10	7			100%	100%		0	0	10	10	0	0	0	10	10	0
D23	Vulnerabilidades de los programas (software)	1	9	6	9	6	9	80%		80%		80%	7,2	0	7,2	0	7,2	7,2	0	7,2	0	7,2
P1	Indisponibilidad del personal	1	9	9	0	9	0				50%		0	0	0	4,5	0	0	0	0	4,5	0
P5	Indisponibilidad del personal	1	7	7	0	7	0				50%		0	0	0	3,5	0	0	0	0	3,5	0
P8	Indisponibilidad del personal	1	8	8	0	8	0				50%		0	0	0	4	0	0	0	0	4	0

Tabla 4: Análisis de riesgos inicial con riesgos no aceptables

Activo	Amenaza	F	Valor					Impacto					Impacto potencial					Riesgo Residual				
			A	C	I	D	A	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
HW2	Fallos de servicios de comunicación	1	4	6	6	6	4				50%		0	0	0	3	0	0	0	0	3	0
	Caída del sistema por agotamiento de recursos	1	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	6	0
HW3	Caída del sistema por agotamiento de recursos	1	7	9	9	9	7				50%		0	0	0	4,5	0	0	0	0	4,5	0
HW7	Denegación del servicio	0,1	6	4	6	4	4				100%		0	0	0	4	0	0	0	0	0,4	0
HW10	Caída del sistema por agotamiento de recursos	1	7	6	7	6	6				50%		0	0	0	3	0	0	0	0	3	0
HW12	Avería de origen Físico o lógico	1	1	9	9	7	1				100%		0	0	0	7	0	0	0	0	7	0
	Fallos de servicios de comunicación	1	1	9	9	7	1				75%		0	0	0	5,25	0	0	0	0	5,25	0
HW13	Corte del suministro eléctrico	1	1	6	3	4	1				100%		0	0	0	4	0	0	0	0	4	0
SW7	Errores de mantenimiento / actualización de programas (software)	1	3	7	7	7	2		50%		80%		0	3,5	0	5,6	0	0	3,5	0	5,6	0
SW8	Errores de mantenimiento / actualización de programas (software)	1	3	7	7	7	2		50%		50%		0	3,5	0	3,5	0	0	3,5	0	3,5	0
SW9	Errores de mantenimiento / actualización de programas (software)	1	7	7	7	7	7		50%		50%		0	3,5	0	3,5	0	0	3,5	0	3,5	0

A3	Introducción de información incorrecta	0,1	7	9	9	9	7			40%			0	0	3,6	0	0	0	0	0,36	0	0
	Denegación de servicio	1	7	9	9	9	7				40%		0	0	0	3,6	0	0	0	0	3,6	0
	Vulnerabilidades de los programas (software)	1	7	9	9	9	7		40%	40%		45%	0	3,6	3,6	0	3,15	0	3,6	3,6	0	3,15
D1	Escapes de información	0,1	7	9	9	9	7		50%				0	4,5	0	0	0	0	0,45	0	0	0
	Degradación de la información	0,1	7	9	9	9	7		80%	80%			0	7,2	7,2	0	0	0	0,72	0,72	0	0
D4	Introducción de información incorrecta	0,1	4	4	4	4	4			80%			0	0	3,2	0	0	0	0	0,32	0	0
D5	Introducción de información incorrecta	0,1	4	4	4	4	4			80%			0	0	3,2	0	0	0	0	0,32	0	0
D6	Introducción de información incorrecta	0,1	9	9	9	9	9			80%			0	0	7,2	0	0	0	0	0,72	0	0
D12	Fallos de servicios de comunicación	0,1	10	7	10	10	7				100%		0	0	0	10	0	0	0	0	1	0
	Acceso de personal no autorizado	0,1	10	7	10	10	7		100%				0	7	0	0	0	0	0,7	0	0	0
D13	Fallos de servicios de comunicación	0,1	9	4	9	9	4			100%	100%		0	0	9	9	0	0	0	0,9	0,9	0
	Encaminamiento de mensajes	0,1	7	7	7	7	7		100%				0	7	0	0	0	0	0,7	0	0	0
D15	Degradación de los soportes de almacenamiento de la información	1	7	7	9	9	4			50%	50%		0	0	4,5	4,5	0	0	0	4,5	4,5	0
	Alteración de la información	1	7	7	9	9	4	50%	100%	50%			3,5	7	4,5	0	0	3,5	7	4,5	0	0
D16	Errores de los usuarios	0,1	4	3	4	4	3			100%	100%		0	0	4	4	0	0	0	0,4	0,4	0
D17	Errores de los usuarios	0,1	4	3	4	4	3			100%	100%		0	0	4	4	0	0	0	0,4	0,4	0
D18	Errores de secuencia	0,1	10	7	10	10	7			100%	100%		0	0	10	10	0	0	0	1	1	0
D23	Vulnerabilidades de los programas (software)	1	9	6	9	6	9	50%		50%		50%	4,5	0	4,5	0	4,5	4,5	0	4,5	0	4,5
P1	Indisponibilidad del personal	1	9	9	0	9	0				30%		0	0	0	2,7	0	0	0	0	2,7	0
P5	Indisponibilidad del personal	1	7	7	0	7	0				30%		0	0	0	2,1	0	0	0	0	2,1	0
P8	Indisponibilidad del personal	1	8	8	0	8	0				30%		0	0	0	2,4	0	0	0	0	2,4	0

Tabla 5: Riesgos calculados después de la ejecución de los proyectos propuestos de la fase 4

2.5 Proyectos planteados a la dirección para el futuro

Dominio	Política de seguridad		
Área Responsable	Área de seguridad		
Áreas involucradas	Áreas de Tecnología, Desarrollo y procesos		
Tiempo de ejecución	2 meses		
Objetivos/ Controles/Amenazas			
N°	Descripción		
A.5.1.1	Políticas para la seguridad de la información		
A.5.1.2	Revisión de las políticas para la seguridad de la información		
Actividades			
N°	**Actividad**	**Responsable**	**Costo**
P_1	Ajustar procedimiento de actualización de las políticas de seguridad en consideración de las tendencias de vulnerabilidades y amenazas	Áreas de Tecnología, Desarrollo y procesos	

Tabla 6: Proyecto | Política de seguridad

Dominio	Organización de la seguridad de la información		
Área Responsable	Área de seguridad		
Áreas involucradas	Áreas de Tecnología, Desarrollo y procesos		
Tiempo de ejecución	6 meses		
Objetivos/ Controles/Amenazas			
N°	Descripción		
A.6.1.4	Contacto con grupos de interés especial		
A.6.1.5	Seguridad de la información en la gestión de proyectos		
Actividades			
N°	**Actividad**	**Responsable**	**Costo**
P2_1	Definir procedimiento para establecer contacto con grupos de interés	Área de Procesos	
P2_2	Establecer contacto con grupos de interés para estar a la vanguardia en temas de seguridad	Área de Tecnología y área de seguridad informática	500 €
P2_3	Capacitar al personal de Desarrollo de la aplicación en los principales aspectos de seguridad de la información que deben considerarse en un proyecto	Área de desarrollo	2400 €

Tabla 7: Proyecto |Organización de la seguridad de la información

Dominio	Seguridad en los recursos humanos		
Área Responsable	Área de seguridad		
Áreas involucradas	Todas las áreas incluidas en el alcance		
Tiempo de ejecución	6 meses		
Objetivos/ Controles/Amenazas			
N°	Descripción		
A.7.2.3	Proceso disciplinario		
Actividades			
N°	**Actividad**	**Responsable**	**Costo**
P2_1	Ajustar los procesos disciplinarios relacionados al incumplimiento de las	Área de Procesos	

	normas y políticas de seguridad		

Tabla 8: Proyecto | Seguridad en los recursos humanos

Dominio	Gestión de activos		
Área Responsable	Área de seguridad informática y de control de riesgos		
Áreas involucradas	Área de seguridad informática y de control de riesgos		
Tiempo de ejecución	6 meses		
Objetivos/ Controles/Amenazas			
N°	Descripción		
A.8.1.1	Inventario de activos		
A.8.1.2	Propiedad de los activos		
A.8.1.3	Uso aceptable de los activos		
A.8.1.4	Devolución de activos		
Actividades			
N°	**Actividad**	**Responsable**	**Costo**
P3_1	Crear indicadores que completen la evaluación de éste dominio	Área de seguridad informática y de control de riesgos	
P3_2	Crear procedimiento relacionado con la actualización del inventario de activos	Área de procesos	

Tabla 9: Proyecto | Gestión de activos

Dominio	Control de acceso		
Área Responsable	Área de seguridad informática y de control de riesgos		
Áreas involucradas	Área de seguridad informática y de control de riesgos		
Tiempo de ejecución	6 meses		
Objetivos/ Controles/Amenazas			
N°	Descripción		
A.9.2.1	Registro de usuarios		
A.9.2.2	Gestión de privilegios		
A.9.2.3	Gestión de contraseñas para usuario		
A.9.2.4	Revisión de los derechos de acceso de los usuarios		
A.9.3.1	Uso de contraseñas		
A.9.3.2	Equipo de usuario desatendido		
A.9.4.6	Control de conexión a las redes		
A.9.4.7	Control de enrutamiento en la red		
A.9.5.1	Procedimientos de ingreso seguro		
A.9.5.2	Identificación y autenticación de usuarios		
A.9.5.3	Sistema de gestión de contraseñas		
A.9.5.4	Uso de las utilidades del sistema		
A.9.5.5	Tiempo de inactividad de la sesión		
A.9.5.6	Limitación del tiempo de conexión		
A.9.6.1	Restricción de acceso a la información		
A.9.6.2	Aislamiento de sistemas sensibles		
A.13.1.1	Controles de red		
Actividades			
N°	**Actividad**	**Responsable**	**Costo**

P4_1	Crear indicadores que completen la evaluación de éste dominio	Área de seguridad informática y de control de riesgos	

Tabla 10: Proyecto | Control de acceso

Dominio	Seguridad física y ambiental		
Área Responsable	Área de seguridad informática y de control de riesgos		
Áreas involucradas	Área de seguridad informática y de control de riesgos		
Tiempo de ejecución	4 meses		
Objetivos/ Controles/Amenazas			
N°	Descripción		
	Todos los controles que corresponden a éste dominio		
Actividades			
N°	**Actividad**	**Responsable**	**Costo**
P5_1	Crear indicadores que completen la evaluación de éste dominio	Área de seguridad informática y de control de riesgos	

Tabla 11: Proyecto | Seguridad física y ambiental

Dominio	Gestión de comunicaciones y operaciones		
Área Responsable	Área de seguridad informática y de control de riesgos		
Áreas involucradas	Área de seguridad informática y de control de riesgos		
Tiempo de ejecución	4 meses		
Objetivos/ Controles/Amenazas			
N°	Descripción		
A.12.3.1	Respaldo de la información		
1	Avería de origen Físico o lógico	Equipo de computo (repositorio)	
2	Fallos de servicios de comunicación	Equipo de computo (repositorio)	
Actividades			
N°	**Actividad**	**Responsable**	**Costo**
P6_1	Licitación y solicitud de cotizaciones para adquirir servidor de acuerdo a las condiciones requeridas para que sirva de repositorio	Área de Tecnología	
P6_2	Compra y configuración de servidor	Área de Tecnología	6000 €
P6_3	Adquisición de licencias para herramienta de versionamiento ClearCase	Área de Tecnología	3000 €
P6_4	Instalación de herramienta ClearCase en equipos del área de desarrollo	Área de Tecnología	
P6_5	Capacitación para uso de la herramienta de ClearCase	Área de Tecnología	
P6_6	Ajuste para versionar código fuente en el nuevo servidor	Área de Desarrollo	
P6_7	Identificar los controles para los cuales pueden crearse indicadores	Área de seguridad informática y de control de riesgos	
P6_8	Crear los indicadores necesarios para completar la evaluación de éste dominio	Área de seguridad informática y de control de riesgos	

Tabla 12: Proyecto | Gestión de comunicaciones y operaciones

Dominio	Adquisición, desarrollo y mantenimiento de Sistemas de Información		
Área Responsable	Área de seguridad informática y de control de riesgos		
Áreas involucradas	Área de seguridad informática y de control de riesgos		
Tiempo de ejecución	4 meses		
Objetivos/ Controles/Amenazas			
N°	Descripción		
	Todos los controles que corresponden a éste dominio		
1	Caída del sistema por agotamiento de recursos	Servidor de BD (Desarrollo)	
		Servidor de BD (Pruebas)	
		Servidor de BD (Producción)	
2	Avería de origen Físico o lógico	Servidor de Aplicaciones (Desarrollo)	
Actividades			
N°	**Actividad**	**Responsable**	**Costo**
P7_1	Completar los procedimientos relacionados con éste dominio	Área de procesos	
P7_2	Crear los documentos mínimos necesarios para evidenciar la implementación de los controles incluidos en el presente dominio	Área de procesos	
P7_3	Programar tareas automáticas para eliminar archivos históricos innecesarios que pueden ser eliminados de los servidores de BD	Área de Tecnología	
P7_4	Licitación y solicitud de cotizaciones para adquirir servidor de acuerdo a las condiciones requeridas para que sirva como servidor de aplicaciones	Área de Tecnología	
P7_5	Compra y configuración de servidor	Área de Tecnología	9000 €
P7_6	Adquisición de licencias para herramienta de administración del servidor elegido	Área de Tecnología	3000 €
P7_7	Crear la documentación necesaria (manuales técnicos) para realizar el mantenimiento del servidor y la instalación de aplicaciones	Área de Tecnología	
P7_8	Migración del aplicativo para utilizar el nuevo servidor de aplicaciones	Área de Desarrollo	
P7_9	Realizar las pruebas correspondientes al funcionamiento general del aplicativo	Área de pruebas	
P7_10	Actualizar el manual del aplicativo en consideración de los cambios realizados en el aplicativo	Área de procesos	
P7_11	Servir de apoyo en piloto de la nueva versión del aplicativo	Área de administración documental	
P7_12	Gestionar la publicación del nuevo enlace de la intranet	Área de procesos	
P7_13	Realizar los ajustes requeridos a partir de los resultados del piloto	Área de Desarrollo	

Tabla 13: Proyecto | Adquisición, desarrollo y mantenimiento de Sistemas de Información

Dominio	Gestión de incidentes		
Área Responsable	Área de seguridad informática y de control de riesgos		
Áreas involucradas	Área de seguridad informática y de control de riesgos		
Tiempo de ejecución	4 meses		
Objetivos/ Controles/Amenazas			
N°	Descripción		
A.16.1.3	Notificación de puntos débiles de la seguridad		
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones		
A.16.1.5	Respuesta a los incidentes de seguridad		
Actividades			
N°	**Actividad**	**Responsable**	**Costo**
P7_1	Investigar si en el mercado existe una herramienta para gestionar hallazgos de seguridad o generados en auditoría y validar la viabilidad para su adquisición	Área de seguridad informática y de control de riesgos	

Tabla 14: Proyecto | Gestión de incidentes

Dominio	Gestión de continuidad de negocio		
Área Responsable	Área de seguridad informática y de control de riesgos		
Áreas involucradas	Área de seguridad informática y de control de riesgos		
Tiempo de ejecución	4 meses		
Objetivos/ Controles/Amenazas			
N°	Descripción		
A.17.1.4	Estructura para la planificación de la continuidad del negocio		
A.17.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio		
Actividades			
N°	**Actividad**	**Responsable**	**Costo**
P8_1	Capacitar al personal en los principales aspectos técnicos a considerar para gestionar procedimientos de éste tipo	Área de procesos Área de seguridad informática	3000 €
P8_2	Ajustar procedimientos relacionados con el dominio	Área de procesos Área de seguridad informática	
P8_3	Revisar si las pruebas de recuperación técnica corresponden con los esperado y ajustarlas de ser necesario	Área de seguridad informática, de tecnología y de desarrollo	

Tabla 15: Proyecto | Gestión de continuidad de negocio

2.6 Auditoría de cumplimiento

Anexo 6: INFORME AUDITORÍA INTERNA

3. Conclusiones

- El compromiso por parte de las directivas a permitido dar prioridad a la ejecución de las actividades de los proyectos propuestos, con lo cual se observa un notable avance en cuanto a la implementación de los controles descritos por la ISO/IEC 27002
- Por fortuna, la compañía ya había empezado a dar sus primeros pasos en cuanto a seguridad de la información se refiere y esto ha permitido que el proceso de involucrar al personal en el SGSI sea mucho más manejable
- El personal de las áreas de control de riesgos y de seguridad informática requieren de capacitaciones un poco más técnicas que permitan brindar un mayor aporte a la definición de procedimientos, políticas y normas
- El relacionarnos con grupos de interés que puedan informarnos a tiempo sobre temas de seguridad como nuevas amenazas, nuevas vulnerabilidades nos permite ir un paso más adelante y prevenir riesgos, lo cual es de gran ayuda
- Al igual que todo sistema, el SGSI propuesto requiere de un seguimiento adecuado para su evolución y todos podemos realizar aportes a su mejora continua
- Ahora la compañía cuenta con un plus considerable que puede verse incluso como ventaja competitiva, dado que muy pocas empresas de Colombia cuentan con la implementación de estos controles

4. Glosario

Acción correctiva: Es una medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI con el fin de prevenir que vuelva a presentarse. [17]

Acción preventiva: Corresponde a una Medida de tipo pro-activo orientada a prevenir potenciales no conformidades asociadas a la implementación y operación del SGSI. [17]

Aceptación del Riesgo: Se refiere a la decisión de aceptar un riesgo. [17]

Activo: Según [ISO/IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos del SGSI. Se pueden clasificar de la siguiente manera:

- Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en el SAAG. Ejemplo:

- Aplicaciones: Es todo el software que se utiliza para la gestión de la información. Ejemplo: SAAG (Sistema de Administración de Avales y Garantías).

- Personal: Es todo el personal relacionado con los sistemas de información de SAAG, el personal subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información del BANCO. Ejemplo: Pedro Pérez.

- Servicios: Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios. Ejemplo: Publicación de hojas de vida, solicitud de vacaciones.

-Tecnología: Son todos los equipos utilizados para gestionar la información y las comunicaciones Ejemplo: equipo de cómputo, servidores, etc.

- Instalaciones: Son todos los lugares en los que se alojan los sistemas de información. Ejemplo: Oficina, bodega de custodia.

- Equipamiento auxiliar: Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. Ejemplo: Aire acondicionado, destructora de papel. [17]

Administración de riesgos: Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular. [17]

Alcance: Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización. [17]

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre. [17]

Amenaza: Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización. [17]

Análisis de riesgos: Según [ISO/IEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo. [17]

Auditabilidad: Los activos de información deben tener controles que permitan su revisión. Permitir la reconstrucción, revisión y análisis de la secuencia de eventos. [17]

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular. [17]

Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización. [17]

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema. [17]

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, Propiedad que garantiza que la identidad de un sujeto o recurso es la que declara, Se aplica a entidades tales como usuarios, procesos, sistemas de información. [17]

Base de datos de gestión de configuraciones (CMDB, Configuration Management Database): Es una base de datos que contiene toda la información pertinente acerca de los componentes del sistema de información utilizado en una organización de servicios de TI y las relaciones entre esos componentes. Una CMDB ofrece una vista organizada de los datos y una forma de examinar los datos desde cualquier perspectiva que desee. En este contexto, los componentes de un sistema de información se conocen como elementos de configuración (CI). Un CI puede ser cualquier elemento imaginable de TI, incluyendo software, hardware, documentación y personal,

así como cualquier combinación de ellos. Los procesos de gestión de la configuración tratan de especificar, controlar y realizar seguimiento de elementos de configuración y los cambios introducidos en ellos de manera integral y sistemática. B57799: Estándar británico de seguridad de la información, publicado por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera es un conjunto de buenas prácticas para la gestión de la seguridad de la información –no es certificable- y la parte segunda especifica el sistema de gestión de seguridad de la información -es certificable- o La parte primera es el origen de ISO 17799 e ISO 27002 Y la parte segunda de ISO 27001. Como tal el estándar, ha sido derogado ya, por la aparición de estos últimos. [17]

Características de la Información: las principales características son la confidencialidad, la disponibilidad y la integridad. [17]

Checklist: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo, Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo. [17]

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas. [17]

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados. [17]

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda). [17]

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma. [17]

Denegación de servicios: Acción iniciada por una persona u otra causa que incapacite el hardware o el software, o ambos y después niegue el servicio. [17]

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa. [17]

Directiva: Según [ISO/IEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas. [17]

Disponibilidad: Según [ISO/IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada. [17]

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo. [17]

Evento: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad. [17]

Gestión de claves: Controles referidos a la gestión de claves criptográficas. [17]

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. [17]

Impacto: Resultado de un incidente de seguridad de la información. [17]

Incidente: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [17]

Información: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras. Puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones. [17]

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. [17]

Legalidad: El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al

Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información. [17]

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor. [17]

No conformidad grave: Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable. [17]

No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente. [17]

PDCA Plan-Do-Check-Act: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).
Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). [17]

Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro. [17]

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. [17]

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:20005): intención y dirección general expresada formalmente por la Dirección. [17]

Política dé escritorio despejado: La política de la empresa que indica a los funcionarios, contratista y demás colaboradores del SGSI, que deben dejar su escritorio libre de cualquier tipo de informaciones susceptibles de mal uso al finalizar el día. [17]

Protección a la duplicidad: La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la

duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha comprado de manera legal, el instalar un software de computadora en varias computadoras, o el subir la música a reproductores de audio digital para facilitar el acceso y escucharla. [17]

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias. [17]

Riesgo Residual: Según [ISOIIEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo. [17]

Salvaguarda: Véase: Control. [17]

Segregación de tareas: Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia. [17]

Seguridad de la información: Según [ISO/IEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas. [17]

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable. [17]

SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO/IEC 27001: 2013]: la parle de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.) [17]

Servicios de tratamiento de información: Según [ISO/IEC 27002:20005]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento. [17]

Spamming: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico. [17]

Sniffers: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos. [17]

Spoofing: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address. [17]

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo. [17]

Trazabilidad: Propiedad que garantiza que las acciones de una entidad se puede rastrear únicamente hasta dicha entidad. [17]

Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad. [17]

Usuario: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores del SGSI, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red del SGSI y a quienes se les otorga un nombre de usuario y una clave de acceso. [17]

Valoración de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos. [17]

Virus: tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario. [17]

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza. [17]

5. Bibliografía

- International Standards Organization, ISO/IEC 27001: Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la seguridad de la Información (SGSI) – Requisitos.
- International Standards Organization, ISO/IEC 27002: Tecnología de la Información – Técnicas de Seguridad – Código de práctica para la gestión de la seguridad de la información.

Referencias WEB

[1] http://www.iso27000.es/iso27002.html [27/12/2016]
[2] http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/511_fase_1_planificar_anlisis_diferencial_para_definicin_del_alcance_y_otras_actividades_de_planeacin.html [27/12/2016]
[3] http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html#02 [27/12/2016]
[4]http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf [27/12/2016]
[5]https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WFb5Xfk1_IU [27/12/2016]
[6] http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/511_fase_1_planificar_anlisis_diferencial_para_definicin_del_alcance_y_otras_actividades_de_planeacin.html [27/12/2016]
[7] http://186.116.129.40/gat/html/4_fase_ejecu/4_p6_FaseEjecucion.html [27/12/2016]
[8]http://repositorio.utn.edu.ec/bitstream/123456789/855/2/02%20IME%2029%20RESUMEN%20EJECUTIVO.pdf [27/12/2016]
[9]http://www.corporacionloprado.cl/Docs/SGC%202013.1/control%20y%20mejora/auditoria%20interna/Auditorias%20al%20sgc%2005.pdf [27/12/2016]
[10]http://www.uca.es/recursos/doc/Gabinete_Ordenacion_Acade/Sistema_Gestion_Calidad/1861080242_232012145434.pdf [27/12/2016]
[11]http://www.mapama.gob.es/es/ganaderia/temas/sanidad-animal-e-higiene-ganadera/ANALISIS_DE_RIESGOS__J_M_Vizcaino_tcm7-5638.pdf [27/12/2016]
[12]https://www.datasec-soft.com/es/empresa/politica-de-seguridad-de-la-informacion [27/12/2016]
[13]https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf [27/12/2016]
[14]http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/324_paso_4_salvaguardias.html [27/12/2016]
[15]http://www.securityartwork.es/2012/04/26/analisis-de-riesgos-con-magerit-en-el-ens-ii/ [27/12/2016]
[16]http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf [27/12/2016]
[17]http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Sistema-Seguridad-Informacion.pdf

6. Anexos

ANEXO 1: POLÍTICA DE SEGURIDAD

POLÍTICA DE SEGURIDAD PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO

Definir los elementos que hacen parte de la política de seguridad que deben darse a conocer y cumplir a los funcionarios que se encuentran relacionados a los sistemas de información que dan soporte al aplicativo de administración de garantías del banco.

ALCANCE

Las políticas de seguridad de la información se aplicarán a todo aspecto que deba ser realizado por los directivos, funcionarios y contratistas que presten sus servicios al aplicativo de Administración de garantías para el apropiado cumplimiento de sus funciones y conseguir un nivel adecuado de cada una de las dimensiones que hacen parte de la información (Disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad).

TERMINOS Y DEFINICIONES

Acción correctiva: Es una medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI con el fin de prevenir que vuelva a presentarse.

Acción preventiva: Corresponde a una Medida de tipo pro-activo orientada a prevenir potenciales no conformidades asociadas a la implementación y operación del SGSI.

Aceptación del Riesgo: Se refiere a la decisión de aceptar un riesgo.

Activo: Según [ISO/IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos del SGSI. Se pueden clasificar de la siguiente manera:

- Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en el SAAG. Ejemplo:

- Aplicaciones: Es todo el software que se utiliza para la gestión de la información. Ejemplo: SAAG (Sistema de Administración de Garantías).

- Personal: Es todo el personal relacionado con los sistemas de información de SAAG, el personal subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información del BANCO. Ejemplo: Pedro Pérez.

- Servicios: Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios. Ejemplo: Publicación de hojas de vida, solicitud de vacaciones.

-Tecnología: Son todos los equipos utilizados para gestionar la información y las comunicaciones Ejemplo: equipo de cómputo, servidores, etc.

- Instalaciones: Son todos los lugares en los que se alojan los sistemas de información. Ejemplo: Oficina, bodega de custodia.

- Equipamiento auxiliar: Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. Ejemplo: Aire acondicionado, destructora de papel.

Administración de riesgos: Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

Alcance: Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza: Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Según [ISO/IEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditabilidad: Los activos de información deben tener controles que permitan su revisión. Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, Propiedad que garantiza que la identidad de un sujeto o recurso es la que declara, Se aplica a entidades tales como usuarios, procesos, sistemas de información.

Base de datos de gestión de configuraciones (CMDB, Configuration Management Database): Es una base de datos que contiene toda la información pertinente acerca de los componentes del sistema de información utilizado en una organización de servicios de TI y las relaciones entre esos componentes. Una CMDB ofrece una vista organizada de los datos y una forma de examinar los datos desde cualquier perspectiva que desee. En este contexto, los componentes de un sistema de información se conocen como elementos de configuración (CI). Un CI puede ser cualquier elemento imaginable de TI, incluyendo software, hardware, documentación y personal, así como cualquier combinación de ellos. Los procesos de gestión de la configuración tratan de especificar, controlar y realizar seguimiento de elementos de configuración y los cambios introducidos en ellos de manera integral y sistemática. B57799: Estándar británico de seguridad de la información, publicado por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera es un conjunto de buenas prácticas para la gestión de la seguridad de la información –no es certificable- y la parte segunda especifica el sistema de gestión de seguridad de la información -es certificable- o La parte primera es el origen de ISO 17799 e ISO 27002 Y la parte segunda de ISO 27001. Como tal el estándar, ha sido derogado ya, por la aparición de estos últimos.

Características de la Información: las principales características son la confidencialidad, la disponibilidad y la integridad.

Checklist: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo, Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC 13335-1:2004]:" característica/propiedad

por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

Denegación de servicios: Acción iniciada por una persona u otra causa que incapacite el hardware o el software, o ambos y después niegue el servicio.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva: Según [ISO/IEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Según [ISO/IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Impacto: Resultado de un incidente de seguridad de la información.

Incidente: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras. Puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Legalidad: El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No conformidad grave: Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

PDCA Plan-Do-Check-Act: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).
Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:20005): intención y dirección general expresada formalmente por la Dirección.

Política dé escritorio despejado: La política de la empresa que indica a los funcionarios, contratista y demás colaboradores del SGSI, que deben dejar su escritorio libre de cualquier tipo de informaciones susceptibles de mal uso al finalizar el día.

Protección a la duplicidad: La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha comprado de manera legal, el instalar un software de computadora en varias computadoras, o el subir la música a reproductores de audio digital para facilitar el acceso y escucharla.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Residual: Según [ISOIIEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

Salvaguarda: Véase: Control.

Segregación de tareas: Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Según [ISO/IEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO/IEC 27001: 2013]: la parle de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Servicios de tratamiento de información: Según [ISO/IEC 27002:20005]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

Spamming: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

Sniffers: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

Spoofing: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

Trazabilidad: Propiedad que garantiza que las acciones de una entidad se puede rastrear únicamente hasta dicha entidad.

Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

Usuario: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores del SGSI, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red del SGSI y a quienes se les otorga un nombre de usuario y una clave de acceso.

Valoración de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Virus: tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

RESPONSABLES

JEFE DEL ÁREA DE AUDITORÍA– REPRESENTANTE DE LA DIRECCIÓN
Es la persona encargada de dar a conocer éste procedimiento al interior de la organización, garantizar su cumplimiento y asegurar que se preste el debido entrenamiento al personal para adquirir el conocimiento y la aplicabilidad del mismo.

EQUIPO AUDITOR
Personal competente de diversas áreas que conforma un equipo de trabajo encargado de llevar a cabo la auditoría de acuerdo a los lineamientos definidos en el presente documento

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
Estas políticas se definen para que sirvan de herramienta organizacional y sensibilizar sobre la importancia y tratamiento de la información a cada uno de los funcionarios y puedan desarrollar adecuadamente sus labores.

Objetivo:
Establecer las directrices necesarias para asegurar las dimensiones que hacen parte de la información (Disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) relacionada con el alcance definido en el Sistema de Gestión de la Información.

Aplicabilidad:
Éstas políticas aplican a todo el personal del BANCO

Directrices:
Verificar la definición, implementación, revisión y actualización de las políticas de seguridad de la información

Apoyar el diseño, programación y realización de los programas de auditoría del sistema de gestión de seguridad de la información, los cuales estarán a cargo de la Gerencia de Control Interno.

Todo aplicativo informático o software debe ser aprobado por el Área de Tecnología en caso de no tratarse de un desarrollo en casa

Todo aplicativo del BANCO debe contar con un firewall o dispositivo de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros.

La conexión remota a equipos del BANCO solo podrá realizarse a través de VPN (red virtual privada)

Cada jefe de área debe asegurarse que todos los procedimientos de seguridad de la información dentro de su área, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información del SGSI

POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACION

El BANCO se encargará de establecer un esquema de seguridad de la información para el alcance definido, donde existan roles y responsabilidades definidos que incluyan actividades administrativas, operacionales y de gestión de la seguridad de la información.

NORMAS PARA LA JUNTA DIRECTIVA

La Junta Directiva se encarga de crear los roles y asignar las responsabilidades a cada funcionario que se encuentre relacionado con la seguridad de la información a nivel directivo y operativo.

La Junta Directiva debe Definir el procedimiento de contacto con las autoridades de ser requerido, incluyendo los responsables a quienes debe contactarse

La Junta Directiva debe encargarse de revisar y aprobar las políticas de seguridad de la información incluidas en el presente documento

La Junta Directiva debe encargarse de promover activamente una cultura de seguridad de la información en la organización.

La Junta Directiva debe incentivar la divulgación de las políticas de Seguridad de la información presentes en éste documento a los funcionarios relacionados en el alcance definido.

NORMAS PARA EL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información debe actualizar y presentar ante la Junta Directiva las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.

El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

El Comité de Seguridad de la Información debe verificar el cumplimiento de las políticas de seguridad de la información mencionadas en éste documento

NORMAS PARA EL ÁREA DE CONTROL DE RIESGOS

El Área de Control de Riesgos debe liderar la generación de lineamientos para gestionar la seguridad de la información del BANCO y el establecimiento de controles necesarios (técnicos, físicos y administrativos) derivados de análisis de riesgos de seguridad.

La Área de Control de Riesgos debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.

NORMAS PARA EL ÁREA DE CONTROL INTERNO

El Área de Control Interno debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información del BANCO con el objetivo de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.

El Área de Control Interno debe ejecutar revisiones totales o parciales de los procesos o pareas con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.
El Área de Control Interno debe encargarse de informar a las áreas responsables los hallazgos de las auditorías.

NORMAS PARA EL ÁREA DE TECNOLOGIA

El Área de Tecnología debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración que se encuentren relacionados en el alcance del Sistema de Gestión de Seguridad de la información. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y segregadas apropiadamente.

NORMAS PARA TODOS LOS FUNCIONARIOS

Los funcionarios y personal provisto por terceras partes que realicen labores para el BANCO relacionadas en el alcance, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

POLITICA PARA USO DE DISPOSITIVOS MOVILES

El BANCO definirá las condiciones para el manejo responsable de dispositivos móviles de uso institucional y/o personal que utilicen los servicios de la organización .

NORMAS PARA EL ÁREA DE TECNOLOGIA

Debe investigar y validar las opciones de protección para dispositivos móviles de la organización o personales que hagan uso de los servicios provistos por la organización

NORMAS PARA TODOS LOS FUNCIONARIOS

Todo usuario debe evitar el uso de dispositivos móviles de la organización en lugares que no brinden garantías de seguridad física suficientes para evitar su pérdida o robo

Ningún usuario debe modificar las condiciones de seguridad realizadas en los dispositivos ni desinstalar software existente al momento de ser entregado

POLITICA PARA USO DE CONEXIONES REMOTAS

El BANCO establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a los recursos tecnológicos de la organización; de igual manera, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

NORMAS PARA EL ÁREA DE CONTROL DE RIESGOS Y EL ÁREA DE TECNOLOGÍA

El Área de Control de Riesgos, de manera conjunta con El Área de Tecnología, deben analizar y aprobar los métodos de conexión remota a la plataforma tecnológica del BANCO.

NORMAS PARA EL ÁREA DE TECNOLOGIA

El Área de Tecnología debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica del BANCO.
El Área de Tecnología debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
El Área de Tecnología debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica del BANCO de manera permanente.

NORMAS PARA EL ÁREA DE CONTROL INTERNO
El Área de Control Interno debe, dentro de su autonomía, realizar auditorías sobre los controles implantados para las conexiones remotas a la plataforma tecnológica del BANCO.

NORMAS PARA TODOS LOS FUNCIONARIOS
Los funcionarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica del BANCO y deben acatar las condiciones de uso establecidas para dichas conexiones
Los funcionarios únicamente deben establecer conexiones remotas en computadores personales utilizando la Red virtual privada VPN y utilizando el usuario de red y combinación de la clave de usuario y la clave generada por token.

POLÍTICAS DE SEGURIDAD DEL PERSONAL

Política relacionada con la vinculación de funcionarios
Dada la importancia de los funcionarios en el cumplimiento de los objetivos misionales de la organización, el BANCO muestra especial interés en incorporar personal altamente calificado y debe garantizarse que su vinculación se realice utilizando un proceso formal de selección, en consideración de las leyes vigentes, de los roles y las funciones a desempeñar.

NORMAS PARA EL ÁREA DE TALENTO HUMANO
Debe validarse toda información suministrada por los candidatos antes se de ser contratados para confirmar su veracidad.
Debe certificar que todo funcionario nuevo firme un Acuerdo y/o Clausula de confidencialidad y la aceptación de políticas de seguridad de la información, los cuales deben archivarse junto a toda la documentación del funcionario.

NORMAS PARA FUNCIONARIOS CON PERSONAS A CARGO
Antes de permitir el acceso a recursos físicos y/o tecnológicos se debe validar la aceptación firmada de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas por parte del contratista

NORMAS PARA PERSONAL CONTRATISTA
Cada contratista debe firmar un Acuerdo y/o Clausula de confidencialidad y la aceptación de políticas de seguridad de la información, antes de otorgar permisos de acceso a recursos físicos y/o tecnológicos

Deben garantizar el cumplimiento de los documentos firmados que fueron relacionados en la norma previa

Política aplicable durante la vinculación de funcionarios directos y de personal contratista
Con ánimos de proteger la información, el BANCO muestra su compromiso promoviendo planes de comunicación para elevar la concientización en temas de seguridad de la información y ejecutando procesos disciplinarios (de ser necesario) cuando se incumplan las políticas establecidas en relación a ello.

NORMAS PARA LA JUNTA DIRECTIVA
La Junta Directiva debe mostrarse comprometida con la seguridad de la información a partir de la aprobación de políticas, normas entre otras directrices necesarias.
Debe dar a conocer la importancia de la información y su seguridad a los funcionarios y proveedores del BANCO, mediante la toma de conciencia y el cumplimiento de las políticas, normas, procedimiento y estándares definidos.
Es deber de la Junta Directiva definir el proceso disciplinario o incluir políticas de seguridad más importantes

NORMAS PARA EL ÁREA DE CONTROL DE RIESGOS
Diseñar un plan de comunicaciones y ponerlo en práctica para crear conciencia acerca de la seguridad de la información, con el objetivo de proteger la información adecuadamente

POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN
Política de responsabilidad por los activos
El BANCO debe asegurarse de asignar a cada área responsabilidades sobre los activos de información que manejan, previo inventario, clasificación y conforme a los requisitos definidos por el área de Control de Riesgos.

NORMAS PARA LOS PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN
Los propietarios de activos de información como responsables de la misma podrán administrar los permisos de acceso relacionados con ellos.
Validar con periodicidad definida la matriz de acceso para validar que los usuarios y permisos asignados correspondan
Los propietarios de los activos de información deben estar conscientes y preparados ante auditorías y revisiones de cumplimiento que pueden ser internas o externas.

NORMAS PARA ÁREA DE TECNOLOGIA
El Área de Tecnología como responsable de la infraestructura tecnológica del BANCO, debe garantizar una apropiada operación y administración.
Se hará responsable de adecuar instalaciones físicas según las normas que apliquen
Debe generar las copias de seguridad cuando se requieran (por cambio de equipos) o se soliciten

NORMAS PARA JEFES DE ÁREA

Se encargarán de autorizar el uso de los recursos requeridos por los funcionarios
Deben recibir los recursos asignados a sus funcionarios cuando ellos se retiren o sean trasladados

NORMAS PARA TODOS LOS FUNCIONARIOS
Utilizar los recursos tecnológicos asignados de forma ética y dando cumplimiento a las leyes y reglas vigentes
Dar adecuado y eficiente uso de los recursos asignados, limitando su uso a actividades propias de la organización.
No hacer uso de software no autorizado o del cual no se tenga la licencia correspondiente
Los funcionarios que cambian de área o se desvinculan, deben realizar una entrega formal del puesto al Jefe de área, y solicitar el paz y salvo tras la entrega de los recursos

Política para uso de tokens de seguridad
El BANCO definirá las condiciones para el manejo adecuado de los tokens de seguridad de los procesos y funcionarios responsables

NORMA PARA LAS ÁREAS USUARIAS DE TOKENS DE SEGURIDAD
El jefe de cada área realizará las solicitudes diligenciando el formato que corresponda y limitando los accesos en la solicitud.

NORMA PARA LOS ADMINISTRADORES DE TOKENS DE SEGURIDAD
Solicitar a la entidad proveedora los tokens necesarias de acuerdo a los requerimientos definidos y diligenciar la documentación y copias necesarias para su adquisición
Validar la información de formatos de solicitud, solicitar las modificaciones pertinentes y procesarlas, guardando la información necesaria
Recibir, almacenar y activar los tokens en los portales que correspondan
Crear usuarios y perfiles de acceso, configurar los accesos permitidos por cada perfil según la asignación realizada
Enviar de manera segura (tula o sobre sellado) y formalizar la entrega de los dispositivos mediante formato a cada usuario donde se indique entre otras cosas el serial del token
En caso de robo o perdida informar a las entidades emisoras para su respectivo bloqueo y reposición
Ante fallas en los dispositivos deben encargarse de gestionar el reemplazo de los dispositivos

NORMA PARA LOS USUARIOS DE TOKENS DE SEGURIDAD
Se hará responsable del dispositivo y éste será incluido dentro del inventario físico que lleve el usuario
Solicitar cuenta en los portales para uso de tokens y velar por la seguridad física del dispositivo (mantener en lugar seco y limpio, evitar golpes, exposición a temperaturas extremas) y de la clave obtenida
Devolver el token en perfecto estado y funcionamiento a los administradores de tokens al retirarse del BANCO como requisito para obtener su paz y salvo

El token, la cuenta y la contraseña es de uso personal, exclusivo e intransferible, por tanto el acceso no deberá ser realizado por alguien diferente del funcionario asignado

En caso de pérdida, robo o daño en el dispositivo informar a los administradores de token

Los usuarios serán directamente responsables administrativa, disciplinaria y económicamente ante eventos irregulares por las transacciones realizadas con su cuenta clave y token asignado.

Política de uso de periféricos y medios de almacenamiento

El área de Tecnología y el área de Control de Riesgos se encargará de reglamentar el uso de periféricos y medios de almacenamiento en los recursos tecnológicos, de acuerdo a las tareas y necesidades de cada usuario

NORMA PARA LAS ÁREAS DE TECNOLOGÍA Y ÁREA DE CONTROL DE RIESGOS

Deben definir las condiciones de uso de los periféricos y medios de almacenamiento tecnológico del BANCO

NORMA PARA EL ÁREA DE TECNOLOGÍA

Implantar los controles necesarios para regular el uso de los periféricos y medios de almacenamiento tecnológicos de acuerdo a las condiciones de uso definidas

Generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento del BANCO, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

NORMA PARA EL ÁREA DE CONTROL DE RIESGOS

Autorizar el uso de periféricos dependiendo del cargo del funcionario y los temas que trabajante.

NORMAS PARA TODOS LOS FUNCIONARIOS

Conocer las condiciones de uso de periféricos y medios de almacenamiento que le fueron asignados y acogerse a ellas

No alterar las configuraciones realizadas a los periféricos y medios de almacenamiento establecidas por el área de Tecnología

No utilizar periféricos y/o medios de almacenamiento externos en los recursos tecnológicos de la organización

POLÍTICAS DE CONTROL DE ACCESO

POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED

El BANCO como dueño y responsable de la información administrada debe velar para que las redes por donde viaja la información estén protegidas de accesos no autorizados mediante el uso de los mecanismos necesarios

NORMA PARA EL ÁREA DE TECNOLOGÍA

Definir el procedimiento de autorización y los controles necesarios para proteger el accedo a redes de datos y recursos tecnológicos del BANCO

Asegurar que las redes inalámbricas del instituto cuenten con métodos fuertes de autenticación para evitar accesos no autorizados

NORMA PARA EL ÁREA DE CONTROL DE RIESGOS

Se encargará de autorizar, crear o modificar cuentas de acceso a redes y recursos de red

Debe validar en forma periódica los controles de acceso y validar si se están restringiendo los accesos según los que fueron autorizados

NORMAS PARA TODOS LOS FUNCIONARIOS

Deben solicitar cuenta de usuario para tener acceso lógico a la red y contar con el acuerdo de confidencialidad firmado previamente

Los equipos que harán uso de la red deben cumplir con requisitos y controles mínimos de autenticación y sólo podrán utilizarse para realizar tareas que fueron autorizadas

POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

El BANCO debe definir privilegios para controlar el acceso lógico por usuarios o grupo de usuario a todo recursos tecnológico de la organización y debe velar para que funcionarios y contratistas tengan acceso limitado a los recursos que requieran para desarrollo de sus actividades y a las normas definidas para ello.

NORMA PARA EL ÁREA DE TECNOLOGÍA

Definir un procedimiento formal para la administración (creación, modificación, eliminación, bloqueo, desbloqueo, asignación y eliminación de permisos) de usuarios de los recursos tecnológicos

Hacer efectivas las solicitudes relacionadas con la administración de usuarios las cuales deben ser diligenciadas por los jefes inmediatos del usuario final

Definir lineamientos para configuración de contraseñas de acceso a los recursos tecnológicos del BANCO considerando aspecto tales como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

Asegurar que los permisos asignados por defecto y sin solicitud de por medio sean eliminados o inhabilitados

NORMAS PARA EL ÁREA DE CONTROL DE RIESGOS

Autorizar la creación y modificación de las cuentas de acceso a los recursos tecnológicos

NORMAS PARA LOS PROPIETARIOS DE ACTIVOS DE INFORMACIÓN

En conjunto con el área de Control de Riesgos definir perfiles y privilegios por cada uno

Verificar y validar de manera periódica las autorizaciones de accesos a los activos que tiene a su cargo

NORMAS PARA JEFES DE ÁREA

Deben realizar las solicitudes relacionadas con la administración de usuarios para los funcionarios que tienen a cargo conforme al procedimiento definido para ello

POLÍTICA DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

Todo usuario con acceso a los recursos tecnológicos debe realizar un uso adecuado y responsable de los mismo

NORMAS PARA TODOS LOS USUARIOS

Todo usuario será responsable de las actividades realizadas bajo el usuario y contraseña que le fueron asignados

No deben compartir su cuenta de usuario y contraseña con nadie, son de uso personal y exclusivo

Deben acogerse a los lineamientos de configuración de contraseñas establecidos

POLÍTICA DE USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACION

El área de Tecnología velará para que los recursos tecnológicos sean operados y administrados de manera segura y controlada, permitiendo el monitoreo de actividades de los usuarios que los utilizan

NORMA PARA LOS ADMINISTRADORES DE RECURSOS TECNOLÓGICOS

Asignar privilegios de administración de los recursos tecnológicos sólo al personal que se encuentre asignado para estas funciones en consideración de las cuentas personalizadas que deben existir para estos usuarios específicos

El área de tecnología debe validar que los administradores de recursos tecnológicos no cuenten con acceso a recursos tecnológicos de producción

El área de tecnología deben encargarse de restringir el acceso autorizado a conexiones remotas

NORMAS PARA EL ÁREA DE TECNOLOGÍA

Debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.

Los administradores de los recursos tecnológicos y servicios de red, funcionarios del área de Tecnología, no deben hacer uso de los utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para pasar por alto la seguridad de los sistemas de información alojados sobre la plataforma tecnológica del BANCO

Los administradores de los recursos tecnológicos deben encargarse de deshabilitar las funcionalidades o servicios no utilizados de los sistemas operativos, el firmware y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.

El área de Tecnología debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

NORMA PARA EL ÁREA DE CONTROL DE RIESGOS

Validar que las políticas de contraseñas definidas se acojan al procedimiento definido con esa finalidad

Revisar periódicamente las actividades realizadas por funcionarios con altos privilegios

POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

El personal asignado como responsable de cada área velará por el adecuado mantenimiento (asignación, modificación, revocación) de privilegios, de manera controlada. El área de Tecnología como responsable de los recursos tecnológicos del BANCO se encargará de protegerlos de accesos no autorizados mediante el uso de los controles que considere necesarios y velará por promover el uso de buenas prácticas en el área de desarrollo que apoyen estos objetivos

NORMAS PARA EL ÁREA DE TECNOLOGÍA

Debe definir un procedimiento para realizar la asignación de accesos a los diferentes sistemas y aplicativos del BANCO

POLÍTICAS DE SEGURIDAD FISICA Y MEDIOAMBIENTAL

POLÍTICA DE AREAS SEGURAS

El BANCO promoverá la implantación de mecanismos de seguridad física y de control de acceso asegurando sus instalaciones. De igual manera evaluará la efectividad de estos mecanismos y se encargará de controlar amenazas físicas internas, externas y medioambientales en sus instalaciones. Las instalaciones destinadas al procesamiento o almacenamiento de información sensible o de infraestructura tecnológica, serán consideradas áreas de acceso restringido y se tendrán mayores medidas de seguridad

POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

El BANCO proveerá los recursos necesarios para garantizar la mitigación de Control de Riesgos asociados a pérdida, robo o exposición al peligro de los recursos tecnológicos de la institución.

NORMAS PARA TODOS LOS FUNCIONARIOS

Si el funcionario no pertenece al área de tecnología no podrá asignar o realizar movimiento de recursos tecnológicos

Todo recurso tecnológico de personal externo que quiera hacer uso de la red de datos del BANCO debe acogerse a las instrucciones técnicas indicadas por tecnología

De presentarse algún fallo en hardware o software que sea de propiedad del BANCO el usuario responsable del mismo deberá crear una solicitud al área de soporte.

POLITICAS DE SEGURIDAD EN LAS OPERACIONES

POLÍTICA DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

El área de Tecnología , asignará funciones específicas a sus funcionarios, quienes deben efectuar la operación y administración de los recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades, también se encargará de las proyecciones y provisiones necesarias para el crecimiento de la infraestructura tecnológica de ser requerida. De igual manera debe velar por la eficiencia de los controles que han sido implantados y su mantenimiento.

NORMA PARA EL ÁREA DE TECNOLOGÍA

Los funcionarios del área de Tecnología deben encargarse de la documentación y actualización de procedimiento relacionados con la administración y operación de los recursos tecnológicos del BANCO

POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO
El BANCO se encargará de proporcionar los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso.

NORMAS PARA TODOS LOS USUARIOS

Los funcionarios que cuenten con recursos tecnológicos a su cargo no deben modificar o eliminar la configuración de software de protección (antivirus, antispyware, antimalware, antispam) establecida por el área de Tecnología

Todo usuario debe asegurarse de que los archivos descargados de correos o internet y/o de almacenamiento externo provienen de fuentes confiables para evitar el contagio con software malicioso a los recursos tecnológicos del BANCO

POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN
El BANCO certificará la generación de copias de respaldo y almacenamiento de información considerada como crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos necesarios para realizar estas actividades.

NORMA PARA TODOS LOS USUARIOS

Es responsabilidad de cada usuario de los recursos tecnológicos identificar la información crítica que debe ser respaldada y almacenarla o solicitar su almacenamiento de acuerdo con su nivel de clasificación

POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN
El BANCO realizará monitoreo permanente del uso que dan los funcionarios y los contratistas a los recursos tecnológicos y los sistemas de información del instituto. Además, velará por la custodia de los registros de auditoría en cumplimiento de los periodos de retención establecidos para dichos registros.

NORMA PARA EL ÁREA DE TECNOLOGÍA Y EL ÁREA DE CONTROL DE RIESGOS

Deben definir cuáles son los eventos que deben generar registros de auditoría en los recursos tecnológicos y los sistemas de información del BANCO

Los funcionarios del área de Tecnología, deben habilitar la creación de registros de auditoría y los sistemas de monitoreo para los recursos tecnológicos de acuerdo a los eventos definidos como auditables

POLITICA DE CONTROL AL SOFTWARE OPERATIVO
El BANCO asignará a los funcionarios responsables y definirá los procedimientos necesarios para controlar la instalación de software y sus

actualizaciones, funcionamiento del mismo, asignación de permisos a las herramientas y soporte del software utilizado

NORMA PARA EL ÁREA DE TECNOLOGÍA

Debe asegurarse de que el software operativo que se encuentre instalado cuente con el respectivo soporte de los proveedores

Debe definir las restricciones y limitaciones existente para la instalación de software operativo en los equipos de computo del BANCO

POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES

POLÍTICA DE GESTION Y ASEGURAMIENTO DE LAS REDES DE DATOS

El BANCO a través del área de Tecnología establecerá los controles necesarios ofrecer la disponibilidad en redes y servicios mínima requerida y realizar monitoreo de tráfico, así la protección a la integridad y confidencialidad de la información que viaja a través de esas redes.

NORMA PARA EL ÁREA DE TECNOLOGÍA

Debe encargarse de la instalación de recursos tecnológicos que se encarguen de la protección de redes internas y su conexión a redes externas a la organización

Debe velar por la confidencialidad de la información durante el direccionamiento y enrutamiento de las redes de datos del BANCO

POLÍTICA DE USO DEL CORREO ELECTRONICO

El BANCO proporcionará un servicio de correo idóneo y seguro para el normal desempeño de las actividades de los funcionarios que requieran el uso de ésta herramienta respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

NORMAS PARA TODOS LOS USUARIOS

Toda cuenta de correo electrónico asignada es de carácter individual e institucional, por tanto no debe compartirse y sólo podrá ser utilizada para desempeño de sus actividades laborales

El contenido de los correos electrónicos sólo debe corresponder a actividades propias del dueño de la cuenta

POLÍTICA DE USO ADECUADO DE INTERNET

El BANCO se encargará de garantizar el acceso a internet limitando el acceso a los recursos necesarios por cada funcionario para el normal desarrollo de sus actividades

NORMAS PARA TODOS LOS USUARIOS

Todo usuario con acceso a internet debe evitar la descarga de software, así como su instalación en equipos de propiedad del banco que le fueron asignados para desempeño de sus labores

POLÍTICA PARA EL INTERCAMBIO DE INFORMACIÓN
El BANCO se encargará de asegurar la información al ser compartida o intercambiada con otras entidades en función del establecimiento de los procedimientos y controles necesarios para ello. También se establecerán acuerdos de confidencialidad y/o intercambio de información con terceros a quienes llega la información

NORMAS PARA EL ÁREA DE CONTROL DE RIESGOS
Definir y establecer procedimientos para el intercambio de información con entidades externas que envían o reciben información confidencial propia de la organización o de sus clientes, estos procedimientos deben incluir el uso de medios de transmisión confiables y los controles necesarios para proteger su confidencialidad e integridad

POLÍTICAS QUE RIGEN DE LA RELACION CON TERCERAS PARTES

POLÍTICA DE INCLUSION DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON TERCERAS PARTES
El BANCO definirá mecanismos de control para establecer relaciones con contratistas, considerando el cumplimiento de las políticas, normas y procedimientos de seguridad definidos

NORMAS PARA EL ÁREA DE TECNOLOGÍA, OFICINA ASESORA JURÍDICA Y ÁREA DE CONTROL DE RIESGOS
Éstas áreas se encargarán de generar modelos que sirvan de base para la creación de acuerdos de niveles de servicio y requisitos de seguridad de la información que deben cumplir los contratistas. Éste modelo de ser divulgado a las áreas encargadas de su supervisión

POLÍTICA DE GESTION DE LA PRESTACION DE SERVICIOS DE TERCERAS PARTES
El BANCO tratará de conservar los niveles de seguridad de la información acordados, según los acuerdos establecidos, así como la gestión de cambios de estos acuerdos.

NORMAS PARA EL ÁREA DE CONTROL DE RIESGOS Y SUPERVISORES DE CONTRATOS CON TERCEROS
El área de Control de Riesgos y los supervisores de contratos con terceros debe encargarse de monitorear de forma periódica el cumplimiento de todo acuerdo de confidencial, intercambio de información y niveles de servicio.

POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD
El BANCO debe motivar a los funcionarios a reportar los incidentes de seguridad que se presenten y sus medios de procesamiento y almacenamiento. A su vez, debe asignar responsables para el tratamiento de incidentes de seguridad de la información quienes estarán encargados de de investigar y dar solución a los incidentes que sean reportados, realizando los cambios necesarios para que no vuelvan a ocurrir o escalándolos. La Junta Directiva se

encargará o delegará personal autorizado para reportar incidentes de seguridad de gran envergadura que deban ser comunicados ante autoridades pertinentes como único canal de comunicación por pronunciamiento oficial antes entidades externas en éstos casos.

NORMAS PARA EL ÁREA DE CONTROL DE RIESGOS

Deben definir responsabilidades y procedimientos para asegurar una pronta respuesta, ordenada y efectiva.

Debe evaluar todos los incidentes de seguridad considerando todo aspecto influyente para escalar al Comité de Seguridad de la información los que se consideren necesarios.

NORMAS PARA COMITÉ DE SEGURIDAD DE LA INFORMACION

Debe analizar los incidentes de seguridad que le fueron escalados y de ser necesario realizar el procedimiento de contacto con las autoridades.

NORMAS PARA TODOS LOS FUNCIONARIOS

Es responsabilidad de todo funcionario reportar a brevedad posible cualquier incidente o eventualidad relacionada con la información o los medios que la maneja.

Notificar al Área de Control de Riesgos casos de pérdida o divulgación de información confidencial o de uso interno, para que tomen las medidas necesarias

POLÍTICAS DE INCLUSION DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

POLÍTICA DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACION

El BANCO debe proporcionar suficientes recursos para dar respuesta efectiva a funcionarios y procesos en caso de contingencia o catástrofe presentada en la organización que afecte la continuidad de negocio. De igual forma, debe responder efectivamente ante éstas eventualidades e intentar restablecer las operaciones con el menor costo y pérdida posibles, conservando la seguridad de la información mientras se producen estos eventos.

NORMAS PARA COMITÉ SARO-SARLAFT Y EL ÁREA DE CONTROL DE RIESGOS

El comité SARO-SARLAFT y el Área de control de riesgos deben reconocer cuales son las situaciones pueden ser consideradas como emergencia o desastre para el BANCO, con qué áreas o procesos y como actuar si se presentan.

El comité SARO-SARLAFT y el Área de control de riesgos deben encargarse de liderar temas ligados con la continuidad de negocio y recuperación ante desastres

Es deber del Área de control de riesgos analizar los riesgos de continuidad y el impacto al negocio, para poner en práctica planes de continuidad, planes de contingencia o las consideraciones de seguridad necesario

El comité SARO-SARLAFT y el Área de control de riesgos deben seleccionar estrategias de recuperación más apropiadas en función del producto del análisis BIA
El Área de control de riesgos debe encargase de revisar los procedimientos de contingencia y recuperación que involucren aspectos de seguridad de la información
Es deber del comité SARO-SARLAFT y el Área de control de riesgos documentar y asegurar que se efectúen pruebas periódicas de los planes de recuperación y/o continuidad del negocio, validando la seguridad de la información mientras se realizan.

POLÍTICA DE REDUNDANCIA

POLÍTICA DE REDUNDANCIA
El BANCO velará por la existencia de sistemas y bases de datos redundantes que puedan satisfacer los requerimientos de disponibilidad mínimos.

NORMAS PARA EL ÁREA DE TECNOLOGÍA Y EL ÁREA DE CONTROL DE RIESGOS
El área de Tecnología y el área de Control de Riesgos deben encargarse de analizar y definir requerimientos de redundancia para los sistemas de información que se consideren críticos para la organización

POLÍTICAS DE CUMPLIMIENTO

POLÍTICA DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES
El BANCO velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, incluyendo derechos de autor y propiedad intelectual, motivo por el cual todo software instalado en los recursos tecnológicos del banco deberá cumplir con los requisitos legales y de licenciamiento que apliquen.

NORMAS PARA TODOS LOS USUARIOS
Los usuarios no deben instalar ningún tipo de software en los equipos de computo o dispositivos que le fueron asignados
Todo usuarios debe dar cumplimiento a las leyes de derechos de autor y los acuerdos de licenciamiento establecidos. Es ilegal duplicar software, duplicar documentación o la reproducción no autorizada del propietario de los derechos de autor pero podrá distribuirse el número de copias que indique la licencia.

POLÍTICA DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES
El BANCO mediante el área de Control de Riesgos tenderá a proteger los datos personales en cumplimiento de la Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales

NORMAS PARA LAS ÁREAS QUE PROCESAN DATOS PERSONALES
Las áreas en cargadas de procesar datos personales de personas propias y ajenas a la organización deben obtener previa autorización para el tratamiento de estos datos en el desarrollo de sus actividades

NORMAS PARA TODOS LOS USUARIOS

Todo usuario será responsable de guardar discreción y reserva absoluta con respecto a la información personal de personas propias y ajenas a la institución, así como información del BANCO de carácter crítico de la cual tengan conocimiento y/o manejo durante ejercicio sus actividades

POLÍTICAS DE DESARROLLO SEGURO

POLÍTICA DE DESARROLLO SEGURO

El BANCO se encargará de velar para que los desarrollos internos y externos que se realicen cumplan con los requerimientos esperados, se realicen en uso de buenas prácticas que garanticen el desarrollo seguro de los mismos. De igual manera, se asegurará de que se realicen las pruebas necesarias en uso de metodologías apropiadas para garantizar un paso a producción exitoso de los mismos. A su vez, se encargará de garantizar que toda aplicación cuente con el soporte necesario para funcionamiento de todos las aplicaciones utilizadas.

NORMAS PARA PROPIETARIOS O RESPONSABLES DE LOS SISTEMAS DE INFORMACIÓN

Los propietarios de los Sistemas de información se harán cargo de garantizar que las pruebas de las aplicaciones antes del paso a producción se realicen en uso de metodologías apropiadas, contemplando los escenarios necesarios y validando que se da cumplimiento a los requisitos mínimos de seguridad sugeridos.

Los propietarios de los Sistemas de información deben asegurarse de realizar las pruebas cuando los sistemas se vean afectados en cuanto a su estructura, ambiente tecnológico, creación y/o modificación de sus funcionalidades.

NORMAS PARA EL ÁREA DE DESARROLLO

Hacer uso de buenas prácticas que garanticen el desarrollo seguro de las aplicaciones

Prestar soporte a las aplicaciones para dar solución a los problemas que se presenten

Las aplicaciones desarrolladas deben cumplir con niveles de validación de la información previo registro de ella (de tipo de dato, de tamaño, etc.)

Los aplicativos no deben incluir claves de usuario en claro, estás deben utilizarse como parámetro propio de cada ambiente (preferiblemente) y deben estar encriptadas y fuera del alcance de personal diferente de quién realice configuraciones en el área de tecnología.

Realizar el control de versiones y almacenar los fuentes en un repositorio para salvaguardar el código fuente

Realizar las pruebas necesarias (técnicas, funcionales, de carga, etc.) considerando los escenarios propuestos para garantizar que se da cumplimiento a todos los requisitos establecidos.

Garantizar que los aplicativos cuenten con el correspondiente registro de actividades críticas como auditoría teniendo en cuenta datos básicos para su registro (usuario, tiempo, máquina, acción realizada, tabla afectada, etc.)

Garantizar que el paso entre ambientes se realice bajo controles adecuados

NORMAS PARA EL ÁREA DE TECNOLOGÍA

Asegurar que los ambientes segregados (desarrollo, pruebas y producción) sean tecnológicamente semejantes
Los desarrollos deben proteger el código de fuente de consultas y especialmente de manipulación

Realizar la instalación y mantenimiento de los sistemas de información previa certificación de los cambios propuestos
Asegurar que todo aplicativo instalado cumpla con las condiciones de uso de software y derechos de propiedad intelectual

ANEXO 2: PROCEDIMIENTO DE AUDITORÍAS INTERNAS

OBJETIVO
Definir los lineamientos para la planificación, ejecución y documentación de las auditorías internas de Sistema de Gestión de Calidad (SGC) del BANCO
ALCANCE
Éste procedimiento aplica para las auditorías internas realizadas al SCG del BANCO
GLOSARIO
Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización. **PDCA Plan-Do-Check-Act:** Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). **Auditor:** Persona con la competencia necesaria para llevar a cabo una auditoría **Criterios de auditoría:** Conjunto de políticas, procedimientos y requisitos

PASOS DEL PROCEDIMIENTO				
N°	**ACTIVIDAD**	**RESPONSABLE**	**DOCUMENTO DE ENTRADA**	**DOCUMENTO DE SALIDA**
1	Elaborar de manera anual el programa de auditorías	Representante de la Junta directiva	Programa de auditorías del año anterior	Programa de auditorías vigente
2	Aprobar el programa anual las auditorías	Representante de la Junta directiva	Programa de auditorías vigente	
3	Analizar los documentos de entrada, para identificar aquellos con bajo desempeño	Representante de la Junta directiva	Programa de auditorías del año anterior, Reporte de auditorías previas, Revisiones de la Junta Directiva	
4	Definir la auditoría interna a realizar de acuerdo con las necesidades del sistema de gestión	Representante de la Junta directiva	Programa de auditoría	
5	Conformar el equipo auditor y asignar un líder	Representante de la Junta directiva	Listado de auditores internos	Lista de conformación del equipo

				auditor
6	Notificar por escrito sobre la asignación realizada	Representante de la Junta directiva	Lista de conformación del equipo auditor	Notificación oficial
7	Elaborar el plan de auditoría definiendo claramente su alcance	Auditor Líder	Requerimientos del Sistema de gestión de calidad	Plan de auditoría
8	Notificar oficialmente a las áreas que serán auditadas y el alcance definido	Auditor Líder	Plan de auditoría	
9	Elaborar guía de auditoría	Auditor Líder	Plan de auditoría	Guía de auditoría
10	Convocar a reunión a los responsables de las áreas auditadas para dar a conocer el plan diseñado y poder despejar las dudas que aparezcan	Auditor Líder	Plan de auditoría	Lista de asistencia
11	Ejecutar la auditoría interna ejecutando paso a paso el plan diseñado	Equipo auditor	Plan de auditoría	
12	Notificar por escrito las no conformidades encontradas	Auditor		
13	Entregar al auditor líder los resultados de la auditoría: no conformidades, hallazgos y observaciones	Auditor	Plan de auditoría	Informe de auditoría
14	Elaborar un compendio de las no conformidades, hallazgos y observaciones en la auditoría	Auditor Líder	Informe de auditoría	Consolidación de no conformidades, hallazgos y observaciones en la auditoría
15	Realizar reunión de cierre de auditorías con los responsables de las áreas auditadas y un representante de la Junta directiva para dar a conocer no conformidades,	Representante de la junta directiva, Auditor Líder	Consolidación de no conformidades, hallazgos y observaciones en la auditoría	Lista de asistencia

	hallazgos y observaciones encontradas			
16	Hacer entrega del informe de auditoría a cada área	Auditor Líder	Informe de auditoría	Informe de auditoría
17	Entregar todos los informes al responsable del área de calidad	Representante del área	Reporte de auditoría	
18	Entregar el plan de acciones correctivas al área de calidad	Áreas auditadas	Reporte de auditoría	Plan de acciones correctivas
19	Dar seguimiento al plan de acciones correctivas al área de calidad	Responsable del proceso	Plan de acciones correctivas	Documento para la notificación de avances
20	Hacer seguimiento a las acciones correctivas propuestas por las áreas auditadas, hasta que se complete su ejecución	Auditor Líder	Plan de acciones correctivas	Solicitud de información
21	Almacenar las evidencias del proceso de auditorías internas	Representante de la Junta directiva		Registro de auditorías

Código	Descripción	Almacenamiento	Protección	Recuperación	Retención	Disposición
FSGC01	Programa de auditorías	Papel	Carpeta	Papel	3 años	Destrucción
FSGC02	Plan de auditoría	Papel	Carpeta	Papel	3 años	Destrucción
FSGC03	Guía de auditoría	Papel	Carpeta	Papel	3 años	Destrucción
FSGC04	Informe de auditoría	Papel	Carpeta	Papel	3 años	Destrucción

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE			
CARGO			

ANEXO 3: GESTIÓN DE INDICADORES

OBJETIVO			
Diseñar, medir, programar, evaluar indicadores y sus resultados, con el			
GLOSARIO			
Indicador: Relación entre variables que mide la situación y las tendencias de cambio generadas en el objeto o fenómeno observado respecto de objetivos y metas previstos. **Periodicidad:** Frecuencia con la que se realizará la medición del indicador. **Qué del objetivo:** Componente del objetivo referido a las acciones o tareas a realizar, con su medición se obtienen indicadores de eficiencia y eficacia. **Para qué del objetivo:** Componente del objetivo referido al impacto generado por las acciones realizadas.			
DESCRIPCIÓN DEL PROCEDIMIENTO			
Paso	**ACTIVIDAD**	**RESPONSABLE**	**REGISTRO O DOCUMENTO**
1	Identificar los objetivos que el indicador pretende apoyar	Líder de proceso	
2	Mostrar cada objetivo con mayor detalle, definiendo el qué y el para qué, e identificar los factores críticos de éxito.	Líder de proceso	
3	Diligenciar la hoja de vida del indicador	Líder de proceso	Hoja de vida del indicador
4	Solicitar aprobación, modificación o supresión de indicadores al área de control de riesgos.	Líder de proceso	
5	Programar evaluación de los indicadores	Analista del área de control de riesgos	
6	Evaluar los indicadores generados	Analista del área de control de riesgos	
7	Si fue aprobado se debe presentar circular para su firma, si no fue aprobado se debe devolver al paso 2		
8	Expedir circular de adopción de los indicadores	Líder de proceso	
9	Reportar las mediciones de los indicadores e interpretación de los resultados obtenidos	Analista del área de control de riesgos	Reporte de la medición en la hoja de vida del indicador
10	Incorporar el reporte de las mediciones por cada indicador	Analista del área de control de riesgos	Informe de gestión
11	Generar informe de gestión basado en la medición y análisis de los indicadores.	Analista del área de control de riesgos	

12	Avalar el informe de gestión basado en la medición y análisis de indicadores	Líder de proceso	
13	Presentar conclusiones y recomendaciones a la Junta Directiva	Analista del área de control de riesgos	Acta Junta Directiva
14	Presentar acciones de mejora	Líder de proceso	

INDICADORES PROPUESTOS

INDICADOR 01: Porcentaje de asignación de personal al SGSI

TIPO: Indicador de gestión	**ID:**SGSII01

DESCRIPCIÓN

Determina el avance en cuanto a la asignación de roles y responsabilidades definidas

OBJETIVO

Realizar seguimiento a la asignación de roles y responsabilidades requeridas para apoyar al SGSI

VARIABLES	FÓRMULA	FUENTE DE INFORMACIÓN
PA: Cantidad de personas con rol y responsabilidades asignadas que fueron descritas en el plan de SGSI	(PA7PT)*100	Plan de seguridad del sistema de gestión de la seguridad de la información
PT: Cantidad de personas requeridas para apoyar el SGSI		

META

MÍNIMA	75-80%	SATISFACTORIA	81-90%	SOBRESALIENTE	91-100%

INDICADOR 02: Cobertura de SGSI en los activos de información propuestos

TIPO: Indicador de gestión	**ID:**SGSII02

DESCRIPCIÓN

Éste indicador permite calcular el porcentaje de avance en la asignación de recursos humanos del SGSI con respecto al personal requerido.

OBJETIVO

Realizar seguimiento a medida que se van incluyendo los activos críticos de información y validar el nivel de avance.

VARIABLES	FÓRMULA	FUENTE DE INFORMACIÓN
AI: Número de activos de información incluidos en el alcance de implementación que se encuentran bajo la cobertura del SGSI en éste momento	(AI/AA)*100	Alcance del SGSI, Actas de asignación del personal
AA: Número de activos de información incluidos en el alcance de implementación		

META

MÍNIMA	75-80%	SATISFACTORIA	81-90%	SOBRESALIENTE	91-100%

OBSERVACIONES

INDICADOR 03: Tratamiento de eventos relacionados con el SGSI					
TIPO: Indicador de gestión				**ID:**SGSII03	
DESCRIPCIÓN					
Determina el nivel de eficiencia del SGSI en el tratamiento de eventos relacionados con la seguridad de la información, los cuales son reportados por usuarios o en función de los resultados de auditorías.					
OBJETIVO					
Realizar seguimiento para validar la evolución del SGSI en materia de respuesta, al interior de la organización					
VARIABLES		**FÓRMULA**		**FUENTE DE INFORMACIÓN**	
SR: Número de situaciones anómalas resueltas		(SR/ST)*100		Auditorías internas, herramientas de monitoreo, herramienta para reportar incidentes	
ST: Número de inconvenientes o situaciones presentadas fuera de lo común					
META					
MÍNIMA	75-80%	SATISFACTORIA	81-90%	SOBRESALIENTE	91-100%

INDICADOR 04: Avance del plan de sensibilización					
TIPO: Indicador de gestión				**ID:**SGSII04	
DESCRIPCIÓN					
A medida que con sensibilizados temas de seguridad con los usuarios, es importante validar que ellos estén realizando sus actividades teniendo en cuenta las indicaciones y recomendaciones dadas durante las capacitaciones de sensibilización.					
OBJETIVO					
Establecer el grado de efectividad del plan de sensibilización y capacitación utilizado					
VARIABLES		**FÓRMULA**		**FUENTE DE INFORMACIÓN**	
PI: Número de personas que fueron capacitadas y que están relacionadas con fallas e incumplimiento de recomendaciones dadas		(PI/PC)*100		Auditorías internas especializadas en el tema, atención al usuario	
PC: Total de personas capacitadas					
META					
MÍNIMA	75-80%	SATISFACTORIA	81-90%	SOBRESALIENTE	91-100%

INDICADOR 05: Cumplimiento de políticas de seguridad de la información	
TIPO: Indicador de cumplimiento	**ID:**SGSII05
DESCRIPCIÓN	
A medida que con sensibilizados temas de seguridad con los usuarios, es importante	

validar que ellos estén realizando sus actividades teniendo en cuenta las indicaciones y recomendaciones dadas durante las capacitaciones de sensibilización.		
OBJETIVO		
Establecer el grado de efectividad del plan de sensibilización y capacitación utilizado		
VARIABLES	**FÓRMULA**	**FUENTE DE INFORMACIÓN**
¿EL BANCO ha definido una política general de seguridad de la información?	1 (SÍ se evidencia) 0 (NO se evidencia)	Pla de seguridad de la información, funcionarios
¿El BANCO ha definido un grupo de personas y responsabilidades específicas asignadas para cumplir con las políticas?		
¿EL BANCO cumple con los requisitos necesarios respecto al manejo de la información?		

META			
CUMPLE	1	NO CUMPLE	0

INDICADOR 06: Porcentaje de implementación de controles					
TIPO: Indicador de gestión				**ID:**SGSII06	
DESCRIPCIÓN					
Indica el nivel de avance en la implementación de controles					
OBJETIVO					
Verificar el porcentaje de avance en la implementación de controles de seguridad					
VARIABLES		**FÓRMULA**		**FUENTE DE INFORMACIÓN**	
CI: Cantidad de controles implementados que corresponden a la planeación inicial		(CI/CP)*100		Plan de tratamiento de riesgos	
CP: Cantidad de controles que se planea implementar					
META					
MÍNIMA	75-80%	SATISFACTORIA	81-90%	SOBRESALIENTE	91-100%

INDICADOR 07: Identificación de los lineamientos de seguridad de la organización		
TIPO: Indicador de cumplimiento		**ID:**SGSII07
DESCRIPCIÓN		
Medir el grado de seguridad de la información		
OBJETIVO		
Medir la preparación		
VARIABLES	**FÓRMULA**	**FUENTE DE INFORMACIÓN**
¿El BANCO ha definido		Funcionarios

lineamientos de trabajo a través del comité o responsable de seguridad para que sus funcionarios cumplan las políticas de seguridad? ¿Se evalúa periódicamente su cumplimiento?	1 (SÍ se evidencia) 0 (NO se evidencia)	
¿El BANCO ha definido lineamientos en cuanto a la protección de las instalaciones físicas, equipos de cómputo y su entorno para evitar accesos no autorizados y minimizar riesgos de la información de la entidad?		

META			
CUMPLE	1	NO CUMPLE	0

INDICADOR 08: Verificación de control de acceso		
TIPO: Indicador de cumplimiento		**ID:**SGSII08
DESCRIPCIÓN		
Nivel de control de acceso		
OBJETIVO		
Validar si existen lineamientos, normas o estándares relacionados con el control de acceso		
VARIABLES	**FÓRMULA**	**FUENTE DE INFORMACIÓN**
¿El BANCO ha definido lineamientos, normas o estándares relacionados con el control de acceso a redes?	1 (SÍ se evidencia) 0 (NO se evidencia)	Funcionarios
¿El BANCO ha definido lineamientos, normas o estándares relacionados con el control de acceso a recursos físicos?		
¿El BANCO ha definido lineamientos, normas o estándares relacionados con el control de acceso a recursos tecnológicos?		

META			
CUMPLE	1	NO CUMPLE	0

INDICADOR 09: Aseguramiento de creación y mantenimiento de software

TIPO: Indicador de cumplimiento			**ID:**SGSII09
DESCRIPCIÓN			
Nivel de protección de los servicios prestados por la entidad			
OBJETIVO			
Validar si existen lineamientos, normas o estándares relacionados con la adquisición, el desarrollo y mantenimiento de aplicaciones			
VARIABLES	**FÓRMULA**		**FUENTE DE INFORMACIÓN**
¿El BANCO ha definido lineamientos, normas o estándares relacionados con la adquisición, el desarrollo y/o mantenimiento de aplicaciones?	1 (SÍ se evidencia) 0 (NO se evidencia)		Funcionarios
¿El BANCO ha definido lineamientos, normas o estándares relacionados con la gestión de incidentes relacionados con el servicio?			
META			
CUMPLE	1	NO CUMPLE	0

INDICADOR 10: Implementación de los procesos y registros de auditoría			
TIPO: Indicador de cumplimiento			**ID:**SGSII10
DESCRIPCIÓN			
Grado de existencia de normas y lineamientos en cuanto al registro y auditoría de seguridad			
OBJETIVO			
Validar la existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.			
VARIABLES	**FÓRMULA**		**FUENTE DE INFORMACIÓN**
¿El BANCO ha definido lineamientos, normas o estándares relacionados con el registro y control de eventos que sucedan en equipos, sistemas y servicios?	1 (SÍ se evidencia) 0 (NO se evidencia)		Funcionarios
¿El BANCO verifica interna y periódicamente sus procesos de seguridad de la información para asegurar su cumplimiento?			
META			
CUMPLE	1	NO CUMPLE	0

INDICADOR 11: Detección de anomalías en la prestación de servicios			
TIPO: Indicador de cumplimiento		**ID:**SGSII11	
DESCRIPCIÓN			
Validar nivel de implementación de mecanismos encaminados a la detección de anomalías e irregularidades.			
OBJETIVO			
Medir el porcentaje de mecanismos orientados a la detección de anomalías e irregularidades			
VARIABLES	**FÓRMULA**	**FUENTE DE INFORMACIÓN**	
¿El BANCO ha implementado mecanismos para detectar periódicamente vulnerabilidades de seguridad en el funcionamiento de: a) su infraestructura, b) redes, c) sistemas de información, d) aplicaciones y/o e) uso de los servicios?	1 (SÍ se evidencia) 0 (NO se evidencia)	Funcionarios	
META			
CUMPLE	1	NO CUMPLE	0

INDICADOR 12: Políticas de privacidad y confidencialidad			
TIPO: Indicador de cumplimiento		**ID:**SGSII12	
DESCRIPCIÓN			
Validar nivel de implementación las políticas de privacidad y confidencialidad			
OBJETIVO			
Identificar el nivel de implementación las políticas de privacidad y confidencialidad			
VARIABLES	**FÓRMULA**	**FUENTE DE INFORMACIÓN**	
¿El BANCO ha implementado los lineamientos, normas y/o estándares para proteger la información personal y privada de los ciudadanos que utilicen sus servicios?	1 (SÍ se evidencia) 0 (NO se evidencia)	Funcionarios	
¿El BANCO ha implementado lineamientos, normas y/o estándares para proteger la información privada de las entidades que utilicen sus servicios?			
META			
CUMPLE	1	NO CUMPLE	0

INDICADOR 13: Verificación de las políticas de integridad de la información		
TIPO: Indicador de cumplimiento		**ID:**SGSII13
DESCRIPCIÓN		
Corresponde al nivel de implementación de mecanismos para la integridad de la información de la entidad		
OBJETIVO		
Validar el nivel de implementación de políticas privacidad y confidencialidad de la entidad.		
VARIABLES	**FÓRMULA**	**FUENTE DE INFORMACIÓN**
¿El BANCO ha implementado lineamientos contra modificación o pérdida accidental de información?	1 (SÍ se evidencia) 0 (NO se evidencia)	Funcionarios
¿El BANCO ha implementado lineamientos, normas y/o estándares para recuperar información en caso de modificación o pérdida intencional o accidental?		

META			
CUMPLE	1	NO CUMPLE	0

INDICADOR 14: Políticas de disponibilidad del servicio y la información		
TIPO: Indicador de cumplimiento		**ID:**SGSII14
DESCRIPCIÓN		
Hace referencia al grado de cumplimiento de las políticas de disponibilidad del servicio y la información.		
OBJETIVO		
Validar el nivel de implementación de políticas de disponibilidad del servicio y la información.		
VARIABLES	**FÓRMULA**	**FUENTE DE INFORMACIÓN**
¿El BANCO verifica que los lineamientos, normas y/o estándares orientados a la continuidad en la prestación de los servicios se cumplan?	1 (SÍ se evidencia) 0 (NO se evidencia)	Funcionarios
¿El BANCO ha implementado mecanismos para que los servicios tengan altos índices de disponibilidad?		
META		

CUMPLE	1	NO CUMPLE	0

INDICADOR 15: Ataques informáticos					
TIPO: Indicador de gestión				**ID:**SGSII15	
DESCRIPCIÓN					
Corresponde al porcentaje de ataques informáticos recibidos en la entidad que impidieron la prestación de alguno de sus servicios.					
OBJETIVO					
Dar a conocer el número de ataques informáticos que recibe la entidad					
VARIABLES		**FÓRMULA**		**FUENTE DE INFORMACIÓN**	
¿Cuántos ataques informáticos ha recibido el BANCO en el último año? AT		(AE/AT)*100		Herramientas de monitoreo	
¿Cuántos de estos ataques han impedido la prestación de algunos servicios? AE					
META					
MÍNIMA	<20%	SATISFACTORIA	1.1-10%	SOBRESALIENTE	0-1%

ANEXO 4: PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN

OBJETIVO
Medir, programar evaluación, evaluar indicadores y sus resultados, con al ánimo de validar el estado en que se encuentra el SGSI, buscar oportunidades de mejora y retroalimentar al SGSI con respecto a las impresiones recibidas
GLOSARIO
Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización. **PDCA Plan-Do-Check-Act:** Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/lEC 27002:20005): intención y dirección general expresada formalmente por la Dirección.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la información: Según [ISO/lEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO/lEC 27001: 2013]: la parle de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Trazabilidad: Propiedad que garantiza que las acciones de una entidad se puede rastrear únicamente hasta dicha entidad.

PASOS DEL PROCEDIMIENTO			
N°	**ACTIVIDAD**	**RESPONSABLE**	**REGISTRO O DOCUMENTO**
1	PLANEAR Y PROGRAMAR LA REVISIÓN POR LA JUNTA DIRECTIVA AL SGSI Se programará la revisión una vez al año o en caso de que se presenten situaciones que afecten el desempeño del SGSI. Una vez definida la fecha se enviará la citación a la Junta Directiva	Representante de la Junta Directiva	Correo electrónico o memorando de citación
2	RECOPILAR LA INFORMACIÓN NECESARIA PARA LA REVISIÓN POR LA JUNTA DIRECTIVA Cada responsable de los activos de información debe entregar información como:	Personal responsable según el alcance definido	Información recibida

	a) el estado de las acciones con relación a las revisiones previas por la Junta Directiva; b) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información; c) retroalimentación sobre el desempeño de la seguridad de la información, incluidas las tendencias relativas a: 1) no conformidades y acciones correctivas; 2) seguimiento y resultados de las mediciones; 3) resultados de la auditoría; y 4) cumplimiento de los objetivos de la seguridad de la información; d) retroalimentación de las partes interesadas; e) resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos; y f) las oportunidades de mejora continua.		
3	CONSOLIDAR Y ANALIZAR INFORMACIÓN Teniendo en cuenta el resultado de la información recopilada en la actividad anterior, se debe verificar dicha información para garantizar la confiabilidad.	Representante de la Junta Directiva	Formato Informe de revisión por la Junta Directiva al SGSI FRJD01
4	PRESENTAR INFORMACIÓN QUE SERÁ ANALIZADA EN LA REUNIÓN DE REVISIÓN POR LA JUNTA DIRECTIVA Presentar a la Junta Directiva la información acerca del desempeño del SGSI generado como resultado de la actividad anterior	Representante de la Junta Directiva	Formato Informe de revisión por la Junta Directiva al SGSI FRJD01

5	RESULTADOS DE LA REVISIÓN POR LA JUNTA DIRECTIVA Toda sugerencia, decisión y/o conclusión generada, debe ser registrada en el formato correspondiente, así como las decisiones y acciones que tengan que ver con: mejora de eficacia, eficiencia y efectividad del SGSI, la mejora propuesta a productos y servicios en relación con lo requerido, decisiones sobre política u objetivos de SGSI, necesidad de nuevos recursos para implementar mejoras. Se definen responsables y tiempos de implementación de las recomendaciones en el formato de Seguimiento a las Recomendaciones para la Mejora	Integrantes de la Junta Directiva	Formato Informe de revisión por la Junta Directiva al SGSI FRJD01 Formato de Seguimiento a las Recomendaciones para la Mejora FRJD02
6	REALIZAR SEGUIMIENTO A LOS PLANES DE MEJORA ESTABLECIDOS Cada uno de los funcionarios responsables de implementar las acciones definidas en el formato de Seguimiento a las Recomendaciones para la Mejora está a cargo de un líder, el cual realizará el seguimiento correspondiente. El representante de la Junta Directiva debe validar el avance de implementación de éstas acciones según formato FRJD02. El Área de Control de riesgos en sus actividades de auditoría al SGSI debe realizar seguimiento a los planes de mejora que fueron generados a partir de la revisión por la Junta Directiva. En caso de que no se cumplan los planes definidos, se deben analizar las causas y definir las acciones correctivas necesarias para ser comunicadas a la Junta directiva en busca de su solución.	Personal responsable según el alcance definido / Representante de la Junta Directiva	Formato de Seguimiento a las Recomendaciones para la Mejora FRJD02

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE			
CARGO			

ANEXO 5: GESTIÓN DE ROLES Y RESPONSABILIDADES

ÁREA	RESPONSABILIDADES
REPRESENTANTE DE LA JUNTA DIRECTIVA	Aprobar los cambios y propuestas sugeridos Apoyar el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.

	Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. Supervisar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información. Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados.
REPRESENTANTE DEL ÁREA DE SEGURIDAD DE LA INFORMACIÓN	Liderar la gestión de riesgos de seguridad sobre la gestión de TI (Tecnologías de la información) y de información de la institución. Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.
REPRESENTANTE DEL ÁREADE TECNOLOGÍA	Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. Trabajar con la Junta directiva y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información. Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Encargado monitorear y gestionar la

	prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.
REPRESENTANTE DEL ÁREA DE CONTROL DE RIESGOS	Apoyar la gestión de riesgos de seguridad sobre la gestión de TI (Tecnologías de la información) y de información de la institución. Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. Trabajar con la Junta directiva y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
REPRESENTANTE DEL ÁREA DESARROLLO	Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad. Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. Liderar el proceso de gestión de incidentes de seguridad así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. Trabajar con la Junta directiva y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio

ANEXO 6: INFORME AUDITORÍA INTERNA

Organización	Banco
Fecha de auditoría	16/10/2016 - 16/12/2016
Auditor Jefe	
Equipo Auditor	
Criterio	Norma ISO/IEC 27002

Objeto de la auditoría
La presente auditoría tiene por principal objetivo evaluar el nivel de cumplimiento alcanzado por la compañía al considerar la implementación de los controles establecidos en la norma ISO/IEC 27002

Alcance de la auditoría
El alcance de la auditoría corresponde al mismo alcance que tiene el SGSI, es decir para "Los sistemas de información que dan soporte al aplicativo de administración de

garantías"

Fecha de la auditoría

Lugar
Instalaciones del Banco

Áreas auditadas
Se auditaron las áreas que corresponden con el alcance indicado para el SGSI • Área de administración documental • Área de control de riesgos • Área de seguridad de la información • Área de Tecnología • Área de desarrollo • Área de pruebas • Área de procesos

Equipo auditor
Personal con habilidades • Área de administración documental • Área de control de riesgos • Área de seguridad de la información • Área de Tecnología • Área de desarrollo • Área de pruebas • Área de procesos

ID	Tipo de hallazgo
NC	No conformidad menor
NC	No conformidad mayor
OM	Oportunidad de mejora

ID	Hallazgo	Numeral norma	Descripción	Tipo
1	El personal de proyectos no está suficientemente capacitado para considerar aspectos de seguridad en los proyectos	A.6.1.5	Es necesario capacitar al personal de proyectos en aspectos básicos relacionados con seguridad de la información o involucrar a personal que lo esté en los proyectos	OM
2	Inventario de activos	A.8.1.1	Falta crear procedimiento para actualizar el inventario de activos de forma periódica de tal forma que siempre se tenga la última versión	OM

3	No se han definido claramente las consecuencias de las violaciones de la política de seguridad en el documento	A.5.2	Es necesario definir y dar a conocer las acciones a tomar ante la violación de las normas y políticas establecidas en forma más detallada	OM
4	Los procedimientos no corresponde con los aspectos técnicos manejados	A.14.2.2	Se requiere ajustar los procedimientos dado que no corresponden con los aspectos técnicos manejados, será necesario capacitar al área de procesos en estos temas o involucrar al área de tecnología y/o desarrollo para orientarlos de forma adecuada.	NC
5	Falta incluir como se realizarán las entregas de revisiones por área para consolidar la información durante la revisión general de la política	A.5.1.2	Es necesario definir formatos para formalizar la entrega de los informes si hay lugar, o contemplar la posibilidad de envío por correo certificado	NC
6	El servidor de aplicaciones no cuenta con soporte		Es necesario realizar la migración del servidor de aplicaciones	NC
7	El personal no cuenta con suficiente capacitación sobre la metodología MAGERITH		Realizar capacitaciones al personal seleccionado sobre metodología MAGERITH	OM
8	Falta diseñar más indicadores para evaluar el SGSI en mayor detalle		Es necesario diseñar y aplicar nuevos indicadores que permitan evaluar más aspectos del SGSI	OM
9	No se tiene evidencia de llevar una bitácora de incidentes para el aplicativo		Las áreas de desarrollo y tecnología deben llevar una bitácora de incidentes donde se indiquen detalles de solución de los incidentes y una clasificación de ellos que permitan un mejor manejo y oportunidad si se presentan en el futuro situaciones similares	OM
10	No se evidencia en qué momentos se debe hacer uso de la encripción	A.18.1.6	Es necesario identificar las situaciones que requieren la encripción de archivos y/o correos para su envío	OM
11	No cuenta con auditores externos para evaluar el SGSI	A.6.1.5	Contratar un auditor externo para que audite los procesos relacionados con el alcance del SGSI	OM
12	No se tienen acuerdos de cooperación mutua con grupos de interés especiales	A.6.1.4	Es necesario prestar especial atención a éste tema puesto que permitirá obtener asesoría especializada, estar a la	NC

			vanguardia en temas de seguridad para actuar de forma preventiva	
13	Falta generar la documentación necesaria que sirva como evidencia de la implementación de controles al dominio ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN		Hace falta incluir la documentación mínima necesaria como evidencia de cumplimiento	NC

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE			
CARGO			