Luz Dary Méndez Uribe

Trabajo de Final de Máster

Tutor

Antonio José Segovia Henares

Universitat Oberta de Catalunya

Máster Interuniversitario en Seguridad de las TIC (MISTIC)

2016

TABLA DE CONTENIDO

1. FASE 1. SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL 6
1.1. INTRODUCCIÓN 6
1.2. ESTÁNDARES ISO/IEC 27001 E ISO/IEC 27002 6
1.3. CONTEXTUALIZACIÓN 8
1.3.1. CONTEXTO DE LA EMPRESA 8
1.3.2. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 11
1.3.2.1. ÁREAS INVOLUCRADAS 11
1.3.2.2. PROCESOS INVOLUCRADOS 13
1.3.2.3. APLICATIVOS INVOLUCRADOS 15
1.4. OBJETIVOS DEL PLAN DIRECTOR 17
1.5. ANÁLISIS DIFERENCIAL 19
1.6. RESULTADOS 35
2.1. INTRODUCCIÓN 35
2.2. ESQUEMA DOCUMENTAL 36
2.2.1. POLÍTICA DE SEGURIDAD 36
2.2.2. PROCEDIMIENTO DE AUDITORÍAS INTERNAS 36
2.2.3. GESTIÓN DE INDICADORES 36
2.2.4. PROCEDIMIENTO REVISIÓN POR DIRECCIÓN 36
2.2.5. GESTIÓN DE ROLES Y RESPONSABILIDADES 36
2.2.6. METODOLOGÍA DE ANÁLISIS DE RIESGOS 39
2.2.7. DECLARACIÓN DE APLICABILIDAD 46
2.2.8. RESULTADOS 63
3. FASE 3. ANÁLISIS DE RIESGOS 64
3.1. INTRODUCCIÓN 64
3.2. INVENTARIO DE ACTIVOS 64
3.3. VALORACIÓN DE LOS ACTIVOS 66
3.4. DIMENSIONES DE SEGURIDAD 69
3.5. TABLA RESUMEN DE VALORACIÓN 72
3.6. ANÁLISIS DE AMENAZAS 75
3.7. IMPACTO POTENCIAL 75
3.8. NIVEL DE RIESGO ACEPTABLE Y RIESGO RESIDUAL 76

3.9. RESULTADOS 95
4. FASE 4. PROPUESTAS DE PROYECTOS 96
4.1. INTRODUCCIÓN 96
4.2. PROPUESTAS 96
4.2.1. PROYECTO 1: AJUSTE DE POLÍTICAS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN EXISTENTES 96
4.2.2. PROYECTO 2: CREACIÓN Y AJUSTE DE PROCEDIMIENTOS 97
4.2.3. PROYECTO 3: ACTUALIZACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN 98
4.2.4. PROYECTO 4: ACCIONES DE MEJORA DE INFRAESTRUCTURA 98
4.2.5. PROYECTO 5: OPTIMIZACIÓN DEL APLICATIVO 99
4.2.6. PROYECTO 6: SOCIALIZACIÓN DE POLÍTICAS DE SEGURIDAD 100
4.3. RESULTADOS 101
5. FASE 5. AUDITORÍA DE CUMPLIMIENTO 105
5.1. INTRODUCCIÓN 105
5.2. METODOLOGÍA 105
5.3. EVALUACIÓN DE LA MADUREZ 107
5.4. PRESENTACIÓN DE RESULTADOS 116
5.5. RESULTADOS 116
6. FASE 6. PRESENTACIÓN DE RESULTADOS Y ENTREGA DE INFORME 117
6.1. INTRODUCCIÓN 117
6.2. OBJETIVOS DE LA FASE 117
6.3. ENTREGABLES 117
6.3.1. RESUMEN EJECUTIVO 117
6.3.2. MEMORIA DE PROYECTO 119
BIBLIOGRAFÍA 120
ANEXO 1: POLÍTICA DE SEGURIDAD 122
ANEXO 2: PROCEDIMIENTO DE AUDITORÍAS INTERNAS 144
ANEXO 3: GESTIÓN DE INDICADORES 147
ANEXO 4: PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN 155
ANEXO 5: INFORME AUDITORÍA INTERNA 158

TABLA DE FIGURAS

FIGURA 1: ORGANIGRAMA GENERAL DE 1ER NIVEL 11
FIGURA 2: ÁREAS INVOLUCRADAS PARTE 1 12
FIGURA 3: ÁREAS INVOLUCRADAS PARTE 2 13
FIGURA 4: PROCESOS INVOLUCRADOS 14
FIGURA 5: ESTRUCTURA DEL APLICATIVO 15
FIGURA 6: DIAGRAMA DE ARQUITECTURA 16
FIGURA 7: ANÁLISIS DIFERENCIAL DE ISO/IEC27001 35
FIGURA 8: ANÁLISIS DIFERENCIAL DE ISO/IEC27002 35
FIGURA 9:VALORACIÓN DE ACTIVOS 45
FIGURA 10: CRONOGRAMA PROYECTOS 104
FIGURA 11: COMPARACIÓN DE DOMINIOS PARA EVALUACIÓN DE MADUREZ INICIAL Y ACTUAL 116

TABLA DE TABLAS

TABLA 1: APLICATIVOS RELACIONADOS CON SAAG 17
TABLA 2: ANÁLISIS DIFERENCIAL NORMA ISO/IEC 27001 22
TABLA 3: ANÁLISIS DIFERENCIAL NORMA ISO/IEC 27002 34
TABLA 4: ROLES Y RESPONSABILIDADES 39
TABLA 5: TIPOS DE AMENAZA SEGÚN METODOLOGÍA MAGERIT 42
TABLA 6: VALORES DE DEGRADACIÓN 42
TABLA 7: PROBABILIDAD DE OCURRENCIA 42
TABLA 8: DECLARACIÓN DE APLICABILIDAD 63
TABLA 9: INVENTARIO DE ACTIVOS 66
TABLA 10: VALORACIÓN DE ACTIVOS 69
TABLA 11: POSIBLES VALORES DE DIMENSIÓN 69
TABLA 12: VALORACIÓN DE DIMENSIONES DE SEGURIDAD 72
TABLA 13: RESUMEN DE VALORACIÓN 75
TABLA 14: ANÁLISIS DE AMENAZAS 80
TABLA 15: RESUMEN RIESGO RESIDUAL 95
TABLA 16: PROYECTO 1. AJUSTE A POLÍTICAS 97
TABLA 17: PROYECTO 2. AJUSTE A PROCEDIMIENTOS 98
TABLA 18: PROYECTO 3. CLASIFICACIÓN DE LA INFORMACIÓN 98
TABLA 19: PROYECTO 4. ACCIONES DE MEJORA DE INFRAESTRUCTURA 99
TABLA 20: PROYECTO 5. OPTIMIZACIÓN DEL APLICATIVO 100
TABLA 21: PROYECTO 6: SOCIALIZACIÓN DE POLÍTICAS DE SEGURIDAD 101
TABLA 22: NIVELES DE MADUREZ CMM 106
TABLA 23: EVALUACIÓN DE LA MADUREZ |POLÍTICA DE SEGURIDAD 107
TABLA 24: EVALUACIÓN DE LA MADUREZ |ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 108
TABLA 25: EVALUACIÓN DE LA MADUREZ |SEGURIDAD EN LOS RECURSOS HUMANOS 108
TABLA 26: EVALUACIÓN DE LA MADUREZ | GESTIÓN DE ACTIVOS 109
TABLA 27: EVALUACIÓN DE LA MADUREZ | CONTROL DE ACCESO 110
TABLA 28: EVALUACIÓN DE LA MADUREZ | SEGURIDAD FÍSICA Y AMBIENTAL 111
TABLA 29: EVALUACIÓN DE LA MADUREZ | GESTIÓN DE COMUNICACIONES Y OPERACIONES 113
TABLA 30: EVALUACIÓN DE LA MADUREZ | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN 114
TABLA 31: EVALUACIÓN DE LA MADUREZ | GESTIÓN DE INCIDENTES 115
TABLA 32: EVALUACIÓN DE LA MADUREZ | GESTIÓN DE CONTINUIDAD DE NEGOCIO 115
TABLA 33: EVALUACIÓN DE LA MADUREZ | CUMPLIMIENTO 116

1. FASE 1. SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL

1.1. 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 y para facilitar ésta tarea existen normas, metodologías y compendios de buenas prácticas que han generado resultados de éxito a muchas compañías. Con el ánimo de aplicar el conocimiento adquirido durante el máster y hacer uso de estos recursos se incluye en éste documento la elaboración de un plan de seguridad de la información que será creado en varias etapas y el cual fue diseñado para una compañía que servirá como caso de estudio en el cual se utilizarán especialmente las normas ISO/IEC27001:2013, ISO/IEC27002:2013 y la metodología MAGERITH para el análisis y gestión de los riesgos detectados.

1.2. ESTÁNDARES ISO/IEC 27001 e ISO/IEC 27002

Dados los múltiples avances tecnológicos, aparecen nuevas amenazas que atentan contra la información y para estar preparados o saber cómo actuar frente a estas situaciones existe toda una familia de estándares internacionales que ofrece mejores prácticas para diseñar, implantar y mantener todo un Sistema de Gestión de seguridad de la información que se ajuste a las necesidades de la compañía de la cual hará parte. Esta familia de estándares está conformada por múltiples normas, pero en el presente proyecto prestaremos especial atención a las normas ISO/IEC27001:2013 e ISO/IEC27002:2013 que servirán como base en la planeación,

implementación y/o mejora de un sistema de gestión de seguridad de la información al interior de una empresa que será objeto de estudio.

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. CONTEXTUALIZACIÓN

1.3.1. CONTEXTO DE LA EMPRESA

El presente proyecto tiene por 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. Éste plan de seguridad será diseñado para una empresa específica, por lo cual se ha seleccionado una entidad del sector financiero, para ser más exactos un banco.

La entidad bancaria (ficticia) 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 durante su trayectoria se ha fusionado con otras empresas para explorar nuevos mercados y trabajar en la prestación de productos y servicios financieros para diversos segmentos de mercado, desde personas naturales promedio hasta grupos económicos. Para cada segmento aplica un portafolio específico de productos y los requisitos para su adquisición varían entre uno y otro. A la fecha cuenta con cobertura a nivel nacional y su nómina actual alcanza los 8532 empleados directos y 3964 empleados subcontratados, en cabeza de todos un presidente, una Junta Directiva y 4 vicepresidencias en las cuales se encuentran agrupados todos los empleados: vicepresidencia de estrategia y finanzas, vicepresidencia de servicios administrativos, vicepresidencia de servicios operativos y vicepresidencia de innovación y transformación tecnológica.

La compañía 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 limitará el alcance a crear el plan de seguridad de la información para "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. Para entrar en contexto del alcance seleccionado hablaremos de los procesos que se encuentran involucrados con el aplicativo. Como se mencionaba previamente, el BANCO ofrece productos financieros y estos se clasifican en 2 tipos de ahorro y de crédito, dentro de los productos de crédito encontramos: Tarjeta de crédito, adelanto de nómina, crédito libre destino, crédito de servicio, crédito estudiantil, crédito de vehículo, crédito de libranza, portafolio de vivienda, leasing de arrendamiento financiero y crédito de aportes voluntarios, los productos mencionados tienen en común que al ser solicitados el cliente debe presentar bienes mobiliarios o inmobiliarios o documentos de compromiso de pago que sirvan como garantía o prenda del producto que será adquirido. Se define como garantía al grupo de documentos que representan bienes o documentos de compromiso de pago que respaldan los productos adquiridos por los clientes del banco, por ejemplo cuando se solicita una tarjeta de

crédito el cliente entrega entre otros documentos un pagaré en blanco que respaldará la deuda adquirida en caso de llegar a un cobro jurídico.

Las garantías se reciben en las oficinas con cobertura nacional y posteriormente se trasladan a la bodega más cercana que corresponda para centralizar su almacenamiento y custodia. En éste proceso descrito a grandes rasgos se encuentra involucrado el aplicativo de administración de avales y garantías, donde cada garantía adquiere diversos estados durante su recorrido hasta las bodegas para tener control sobre ellos.

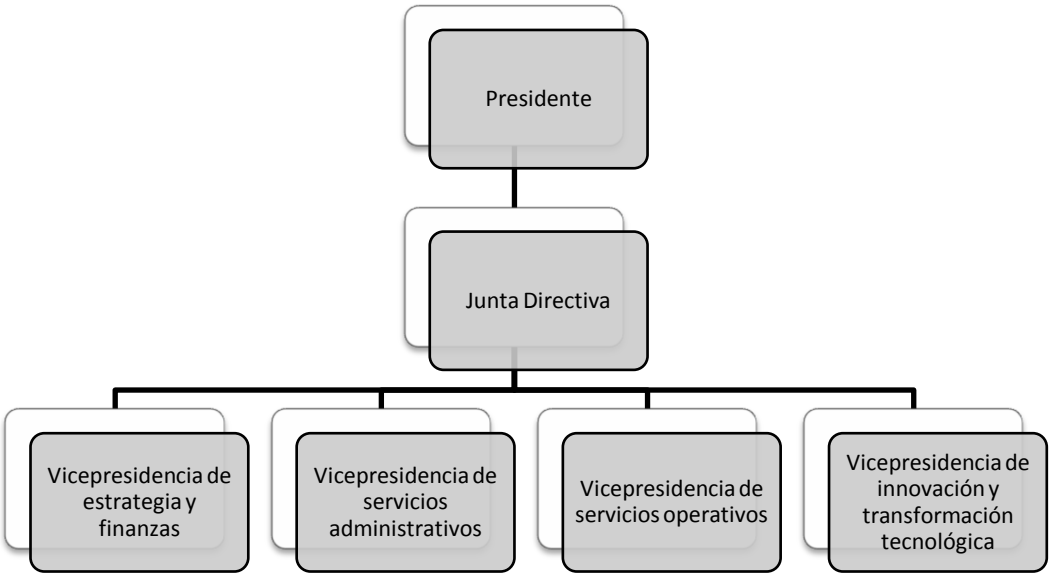


Figura 1: Organigrama general de 1er nivel

1.3.2. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1.3.2.1. ÁREAS INVOLUCRADAS

- Área de administración documental: Encargada de la administración y control de las garantías y avales
- 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

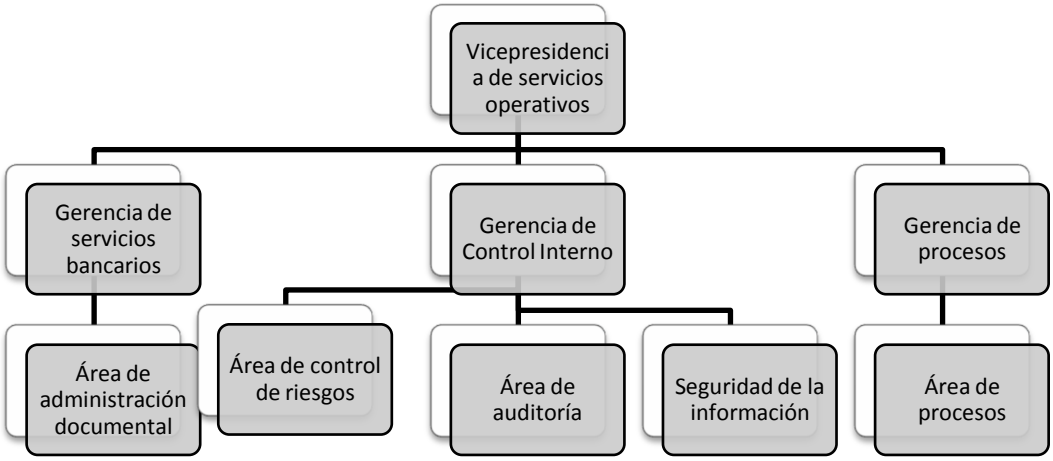


Figura 2: Áreas involucradas parte 1

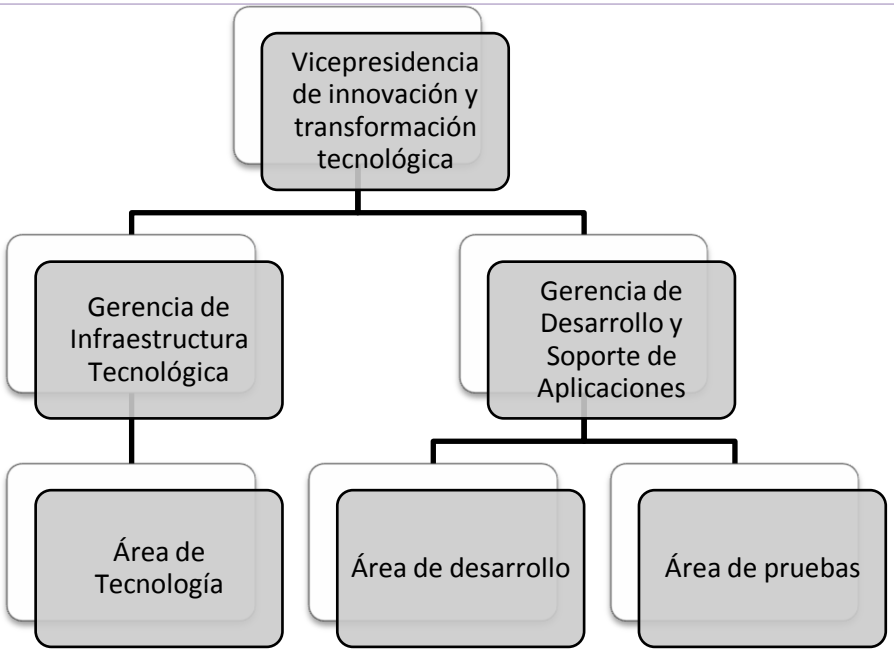


Figura 3: Áreas involucradas parte 2

1.3.2.2. 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 y clasificación de datos

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.

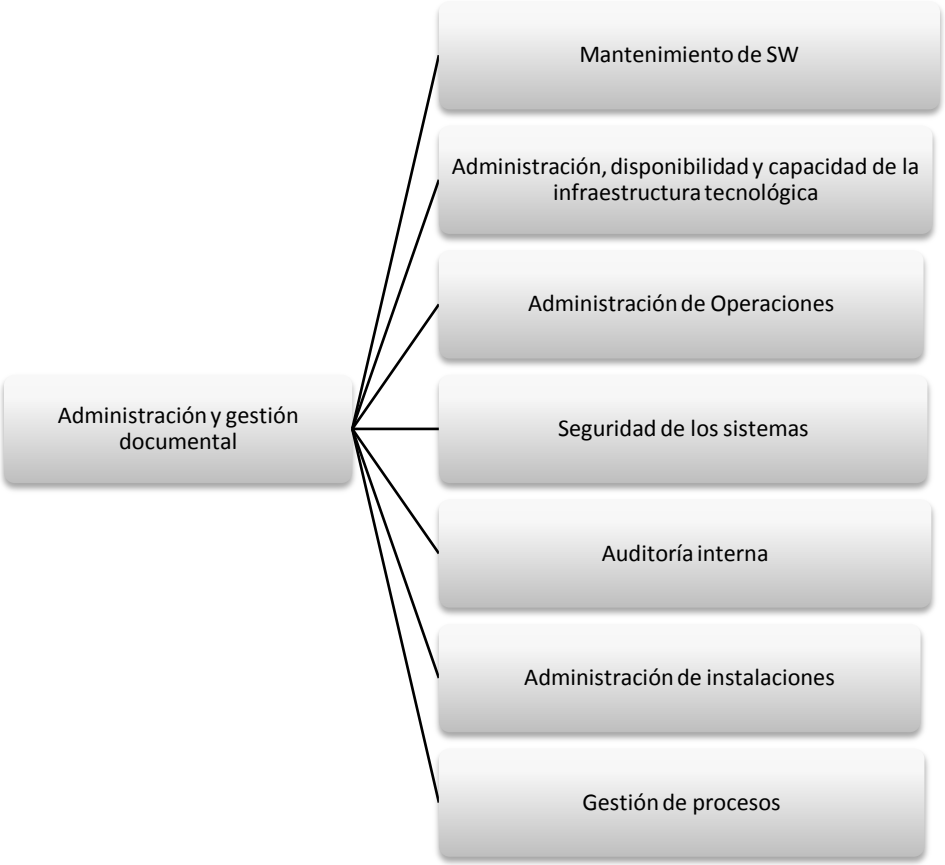


Figura 4: Procesos involucrados

1.3.2.3. 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.

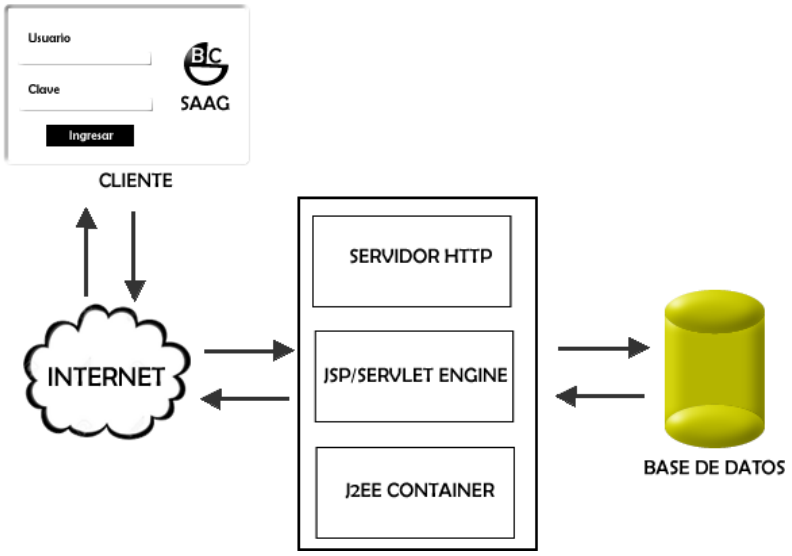


Figura 5: Estructura del aplicativo

Usuarios de oficinas: Consultan información sobre el estado de las garantías de los clientes y solicitan garantías o documentos en préstamos

Usuarios CAAG: Son los usuarios que hacen parte del Centro de Administración de Avales y 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

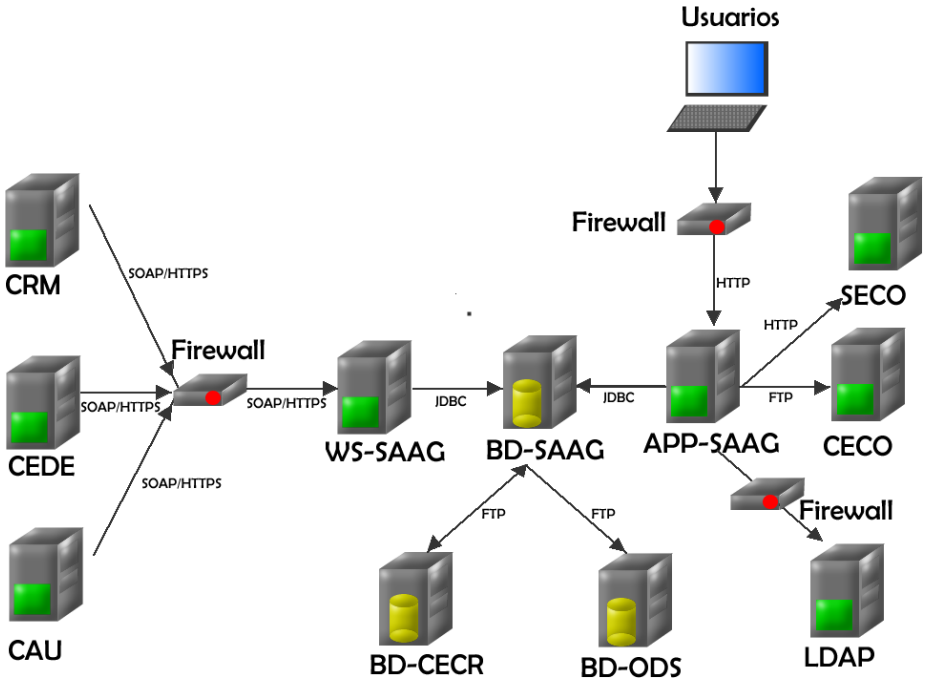


Figura 6: Diagrama de arquitectura

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

1.4. OBJETIVOS DEL PLAN DIRECTOR

- 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

1.5. ANÁLISIS DIFERENCIAL

ANÁLISIS DIFERENCIAL EN FUNCIÓN DE LA NORMA ISO/IEC 27001

ANÁLISIS DIFERENCIAL NORMA ISO/IEC 27001				
REQUISITOS		ESTADO	%	DESCRIPCIÓN
4.	**CONTEXTO DE LA ORGANIZACIÓN**	**L1**	**38%**	
4.1	CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO	L2	60%	Falta definir completamente los factores externos e internos que pueden afectar el cumplimiento del SGSI
4.2	COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	L1	30%	se tiene claridad sobre cuales son algunas de las partes interesadas en la implementación, falta definir cuáles son los requisitos propuestos por éstas
4.3	DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	L1	20%	El alcance del Sistema para la Gestión de la Seguridad de la Información corresponderá a "Los sistemas de información que dan soporte al aplicativo de administración de garantías", éste aplicativo respalda al proceso de administración y gestión documental, no se tiene total cobertura del alcance propuesto
4.4	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	L1	40%	Actualmente el banco cuenta con un Modelo de seguridad de la información genérico, pero no cuenta con ningún sistema de gestión de la seguridad.
5.	**LIDERAZGO**			
5.1	LIDERAZGO Y COMPROMISO	L1	75%	Con respecto a la propuesta se tiene compromiso de la Dirección de Sistemas para facilitar la documentación, personal, información y recursos tecnológicos necesarios en cada una de las fases y el de la junta directiva para conseguir la aprobación de los recursos de tipo económico necesarios para llevar cabo el plan generado como resultado del estudio al incluirlo dentro del PETI (Plan Estratégico de Tecnologías de la información) cuya aprobación se realiza cada año. Una vez implementado el Sistema de Gestión de la Seguridad se realizará el debido seguimiento con el ánimo de evaluar los resultados y beneficios obtenidos, dada la inversión se tiene motivación con respecto a velar por la mejora continua del sistema.

5.2	Política	L2	50%	De momento, el banco cuenta con una serie de políticas dirigidas a toda la organización en busca de garantizar la seguridad, confidencialidad y disponibilidad de la información que trabajan en función del modelo de seguridad de la información que ha sido implementado previamente, uno de los objetivos del proyecto consiste en revisarlas, validar su eficacia y proponer mejoras pertinentes, así como promover su publicación.
5.3	Roles, responsabilidades y autoridades en la organización	L1	40%	Se tienen identificados a los funcionarios responsables de auditorías existentes, pero no se han definido los funcionarios para las auditorias que no han sido definidas hasta el momento, así como las nuevas responsabilidades
6.	**PLANIFICACIÓN**	L1	40%	
6.1	ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES	L1	40%	De momento no se cumple con todos los requisitos de ésta norma y a la Junta Directiva se informa sobre el desempeño del modelo de seguridad
6.1.1	Generalidades	L1	40%	Existe actualmente un proceso para la gestión del riesgo operativo denominado SARO, es difundido por capacitación virtual al ingresar al banco y cada año por solicitud de comunicado. En éste proceso se incluye la gestión de riesgos lo cual le permite a la entidad estar familiarizada con ésta gestión, sin embargo se ha informado acerca del uso de la metodología MAGERIT la cual está enfocada específicamente en el análisis y gestión de riesgos de los sistemas de información. Aunque está orientada a la administración pública aplica para compañías del sector privado y nos permitirá crear un proceso para la gestión de riesgos que asegure cada una de las dimensiones que hacen parte de la información (Disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad).
6.1.2	Valoración de riesgos de la seguridad de la información	L1	40%	En consideración del Modelo de seguridad de la información se tienen algunos riesgos identificados, pero no se ha realizado un análisis completo y detallado de los mismos para el alcance definido
6.1.3	Tratamiento de riesgos de la seguridad de la información	L1	40%	Existe un área para el control de riesgos, tiene especial énfasis en los riesgos de tipo operativo que en general se encuentran relacionados con los procesos
6.2	OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLOS	L1	40%	Se han propuesto los siguientes objetivos pero de momento no se tienen planes para hacerlos realidad
7.	**SOPORTE**	L2	60%	
7.1	RECURSOS	L2	60%	La organización asigna los recursos necesarios para el modelo de seguridad de la información, pero hace falta incluir los requeridos por plan de SGSI

7.2	COMPETENCIA	L2	70%	La organización cuenta con personal calificado y sus capacidades corresponden con las actividades que deben desempeñar, aunque se tienen ciertas excepciones. Adicional a esto en cuanto a nuevas tecnologías se refiere se involucra a consultores externos expertos en lo relacionado a asesorías tecnológicas, respaldo o conceptos sobre cambios de alto impacto. Algunas veces de ser necesario se ofrecen capacitaciones técnicas al personal para afianzar o adquirir nuevos conocimientos mediante asignación de diplomados de preparación para certificaciones o de temas puntuales, en busca de que el conocimiento adquirido sea utilizado al interior de la compañía, pero en ocasiones éste personal deja la empresa después de un tiempo.
7.3	TOMA DE CONCIENCIA	L2	70%	Normalmente se utilizan los diversos medios de comunicación para difundir información necesaria para la toma de conciencia en diversos aspectos, incluyendo el modelo de seguridad de la información que actualmente se está utilizando
7.4	COMUNICACIÓN	L2	80%	Se tienen varias fuentes de comunicación y contacto con los usuarios, comunicados que se publican en la intranet, correos informativos, aplicación para capacitar a las personas con acceso desde la intranet
7.5	INFORMACIÓN DOCUMENTADA	L1	20%	
7.5.1	Generalidades	L1	20%	Los documentos existentes cuentan con las características requeridas
7.5.2	Creación y actualización	L1	20%	Al crear y actualizar los documentos existentes se tienen en cuenta las características necesarias
7.5.3	Control de la información documentada	L1	20%	Cuenta con algunos de los documentos requeridos y estos cuentan con los controles requeridos
8	**OPERACIÓN**			
8.1	PLANIFICACIÓN Y CONTROL OPERACIONAL	L1	40%	La organización cuenta con la planificación, implementación y control de algunos de los procesos necesarios para cumplir los requisitos
8.2	VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	L1	40%	Se tiene una valoración de riesgos general de los procesos que corresponden al alcance
8.3	TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	L1	40%	Para los riesgos identificados se tiene un tratamiento de riesgos pero se requiere utilizar la metodología MAGERIT para optimizar el proceso
9.	**EVALUACIÓN DEL DESEMPEÑO**			
9.1	SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN	L2	55%	

9.2	AUDITORÍA INTERNA	L2	60%	Actualmente la organización se encuentra familiarizada con las auditorías internas para los procesos existentes, pero antes de incorporar los programas de auditoría relacionados con éste sistema es necesario definir claramente los responsables, las tareas a cumplir, como se realizará la generación de informes, la importancia de los resultados de auditorías previas con el fin de validar el progreso paulatino del sistema, el alcance, entre otros.
9.3	REVISIÓN POR LA DIRECCIÓN	L2	50%	Actualmente la Junta Directiva es informada de los resultados consolidados a partir de las auditorías realizadas.
10.	**MEJORA**			
10.1	NO CONFORMIDADES Y ACCIONES CORRECTIVAS	L2	60%	Actualmente, según el modelo de seguridad debe informarse con detalle sobre la situación presentada a los dueños de los procesos a quienes se asocia el problema esto debe ser comunicado formalmente, comprometiendo la respuesta en un plazo máximo que podrá definirse en función del impacto o prioridad y de ser posible proponer los ajustes necesarios para tratar de resolver la situación.
10.2	MEJORA CONTINUA	L0	9%	De momento, el modelo de seguridad como tal no cuenta con un ciclo que permita su mejora continua, pero los procesos mejoran a medida que se realizan auditorías y se corrigen inconvenientes.

Tabla 2: Análisis Diferencial norma ISO/IEC 27001

ANÁLISIS DIFERENCIAL EN FUNCIÓN DE LA NORMA ISO27002

ANÁLISIS DIFERENCIAL NORMA ISO/IEC 27002				
Versión 1.0 de Octubre de 2016				
N	**Descripción**	**Estado**	**%**	**Evidencia o registro de implementación**
A.5	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN** 65%			
A 5.1	Orientación de la dirección para la gestión de la seguridad de la información 65%			
A.5.1.1	Políticas para la seguridad de la información	L2	60%	La política existe, se ajusta a las necesidades del banco, fue creada en función los objetivos de seguridad de la información y en su momento fue documentada y comunicada al interior de la organización. Sin embargo no existe un compromiso para cumplir con requisitos aplicables ni de mejora continua que incluya el compromiso de mejora continua del sistema de gestión de la

				seguridad de la información. Adicional a esto no cuenta con indicadores para validar su efectividad.
A.5.1.2	Revisión de las políticas para la seguridad de la información	L2	70%	Cuenta con personas responsables de su desarrollo, revisión y valoración, pero no se tiene programada su revisión periódica para incluir los ajustes necesarios
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 69%**			
A.6.1	Organización de la seguridad de la Información 63%			
A.6.1.1	Roles y responsabilidades para la seguridad de la información	L2	65%	Hace falta validar la eficacia de la política pero se apoyan las iniciativas de seguridad y se han aprobado los recursos necesarios para iniciar el plan de seguridad de la información y promover la concientización sobre seguridad.
A.6.1.2	Separación de deberes	L2	70%	Cuenta con segregación de ambientes y existe grupo de personas responsables por cada uno. Los procesos y activos de información se encuentran definidos pero actualmente no cuenta con dueños de información
A.6.1.3	Contacto con las autoridades	L2	85%	La empresa se mantiene en contacto con la superintendencia financiera de Colombia
A.6.1.4	Contacto con grupos de interés especial	L1	40%	Se tiene contacto con grupos especiales pero de momento no se tienen acuerdos de cooperación mutua
A.6.1.5	Seguridad de la información en la gestión de proyectos	L2	55%	En las fases iniciales de los proyectos se trata de involucrar temas relacionados a seguridad de la información, pero falta dar a conocer de forma masiva la importancia de ello.
A 6.2	Dispositivos móviles y teletrabajo 75%			
A 6.2.1	Política para dispositivos móviles	L2	70%	Cuenta con la política para uso de dispositivos móviles
A 6.2.2	Teletrabajo	L2	80%	Sólo personal autorizado puede acceder desde el portal indicando no sólo la clave de acceso, también la generada por token basado en red privada virtual (VPN)
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS 73%**			
A.7.1	Antes de la contratación 80%			

A.7.1.1	Investigación de antecedentes.	L2	80%	El banco realiza el proceso de selección de personal utilizando varios filtros y pruebas de desempeño (psicológico, psicotécnico, de aptitud, técnico, etc.), toda información obtenida del nuevo empleado es verificada: datos personales, referencias, estudios, antecedentes, historial de comportamiento crediticio, etc.
A.7.1.2	Términos y condiciones de contratación	L2	80%	Cláusulas contractuales, modelos de contratos con las cláusulas de confidencialidad.
A.7.2	Durante la contratación 70%			
A.7.2.1	Responsabilidades de gestión	L2	70%	Las políticas han sido documentadas y publicadas informando que debe cumplirse a cabalidad las recomendaciones dadas ante posibles medidas de sanción por su incumplimiento.
A.7.2.2	Concienciación, educación y capacitación en segur. de la información	L2	70%	Por cada cargo existe un respectivo manual de funciones y se tienen unos cursos de capacitación virtual con acceso desde la intranet que deben ser tomados por los empleados en relación a diversos temas incluyendo la seguridad de la información
A.7.2.3	Proceso disciplinario	L2	70%	En función del incumplimiento de las políticas de seguridad definidas se pueden tomar sanciones sobre el personal que pueden ir desde llamado de atención hasta despido dependiendo del impacto generado en la organización. Esto se encuentra documentado y publicado, sin embargo no se ha realizado una campaña para que sea de conocimiento de todo el personal.
A.7.3	Cese o cambio de puesto de trabajo 70%			
A.7.3.1	Cese o cambio de puesto de trabajo	L2	70%	Cuando un empleado se retira del banco su usuarios de red queda eliminado junto con sus privilegios, como ésta creación es centralizada por directorio activo ya podrá ingresar a ningún aplicativo. Si se trata de un cambio de perfil, implicará un cambio de accesos en función de la matriz de acceso. Para los usuarios que dejan de ser empleados del banco, se requiere una generación de paz y salvos en diversas áreas lo cual implica entrega de tarjetas de acceso, entrega del cargo como tal, entrega de token de acceso, etc.
A.8	**GESTIÓN DE ACTIVOS 65.4%**			
A.8.1	Responsabilidad sobre los activos 67,5%			

A.8.1.1	Inventario de activos	L2	70%	Anualmente el banco realiza una campaña entre los usuarios para actualizar el inventario de activos a cargo de cada persona diligenciando un formulario, en éste se ingresa el tipo de activo, el número de inventario físico que corresponde, descripción general del artículo, etc. A su vez, el personal actualiza información de su hoja de vida también de forma anual y la información relacionada con los activos de información se actualiza con cierta frecuencia. En cuanto a los activos de software, de momento no se han asignado los dueños de los activos y falta incluir información.
A.8.1.2	Propiedad de los activos	L1	40%	Se ha relacionado en cada caso el área a quién corresponde pero no se ha asignado un usuario específico para ello en cada caso, por tanto no se puede restringir o clasificar accesos a éste nivel
A.8.1.3	Uso aceptable de los activos	L2	70%	El banco cuenta con reglamentación al interior de la compañía para emisión y recepción de correos electrónicos por temas de seguridad. De igual modo se tiene restringida la red para usuarios específicos dependiendo de las tareas que desempañan.
A.8.1.4	Devolución de activos	L3	90%	Como se indicaba previamente al momento en que una persona se retira del banco debe solicitar paz y salvos a diversas áreas, donde cada uno se encarga de validar la entrega correspondiente de los activos que correspondan
A.8.2	Clasificación de la información 63%			
A.8.2.1	Directrices de clasificación	L2	70%	Se tienen definidas algunas directrices para clasificar información dependiendo de su confidencialidad, integridad y disponibilidad, el inconveniente que se tiene de momento es que no se actualiza dicha clasificación en momentos de cambio, dado que el área encargada no informa a tiempo de cambios generados que puedan generar activos de información por re-clasificar o nuevos activos de información
A.8.2.2	Etiquetado y manejo de información	L2	60%	El etiquetado de información ha sido realizado en uso de un proceso diseñado específicamente para esto, pero normalmente se realiza al inicio y no se reevalúan las etiquetas. Nota: Falta aclarar si las etiquetas son sólo de tipo físico o también existen digitales

A.8.2.3	Manipulación de activos	L2	60%	Se tiene implementado un proceso de clasificación de activos, pero se debe validar si todos los activos se encuentran clasificados en función de éste
A.9	**CONTROL DE ACCESO 66.81%**			
A.9.1	Requisitos de negocio para el control de accesos 80%			
A.9.1.1	Política de control de acceso	L2	80%	Cuenta con política y las correspondientes normas para dar cumplimiento a los requisitos
A.9.2	Gestión de acceso de usuario 80%			
A.9.2.1	Registro de usuarios	L2	80%	Cuenta con política y las correspondientes normas para dar cumplimiento a los requisitos
A.9.2.2	Gestión de privilegios	L2	80%	Cuenta con política y las correspondientes normas para dar cumplimiento a los requisitos
A.9.2.3	Gestión de contraseñas para usuario	L2	80%	Cuenta con política y las correspondientes normas para dar cumplimiento a los requisitos
A.9.2.4	Revisión de los derechos de acceso de los usuarios	L2	80%	Cuenta con política y las correspondientes normas para dar cumplimiento a los requisitos
A.9.3	Responsabilidades del usuario. 46.67%			
A.9.3.1	Uso de contraseñas	L2	80%	cuenta con la política para uso de token de seguridad y las correspondientes normas para dar cumplimiento a los requisitos
A.9.3.2	Equipo de usuario desatendido	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.9.3.3	Política de escritorio despejado y de pantalla despejada	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.9.4	Control de acceso a sistemas y aplicaciones 60.6%			
A.9.4.1	Política de uso de los servicios de red	L2	80%	Existe la política y las correspondientes normas para dar cumplimiento a los requisitos
A.9.4.2	Autenticación de usuarios para conexiones externas	L2	80%	cuenta con la política para uso de token de seguridad y las correspondientes normas para dar cumplimiento a los requisitos
A.9.4.3	Identificación de los equipos en las redes	L2	80%	cuenta con la política para uso de token de seguridad y las correspondientes normas para dar cumplimiento a los requisitos

A.9.4.4	Protección de los puertos de configuración y diagnóstico remoto	L2	80%	cuenta con la política para uso de token de seguridad y las correspondientes normas para dar cumplimiento a los requisitos
A.9.4.5	Separación en las redes	L1	20%	No cuenta con política asociada ni normas que estén asociadas al cumplimiento de estos requisitos
A.9.4.6	Control de conexión a las redes	L2	80%	Cuenta con política y las correspondientes normas para dar cumplimiento a los requisitos
A.9.4.7	Control de enrutamiento en la red	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.9.5.1	Procedimientos de ingreso seguro	L2	80%	Cuenta con política y las correspondientes normas para dar cumplimiento a los requisitos
A.9.5.2	Identificación y autenticación de usuarios	L2	80%	Cuenta con política y las correspondientes normas para dar cumplimiento a los requisitos
A.9.5.3	Sistema de gestión de contraseñas	L2	80%	Cuenta con política y las correspondientes normas para dar cumplimiento a los requisitos
A.9.5.4	Uso de las utilidades del sistema	L2	80%	Cuenta con política y las correspondientes normas para dar cumplimiento a los requisitos
A.9.5.5	Tiempo de inactividad de la sesión	L1	20%	No cuenta con política asociada ni normas que estén asociadas al cumplimiento de estos requisitos
A.9.5.6	Limitación del tiempo de conexión	L1	20%	No cuenta con política asociada ni normas que estén asociadas al cumplimiento de estos requisitos
A.9.6.1	Restricción de acceso a la información	L2	80%	Cuenta con política y las correspondientes normas para dar cumplimiento a los requisitos
A.9.6.2	Aislamiento de sistemas sensibles	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.9.7.1	Computación y comunicaciones móviles	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.9.7.2	Trabajo remoto	L2	80%	cuenta con la política para uso de token de seguridad y las correspondientes normas para dar cumplimiento a los requisitos
A.10	**CIFRADO 60%**			

A.10	Controles criptográficos. 60			
A.10.1.1	Política de uso de los controles criptográficos	L2	50%	Falta definir la política y las normas para su cumplimiento pero existe procedimiento definido para ello
A.10.1.2	Gestión de claves	L2	70%	Falta incluir normas más precisas para garantizar el cumplimiento
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL 62%**			
A.11.1	Requisitos de negocio para el control de acceso 78.33			
A.11.1.1	Perímetro de seguridad física	L2	80%	Las instalaciones cuentan con tarjetas de acceso limitado a las áreas de interés de los usuarios por cargo desempeñado y cuenta con personal para controlar el ingreso.
A.11.1.2	Controles de acceso físico	L2	80%	El personal que controla el ingreso registra los datos de todo visitante con fecha, hora de salida persona que autoriza su ingreso y solicita un documento de identificación para asignar tarjeta de visitante. El acceso a áreas con activos de información más sensible tienen acceso más restringido.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	L2	80%	Las instalaciones más críticas no son de acceso a público general y aunque se identifican como pertenecientes a la corporación no cuentan con letrero que indique su actividad. El directorio general con información sobre éstas instalaciones (dirección, teléfono, etc.) es de uso y publicación por la intranet.
A.11.1.4	Protección contra amenazas externas y ambientales	L2	80%	Las instalaciones cuentan con extintores, alarma de incendio. No se manejan materiales combustibles o inflamables al interior y los materiales de trabajo son ubicados en lugares estratégicos para su protección
A.11.1.5	Trabajo en áreas seguras	L2	80%	El conocimiento sobre áreas seguras por parte del personal es limitado, no se permite uso de dispositivos de ninguna forma de grabación al interior de éstas áreas. Falta validar si la forma de validación a trabajo no supervisado es efectiva
A.11.1.6	Áreas de carga, despacho y acceso público	L2	70%	Se da cumplimiento a las directrices sugeridas en general. Se permite acceso a personal que despacha a ciertas instalaciones para entrega directa puesto que no cuenta con zonas de despacho y entrega o porque los suministros son de tamaño menor, pero no cuentan con acompañamiento.
A.11.2	Seguridad de los equipos 45.5%			

A.11.2.1	Emplazamiento y protección de equipos	L2	70%	En general se cumple con las directrices propuestas, pero falta definir la que se encuentra relacionada con beber y comer cerca de servicios de procesamiento de información. Adicional a esto, las bodegas cumplen con las normas archivísticas para almacenamiento de documentos.
A.11.2.2	Instalaciones de suministro	L2	80%	Las instalaciones de la compañía cumplen en general con las recomendaciones indicadas.
A.11.2.3	Seguridad del cableado	L2	80%	Las instalaciones dan cumplimiento a los requisitos propuestos en cuanto a seguridad de cableado
A.11.2.4	Mantenimiento de los equipos	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.11.2.5	Salida de activos fuera de las dependencias de la empresa	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.11.2.8	Equipo informático de usuario desatendido	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.12	**GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES 52.5%**			
A.12.1	Responsabilidades y procedimientos de operación 75%			
A.12.1.1	Documentación de los procedimientos de operación	L2	80%	Existe la documentación y procedimientos pertinentes
A.12.1.2	Gestión del cambio	L2	80%	Existe la documentación y procedimientos pertinentes
A.12.1.3	Gestión de capacidades	L2	80%	Existe la documentación y procedimientos pertinentes
A.12.1.4	Separación de entornos de desarrollo, prueba y producción	L1	60%	Existe la segregación de ambientes pero no se encuentra relacionada con alguna política específica
A.12.2	Protección contra código malicioso 60%			
A.12.2.1	Controles contra el código malicioso	L1	60%	Existe la respectiva política existen los procedimientos asociados pero falta definir las normas para su cumplimiento

A.12.2.2	Monitoreo y revisión de los servicios por terceras partes	L1	60%	Existe la respectiva política existen los procedimientos asociados pero falta definir las normas para su cumplimiento
A.12.3	Copias de seguridad 60%			
A.12.3.1	Respaldo de la información	L1	60%	Existe la respectiva política existen los procedimientos asociados pero falta definir las normas para su cumplimiento
A.12.4	Registro de actividad y supervisión 52.5%			
A.12.4.1	Registro y gestión de eventos de actividad	L1	60%	Existe la respectiva política existen los procedimientos asociados pero falta definir las normas para su cumplimiento
A.12.4.2	Protección de los registros de información	L1	60%	Existe la respectiva política existen los procedimientos asociados pero falta definir las normas para su cumplimiento
A.12.4.3	Registros de actividad del administrador y operador del sistema.	L1	60%	Existe la respectiva política existen los procedimientos asociados pero falta definir las normas para su cumplimiento
A.12.4.4	Sincronización de relojes	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.12.5	Control del software en explotación. 30%			
A.12.5.1	Instalación del software en sistemas en producción	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.12.6	Gestión de la vulnerabilidad técnica 30%			
A.12.6.1	Gestión de las vulnerabilidades técnicas	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.12.7	Consideraciones de las auditorías de los sistemas de información. 60%			
A.12.7.1	Controles de auditoría de los sistemas de información.	L1	60%	Existe la respectiva política existen los procedimientos asociados pero falta definir las normas para su cumplimiento
A.13	**SEGURIDAD EN LAS TELECOMUNICACIONES 60%**			
A.13.1	Gestión de la seguridad en las redes 60%			
A.13.1.1	Controles de red	L1	60%	Existe la respectiva política existen los procedimientos asociados pero falta definir las normas para su cumplimiento
A.13.1.2	Mecanismos de seguridad asociados a servicios en red	L1	60%	Existe la respectiva política existen los procedimientos asociados pero falta definir las normas para su cumplimiento
A.13.1.3	Segregación de redes	L1	60%	Existe la respectiva política existen los procedimientos asociados

				pero falta definir las normas para su cumplimiento
A.13.2	Intercambio de información con partes externas 60%			
A.13.2.1	Políticas y procedimientos de intercambio de información	L1	60%	Existe la respectiva política existen los procedimientos asociados pero falta definir las normas para su cumplimiento
A.13.2.2	Acuerdos de intercambio	L1	60%	Existe la respectiva política existen los procedimientos asociados pero falta definir las normas para su cumplimiento
A.13.2.3	Mensajería electrónica	L1	30%	Existe la respectiva política, pero falta definir las normas para su cumplimiento
A.13.2.4	Acuerdos de confidencialidad y secreto	L1	60%	Existe la respectiva política existen los procedimientos asociados pero falta definir las normas para su cumplimiento
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN 10%**			
A.14.1	Requisitos de seguridad de los sistemas de información 20%			
A.14.1.1	Análisis y especificación de los requisitos de seguridad	L1	20%	Existe la respectiva política, pero falta definir las normas para su cumplimiento y los procedimientos
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	L1	20%	Existe la respectiva política, pero falta definir las normas para su cumplimiento y los procedimientos
A.14.1.3	Protección de las transacciones por redes telemáticas	L1	20%	Existe la respectiva política, pero falta definir las normas para su cumplimiento y los procedimientos
A.14.2	Seguridad en los procesos de desarrollo y soporte 5%			
A.14.2.1	Política de desarrollo seguro de software	L0	0%	No existe la respectiva política, ni las normas y procedimientos para su cumplimiento
A.14.2.2	Procedimientos de control de cambios en los sistemas	L0	5%	Falta definir las normas para su cumplimiento y los procedimientos existentes no se encuentran especialmente diseñados para el desarrollo
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L0	5%	Falta definir las normas para su cumplimiento y los procedimientos existentes no se encuentran especialmente diseñados para el desarrollo
A.14.2.4	Restricciones a los cambios en los paquetes de software	L0	5%	Falta definir las normas para su cumplimiento y los procedimientos existentes no se encuentran especialmente diseñados para el desarrollo

A.14.2.5	Uso de principios de ingeniería en protección de sistemas	L0	5%	Falta definir las normas para su cumplimiento y los procedimientos existentes no se encuentran especialmente diseñados para el desarrollo
A.14.2.6	Seguridad en entornos de desarrollo	L0	5%	Falta definir las normas para su cumplimiento y los procedimientos existentes no se encuentran especialmente diseñados para el desarrollo
A.14.2.7	Externalización del desarrollo de software	N/A		
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	L0	5%	Falta definir las normas para su cumplimiento y los procedimientos existentes no se encuentran especialmente diseñados para el desarrollo
A.14.2.9	Pruebas de aceptación.	L0	5%	Falta definir las normas para su cumplimiento y los procedimientos existentes no se encuentran especialmente diseñados para el desarrollo
A.14.3	Datos de prueba 5%			
A.14.3.1	Protección de los datos utilizados en pruebas	L0	5%	Falta definir las normas para su cumplimiento y los procedimientos existentes no se encuentran especialmente diseñados para el desarrollo
A.15	**RELACIONES CON SUMINISTRADORES**			
A.15.1	Seguridad de la información en las relaciones con suministradores.			
A.15.1.1	Política de seguridad de la información para suministradores	N/A		
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	N/A		
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	N/A		
A.15.2	Gestión de la prestación del servicio por suministradores			
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros	N/A		
A.15.2.2	Gestión de cambios en los servicios prestados por terceros	N/A		
A.16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN 45.71%**			

A.16.1	Gestión de incidentes de seguridad de la información y mejoras 45.71%			
A.16.1.1	Responsabilidades y procedimientos	L1	30%	Existe la respectiva política existen los procedimientos asociados pero falta completar las normas para su cumplimiento
A.16.1.2	Notificación de los eventos de seguridad de la información	L1	60%	Existe la respectiva política existen los procedimientos asociados pero falta completar las normas para su cumplimiento
A.16.1.3	Notificación de puntos débiles de la seguridad	L2	70%	Existen las normas pero falta definir detalles para ello
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	L1	30%	Existe la respectiva política existen los procedimientos asociados pero falta completar las normas para su cumplimiento
A.16.1.5	Respuesta a los incidentes de seguridad	L2	70%	Existen las normas pero falta definir detalles para la entrega de respuestas
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	L1	30%	Falta definir normas y procedimientos para su cumplimiento
A.16.1.7	Recopilación de evidencias	L1	30%	Falta definir normas y procedimientos para su cumplimiento
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO 68%**			
A.17.1	Continuidad de la seguridad de la información 66%			
A.17.1.1	Inclusión de la seguridad de la inf. En el proceso de gestión de la continuidad del negocio	L2	60%	Actualmente cuenta con un Plan de continuidad del negocio (BCP - Business Continuity Plan). El plan de continuidad de negocio se encuentra implementado, es necesario validar si aplica para la seguridad
A.17.1.2	Continuidad del negocio y evaluación de riesgos	L2	60%	El plan de continuidad de negocio se encuentra implementado, es necesario validar si aplica para la seguridad
A.17.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la inf.	L2	70%	El plan de continuidad de negocio se encuentra implementado, es necesario validar si aplica para la seguridad
A.17.1.4	Estructura para la planificación de la continuidad del negocio	L2	70%	El plan de continuidad de negocio se encuentra implementado, es necesario validar si aplica para la seguridad
A.17.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	L2	70%	El plan de continuidad de negocio se encuentra implementado, es necesario validar si aplica para la seguridad
A.17.2	Redundancias 70%			
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	L2	70%	Se cuenta con instalaciones con éste propósito específico y se tienen sitios de trabajo que pueden ser dedicados a esto de ser necesario

A.18	CUMPLIMIENTO 36.25%			
A.18.1	Cumplimiento de los requisitos legales y contractuales 42.5%			
A.18.1.1	Identificación de legislación aplicable	L2	50%	El modelo de seguridad de la información existente cuenta con información relacionada, falta validar si se da cumplimiento o si falta agregar elementos dado el alcance del SGSI
A.18.1.2	Derechos de propiedad intelectual (DPI)	L2	50%	El modelo de seguridad de la información existente cuenta con información relacionada, falta validar si se da cumplimiento o si falta agregar elementos dado el alcance del SGSI
A.18.1.3	Protección de los registros de la organización	L2	50%	El modelo de seguridad de la información existente cuenta con información relacionada, falta validar si se da cumplimiento o si falta agregar elementos dado el alcance del SGSI
A.18.1.4	Protección de los datos y privacidad de la información personal	L2	50%	El modelo de seguridad de la información existente cuenta con información relacionada, falta validar si se da cumplimiento o si falta agregar elementos dado el alcance del SGSI
A.18.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	L2	50%	El modelo de seguridad de la información existente cuenta con información relacionada, falta validar si se da cumplimiento o si falta agregar elementos dado el alcance del SGSI
A.18.1.6	Regulación de los controles criptográficos.	L0	5%	Existe el procedimiento y algunos controles definidos pero no existe regulación de los mismos
A.18.2	Revisiones de la seguridad de la información 30%			
A.18.2.1	Revisión independiente de la seguridad de la información	L2	50%	Es necesario validar los resultados existentes y generar nuevas revisiones
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	L1	20%	Es necesario realizar validaciones propias y validar el avance en función de validaciones previas realizadas por la organización
A.18.2.3	Comprobación del cumplimiento	L1	20%	Es necesario realizar validaciones propias y validar el avance en función de validaciones previas realizadas por la organización

Tabla 3: Análisis Diferencial norma ISO/IEC 27002

1.6. RESULTADOS

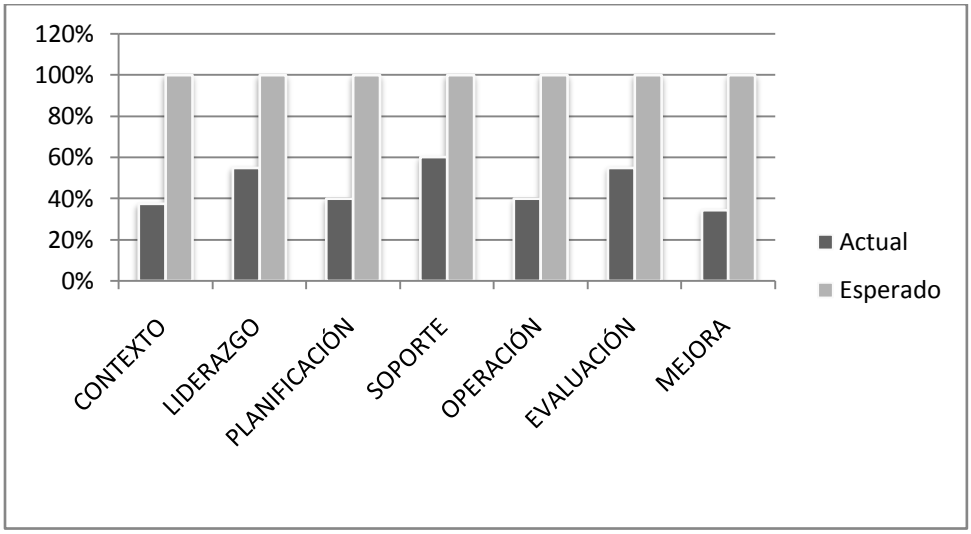


Figura 7: Análisis diferencial de ISO/IEC27001

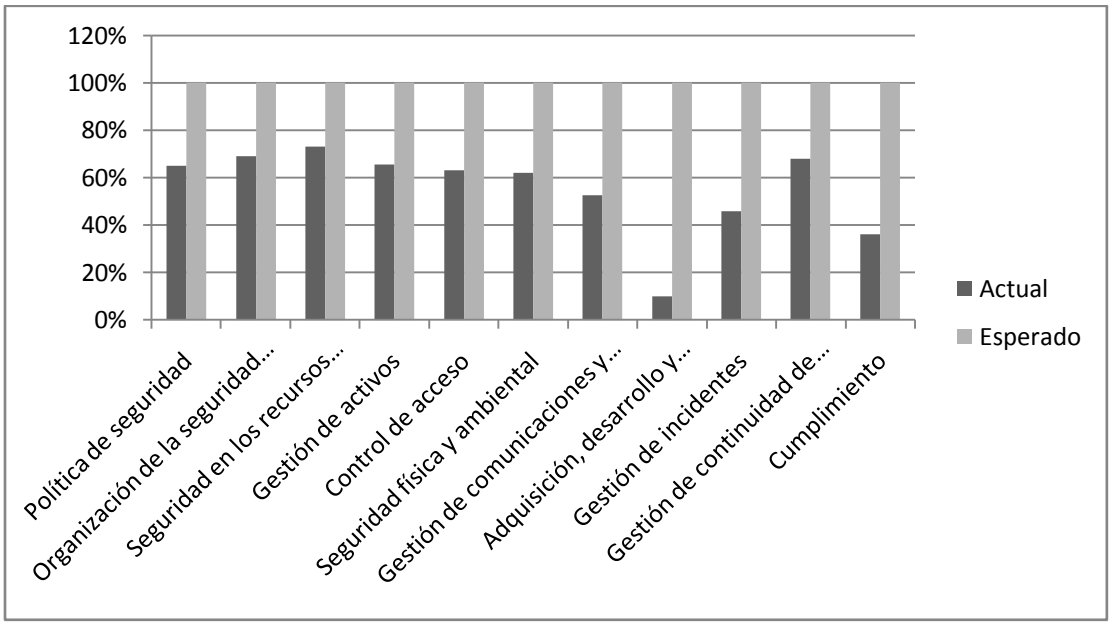


Figura 8: Análisis diferencial de ISO/IEC27002

2. FASE 2. SISTEMA DE GESTIÓN DOCUMENTAL

2.1. INTRODUCCIÓN

El principal objetivo de ésta fase, consiste en recopilar la documentación existente en la compañía que pueda incluirse o servir en la creación de los documentos que apoyarán al SGSI, así como crear los documentos requeridos.

2.2. ESQUEMA DOCUMENTAL

2.2.1. Política de seguridad

Anexo 1: Política de seguridad

2.2.2. Procedimiento de Auditorías Internas

Anexo 2: Procedimiento de auditorías internas

2.2.3. Gestión de Indicadores

Anexo 3: Procedimiento de Gestión de Indicadores

2.2.4. Procedimiento Revisión por Dirección

Anexo 4: Procedimiento Revisión por dirección

2.2.5. 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

Tabla 4: Roles y Responsabilidades

2.2.6. Metodología de Análisis de Riesgos

INTRODUCCIÓN

El análisis de riesgos es un proceso de gran importancia en todo SGSI puesto que en función de sus resultados nace la mayor parte de iniciativas y propuestas de proyectos, así como la motivación para realizarlos. Por tal motivo es importante conocer cuáles serán los pasos a seguir, los cuales fueron definidos utilizando como referencia la metodología MAGERIT.

PASO 1: Identificar los activos de información relevantes para el BANCO, su interrelación y su valor, en el sentido de qué perjuicio (costo) supondría su degradación

Fase 1: Identificar los activos de información

Definición de activo de información según la norma UNE 71504:2008

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008]

Dentro de éste concepto encaja una buena cantidad de componentes de la organización y es necesario validar según el alcance del SGSI si deben incluirse.

Fase 2: Validar dependencias de los activos

También, es importante identificar la relación existente entre los activos de información identificados con otros, dado que pueden verse afectados con una reacción en cadena o como un efecto colateral. Debe asegurarse la protección de activos de nivel inferior para garantizar la protección de los activos de nivel superior

Fase 3: Valoración de activos

Dando respuesta a la pregunta ¿Porqué es importante el activo? Se define el valor para cada uno de los activos identificados, para los niveles inferiores suele hacerse en función de los activos de nivel superior que se respaldan.

Fase 4: Valorar cada dimensión de la información por cada activo

Por cada una de las dimensiones de la información se deben hacer preguntas básicas sobre el impacto que puede generarse con respecto a cada activo, en caso de qué alguna de ellas falte con el objetivo de conocer cuáles son las dimensiones que deben preservarse por cada activo en mayor medida.

Confidencialidad: ¿Qué ocurriría si el activo es conocido por personal no autorizado?

Integridad: ¿Qué ocurriría si el activo es modificado por personal no autorizado?

Disponibilidad: ¿Qué ocurriría si el activo deja de estar disponible?

Autenticidad: ¿Qué ocurriría si se desconoce quién modifica el activo?

Fase 5: Realizar valoración definitiva

Teniendo en cuenta el resultado de la fase anterior es necesario valorar el costo de pérdida total del activo y éste costo puede ser tangible(monetario, equipos, etc.) o intangible(pérdida de credibilidad, pérdida de reputación, etc.) y pueden darse 3 tipos de valoración dependiendo del activo:

Valoración cualitativa

Valoración cuantitativa

Valor de interrupción de servicio

PASO 2: Determinar a qué amenazas están expuestos aquellos activos

Definición de amenaza según la norma UNE 71504:2008

Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008]

FASE 1: Identificación de amenazas

Tipos de amenaza según metodología MAGERIT	Descripción
De origen natural	Hay accidentes naturales (terremotos, inundaciones, ...). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.
Del entorno (de origen industrial)	Hay desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.
Defectos de las aplicaciones	Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, 'vulnerabilidades'.
Causadas por las personas de forma accidental	Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.
Causadas por las personas de forma deliberada	Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

Tabla 5: Tipos de amenaza según metodología MAGERIT

FASE 2: Valoración de amenazas

Es necesario validar el impacto que puede llegar a producir cada amenaza identificada a los activos, en función de:

Degradación: cuán perjudicado resultaría el [valor del] activo. Para asignar el valor se puede tomar de guía la siguiente tabla

Valor	Posibles descripciones		
MA	Muy alta	casi seguro	Fácil
A	alta	muy alto	medio
M	media	posible	Difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Tabla 6: Valores de degradación

Probabilidad: cuán probable o improbable es que se materialice la amenaza. Para asignar el valor se puede tomar de guía la siguiente tabla

Valor	Posibles descripciones		
MA	100	muy frecuente	A diario
A	10	frecuente	Mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	Siglos

Tabla 7: Probabilidad de ocurrencia

FASE 3: Determinación de impacto potencial

Deben calcularse el impacto, impacto acumulado y el impacto repercutido por cada amenaza de cada activo, esto sin tener en cuenta las salvaguardas existentes.

Definición de impacto

Medida del daño provocado sobre el activo cuando se materializa una amenaza

Definición de impacto acumulado

Corresponde al valor propio más el acumulado de los activos que dependen de él y teniendo en cuenta las amenazas a las que está expuesto, sería conveniente valor la estructura de dependencia por capas de MAGERIT. Es calculado para cada activo, por

cada amenaza y en cada dimensión de valoración.

Definición de impacto repercutido

Corresponde al valor propio y de la degradación causada, que permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es calculado para cada activo, por cada amenaza y en cada dimensión de valoración.

PASO 3: Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo

Una vez identificadas y valoradas las amenazas, debe evaluarse cada amenaza con el objetivo de encontrar salvaguardas para reducir su impacto o prevenir su materialización.

Caracterización de actividades: Incluye 2 actividades

FASE 1: Identificación de salvaguardas

1. Validar cuáles son los tipos de activos a proteger, dado que cada tipo se protege de una forma específica

2. Identificar cuál dimensión o dimensiones de seguridad requieren mayor protección

3. Establecer cuáles son las amenazas de las que necesitamos protegernos

4. Por último, validar si existen salvaguardas alternativas

Una vez identificadas las salvaguardas es necesario descartar y definir cuáles de ellas serán utilizadas, para ello se requiere decidir cuáles no aplican o cuáles no se justifican

FASE 2: Valoración de las salvaguardas

Existen 2 posibles efectos de las salvaguardas en función de los riesgos:

1. Reducir la probabilidad de las amenazas

2. Limitando el daño causado

Estos efectos suelen estar relacionados con el tipo de acción:

[PR] Prevención: Su objetivo es reducir la probabilidad de que ocurra un incidente

[DR] Disuasión: Tiene por efecto que ante su presencia los atacantes no se atreven a atacar.

[EL] Eliminación: Eliminan la amenaza

[IM] Minimización del impacto / limitación del impacto: Reduce las consecuencias en caso de que se materialice la amenaza

[CR] Corrección: Una vez se produzcan los daños los repara

[RC] Recuperación: Si se producen los daños permite la recuperación a su estado original

[MN] Monitorización: Permiten prevenir que se materialicen las amenazas o nos permite aprender de los incidentes

[DC] Detección: Detecta los ataques e informa que están ocurriendo

[AW] Concienciación: Forma a los usuarios sobre sus deberes frente y las actividades que no pueden realizar

[AD] Administración: Relaciona los componentes de seguridad instalados y configurados

PASO 4: Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza

Cuando fue determinado el impacto por cada amenaza en el PASO 2, no se había considerado la influencia de las salvaguardas o controles existentes, pero en éste PASO debe tenerse en cuenta el efecto de las salvaguardas para calcular nuevamente el impacto definitivo.

PASO 5: Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

Por último, se debe definir nuevamente el impacto potencial teniendo en cuenta los valores obtenidos del impacto definitivo y la frecuencia final para obtener el impacto ponderado.

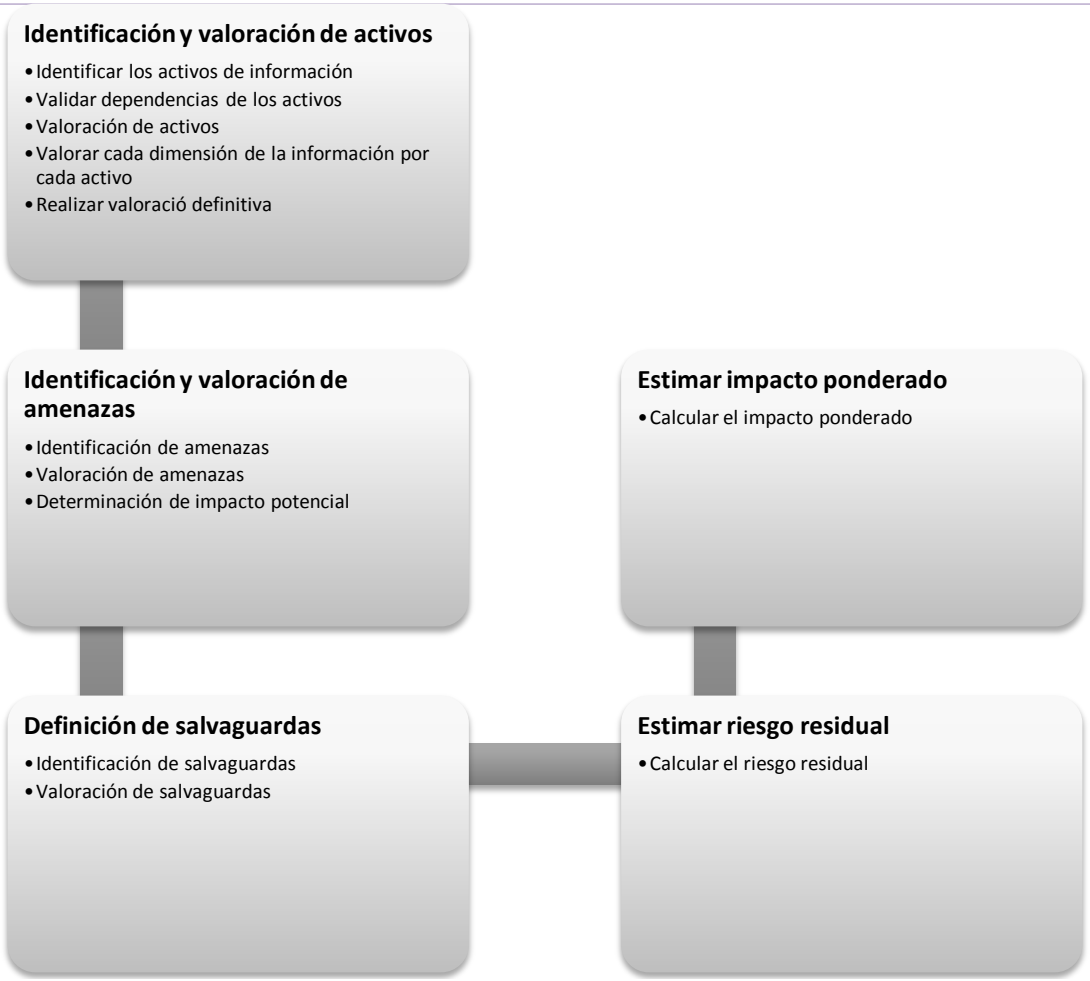


Figura 9: Metodología de Análisis de riesgos

2.2.7. Declaración de Aplicabilidad

DECLARACIÓN DE APLICABILIDAD NORMA ISO27002				
Versión 1.0 de Octubre de 2016				
Numeral	**Descripción**	**A**	**Motivo por el que aplica o no aplica**	**Evidencia o registro de implementación**
A.5	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**			
A 5.1	Orientación de la dirección para la gestión de la seguridad de la información			
A.5.1.1	Políticas para la seguridad de la información	Si	Aplica en todo el SGSI	Documento de política
A.5.1.2	Revisión de las políticas para la seguridad de la información	Si	Se debe revisar periódicamente y documentar las acciones de mejora	
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**			
A.6.1	Organización de la seguridad de la Información			
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Si	A las áreas deben asociarse las responsabilidades frente al SGSI.	Documento con la inclusión de las responsabilidades o en los cargos o en los procesos.
A.6.1.2	Separación de deberes	Si	A las áreas deben asociarse las responsabilidades frente al SGSI.	Documento con la inclusión de las responsabilidades o en los cargos o en los procesos.
A.6.1.3	Contacto con las autoridades	Si	Las reacciones a tiempo frente a incidentes, permite la reducción de riesgos	Listado y procedimiento de cómo contactar a las autoridades legales y de control
A.6.1.4	Contacto con grupos de interés especial	Si	Es necesario mantener informado sobre los acontecimientos en seguridad, con ello, poder retroalimentar el SGSI y los incidentes de seguridad	
A.6.1.5	Seguridad de la información en la gestión de proyectos	Si	Las auditorías externas hacen más fuerte y transparente el proceso de implementación del SGSI	contrato anual con revisores/auditoría externa
A 6.2	Dispositivos móviles y teletrabajo			

A 6.2.1	Política para dispositivos móviles	Si	Es necesario llevar control del personal que puede acceder a información desde dispositivos que pueden ser sacados de las instalaciones de la corporación	
A 6.2.2	Teletrabajo	Si	Es necesario llevar control del personal que puede acceder remotamente a los recursos tecnológicos	Documentos de solicitud para acceso remoto, Documento que describe la política de acceso a información al realizar teletrabajo
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
A.7.1	Antes de la contratación			
A.7.1.1	Investigación de antecedentes.	Si	Desde los procesos iniciales de ingreso del personal, se debe establecer parámetros de seguridad	Inclusión de elementos de seguridad sobre los procesos de selección de personal
A.7.1.2	Términos y condiciones de contratación	Si	La información es fundamental su protección ante develado	Cláusulas contractuales, modelos de contratos con las cláusulas de confidencialidad.
A.7.2	Durante la contratación			
A.7.2.1	Responsabilidades de gestión	Si	Es necesario que a las áreas deben asociarse las responsabilidades frente al SGSI.	Documento con la inclusión de las responsabilidades o en los cargos o en los procesos.
A.7.2.2	Concienciación, educación y capacitación en segur. de la información	Si	Ser competitivos es de gran importancia para la implementación y mantenimiento del SGSI, esto implica tener planes de capacitación frente a los temas de seguridad	
A.7.2.3	Proceso disciplinario	Si	El control es fundamental en cualquier organización, las faltas de los empleados deben ser investigadas y sancionadas	Inclusión de elementos de seguridad sobre los procesos de selección de personal
A.7.3	Cese o cambio de puesto de trabajo			
A.7.3.1	Cese o cambio de puesto de trabajo	Si	A las áreas deben asociarse las responsabilidades frente al SGSI, dentro de éstas, la devolución de activos y accesos que le fueron asignados.	Procedimiento para el retiro de puesto de trabajo y equipos informáticos. Documento con la inclusión de las responsabilidades o en los cargos o en los procesos.

A.8	**GESTIÓN DE ACTIVOS**			
A.8.1	Responsabilidad sobre los activos			
A.8.1.1	Inventario de activos	Si	Es necesario conocer los activos de información acorde al alcance, para una adecuada gestión de riesgos y tratamiento de estos	Listado con activos de información
A.8.1.2	Propiedad de los activos	Si	Cada activo de información debe tener un responsable	Listado con activos de información con responsable
A.8.1.3	Uso aceptable de los activos	Si	Todo sistema informático debe contar con procedimientos de aceptación de los sistemas antes de su funcionamiento.	Actas de aceptación de los sistemas
A.8.1.4	Devolución de activos	Si	A las áreas deben asociarse las responsabilidades frente al SGSI, dentro de éstas, la devolución de activos que le fueron asignados.	Procedimiento para el retiro de puesto de trabajo y equipos informáticos.
A.8.2	Clasificación de la información			
A.8.2.1	Directrices de clasificación	Si	La información debe protegerse acorde a su criticidad, por ello es necesario clasificarla	
A.8.2.2	Etiquetado y manejo de información	Si	La información debe protegerse acorde a su criticidad, por ello es necesario clasificarla	
A.8.2.3	Manipulación de activos	Si	A las áreas deben asociarse las responsabilidades frente al SGSI.	
A.9	**CONTROL DE ACCESO**			
A.9.1.1	Requisitos de negocio para el control de accesos			
A.9.1.1	Política de control de acceso	Si	Tiene una aplicabilidad global en todo el SGSI	Documento de política
A.9.2.1	Registro de usuarios	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general

A.9.2.2	Gestión de privilegios	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general
A.9.2.3	Gestión de contraseñas para usuario	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de contraseñas
A.9.2.4	Revisión de los derechos de acceso de los usuarios	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimientos para la revisión periódica de accesos.
A.9.3.1	Uso de contraseñas	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de contraseñas
A.9.3.2	Equipo de usuario desatendido	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Control de sesiones en equipos.
A.9.3.3	Política de escritorio despejado y de pantalla despejada	Si	La información sensible debe estar coherentemente resguardada	Planes de sensibilización sobre la protección de la información
A.9.4.1	Política de uso de los servicios de red	Si	El control de acceso a las redes debe permitir la reducción de los riesgos	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.9.4.2	Autenticación de usuarios para conexiones externas	Si	El control de acceso a las redes debe permitir la reducción de los riesgos	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento). Definiciones de cómo proteger los canales de comunicación (VPN)
A.9.4.3	Identificación de los equipos en las redes	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de contraseñas

A.9.4.4	Protección de los puertos de configuración y diagnóstico remoto	Si	El control de acceso a las redes debe permitir la reducción de los riesgos	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.9.4.5	Separación en las redes	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos	Documento de arquitectura para la segmentación de las redes y los ambientes de procesamiento, que incluya gestión de la capacidad y expansión de la red
A.9.4.6	Control de conexión a las redes	Si	El control de acceso a las redes debe permitir la reducción de los riesgos	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.9.4.7	Control de enrutamiento en la red	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos	Documento de arquitectura para la segmentación de las redes y los ambientes de procesamiento, que incluya gestión de la capacidad y expansión de la red
A.9.5.1	Procedimientos de ingreso seguro	Si	El control de acceso a las redes debe permitir la reducción de los riesgos	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.9.5.2	Identificación y autenticación de usuarios	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de contraseñas
A.9.5.3	Sistema de gestión de contraseñas	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de contraseñas
A.9.5.4	Uso de las utilidades del sistema	Si	Todo sistema informático debe contar con procedimientos de aceptación de los sistemas antes de su funcionamiento.	Actas de aceptación de los sistemas
A.9.5.5	Tiempo de inactividad de la sesión	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de sesiones
A.9.5.6	Limitación del tiempo de conexión	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de sesiones

A.9.6.1	Restricción de acceso a la información	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de sesiones
A.9.6.2	Aislamiento de sistemas sensibles	Si	Los sistemas sensibles deben tener un nivel de seguridad más alto.	
A.9.7.1	Computación y comunicaciones móviles	Si	La movilidad es fundamental en las organizaciones de hoy y por ello, se deben proteger	
A.9.7.2	Trabajo remoto	Si	El control de acceso a las redes debe permitir la reducción de los riesgos	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento). Definiciones de cómo proteger los canales de comunicación (VPN)
A.10	**CIFRADO**			
A.10	Controles criptográficos.			
A.10.1.1	Política de uso de los controles criptográficos	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales.
A.10.1.2	Gestión de claves	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales.
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL**			
A.11.1	Requisitos de negocio para el control de acceso			
A.11.1.1	Perímetro de seguridad física	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales.
A.11.1.2	Controles de acceso físico	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales.

A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales.
A.11.1.4	Protección contra amenazas externas y ambientales	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales. Tener contacto con las autoridades.
A.11.1.5	Trabajo en áreas seguras	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales. Tener contacto con las autoridades.
A.11.1.6	Áreas de carga, despacho y acceso público	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales. Control de acceso físico en las áreas de carga
A.11.2	Seguridad de los equipos			
A.11.2.1	Emplazamiento y protección de equipos	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Los equipos de misión crítica deben ser protegidos en centros de datos.
A.11.2.2	Instalaciones de suministro	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Procedimientos y control de suministros eléctricos y utilitarios
A.11.2.3	Seguridad del cableado	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Procedimiento de control de acceso a centro de datos y centros de cableados
A.11.2.4	Mantenimiento de los equipos	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Ejecución de contratos sobre equipos informáticos incluyendo mantenimientos preventivos y de soporte.

A.11.2.5	Salida de activos fuera de las dependencias de la empresa	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Ejecución de contratos sobre equipos informáticos incluyendo pólizas y seguros.
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Ejecución de contratos sobre equipos informáticos incluyendo pólizas y seguros.
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Procedimientos de borrado seguro de información sin recuperación
A.11.2.8	Equipo informático de usuario desatendido	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Documentos y manuales de operación
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	Si	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	procedimientos para el ingreso y retiro de equipos tecnológicos a las instalaciones
A.12	**GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES**			
A.12.1	Responsabilidades y procedimientos de operación			
A.12.1.1	Documentación de los procedimientos de operación	Si	Todos los procedimientos operativos deben estar documentados.	Documentos y manuales de operación
A.12.1.2	Gestión del cambio	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos	Procesos y procedimientos para la gestión del cambio.
A.12.1.3	Gestión de capacidades	Si	A las áreas deben asociarse las responsabilidades frente al SGSI.	Documento con la inclusión de las responsabilidades, funciones o en los cargos o en los procesos, los cuales debe estar segregados en la ejecución de actividades

A.12.1.4	Separación de entornos de desarrollo, prueba y producción	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos	Documento de arquitectura para la segmentación de las redes y los ambientes de procesamiento, que incluya gestión de la capacidad y expansión de la red
A.12.2	Protección contra código malicioso			
A.12.2.1	Controles contra el código malicioso	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos	Documento de arquitectura para la segmentación de las redes y los ambientes de procesamiento.
A.12.2.2	Monitoreo y revisión de los servicios por terceras partes	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos	Procesos y procedimientos de monitoreo de funciones ejecutadas
A.12.2.3	Gestión de los cambios en servicios por terceras partes	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos	Procesos y procedimientos de monitoreo de funciones ejecutadas
A.12.3.1	Gestión de la capacidad	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos	Documento de arquitectura para la segmentación de las redes y los ambientes de procesamiento, que incluya gestión de la capacidad y expansión de la red
A.12.3.2	Aceptación del sistema	Si	Todo sistema informático debe contar con procedimientos de aceptación de los sistemas antes de su funcionamiento.	Actas de aceptación de los sistemas
A.12.4.1	Controles contra códigos maliciosos	Si	Se debe controlar de manera adecuada los códigos maliciosos.	
A.12.4.2	Controles contra códigos móviles	Si	Se debe controlar de manera adecuada los códigos maliciosos.	
A.12.4.4	Sincronización de relojes	Si	El tiempo es fundamental en los sistemas y más aún en las aplicaciones de tiempo real Online).	procedimiento para la configuración de NTP.
A.12.5.1	Respaldo de la información	Si	Ante eventos de seguridad, es necesario contar con Backus que permitan la recuperación de la información.	procedimientos para el respaldo de la información.

A.12.6.1	Controles de las redes	Si	El control de acceso a las redes debe permitir la reducción de los riesgos	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.12.6.2	Seguridad de los servicios de la red	Si	El control de acceso a las redes debe permitir la reducción de los riesgos	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.12.7.1	Gestión de los medios removibles	Si	Se debe tener control y planes de sensibilización con respecto a los medios removibles	Procedimientos y políticas en la red para el uso de medios removibles
A.12.7.2	Eliminación de los medios	Si	Se debe tener control y planes de sensibilización con respecto a los medios removibles	Procedimientos de borrado seguro de información sin recuperación
A.12.7.3	Procedimientos para el manejo de la información	Si	Tanto la clasificación como los planes de sensibilización fortalecen la reducción de riesgos sobre el inadecuado manejo de la información.	Documento con niveles de clasificación y ejecución de planes de sensibilización.
A.12.7.4	Seguridad de la documentación del sistema	Si	Tanto la clasificación como los planes de sensibilización fortalecen la reducción de riesgos sobre el inadecuado manejo de la información.	Procedimientos y herramientas técnicas para la protección de la documentación.
A.12.8.1	Políticas y procedimientos para el intercambio de la información	Si	Tanto la clasificación como los planes de sensibilización fortalecen la reducción de riesgos sobre el inadecuado manejo de la información.	Documento con niveles de clasificación, ejecución de planes de sensibilización y procedimientos para el intercambio de información.
A.12.8.2	Acuerdos para el intercambio	Si	Tanto la clasificación como los planes de sensibilización fortalecen la reducción de riesgos sobre el inadecuado manejo de la información.	Documento con niveles de clasificación, ejecución de planes de sensibilización y procedimientos para el intercambio de información. herramientas técnicas para la protección de la documentación
A.12.8.3	Medios físicos en tránsito	Si	Se debe tener control y planes de sensibilización con respecto a los medios removibles	Procedimientos y políticas en la red para el uso de medios removibles

A.12.8.4	Mensajería electrónica	Si	Las áreas hacen uso de la mensajería y aplicaciones de transacciones (online) como una herramienta de trabajo, por ello se debe proteger	
A.12.8.5	Sistemas de información del negocio	Si	Las áreas hacen uso de la mensajería y aplicaciones de transacciones (online) como una herramienta de trabajo, por ello se debe proteger	
A.12.9.1	Comercio electrónico	No	No hace parte del alcance	N/A
A.12.9.2	Transacciones en línea	No	No hace parte del alcance	N/A
A.12.9.3	Información disponible al público	No	No hace parte del alcance	N/A
A.12.10.1	Registro de auditorías	Si	Los logs y registros deben estar configurados y protegidos para validaciones, monitoreos y manejo de incidentes de seguridad	procedimiento con las recomendaciones de configuración de logs y registros de auditorías, así como la protección de estos.
A.12.10.2	Monitoreo del uso del sistema	Si	Los sistemas deben ser monitoreados de manera permanente.	Procedimientos de monitoreo
A.12.10.3	Protección de la información del registro	Si	Los logs y registros deben estar configurados y protegidos para validaciones, monitoreos y manejo de incidentes de seguridad	procedimiento con las recomendaciones de configuración de logs y registros de auditorías, así como la protección de estos.
A.12.10.4	Registros del administrador y del operador	Si	Los logs y registros deben estar configurados y protegidos para validaciones, monitoreos y manejo de incidentes de seguridad	procedimiento con las recomendaciones de configuración de logs y registros de auditorías, así como la protección de estos.
A.12.10.5	Registro de fallas	Si	Los logs y registros deben estar configurados y protegidos para validaciones, monitoreos y manejo de incidentes de seguridad	procedimiento con las recomendaciones de configuración de logs y registros de auditorías, así como la protección de estos.
A.13	**SEGURIDAD EN LAS TELECOMUNICACIONES**			
A.13.1	Gestión de la seguridad en las redes			

A.13.1.1	Controles de red	Si	El control de acceso a las redes debe permitir la reducción de los riesgos	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.13.1.2	Mecanismos de seguridad asociados a servicios en red	Si	El control de acceso a las redes debe permitir la reducción de los riesgos	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.13.1.3	Segregación de redes	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos	Documento de arquitectura para la segmentación de las redes y los ambientes de procesamiento.
A.13.2	Intercambio de información con partes externas			
A.13.2.1	Políticas y procedimientos de intercambio de información	Si	Tanto la clasificación como los planes de sensibilización fortalecen la reducción de riesgos sobre el inadecuado manejo de la información.	Documento con niveles de clasificación
A.13.2.2	Acuerdos de intercambio	Si	Tanto la clasificación como los planes de sensibilización fortalecen la reducción de riesgos sobre el inadecuado manejo de la información.	Documento con niveles de clasificación, ejecución de planes de sensibilización y procedimientos para el intercambio de información.
A.13.2.3	Mensajería electrónica	Si	Las áreas hacen uso de la mensajería y aplicaciones de transacciones (online) como una herramienta de trabajo, por ello se debe proteger	procedimientos para el control de acceso sobre la mensajería, criptografía e implementación de sistemas Anti-X
A.13.2.4	Acuerdos de confidencialidad y secreto	Si	La información es fundamental su protección ante develado	Cláusulas contractuales, modelos de contratos con las cláusulas de confidencialidad.
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**			
A.14.1	Requisitos de seguridad de los sistemas de información			
A.14.1.1	Análisis y especificación de los requisitos de seguridad	Si	Los desarrollos y mantenimiento de sistemas de información son un foco de vulnerabilidades, por ello se les debe dar máxima prioridad en la protección, más aún, cuando son sitios web Online	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones (línea base) que incluya éste numeral.

A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	Si	Los desarrollos y mantenimiento de sistemas de información son un foco de vulnerabilidades, por ello se les debe dar máxima prioridad en la protección, más aún, cuando son sitios web Online	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones (línea base) que incluya éste numeral.
A.14.1.3	Protección de las transacciones por redes telemáticas	Si	Los desarrollos y mantenimiento de sistemas de información son un foco de vulnerabilidades, por ello se les debe dar máxima prioridad en la protección, más aún, cuando son sitios web Online	Planes de sensibilización sobre la protección de la información, controles criptográficos
A.14.2	Seguridad en los procesos de desarrollo y soporte			
A.14.2.1	Política de desarrollo seguro de software	Si	Los desarrollos y mantenimiento de sistemas de información son un foco de vulnerabilidades, por ello se les debe dar máxima prioridad en la protección, más aún, cuando son sitios web Online	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones (línea base) que incluya éste numeral.
A.14.2.2	Procedimientos de control de cambios en los sistemas	Si	Los desarrollos y mantenimiento de sistemas de información son un foco de vulnerabilidades, por ello se les debe dar máxima prioridad en la protección, más aún, cuando son sitios web Online	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones (línea base) que incluya éste numeral.
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Si	Los desarrollos y mantenimiento de sistemas de información son un foco de vulnerabilidades, por ello se les debe dar máxima prioridad en la protección, más aún, cuando son sitios web Online	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones (línea base) que incluya éste numeral.
A.14.2.4	Restricciones a los cambios en los paquetes de software	Si	Los desarrollos y mantenimiento de sistemas de información son un foco de vulnerabilidades, por ello se les debe dar máxima prioridad en la protección, más aún, cuando son sitios web Online	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones (línea base) que incluya éste numeral.

A.14.2.5	Uso de principios de ingeniería en protección de sistemas	Si	Los desarrollos y mantenimiento de sistemas de información son un foco de vulnerabilidades, por ello se les debe dar máxima prioridad en la protección, más aún, cuando son sitios web Online	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones (línea base) que incluya éste numeral.
A.14.2.6	Seguridad en entornos de desarrollo	Si	Los desarrollos y mantenimiento de sistemas de información son un foco de vulnerabilidades, por ello se les debe dar máxima prioridad en la protección, más aún, cuando son sitios web Online	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones (línea base) que incluya éste numeral.
A.14.2.7	Externalización del desarrollo de software	No	Todos los desarrollos relacionados en el alcance son internos	N/A
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	Si	Para tener un control de los riesgos en los sistemas, es fundamental conocer de manera técnica qué tipo de vulnerabilidades se tienen, tanto en las redes, como en los SI y las aplicaciones.	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones (línea base) que incluya éste numeral.
A.14.2.9	Pruebas de aceptación.	Si	Para tener un control de los riesgos en los sistemas, es fundamental conocer de manera técnica qué tipo de vulnerabilidades se tienen, tanto en las redes, como en los SI y las aplicaciones.	Documento de planeación y diseño de las pruebas de seguridad periódicas a realizar.
A.14.3	Datos de prueba			
A.14.3.1	Protección de los datos utilizados en pruebas	Si	Para tener un control de los riesgos en los sistemas, es fundamental conocer de manera técnica qué tipo de vulnerabilidades se tienen, tanto en las redes, como en los SI y las aplicaciones.	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones (línea base) que incluya éste numeral.
A.15	**RELACIONES CON SUMINISTRADORES**			
A.15.1	Seguridad de la información en las relaciones con suministradores.			
A.15.1.1	Política de seguridad de la información para suministradores	No	Los desarrollos son en casa y los servicios que corresponden al alcance no son	N/A

			externos	
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	No	Los desarrollos son en casa y los servicios que corresponden al alcance no son externos	N/A
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	No	Los desarrollos son en casa y los servicios que corresponden al alcance no son externos	N/A
A.15.2	Gestión de la prestación del servicio por suministradores			
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros	No	Los desarrollos son en casa y los servicios que corresponden al alcance no son externos	N/A
A.15.2.2	Gestión de cambios en los servicios prestados por terceros	No	Los desarrollos son en casa y los servicios que corresponden al alcance no son externos	N/A
A.16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**			
A.16.1	Gestión de incidentes de seguridad de la información y mejoras			
A.16.1.1	Responsabilidades y procedimientos	Si	Parte fundamental de la gestión de riesgos es las fuentes de incidentes de seguridad y la gestión sobre éstos, por ello se deben reportar adecuadamente	Documento de políticas de seguridad, documento con las responsabilidades de las áreas frente a los incidentes de seguridad.
A.16.1.2	Notificación de los eventos de seguridad de la información	Si	Parte fundamental de la gestión de riesgos es las fuentes de incidentes de seguridad y la gestión sobre éstos, por ello se deben reportar adecuadamente	Documento de planeación y diseño de las pruebas de seguridad periódicas a realizar.
A.16.1.3	Notificación de puntos débiles de la seguridad	Si	Parte fundamental de la gestión de riesgos es las fuentes de incidentes de seguridad y la gestión sobre éstos, por ello se deben reportar adecuadamente	Herramienta para la documentación de Incidentes de seguridad
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	Si	Parte fundamental de la gestión de riesgos es las fuentes de incidentes de seguridad y la gestión sobre éstos, por ello se deben reportar adecuadamente	Herramienta para la documentación de Incidentes de seguridad y evidencia de la gestión del conocimiento

A.16.1.5	Respuesta a los incidentes de seguridad	Si	Parte fundamental de la gestión de riesgos es las fuentes de incidentes de seguridad y la gestión sobre éstos, por ello se deben reportar adecuadamente	Documento de políticas de seguridad, documento con las responsabilidades de las áreas frente a los incidentes de seguridad.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Si	Parte fundamental de la gestión de riesgos es las fuentes de incidentes de seguridad y la gestión sobre éstos, por ello se deben reportar adecuadamente	Herramienta para la documentación de Incidentes de seguridad y evidencia de la gestión del conocimiento
A.16.1.7	Recopilación de evidencias	Si	Parte fundamental de la gestión de riesgos es las fuentes de incidentes de seguridad y la gestión sobre éstos, por ello se deben reportar adecuadamente	Procedimientos para la identificación, recolección, embalaje y tratamiento de la evidencia digital.
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**			
A.17.1	Continuidad de la seguridad de la información			
A.17.1.1	Inclusión de la seguridad de la inf. En el proceso de gestión de la continuidad del negocio	Si	La recuperación ante desastres y los planes de contingencia son fundamentales y dentro de estos, es necesario asegurar la información	Documento y procedimiento para la continuidad de negocio
A.17.1.2	Continuidad del negocio y evaluación de riesgos	Si	La recuperación ante desastres y los planes de contingencia son fundamentales y dentro de estos, es necesario asegurar la información	Documento y procedimiento para la continuidad de negocio
A.17.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la inf.	Si	La recuperación ante desastres y los planes de contingencia son fundamentales y dentro de estos, es necesario asegurar la información	Documento y procedimiento para la continuidad de negocio
A.17.1.4	Estructura para la planificación de la continuidad del negocio	Si	La recuperación ante desastres y los planes de contingencia son fundamentales y dentro de estos, es necesario asegurar la información	Documento y procedimiento para la continuidad de negocio
A.17.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	Si	La recuperación ante desastres y los planes de contingencia son fundamentales y dentro de estos, es	Documento y procedimiento para la continuidad de negocio

			necesario asegurar la información	
A.17.2	Redundancias			
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	Si	La recuperación ante desastres y los planes de contingencia son fundamentales y dentro de estos, es necesario asegurar la información	Documento y procedimiento para la continuidad de negocio
A.18	**CUMPLIMIENTO**			
A.18.1	Cumplimiento de los requisitos legales y contractuales			
A.18.1.1	Identificación de legislación aplicable	Si	Es necesario conocer las reglamentaciones a nivel Colombia que aplican para el sector de las telecomunicaciones y sistemas informáticos.	Documento con las normas/leyes que aplican al MSI
A.18.1.2	Derechos de propiedad intelectual (DPI)	Si	Es necesario conocer las reglamentaciones a nivel Colombia que aplican para el sector de las telecomunicaciones	Documento con las normas/leyes que aplican al MSI
A.18.1.3	Protección de los registros de la organización	Si	Tanto los log, registros así como las herramientas de auditoría y monitorea deben ser protegidas contra accesos no autorizados.	Procedimiento de control de acceso sobre sistemas de información y aplicaciones
A.18.1.4	Protección de los datos y privacidad de la información personal	Si	Es necesario conocer las reglamentaciones a nivel Colombia que aplican para el sector de las telecomunicaciones	Documento con las normas/leyes que aplican al MSI
A.18.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	Si	Se deben implementar controles persuasivos y disuasivos en los sistemas y plataformas.	Documento con las normas/leyes que aplican al MSI
A.18.1.6	Regulación de los controles criptográficos.	Si	Es necesario conocer las reglamentaciones a nivel Colombia que aplican para el sector de las telecomunicaciones y sistemas informáticos.	Documento con las normas/leyes que aplican al MSI

A.18.2	Revisiones de la seguridad de la información			
A.18.2.1	Revisión independiente de la seguridad de la información	Si	Tanto los log, registros así como las herramientas de auditoría y monitorea deben ser protegidas contra accesos no autorizados.	
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Si	Es fundamental tener planes de auditoría, que validen y ajusten los objetivos del SGSI	
A.18.2.3	Comprobación del cumplimiento	Si	Es fundamental tener planes de auditoría, que validen y ajusten los objetivos del SGSI	

Tabla 8: Declaración de aplicabilidad

2.2.8. RESULTADOS

Se incluye la documentación solicitada

3. FASE 3. ANÁLISIS DE RIESGOS

3.1. Introducción

Ésta fase tiene por principal propósito realizar un análisis de riesgos con el cual se podrá validar el estado actual de la empresa haciendo énfasis en los activos que se encuentran relacionados con el alcance del SGSI. Para ello aplicaremos la metodología indicada y tendremos como resultado

3.2. Inventario de activos

La primera etapa para realizar el análisis de riesgos corresponde a identificar los principales activos de información que se encuentran vinculados con el alcance definido, los cuales fueron agrupados según las indicaciones de la metodología MAGERIT en la siguiente tabla.

ÁMBITO	ID	DESCRIPCIÓN
Instalaciones	I1	Centro de administración de avales y garantías (6)
	I2	Bodegas (6)
	I3	Centro de Tecnología (1)
	I4	Instalaciones del área de desarrollo (1)
Hardware	HW1	Servidor de BD (Desarrollo)
	HW2	Servidor de BD (Pruebas)
	HW3	Servidor de BD (Producción)
	HW4	Servidor de Aplicaciones (Desarrollo)
	HW5	Servidor de Aplicaciones (Pruebas)
	HW6	Servidor de Aplicaciones (Producción)
	HW7	Servidor de correos (Desarrollo y pruebas)
	HW8	Servidor de correos (Producción)
	HW9	Firewall
	HW10	Servidor de ambientes
	HW11	Switch
	HW12	Equipo de computo (repositorio)
	HW13	Equipos de computo de usuarios de SAAG
	HW14	Equipos de computo de desarrolladores
	HW15	Equipos de computo del grupo de ambientes
	HW16	Equipos de computo de grupo de tecnología
	HW17	Equipos de computo de grupo de pruebas
	HW18	VPN
	HW19	Torniquete de acceso

	HW20	Cámara de vigilancia
Software	SW1	Sistema operativo de servidor de BD (Desarrollo)
	SW2	Sistema operativo de servidor de BD (Pruebas)
	SW3	Sistema operativo de servidor de BD (Producción)
	SW4	Sistema operativo de servidor de aplicaciones (Desarrollo)
	SW5	Sistema operativo de servidor de aplicaciones (Pruebas)
	SW6	Sistema operativo de servidor de aplicaciones (Producción)
	SW7	Sistema de gestión de servidor de aplicación (Desarrollo)
	SW8	Sistema de gestión de servidor de aplicación (Pruebas)
	SW9	Sistema de gestión de servidor de aplicación (Producción)
	SW10	Sistema operativo de servidor de correos (Desarrollo y Pruebas)
	SW11	Sistema operativo de servidor de correos (Producción)
	SW12	Motor de BD (Desarrollo)
	SW13	Motor de BD (Pruebas)
	SW14	Motor de BD (Producción)
Aplicación	A1	Sistema de Administración de Avales y Garantías (Desarrollo)
	A2	Sistema de Administración de Avales y Garantías (Pruebas)
	A3	Sistema de Administración de Avales y Garantías (Producción)
Datos	D1	Garantías físicas
	D2	Registro de ingreso de precintos a los CAAG
	D3	Registro de ingreso de precintos a las bodegas
	D4	Base de Datos (Desarrollo)
	D5	Base de Datos (Pruebas)
	D6	Base de datos(Producción)
	D7	Archivos de entrada generados por otros aplicativos (Desarrollo)
	D8	Archivos de entrada generados por otros aplicativos (Pruebas)
	D9	Archivos de entrada generados por otros aplicativos (Producción)
	D10	Archivos de salida por SAAG (Desarrollo)
	D11	Archivos de salida por SAAG (Pruebas)
	D12	Archivos de salida por SAAG (Producción)
	D13	Correos automáticos generados por SAAG
	D14	Informes de auditoría
	D15	Código fuente
	D16	Código ejecutable (Desarrollo)
	D17	Código ejecutable (Pruebas)
	D18	Código ejecutable (Producción)
	D19	Planilla de programación de archivos ejecutables
	D20	Planillas de registro de usuarios externos a los CAAG
	D21	Planillas de registro de usuarios externos a las bodegas
	D22	Backups
	D23	Logs
Red	R1	Red local

	R2	Red de internet
Servicios	S1	Directorio Activo
	S2	Servicio de envío de correos (Desarrollo y pruebas)
	S3	Servicio de envío de correos (Producción)
	S4	Monitorización
	S5	Servicio de acceso remoto
Equipamiento auxiliar	E1	Cintas
	E2	Cajas fuertes
Personal	P1	Administrador del CAAG
	P2	Personal del CAAG
	P3	Personal perteneciente a las bodegas
	P4	Abogado
	P5	Desarrolladores
	P6	Personal de ambientes
	P7	Personal de pruebas
	P8	Personal de Tecnología

Tabla 9: Inventario de activos

3.3. Valoración de los activos

Una vez identificados los activos de información, el segundo paso es asignar un valor a cada uno, estos valores han sido asignados teniendo en cuenta los activos que respaldan y los posibles valores cualitativos se muestran en la siguiente tabla.

ID	Activo superior	Activos inferiores	Valoración
I1	Centro de administración de avales y garantías (6)		Alto
I2	Bodegas (6)		Alto
I3	Centro de Tecnología (1)		Alto
I4	Instalaciones del área de desarrollo (1)		Medio
HW1	Servidor de BD (Desarrollo)	I3	Bajo
HW2	Servidor de BD (Pruebas)	I3	Bajo
HW3	Servidor de BD (Producción)	I3	Alto
HW4	Servidor de Aplicaciones (Desarrollo)	I3	Bajo
HW5	Servidor de Aplicaciones (Pruebas)	I3	Bajo
HW6	Servidor de Aplicaciones (Producción)	I3	Alto
HW7	Servidor de correos (Desarrollo y pruebas)	I3	Bajo
HW8	Servidor de correos (Producción)	I3	Alto
HW9	Firewall	I3	Alto
HW10	Servidor de ambientes	I3	Bajo
HW11	Switch	I3	Muy Bajo

HW12	Equipo de computo (repositorio)	I4	Alto
HW13	Equipos de computo de usuarios de SAAG	I1, I2	Bajo
HW14	Equipos de computo de desarrolladores	I4	Medio
HW15	Equipos de computo del grupo de ambientes	I4	Bajo
HW16	Equipos de computo de grupo de tecnología	I3	Medio
HW17	Equipos de computo de grupo de pruebas	I4	Bajo
HW18	VPN	I3	Bajo
HW19	Torniquete de acceso	I1, I2, I3, I4	Muy Bajo
HW20	Cámara de vigilancia	I1, I2, I3, I4	Muy Bajo
SW1	Sistema operativo de servidor de BD (Desarrollo)	HW1, I3	Bajo
SW2	Sistema operativo de servidor de BD (Pruebas)	HW2, I3	Bajo
SW3	Sistema operativo de servidor de BD (Producción)	HW3, I3	Alto
SW4	Sistema operativo de servidor de aplicaciones (Desarrollo)	HW4, I3	Bajo
SW5	Sistema operativo de servidor de aplicaciones (Pruebas)	HW5, I3	Bajo
SW6	Sistema operativo de servidor de aplicaciones (Producción)	HW6, I3	Alto
SW7	Sistema de gestión de servidor de aplicación (Desarrollo)	SW4, HW4, I3	Bajo
SW8	Sistema de gestión de servidor de aplicación (Pruebas)	SW5, HW5, I3	Bajo
SW9	Sistema de gestión de servidor de aplicación (Producción)	SW6, HW6, I3	Alto
SW10	Sistema operativo de servidor de correos (Desarrollo y Pruebas)	HW7, HW1, I3	Bajo
SW11	Sistema operativo de servidor de correos (Producción)	HW8, HW1, I3	Alto
SW12	Motor de BD (Desarrollo)	SW1, HW1, I3	Bajo
SW13	Motor de BD (Pruebas)	SW2, HW2, I3	Bajo
SW14	Motor de BD (Producción)	SW3, HW3, I3	Muy Alto
A1	Sistema de Administración de Avales y Garantías (Desarrollo)	SW12, SW1, HW1, I3 SW6, HW6, I3	Alto
A2	Sistema de Administración de Avales y Garantías (Pruebas)	SW13, SW2, HW2, I3	Alto
A3	Sistema de Administración de Avales y Garantías (Producción)	SW14, SW3, HW3, I3	Muy Alto
D1	Garantías físicas	I1, I2, A2, A3	Muy Alto
D2	Registro de ingreso de precintos a los CAAG	I1	Alto
D3	Registro de ingreso de precintos a las bodegas	I2	Alto
D4	Base de Datos (Desarrollo)	SW12, SW1, HW1, I3	Medio
D5	Base de Datos (Pruebas)	SW13, SW2, HW2, I3	Alto
D6	Base de datos(Producción)	SW14, SW3, HW3, I3	Muy Alto
D7	Archivos de entrada generados por otros aplicativos (Desarrollo)	HW1, I3	Medio

D8	Archivos de entrada generados por otros aplicativos (Pruebas)	HW2, I3	Alto
D9	Archivos de entrada generados por otros aplicativos (Producción)	HW3, I3	Muy Alto
D10	Archivos de salida por SAAG (Desarrollo)	HW1, I3	Bajo
D11	Archivos de salida por SAAG (Pruebas)	HW2, I3	Medio
D12	Archivos de salida por SAAG (Producción)	HW3, I3	Muy Alto
D13	Correos automáticos generados por SAAG (Producción)	S2, SW11, HW8, HW1, I3	Muy Alto
D14	Informes de auditoría	I3	Alto
D15	Código fuente	HW12, I4	Muy Alto
D16	Código ejecutable (Desarrollo)	HW1, I3	Bajo
D17	Código ejecutable (Pruebas)	HW2, I3	Medio
D18	Código ejecutable (Producción)	HW3, I3	Muy Alto
D19	Planilla de programación de archivos ejecutables	I3	Medio
D20	Planillas de registro de usuarios externos a los CAAG	I1	Medio
D21	Planillas de registro de usuarios externos a las bodegas	I2	Medio
D22	Backups	E1	Alto
D23	Logs	HW6, I3	Alto
R1	Red local	I3	Alto
R2	Red de internet	I3	Medio
S1	Directorio Activo	I3	Alto
S2	Servicio de envío de correos (Desarrollo y pruebas)	I3	Bajo
S3	Servicio de envío de correos (Producción)	I3	Alto
S4	Monitorización	HW1, HW2, HW3, HW4, HW5, HW6, HW7, HW8, HW9, HW10, SW1, SW2, SW3, SW4, SW5, SW6, SW7, SW8, SW9, SW10, SW11, SW12, SW13, SW14	Medio
S5	Servicio de acceso remoto	I3	Bajo
E1	Cintas	I3	Alto
E2	Cajas fuertes	I2	Alto
P1	Administrador del CAAG	I1	Muy Alto
P2	Personal del CAAG	I1	Bajo
P3	Personal perteneciente a las bodegas	I2	Bajo
P4	Abogado	I1	Alto
P5	Desarrolladores	I4	Alto
P6	Personal de ambientes	I4	Bajo

P7	Personal de pruebas	I4	Bajo
P8	Personal de Tecnología	I3	Alto

Tabla 10: Valoración de activos

3.4. Dimensiones de seguridad

A cada activo de información se encuentran asociadas 5 dimensiones:

Autenticidad (A): Se garantiza la identidad de los procesos y usuarios que manipulan la información directamente o mediante procesos

Confidencialidad: Sólo personal autorizado tendrá acceso a información sensible o privada

Integridad: La información se encuentra completa y no ha sido manipulada sin previa autorización

Disponibilidad: El personal autorizado podrá acceder a la información cuando lo requiera

Trazabilidad (T): Para toda actividad realizada se podrá determinar su autor y el momento en que se realizó.

Por cada una de éstas dimensiones se debe asociar el valor que corresponda a cada dimensión de cada activo, teniendo en cuenta la siguiente tabla:

VALOR	CRITERIO
10	Daño muy grave a la organización
7-9	Daño gravea la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Tabla 11: Posibles valores de dimensión

Ámbito	ID	Activo superior	Aspectos críticos				
			A	C	I	D	A
Instalaciones	I1	Centro de administración de avales y garantías (6)	5	9	9	7	7
	I2	Bodegas (6)	5	9	5	7	7
	I3	Centro de Tecnología (1)	5	9	5	7	7
	I4	Instalaciones del área de desarrollo (1)	5	7	5	7	7

Hardware	HW1	Servidor de BD (Desarrollo)	4	6	6	6	4
	HW2	Servidor de BD (Pruebas)	4	6	6	6	4
	HW3	Servidor de BD (Producción)	7	9	9	9	7
	HW4	Servidor de Aplicaciones (Desarrollo)	4	6	6	6	4
	HW5	Servidor de Aplicaciones (Pruebas)	4	6	6	6	4
	HW6	Servidor de Aplicaciones (Producción)	7	9	9	9	7
	HW7	Servidor de correos (Desarrollo y pruebas)	6	4	6	4	4
	HW8	Servidor de correos (Producción)	7	6	7	6	6
	HW9	Firewall	7	1	7	7	7
	HW10	Servidor de ambientes	3	6	6	9	9
	HW11	Switch	3	3	6	9	6
	HW12	Equipo de computo (repositorio)	1	9	9	7	1
	HW13	Equipos de computo de usuarios de SAAG	1	6	3	4	1
	HW14	Equipos de computo de desarrolladores	1	9	6	3	1
	HW15	Equipos de computo del grupo de ambientes	6	6	7	3	6
	HW16	Equipos de computo de grupo de tecnología	1	9	6	7	1
	HW17	Equipos de computo de grupo de pruebas	6	6	7	3	6
	HW18	VPN	5	5	9	7	9
	HW19	Torniquete de acceso	7	0	9	7	1
	HW20	Cámara de vigilancia	7	0	9	7	1
Software	SW1	Sistema operativo de servidor de BD (Desarrollo)	3	3	3	6	2
	SW2	Sistema operativo de servidor de BD (Pruebas)	3	3	3	6	2
	SW3	Sistema operativo de servidor de BD (Producción)	9	7	7	9	9
	SW4	Sistema operativo de servidor de aplicaciones (Desarrollo)	3	1	1	3	2
	SW5	Sistema operativo de servidor de aplicaciones (Pruebas)	3	3	3	6	2
	SW6	Sistema operativo de servidor de aplicaciones (Producción)	9	7	7	9	7
	SW7	Sistema de gestión de servidor de aplicación (Desarrollo)	3	7	7	7	2
	SW8	Sistema de gestión de servidor de aplicación (Pruebas)	3	7	7	7	2
	SW9	Sistema de gestión de servidor de aplicación (Producción)	7	7	7	7	7
	SW10	Sistema operativo de servidor de correos (Desarrollo y Pruebas)	1	1	3	3	1
	SW11	Sistema operativo de servidor de	1	6	9	7	7

		correos (Producción)					
	SW12	Motor de BD (Desarrollo)	3	1	3	3	3
	SW13	Motor de BD (Pruebas)	3	1	3	3	3
	SW14	Motor de BD (Producción)	7	5	7	7	7
Aplicación	A1	Sistema de Administración de Avales y Garantías (Desarrollo)	2	2	2	2	2
	A2	Sistema de Administración de Avales y Garantías (Pruebas)	2	2	2	2	2
	A3	Sistema de Administración de Avales y Garantías (Producción)	7	9	9	9	7
Datos	D1	Garantías físicas	10	10	10	10	10
	D2	Registro de ingreso de precintos a los CAAG	7	9	9	9	7
	D3	Registro de ingreso de precintos a las bodegas	7	9	9	9	7
	D4	Base de Datos (Desarrollo)	4	4	4	4	4
	D5	Base de Datos (Pruebas)	4	4	4	4	4
	D6	Base de datos(Producción)	9	9	9	9	9
	D7	Archivos de entrada generados por otros aplicativos (Desarrollo)	4	3	4	4	3
	D8	Archivos de entrada generados por otros aplicativos (Pruebas)	4	3	4	4	3
	D9	Archivos de entrada generados por otros aplicativos (Producción)	10	7	10	10	7
	D10	Archivos de salida por SAAG (Desarrollo)	4	3	4	4	3
	D11	Archivos de salida por SAAG (Pruebas)	4	3	4	4	3
	D12	Archivos de salida por SAAG (Producción)	10	7	10	10	7
	D13	Correos automáticos generados por SAAG (Producción)	9	4	9	9	4
	D14	Informes de auditoría	7	4	7	7	4
	D15	Código fuente	7	7	9	9	4
	D16	Código ejecutable (Desarrollo)	4	3	4	4	3
	D17	Código ejecutable (Pruebas)	4	3	4	4	3
	D18	Código ejecutable (Producción)	10	7	10	10	7
	D19	Planilla de programación de archivos ejecutables	7	4	9	9	4
	D20	Planillas de registro de usuarios externos a los CAAG	4	6	7	6	4
	D21	Planillas de registro de usuarios externos a las bodegas	4	6	7	6	4
	D22	Backups	4	4	9	7	4
	D23	Logs	9	6	9	6	9

Red	R1	Red local	9	9	9	10	9
	R2	Red de internet	9	9	9	10	9
Servicios	S1	Directorio Activo	9	9	9	10	9
	S2	Servicio de envío de correos (Desarrollo y pruebas)	4	3	4	4	3
	S3	Servicio de envío de correos (Producción)	9	4	9	9	4
	S4	Monitorización	7	7	9	9	9
	S5	Servicio de acceso remoto	6	9	6	7	6
Equipamiento auxiliar	E1	Cintas	6	9	9	6	6
	E2	Cajas fuertes	9	10	10	10	7
Personal	P1	Administrador del CAAG	9	9	0	9	0
	P2	Personal del CAAG	4	4	0	4	0
	P3	Personal perteneciente a las bodegas	4	4	0	4	0
	P4	Abogado	6	6	0	6	0
	P5	Desarrolladores	7	7	0	7	0
	P6	Personal de ambientes	4	4	0	4	0
	P7	Personal de pruebas	4	4	0	4	0
	P8	Personal de Tecnología	8	8	0	8	0

Tabla 12: Valoración de dimensiones de seguridad

3.5. Tabla resumen de valoración

ID	Activo superior	Valoración	Aspectos críticos				
			A	C	I	D	A
Instalaciones	Centro de administración de avales y garantías (6)	Alto	5	9	9	7	7
	Bodegas (6)	Alto	5	9	5	7	7
	Centro de Tecnología (1)	Alto	5	9	5	7	7
	Instalaciones del área de desarrollo (1)	Medio	5	7	5	7	7
	Servidor de BD (Desarrollo)	Bajo	4	6	6	6	4
	Servidor de BD (Pruebas)	Bajo	4	6	6	6	4
	Servidor de BD (Producción)	Alto	7	9	9	9	7
	Servidor de Aplicaciones (Desarrollo)	Bajo	4	6	6	6	4
	Servidor de Aplicaciones (Pruebas)	Bajo	4	6	6	6	4
	Servidor de Aplicaciones (Producción)	Alto	7	9	9	9	7
	Servidor de correos (Desarrollo y pruebas)	Bajo	6	4	6	4	4
	Servidor de correos (Producción)	Alto	7	6	7	6	6
	Firewall	Alto	7	1	7	7	7

Hardware	Servidor de ambientes	Bajo	3	6	6	9	9
	Switch	Muy Bajo	3	3	6	9	6
	Equipo de computo (repositorio)	Alto	1	9	9	7	1
	Equipos de computo de usuarios de SAAG	Bajo	1	6	3	4	1
	Equipos de computo de desarrolladores	Medio	1	9	6	3	1
	Equipos de computo del grupo de ambientes	Bajo	6	6	7	3	6
	Equipos de computo de grupo de tecnología	Medio	1	9	6	7	1
	Equipos de computo de grupo de pruebas	Bajo	6	6	7	3	6
	VPN	Bajo	5	5	9	7	9
	Torniquete de acceso	Muy Bajo	7	0	9	7	1
	Cámara de vigilancia	Muy Bajo	7	0	9	7	1
Software	Sistema operativo de servidor de BD (Desarrollo)	Bajo	3	3	3	6	2
	Sistema operativo de servidor de BD (Pruebas)	Bajo	3	3	3	6	2
	Sistema operativo de servidor de BD (Producción)	Alto	9	7	7	9	9
	Sistema operativo de servidor de aplicaciones (Desarrollo)	Bajo	3	1	1	3	2
	Sistema operativo de servidor de aplicaciones (Pruebas)	Bajo	3	3	3	6	2
	Sistema operativo de servidor de aplicaciones (Producción)	Alto	9	7	7	9	7
	Sistema de gestión de servidor de aplicación (Desarrollo)	Bajo	3	7	7	7	2
	Sistema de gestión de servidor de aplicación (Pruebas)	Bajo	3	7	7	7	2
	Sistema de gestión de servidor de aplicación (Producción)	Alto	7	7	7	7	7
	Sistema operativo de servidor de correos (Desarrollo y Pruebas)	Bajo	1	1	3	3	1
	Sistema operativo de servidor de correos (Producción)	Alto	1	6	9	7	7
	Motor de BD (Desarrollo)	Bajo	3	1	3	3	3
	Motor de BD (Pruebas)	Bajo	3	1	3	3	3
	Motor de BD (Producción)	Muy Alto	7	5	7	7	7
Aplicación	Sistema de Administración de Avales y Garantías (Desarrollo)	Alto	2	2	2	2	2
	Sistema de Administración de Avales y Garantías (Pruebas)	Alto	2	2	2	2	2
	Sistema de Administración de Avales y	Muy Alto	7	9	9	9	7

	Garantías (Producción)						
Datos	Garantías físicas	Muy Alto	10	10	10	10	10
	Registro de ingreso de precintos a los CAAG	Alto	7	9	9	9	7
	Registro de ingreso de precintos a las bodegas	Alto	7	9	9	9	7
	Base de Datos (Desarrollo)	Medio	4	4	4	4	4
	Base de Datos (Pruebas)	Alto	4	4	4	4	4
	Base de datos(Producción)	Muy Alto	9	9	9	9	9
	Archivos de entrada generados por otros aplicativos (Desarrollo)	Medio	4	3	4	4	3
	Archivos de entrada generados por otros aplicativos (Pruebas)	Alto	4	3	4	4	3
	Archivos de entrada generados por otros aplicativos (Producción)	Muy Alto	10	7	10	10	7
	Archivos de salida por SAAG (Desarrollo)	Bajo	4	3	4	4	3
	Archivos de salida por SAAG (Pruebas)	Medio	4	3	4	4	3
	Archivos de salida por SAAG (Producción)	Muy Alto	10	7	10	10	7
	Correos automáticos generados por SAAG (Producción)	Muy Alto	9	4	9	9	4
	Informes de auditoría	Alto	7	4	7	7	4
	Código fuente	Muy Alto	7	7	9	9	4
	Código ejecutable (Desarrollo)	Bajo	4	3	4	4	3
	Código ejecutable (Pruebas)	Medio	4	3	4	4	3
	Código ejecutable (Producción)	Muy Alto	10	7	10	10	7
	Planilla de programación de archivos ejecutables	Medio	7	4	9	9	4
	Planillas de registro de usuarios externos a los CAAG	Medio	4	6	7	6	4
	Planillas de registro de usuarios externos a las bodegas	Medio	4	6	7	6	4
	Backups	Alto	4	4	9	7	4
	Logs	Alto	9	6	9	6	9
Red	Red local	Alto	9	9	9	10	9
	Red de internet	Medio	9	9	9	10	9
Servicios	Directorio Activo	Alto	9	9	9	10	9
	Servicio de envío de correos (Desarrollo y pruebas)	Bajo	4	3	4	4	3
	Servicio de envío de correos (Producción)	Alto	9	4	9	9	4
	Monitorización	Medio	7	7	9	9	9

	Servicio de acceso remoto	Bajo	6	9	6	7	6
Equipamiento auxiliar	Cintas	Alto	6	9	9	6	6
	Cajas fuertes	Alto	9	10	10	10	7
Personal	Administrador del CAAG	Muy Alto	9	9	0	9	0
	Personal del CAAG	Bajo	4	4	0	4	0
	Personal perteneciente a las bodegas	Bajo	4	4	0	4	0
	Abogado	Bajo	6	6	0	6	0
	Desarrolladores	Alto	7	7	0	7	0
	Personal de ambientes	Bajo	4	4	0	4	0
	Personal de pruebas	Bajo	4	4	0	4	0
	Personal de Tecnología	Alto	8	8	0	8	0

Tabla 13: Resumen de valoración

3.6. Análisis de amenazas

Para continuar con la siguiente etapa del análisis de riesgos, por cada activo se identificarán las amenazas a las cuales se encuentran expuestos y utilizaremos la tabla de amenazas de MAGERIT.

A cada amenaza por activo se asignará un valor de frecuencia y un valor por cada dimensión que representará la degradación o impacto, en caso de que la amenaza logre materializarse.

3.7. Impacto potencial

Teniendo en cuenta los resultados del análisis de activos y el análisis de amenazas, podremos calcular el impacto potencial en cada caso utilizando a siguiente fórmula:

Impacto Potencial = Activo x Impacto

En la fórmula indicada **'Activo'** representa el valor asignado a cada dimensión por activo e **'Impacto'** corresponde al valor de impacto o degradación en cada dimensión por activo.

NOTA: Revisar archivo adjunto en la hoja IMPACTO POTENCIAL, los resultados se encuentran disponibles en la columna '**Impacto potencial'** de la Tabla.

3.8. Nivel de Riesgo Aceptable y riesgo Residual

Una vez revisados los resultados obtenidos al calcular el impacto potencial, se define que el riesgo aceptable estará con valores menores a 3. A continuación se definen las amenazas que corresponden a los riesgos que superan el riesgo aceptable.

NOTA: La última columna indica si la salvaguarda se encuentra implementada o no

Activo	Amenaza		Salvaguarda	I
Centro de administración de avales y garantías (6) Bodegas (6) Centro de Tecnología (1) Instalaciones del área de desarrollo (1)	Fuego	**D**	Cuenta con sistemas de detección y extinción de incendios El BANCO cuenta con póliza de seguros para cubrir daños en las instalaciones y los recursos que se encuentran en ellas. Adicional a esto cuenta con grupo brigadista por área que realizan simulacros de evacuación anuales	**S**
	Daños por agua	**D**	El BANCO cuenta con pólizas para cubrir daños en las instalaciones y los recursos que se encuentran en ellas	**S**
	Desastres naturales	**D**	El BANCO cuenta con póliza de seguros para cubrir daños en las instalaciones y los recursos que se encuentran en ellas. Adicional a esto cuenta con grupo brigadista por área que realizan simulacros de evacuación anuales	**S**
	Corte de suministro eléctrico	**D**	Las instalaciones de tecnología cuentan con más de una fuente de energía ante éste tipo de eventos y una de ellas corresponde a una planta Los equipos deben contar con reguladores de energía para protegerlos de posibles apagones o variaciones de voltaje	**S** **S**
Servidor de BD (Pruebas)	Fallos de servicios de comunicación	D	Validar posibles causas de los fallos presentados y realizar los ajustes necesarios	N

	Caída del sistema por agotamiento de recursos	D	Crear un proceso automático para eliminar archivos que elimine los archivos de gran tamaño no requeridos o un procedimiento a seguir por el personal de tecnología en estos casos	N
Servidor de BD (Producción)	Caída del sistema por agotamiento de recursos	D	Crear un proceso automático para eliminar archivos que elimine los archivos de gran tamaño no requeridos o un procedimiento a seguir por el personal de tecnología en estos casos	N
Servidor de correos (Desarrollo y pruebas)	Denegación del servicio	D	Validar posibles causas de los fallos presentados y realizar los ajustes necesarios	N
Servidor de ambientes	Caída del sistema por agotamiento de recursos	D	Crear un procedimiento a seguir por el personal de tecnología en estos casos.	N
Equipo de computo (repositorio)	Avería de origen Físico o lógico	D	Se sugiere utilizar un servidor que cuente con más respaldo y protección, de preferencia custodiado por tecnología	N
	Fallos de servicios de comunicación	D		
Equipos de computo de usuarios de SAAG	Corte del suministro eléctrico	D	Validar viabilidad para contar con planta de suministro de energía Los equipos deben contar con reguladores de energía para protegerlos de posibles apagones o variaciones de voltaje	N S
Servidor de Aplicaciones (Desarrollo)	Caída del sistema por agotamiento de recursos	D	Crear un proceso automático para eliminar archivos que elimine los archivos de gran tamaño no requeridos o un procedimiento a seguir por el personal de tecnología en estos casos	N
Servidor de aplicaciones OC4J (Desarrollo)	Errores de mantenimiento / actualización de programas (software)	C D	Dado que el servidor actual no cuenta con soporte y su mantenimiento es complicado se sugiere migrar la aplicación para el uso de un servidor más actualizado y que cuente con el debido soporte	N
Servidor de aplicaciones OC4J	Errores de mantenimiento / actualización de programas	C D	Dado que el servidor actual no cuenta con soporte y su	N

(Pruebas)	(software)		mantenimiento es complicado se sugiere migrar la aplicación para el uso de un servidor más actualizado y que cuente con el debido soporte	
Servidor de aplicaciones OC4J (Producción)	Errores de mantenimiento / actualización de programas (software)	C D	Dado que el servidor actual no cuenta con soporte y su mantenimiento es complicado se sugiere migrar la aplicación para el uso de un servidor más actualizado y que cuente con el debido soporte	N
Sistema de Administración de Avales y Garantías (Producción)	Introducción de información incorrecta	I	Validar cuales son los casos más frecuentes para que se ajuste el aplicativo y se puedan reducir	N
	Vulnerabilidades de los programas (software)	C I T	Realizar validaciones y auditoría detallada al aplicativo para determinar cuáles son las vulnerabilidades y solicitar a los responsables el respectivo plan de acción Ajustar el aplicativo para el uso de protocolo seguro	N N
	Denegación de servicio	D	Validar procedimiento a seguir y las contingencias existentes en estos casos	S
Base de Datos (Desarrollo)	Introducción de información incorrecta	I	Validar cuales son los casos más frecuentes para que se ajuste el aplicativo y se puedan reducir	N
Base de Datos (Pruebas)	Introducción de información incorrecta	I	Validar cuales son los casos más frecuentes para que se ajuste el aplicativo y se puedan reducir	N
Base de datos(Producción)	Introducción de información incorrecta	I	Validar cuales son los casos más frecuentes para que se ajuste el aplicativo y se puedan reducir	N
Archivos de salida por SAAG (Producción)	Fallos de servicios de comunicación	D	Validar procedimiento a seguir Las contingencias existentes en estos casos	S S
	Acceso de personal no autorizado	C		S
Correos automáticos generados por SAAG (Producción)	Encaminamiento de mensajes	C	Validar la configuración de los correos existente y que esté de la mano con la rotación de personal	N
Código fuente	Destrucción de información	I	Crear política de desarrollo	N

		D	seguro y las respectivas normas que involucren el uso del versionador de código oficial para evitar problemas de comunicación con el repositorio actual	
	Alteración de la información	A C I	Crear política de desarrollo seguro y las respectivas normas que involucren el uso del versionador de código oficial para evitar problemas de comunicación con el repositorio actual	N
Código ejecutable (Desarrollo)	Errores de los usuarios	I D	Validar procedimiento a seguir Las contingencias existentes en estos casos	S S
Código ejecutable (Pruebas)	Errores de los usuarios	I D	Validar procedimiento a seguir Las contingencias existentes en estos casos	S S
Código ejecutable (Producción)	Errores de los usuarios	I D	Crear proceso automático para la ejecución de código	N
Logs	Vulnerabilidades de los programas (software)	A I T	Se implementará un SIEM (Security Information and Event Management) que facilitara la centralización y monitoreo basado en los logs o MONITOR	N
Administrador del CAAG	Indisponibilidad del personal	D	Validar procedimiento a seguir Crear manual detallado de las actividades realizadas por el administrador del aplicativo Definir a nivel de procesos las actividades propias del administrador y sus funciones	S S S
Personal de Tecnología	Indisponibilidad del personal	D	Validar procedimiento a seguir Crear manual detallado de las actividades realizadas por el administrador del aplicativo Definir a nivel de procesos las actividades propias del administrador y sus funciones	S S S
Desarrolladores	Indisponibilidad del personal	D	Validar procedimiento a seguir Crear manual detallado de las actividades realizadas por el administrador del aplicativo Definir a nivel de procesos las	S S S

			actividades propias del administrador y sus funciones	

Tabla 14: Análisis de amenazas

Riesgo Potencial Ponderado

Teniendo en cuenta las salvaguardas y controles existentes, se ajustan los valores para recalcular el riesgo potencial y el acumulado obteniendo el estado actual que servirá de línea base para el SGSI.

Para las amenazas con salvaguardas implementadas se tiene una reducción considerable en la frecuencia cuando se hace referencia a mecanismos para evitar o reducir la amenaza de forma preventiva (Sistema de detección de incendios) y en el impacto generado (si se trata de pólizas de seguro).

Activo	Amenaza	F						Impacto					Impacto ponderado					Riesgo Residual				
			A	C	I	D	A	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
I1	Fuego	0,1	5	9	9	7	7				80%		0	0	0	7	0	0	0	0	0,56	0
	Daños por agua	0,1	5	9	9	7	7				80%		0	0	0	7	0	0	0	0	0,56	0
	Desastres naturales	0,1	5	9	9	7	7				80%		0	0	0	7	0	0	0	0	0,56	0
	Corte del suministro eléctrico	0,1	5	9	9	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
	Condiciones inadecuadas de temperatura y/o humedad	0,1	5	9	9	7	7				80%		0	0	0	7	0	0	0	0	0,56	0
	Interrupción de otros servicios y suministros esenciales	0,1	5	9	9	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
	Acceso no autorizado	0,1	5	9	9	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
I2	Fuego	0,01	5	9	5	7	7				100%		0	0	0	7	0	0	0	0	0,07	0
	Daños por agua	0,01	5	9	5	7	7				100%		0	0	0	7	0	0	0	0	0,07	0
	Desastres naturales	0,01	5	9	5	7	7				100%		0	0	0	7	0	0	0	0	0,07	0
	Corte del suministro eléctrico	0,1	5	9	5	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
	Condiciones inadecuadas de temperatura y/o humedad	0,1	5	9	5	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
	Interrupción de otros servicios y suministros esenciales	0,1	5	9	5	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
	Acceso no autorizado	0,1	5	9	5	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
I3	Fuego	0,01	5	9	5	7	7				100%		0	0	0	7	0	0	0	0	0,07	0
	Daños por agua	0,01	5	9	5	7	7				100%		0	0	0	7	0	0	0	0	0,07	0
	Desastres naturales	0,01	5	9	5	7	7				100%		0	0	0	7	0	0	0	0	0,07	0
	Corte del suministro eléctrico	0,1	5	9	5	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
	Condiciones inadecuadas de temperatura y/o humedad	0,1	5	9	5	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
	Interrupción de otros servicios y suministros esenciales	0,1	5	9	5	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
	Acceso no autorizado	0,1	5	9	5	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
I4	Fuego	0,1	5	9	9	7	7				80%		0	0	0	7	0	0	0	0	0,56	0
	Daños por agua	0,1	5	9	9	7	7				80%		0	0	0	7	0	0	0	0	0,56	0
	Desastres naturales	0,1	5	9	9	7	7				80%		0	0	0	7	0	0	0	0	0,56	0
	Corte del suministro eléctrico	0,1	5	9	9	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
	Condiciones inadecuadas de temperatura y/o humedad	0,1	5	9	9	7	7				80%		0	0	0	7	0	0	0	0	0,56	0
	Interrupción de otros servicios y suministros esenciales	0,1	5	9	9	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
	Acceso no autorizado	0,1	5	9	9	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
HW1	Fuego	0,01	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,06	0
	Daños por agua	0,01	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,06	0
	Desastres naturales	0,01	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,06	0
	Corte del suministro eléctrico	0,1	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,6	0
	Condiciones inadecuadas de temperatura y/o humedad	1	4	6	6	6	4				20%		0	0	0	1,2	0	0	0	0	1,2	0

	Avería de origen Físico o lógico	0,1	4	6	6	6	4				50%		0	0	0	3	0	0	0	0	0,3	0
	Fallos de servicios de comunicación	0,1	4	6	6	6	4				75%		0	0	0	4,5	0	0	0	0	0,45	0
	Errores del administrador	0,1	4	6	6	6	4		50%	50%	20%		0	3	3	1,2	0	0	0,3	0,3	0,12	0
	Errores de configuración	0,1	4	6	6	6	4		60%	60%	25%		0	3,6	3,6	1,5	0	0	0,36	0,36	0,15	0
	Manipulación de la configuración	0,01	4	6	6	6	4		60%	60%	50%		0	3,6	3,6	3	0	0	0,04	0,04	0,03	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	4	6	6	6	4				50%		0	0	0	3	0	0	0	0	0,3	0
	Caída del sistema por agotamiento de recursos	0,1	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,6	0
	Acceso no autorizado	0,01	4	6	6	6	4		70%		40%		0	4,2	0	2,4	0	0	0,04	0	0,02	0
	Denegación del servicio	0,1	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,6	0
HW2	Fuego	0,01	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,06	0
	Daños por agua	0,01	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,06	0
	Desastres naturales	0,01	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,06	0
	Corte del suministro eléctrico	0,1	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,6	0
	Condiciones inadecuadas de temperatura y/o humedad	1	4	6	6	6	4				20%		0	0	0	1,2	0	0	0	0	1,2	0
	Avería de origen Físico o lógico	0,1	4	6	6	6	4				50%		0	0	0	3	0	0	0	0	0,3	0
	Fallos de servicios de comunicación	1	4	6	6	6	4				75%		0	0	0	4,5	0	0	0	0	4,5	0
	Errores del administrador	0,1	4	6	6	6	4		50%	50%	20%		0	3	3	1,2	0	0	0,3	0,3	0,12	0
	Errores de configuración	0,1	4	6	6	6	4		60%	60%	25%		0	3,6	3,6	1,5	0	0	0,36	0,36	0,15	0
	Manipulación de la configuración	0,01	4	6	6	6	4		60%	60%	50%		0	3,6	3,6	3	0	0	0,04	0,04	0,03	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	4	6	6	6	4				50%		0	0	0	3	0	0	0	0	0,3	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
	Acceso no autorizado	0,01	4	6	6	6	4		70%		40%		0	4,2	0	2,4	0	0	0,04	0	0,02	0
	Denegación del servicio	0,1	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,6	0
HW3	Fuego	0,01	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,09	0
	Daños por agua	0,01	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,09	0
	Desastres naturales	0,01	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,09	0
	Corte del suministro eléctrico	0,1	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,9	0
	Condiciones inadecuadas de temperatura y/o humedad	1	7	9	9	9	7				20%		0	0	0	1,8	0	0	0	0	1,8	0
	Avería de origen Físico o lógico	0,1	7	9	9	9	7				50%		0	0	0	4,5	0	0	0	0	0,45	0
	Fallos de servicios de comunicación	0,1	7	9	9	9	7				75%		0	0	0	6,75	0	0	0	0	0,68	0
	Errores del administrador	0,1	7	9	9	9	7		50%	50%	20%		0	4,5	4,5	1,8	0	0	0,45	0,45	0,18	0
	Errores de configuración	0,1	7	9	9	9	7		60%	60%	25%		0	5,4	5,4	2,25	0	0	0,54	0,54	0,23	0
	Manipulación de la configuración	0,01	7	9	9	9	7		60%	60%	50%		0	5,4	5,4	4,5	0	0	0,05	0,05	0,05	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	7	9	9	9	7				50%		0	0	0	4,5	0	0	0	0	0,45	0
	Caída del sistema por agotamiento de recursos	1	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	9	0
	Acceso no autorizado	0,01	7	9	9	9	7		70%		40%		0	6,3	0	3,6	0	0	0,06	0	0,04	0
	Denegación del servicio	0,1	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,9	0

HW4	Fuego	0,01	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,06	0
	Daños por agua	0,01	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,06	0
	Desastres naturales	0,01	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,06	0
	Corte del suministro eléctrico	0,1	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,6	0
	Condiciones inadecuadas de temperatura y/o humedad	1	4	6	6	6	4				20%		0	0	0	1,2	0	0	0	0	1,2	0
	Avería de origen Físico o lógico	0,1	4	6	6	6	4				50%		0	0	0	3	0	0	0	0	0,3	0
	Fallos de servicios de comunicación	0,1	4	6	6	6	4				75%		0	0	0	4,5	0	0	0	0	0,45	0
	Errores del administrador	0,1	4	6	6	6	4		50%	50%	20%		0	3	3	1,2	0	0	0,3	0,3	0,12	0
	Errores de configuración	0,1	4	6	6	6	4		60%	60%	25%		0	3,6	3,6	1,5	0	0	0,36	0,36	0,15	0
	Manipulación de la configuración	0,01	4	6	6	6	4		60%	60%	50%		0	3,6	3,6	3	0	0	0,04	0,04	0,03	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	4	6	6	6	4				50%		0	0	0	3	0	0	0	0	0,3	0
	Caída del sistema por agotamiento de recursos	0,1	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,6	0
	Acceso no autorizado	0,01	4	6	6	6	4		70%		40%		0	4,2	0	2,4	0	0	0,04	0	0,02	0
	Denegación del servicio	0,1	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,6	0
HW5	Fuego	0,01	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,06	0
	Daños por agua	0,01	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,06	0
	Desastres naturales	0,01	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,06	0
	Corte del suministro eléctrico	0,1	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,6	0
	Condiciones inadecuadas de temperatura y/o humedad	1	4	6	6	6	4				20%		0	0	0	1,2	0	0	0	0	1,2	0
	Avería de origen Físico o lógico	0,1	4	6	6	6	4				50%		0	0	0	3	0	0	0	0	0,3	0
	Fallos de servicios de comunicación	0,1	4	6	6	6	4				75%		0	0	0	4,5	0	0	0	0	0,45	0
	Errores del administrador	0,1	4	6	6	6	4		50%	50%	20%		0	3	3	1,2	0	0	0,3	0,3	0,12	0
	Errores de configuración	0,1	4	6	6	6	4		60%	60%	25%		0	3,6	3,6	1,5	0	0	0,36	0,36	0,15	0
	Manipulación de la configuración	0,01	4	6	6	6	4		60%	60%	50%		0	3,6	3,6	3	0	0	0,04	0,04	0,03	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	4	6	6	6	4				50%		0	0	0	3	0	0	0	0	0,3	0
	Caída del sistema por agotamiento de recursos	0,1	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,6	0
	Acceso no autorizado	0,01	4	6	6	6	4		70%		40%		0	4,2	0	2,4	0	0	0,04	0	0,02	0
	Denegación del servicio	0,1	4	6	6	6	4				100%		0	0	0	6	0	0	0	0	0,6	0
HW6	Fuego	0,01	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,09	0
	Daños por agua	0,01	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,09	0
	Desastres naturales	0,01	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,09	0
	Corte del suministro eléctrico	0,1	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,9	0
	Condiciones inadecuadas de temperatura y/o humedad	1	7	9	9	9	7				20%		0	0	0	1,8	0	0	0	0	1,8	0
	Avería de origen Físico o lógico	0,1	7	9	9	9	7				50%		0	0	0	4,5	0	0	0	0	0,45	0
	Fallos de servicios de comunicación	0,1	7	9	9	9	7				75%		0	0	0	6,75	0	0	0	0	0,68	0
	Errores del administrador	0,1	7	9	9	9	7		50%	50%	20%		0	4,5	4,5	1,8	0	0	0,45	0,45	0,18	0
	Errores de configuración	0,1	7	9	9	9	7		60%	60%	25%		0	5,4	5,4	2,25	0	0	0,54	0,54	0,23	0
	Manipulación de la configuración	0,01	7	9	9	9	7		60%	60%	50%		0	5,4	5,4	4,5	0	0	0,05	0,05	0,05	0

	Errores de mantenimiento / actualización de equipos (hardware).	0,1	7	9	9	9	7				50%		0	0	0	4,5	0	0	0	0	0,45	0
	Caída del sistema por agotamiento de recursos	0,1	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,9	0
	Acceso no autorizado	0,01	7	9	9	9	7		70%		40%		0	6,3	0	3,6	0	0	0,06	0	0,04	0
	Denegación del servicio	0,1	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,9	0
HW7	Fuego	0,01	6	4	6	4	4				100%		0	0	0	4	0	0	0	0	0,04	0
	Daños por agua	0,01	6	4	6	4	4				100%		0	0	0	4	0	0	0	0	0,04	0
	Desastres naturales	0,01	6	4	6	4	4				100%		0	0	0	4	0	0	0	0	0,04	0
	Corte del suministro eléctrico	0,1	6	4	6	4	4				100%		0	0	0	4	0	0	0	0	0,4	0
	Condiciones inadecuadas de temperatura y/o humedad	1	6	4	6	4	4				20%		0	0	0	0,8	0	0	0	0	0,8	0
	Avería de origen Físico o lógico	0,1	6	4	6	4	4				50%		0	0	0	2	0	0	0	0	0,2	0
	Fallos de servicios de comunicación	0,1	6	4	6	4	4				75%		0	0	0	3	0	0	0	0	0,3	0
	Errores del administrador	0,1	6	4	6	4	4		50%	50%	20%		0	2	3	0,8	0	0	0,2	0,3	0,08	0
	Errores de configuración	0,1	6	4	6	4	4		60%	60%	25%		0	2,4	3,6	1	0	0	0,24	0,36	0,1	0
	Manipulación de la configuración	0,01	6	4	6	4	4		60%	60%	50%		0	2,4	3,6	2	0	0	0,02	0,04	0,02	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	6	4	6	4	4				50%		0	0	0	2	0	0	0	0	0,2	0
	Caída del sistema por agotamiento de recursos	0,1	6	4	6	4	4				100%		0	0	0	4	0	0	0	0	0,4	0
	Acceso no autorizado	0,01	6	4	6	4	4		70%		40%		0	2,8	0	1,6	0	0	0,03	0	0,02	0
	Denegación del servicio	1	6	4	6	4	4				100%		0	0	0	4	0	0	0	0	4	0
HW8	Fuego	0,01	7	6	7	6	6				100%		0	0	0	6	0	0	0	0	0,06	0
	Daños por agua	0,01	7	6	7	6	6				100%		0	0	0	6	0	0	0	0	0,06	0
	Desastres naturales	0,01	7	6	7	6	6				100%		0	0	0	6	0	0	0	0	0,06	0
	Corte del suministro eléctrico	0,1	7	6	7	6	6				100%		0	0	0	6	0	0	0	0	0,6	0
	Condiciones inadecuadas de temperatura y/o humedad	1	7	6	7	6	6				20%		0	0	0	1,2	0	0	0	0	1,2	0
	Avería de origen Físico o lógico	0,1	7	6	7	6	6				50%		0	0	0	3	0	0	0	0	0,3	0
	Fallos de servicios de comunicación	0,1	7	6	7	6	6				75%		0	0	0	4,5	0	0	0	0	0,45	0
	Errores del administrador	0,1	7	6	7	6	6		50%	50%	20%		0	3	3,5	1,2	0	0	0,3	0,35	0,12	0
	Errores de configuración	0,1	7	6	7	6	6		60%	60%	25%		0	3,6	4,2	1,5	0	0	0,36	0,42	0,15	0
	Manipulación de la configuración	0,01	7	6	7	6	6		60%	60%	50%		0	3,6	4,2	3	0	0	0,04	0,04	0,03	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	7	6	7	6	6				50%		0	0	0	3	0	0	0	0	0,3	0
	Caída del sistema por agotamiento de recursos	0,1	7	6	7	6	6				100%		0	0	0	6	0	0	0	0	0,6	0
	Acceso no autorizado	0,01	7	6	7	6	6		70%		40%		0	4,2	0	2,4	0	0	0,04	0	0,02	0
	Denegación del servicio	0,1	7	6	7	6	6				100%		0	0	0	6	0	0	0	0	0,6	0
HW9	Fuego	0,01	7	1	7	7	7				100%		0	0	0	7	0	0	0	0	0,07	0
	Daños por agua	0,01	7	1	7	7	7				100%		0	0	0	7	0	0	0	0	0,07	0
	Desastres naturales	0,01	7	1	7	7	7				100%		0	0	0	7	0	0	0	0	0,07	0
	Corte del suministro eléctrico	0,1	7	1	7	7	7				100%		0	0	0	7	0	0	0	0	0,7	0
	Avería de origen Físico o lógico	0,01	7	1	7	7	7				60%		0	0	0	4,2	0	0	0	0	0,04	0

	Errores de mantenimiento / actualización de equipos (hardware).	0,01	7	1	7	7	7				60%		0	0	0	4,2	0	0	0	0	0,04	0
	Errores de configuración	0,01	7	1	7	7	7				60%		0	0	0	4,2	0	0	0	0	0,04	0
	Errores del administrador	0,01	7	1	7	7	7				60%		0	0	0	4,2	0	0	0	0	0,04	0
HW10	Fuego	0,01	3	6	6	9	9				100%		0	0	0	9	0	0	0	0	0,09	0
	Daños por agua	0,01	7	6	7	6	6				100%		0	0	0	6	0	0	0	0	0,06	0
	Desastres naturales	0,01	7	6	7	6	6				100%		0	0	0	6	0	0	0	0	0,06	0
	Corte del suministro eléctrico	0,1	7	6	7	6	6				100%		0	0	0	6	0	0	0	0	0,6	0
	Condiciones inadecuadas de temperatura y/o humedad	0,1	7	6	7	6	6				20%		0	0	0	1,2	0	0	0	0	0,12	0
	Avería de origen Físico o lógico	0,1	7	6	7	6	6				50%		0	0	0	3	0	0	0	0	0,3	0
	Fallos de servicios de comunicación	0,1	7	6	7	6	6				75%		0	0	0	4,5	0	0	0	0	0,45	0
	Errores del administrador	0,1	7	6	7	6	6		50%	50%	20%		0	3	3,5	1,2	0	0	0,3	0,35	0,12	0
	Errores de configuración	0,1	7	6	7	6	6		60%	60%	25%		0	3,6	4,2	1,5	0	0	0,36	0,42	0,15	0
	Manipulación de la configuración	0,01	7	6	7	6	6		60%	60%	50%		0	3,6	4,2	3	0	0	0,04	0,04	0,03	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	7	6	7	6	6				50%		0	0	0	3	0	0	0	0	0,3	0
	Caída del sistema por agotamiento de recursos	1	7	6	7	6	6				100%		0	0	0	6	0	0	0	0	6	0
	Acceso no autorizado	0,01	7	6	7	6	6		70%		40%		0	4,2	0	2,4	0	0	0,04	0	0,02	0
	Denegación del servicio	0,1	7	6	7	6	6				100%		0	0	0	6	0	0	0	0	0,6	0
HW11	Fuego	0,01	3	3	6	9	6				100%		0	0	0	9	0	0	0	0	0,09	0
	Daños por agua	0,01	3	3	6	9	6				100%		0	0	0	9	0	0	0	0	0,09	0
	Desastres naturales	0,01	3	3	6	9	6				100%		0	0	0	9	0	0	0	0	0,09	0
	Corte del suministro eléctrico	0,1	3	3	6	9	6				100%		0	0	0	9	0	0	0	0	0,9	0
	Avería de origen Físico o lógico	0,01	3	3	6	9	6				50%		0	0	0	4,5	0	0	0	0	0,05	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,01	3	3	6	9	6				30%		0	0	0	2,7	0	0	0	0	0,03	0
	Errores de configuración	0,01	3	3	6	9	6				20%		0	0	0	1,8	0	0	0	0	0,02	0
	Errores del administrador	0,1	3	3	6	9	6				20%		0	0	0	1,8	0	0	0	0	0,18	0
HW12	Fuego	0,01	1	9	9	7	1				100%		0	0	0	7	0	0	0	0	0,07	0
	Daños por agua	0,01	1	9	9	7	1				100%		0	0	0	7	0	0	0	0	0,07	0
	Desastres naturales	0,01	1	9	9	7	1				100%		0	0	0	7	0	0	0	0	0,07	0
	Corte del suministro eléctrico	0,1	1	9	9	7	1				100%		0	0	0	7	0	0	0	0	0,7	0
	Condiciones inadecuadas de temperatura y/o humedad	1	1	9	9	7	1				20%		0	0	0	1,4	0	0	0	0	1,4	0
	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
	Errores del administrador	0,1	1	9	9	7	1		50%	50%	20%		0	4,5	4,5	1,4	0	0	0,45	0,45	0,14	0
	Errores de configuración	0,1	1	9	9	7	1		60%	60%	25%		0	5,4	5,4	1,75	0	0	0,54	0,54	0,18	0
	Manipulación de la configuración	0,01	1	9	9	7	1		60%	60%	50%		0	5,4	5,4	3,5	0	0	0,05	0,05	0,04	0
	Difusión de software dañino	0,1	1	9	9	7	1		30%	30%	25%		0	2,7	2,7	1,75	0	0	0,27	0,27	0,18	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	1	9	9	7	1				50%		0	0	0	3,5	0	0	0	0	0,35	0
	Caída del sistema por	0,1	1	9	9	7	1				100%		0	0	0	7	0	0	0	0	0,7	0

	agotamiento de recursos																					
	Acceso no autorizado	0,1	1	9	9	7	1		40%		40%		0	3,6	0	2,8	0	0	0,36	0	0,28	0
HW13	Fuego	0,01	1	6	3	4	1				100%		0	0	0	4	0	0	0	0	0,04	0
	Daños por agua	0,01	1	6	3	4	1				100%		0	0	0	4	0	0	0	0	0,04	0
	Desastres naturales	0,01	1	6	3	4	1				100%		0	0	0	4	0	0	0	0	0,04	0
	Corte del suministro eléctrico	1	1	6	3	4	1				100%		0	0	0	4	0	0	0	0	4	0
	Condiciones inadecuadas de temperatura y/o humedad	1	1	6	3	4	1				20%		0	0	0	0,8	0	0	0	0	0,8	0
	Avería de origen Físico o lógico	0,1	1	6	3	4	1				50%		0	0	0	2	0	0	0	0	0,2	0
	Fallos de servicios de comunicación	1	1	6	3	4	1				75%		0	0	0	3	0	0	0	0	3	0
	Errores del administrador	0,1	1	6	3	4	1		50%	50%	20%		0	3	1,5	0,8	0	0	0,3	0,15	0,08	0
	Errores de configuración	0,1	1	6	3	4	1		60%	60%	25%		0	3,6	1,8	1	0	0	0,36	0,18	0,1	0
	Manipulación de la configuración	0,01	1	6	3	4	1		60%	60%	50%		0	3,6	1,8	2	0	0	0,04	0,02	0,02	0
	Difusión de software dañino	0,1	1	6	3	4	1		30%	30%	25%		0	1,8	0,9	1	0	0	0,18	0,09	0,1	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	1	6	3	4	1				50%		0	0	0	2	0	0	0	0	0,2	0
	Caída del sistema por agotamiento de recursos	0,1	1	6	3	4	1				100%		0	0	0	4	0	0	0	0	0,4	0
	Acceso no autorizado	0,1	1	6	3	4	1		40%		40%		0	2,4	0	1,6	0	0	0,24	0	0,16	0
HW14	Fuego	0,01	1	9	6	3	1				100%		0	0	0	3	0	0	0	0	0,03	0
	Daños por agua	0,01	1	9	6	3	1				100%		0	0	0	3	0	0	0	0	0,03	0
	Desastres naturales	0,01	1	9	6	3	1				100%		0	0	0	3	0	0	0	0	0,03	0
	Corte del suministro eléctrico	1	1	9	6	3	1				100%		0	0	0	3	0	0	0	0	3	0
	Condiciones inadecuadas de temperatura y/o humedad	1	1	9	6	3	1				20%		0	0	0	0,6	0	0	0	0	0,6	0
	Avería de origen Físico o lógico	0,1	1	9	6	3	1				50%		0	0	0	1,5	0	0	0	0	0,15	0
	Fallos de servicios de comunicación	1	1	9	6	3	1				75%		0	0	0	2,25	0	0	0	0	2,25	0
	Errores del administrador	0,1	1	9	6	3	1		50%	50%	20%		0	4,5	3	0,6	0	0	0,45	0,3	0,06	0
	Errores de configuración	0,1	1	9	6	3	1		60%	60%	25%		0	5,4	3,6	0,75	0	0	0,54	0,36	0,08	0
	Manipulación de la configuración	0,01	1	9	6	3	1		60%	60%	50%		0	5,4	3,6	1,5	0	0	0,05	0,04	0,02	0
	Difusión de software dañino	1	1	9	6	3	1		30%	30%	25%		0	2,7	1,8	0,75	0	0	2,7	1,8	0,75	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	1	9	6	3	1				50%		0	0	0	1,5	0	0	0	0	0,15	0
	Caída del sistema por agotamiento de recursos	0,1	1	9	6	3	1				100%		0	0	0	3	0	0	0	0	0,3	0
	Acceso no autorizado	0,1	1	9	6	3	1		40%		40%		0	3,6	0	1,2	0	0	0,36	0	0,12	0
HW15	Fuego	0,01	6	6	7	3	6				100%		0	0	0	3	0	0	0	0	0,03	0
	Daños por agua	0,01	6	6	7	3	6				100%		0	0	0	3	0	0	0	0	0,03	0
	Desastres naturales	0,01	6	6	7	3	6				100%		0	0	0	3	0	0	0	0	0,03	0
	Corte del suministro eléctrico	1	6	6	7	3	6				100%		0	0	0	3	0	0	0	0	3	0
	Condiciones inadecuadas de temperatura y/o humedad	1	6	6	7	3	6				20%		0	0	0	0,6	0	0	0	0	0,6	0
	Avería de origen Físico o lógico	0,1	6	6	7	3	6				50%		0	0	0	1,5	0	0	0	0	0,15	0
	Fallos de servicios de comunicación	1	6	6	7	3	6				75%		0	0	0	2,25	0	0	0	0	2,25	0
	Errores del administrador	0,1	6	6	7	3	6		50%	50%	20%		0	3	3,5	0,6	0	0	0,3	0,35	0,06	0

	Errores de configuración	0,1	6	6	7	3	6		60%	60%	25%		0	3,6	4,2	0,75	0	0	0,36	0,42	0,08	0
	Manipulación de la configuración	0,01	6	6	7	3	6		60%	60%	50%		0	3,6	4,2	1,5	0	0	0,04	0,04	0,02	0
	Difusión de software dañino	0,1	6	6	7	3	6		30%	30%	25%		0	1,8	2,1	0,75	0	0	0,18	0,21	0,08	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	6	6	7	3	6				50%		0	0	0	1,5	0	0	0	0	0,15	0
	Caída del sistema por agotamiento de recursos	0,1	6	6	7	3	6				100%		0	0	0	3	0	0	0	0	0,3	0
	Acceso no autorizado	0,1	6	6	7	3	6		40%		40%		0	2,4	0	1,2	0	0	0,24	0	0,12	0
HW16	Fuego	0,01	1	9	6	7	1				100%		0	0	0	7	0	0	0	0	0,07	0
	Daños por agua	0,01	1	9	6	7	1				100%		0	0	0	7	0	0	0	0	0,07	0
	Desastres naturales	0,01	1	9	6	7	1				100%		0	0	0	7	0	0	0	0	0,07	0
	Corte del suministro eléctrico	0,1	1	9	6	7	1				100%		0	0	0	7	0	0	0	0	0,7	0
	Condiciones inadecuadas de temperatura y/o humedad	1	1	9	6	7	1				20%		0	0	0	1,4	0	0	0	0	1,4	0
	Avería de origen Físico o lógico	0,1	1	9	6	7	1				50%		0	0	0	3,5	0	0	0	0	0,35	0
	Fallos de servicios de comunicación	0,1	1	9	6	7	1				75%		0	0	0	5,25	0	0	0	0	0,53	0
	Errores del administrador	0,1	1	9	6	7	1		30%	30%	25%		0	2,7	1,8	1,75	0	0	0,27	0,18	0,18	0
	Errores de configuración	0,1	1	9	6	7	1		50%	50%	20%		0	4,5	3	1,4	0	0	0,45	0,3	0,14	0
	Manipulación de la configuración	0,01	1	9	6	7	1		60%	60%	25%		0	5,4	3,6	1,75	0	0	0,05	0,04	0,02	0
	Difusión de software dañino	0,1	1	9	6	7	1		60%	60%	50%		0	5,4	3,6	3,5	0	0	0,54	0,36	0,35	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	1	9	6	7	1				50%		0	0	0	3,5	0	0	0	0	0,35	0
	Caída del sistema por agotamiento de recursos	0,1	1	9	6	7	1				100%		0	0	0	7	0	0	0	0	0,7	0
	Acceso no autorizado	0,1	1	9	6	7	1		40%		40%		0	3,6	0	2,8	0	0	0,36	0	0,28	0
HW17	Fuego	0,01	6	6	7	3	6				100%		0	0	0	3	0	0	0	0	0,03	0
	Daños por agua	0,01	6	6	7	3	6				100%		0	0	0	3	0	0	0	0	0,03	0
	Desastres naturales	0,01	6	6	7	3	6				100%		0	0	0	3	0	0	0	0	0,03	0
	Corte del suministro eléctrico	1	6	6	7	3	6				100%		0	0	0	3	0	0	0	0	3	0
	Condiciones inadecuadas de temperatura y/o humedad	1	6	6	7	3	6				20%		0	0	0	0,6	0	0	0	0	0,6	0
	Avería de origen Físico o lógico	0,1	6	6	7	3	6				50%		0	0	0	1,5	0	0	0	0	0,15	0
	Fallos de servicios de comunicación	1	6	6	7	3	6				75%		0	0	0	2,25	0	0	0	0	2,25	0
	Errores del administrador	0,1	6	6	7	3	6		30%	30%	25%		0	1,8	2,1	0,75	0	0	0,18	0,21	0,08	0
	Errores de configuración	0,1	6	6	7	3	6		50%	50%	20%		0	3	3,5	0,6	0	0	0,3	0,35	0,06	0
	Manipulación de la configuración	0,01	6	6	7	3	6		60%	60%	25%		0	3,6	4,2	0,75	0	0	0,04	0,04	0,01	0
	Difusión de software dañino	0,1	6	6	7	3	6		60%	60%	50%		0	3,6	4,2	1,5	0	0	0,36	0,42	0,15	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	6	6	7	3	6				50%		0	0	0	1,5	0	0	0	0	0,15	0
	Caída del sistema por agotamiento de recursos	0,1	6	6	7	3	6				100%		0	0	0	3	0	0	0	0	0,3	0
	Acceso no autorizado	0,1	6	6	7	3	6		40%		40%		0	2,4	0	1,2	0	0	0,24	0	0,12	0
HW18	Fuego	0,01	5	5	9	7	9				100%		0	0	0	7	0	0	0	0	0,07	0
	Daños por agua	0,01	5	5	9	7	9				100%		0	0	0	7	0	0	0	0	0,07	0
	Desastres naturales	0,01	5	5	9	7	9				100%		0	0	0	7	0	0	0	0	0,07	0

	Corte del suministro eléctrico	0,1	5	5	9	7	9				100%		0	0	0	7	0	0	0	0	0,7	0
	Condiciones inadecuadas de temperatura y/o humedad	1	5	5	9	7	9				20%		0	0	0	1,4	0	0	0	0	1,4	0
	Avería de origen Físico o lógico	0,1	5	5	9	7	9				50%		0	0	0	3,5	0	0	0	0	0,35	0
	Fallos de servicios de comunicación	0,1	5	5	9	7	9				75%		0	0	0	5,25	0	0	0	0	0,53	0
	Errores del administrador	0,1	5	5	9	7	9		30%	30%	25%		0	1,5	2,7	1,75	0	0	0,15	0,27	0,18	0
	Errores de configuración	0,1	5	5	9	7	9		50%	50%	20%		0	2,5	4,5	1,4	0	0	0,25	0,45	0,14	0
	Manipulación de la configuración	0,01	5	5	9	7	9		60%	60%	25%		0	3	5,4	1,75	0	0	0,03	0,05	0,02	0
	Difusión de software dañino	0,1	5	5	9	7	9		60%	60%	50%		0	3	5,4	3,5	0	0	0,3	0,54	0,35	0
	Errores de mantenimiento / actualización de equipos (hardware).	0,1	5	5	9	7	9				50%		0	0	0	3,5	0	0	0	0	0,35	0
	Caída del sistema por agotamiento de recursos	0,1	5	5	9	7	9				100%		0	0	0	7	0	0	0	0	0,7	0
	Acceso no autorizado	0,1	5	5	9	7	9		40%		40%		0	2	0	2,8	0	0	0,2	0	0,28	0
HW19	Avería de origen Físico o lógico	0,1	7	0	9	7	1			30%	40%		0	0	2,7	2,8	0	0	0	0,27	0,28	0
	Fallos de servicios de comunicación	0,1	7	0	9	7	1			50%	90%							0	0	0	0	0
HW20	Avería de origen Físico o lógico	0,1	7	0	9	7	1			40%	80%		0	0	3,6	5,6	0	0	0	0,36	0,56	0
	Fallos de servicios de comunicación	0,1	7	0	9	7	1				100%		0	0	0	7	0	0	0	0	0,7	0
SW1	Errores del administrador	0,1	3	3	3	6	2		50%	50%	20%		0	1,5	1,5	1,2	0	0	0,15	0,15	0,12	0
	Errores de configuración	0,1	3	3	3	6	2		60%	60%	25%		0	1,8	1,8	1,5	0	0	0,18	0,18	0,15	0
	Difusión de software dañino	0,1	3	3	3	6	2		30%	30%	25%		0	0,9	0,9	1,5	0	0	0,09	0,09	0,15	0
	Análisis de tráfico	0,1	3	3	3	6	2		30%				0	0,9	0	0	0	0	0,09	0	0	0
	Errores de monitorización	0,1	3	3	3	6	2	20%				20%	0,6	0	0	0	0,4	0,06	0	0	0	0,04
	Acceso no autorizado	0,1	3	3	3	6	2		40%		40%		0	1,2	0	2,4	0	0	0,12	0	0,24	0
	Denegación del servicio	0,1	3	3	3	6	2				100%		0	0	0	6	0	0	0	0	0,6	0
	Errores de mantenimiento / actualización de programas (software)	1	3	3	3	6	2				30%		0	0	0	1,8	0	0	0	0	1,8	0
SW2	Errores del administrador	0,1	3	3	3	6	2		50%	50%	20%		0	1,5	1,5	1,2	0	0	0,15	0,15	0,12	0
	Errores de configuración	0,1	3	3	3	6	2		60%	60%	25%		0	1,8	1,8	1,5	0	0	0,18	0,18	0,15	0
	Difusión de software dañino	0,1	3	3	3	6	2		30%	30%	25%		0	0,9	0,9	1,5	0	0	0,09	0,09	0,15	0
	Análisis de tráfico	0,1	3	3	3	6	2		30%				0	0,9	0	0	0	0	0,09	0	0	0
	Errores de monitorización	0,1	3	3	3	6	2	20%				20%	0,6	0	0	0	0,4	0,06	0	0	0	0,04
	Acceso no autorizado	0,1	3	3	3	6	2		40%		40%		0	1,2	0	2,4	0	0	0,12	0	0,24	0
	Denegación del servicio	0,1	3	3	3	6	2				100%		0	0	0	6	0	0	0	0	0,6	0
	Errores de mantenimiento / actualización de programas (software)	1	3	3	3	6	2				30%		0	0	0	1,8	0	0	0	0	1,8	0
SW3	Errores del administrador	0,1	9	7	7	9	9		50%	50%	20%		0	3,5	3,5	1,8	0	0	0,35	0,35	0,18	0
	Errores de configuración	0,1	9	7	7	9	9		60%	60%	25%		0	4,2	4,2	2,25	0	0	0,42	0,42	0,23	0
	Difusión de software dañino	0,1	9	7	7	9	9		30%	30%	25%		0	2,1	2,1	2,25	0	0	0,21	0,21	0,23	0
	Análisis de tráfico	0,1	9	7	7	9	9		30%				0	2,1	0	0	0	0	0,21	0	0	0
	Errores de monitorización	0,1	9	7	7	9	9	20%				20%	1,8	0	0	0	1,8	0,18	0	0	0	0,18
	Acceso no autorizado	0,1	9	7	7	9	9		40%		40%		0	2,8	0	3,6	0	0	0,28	0	0,36	0
	Denegación del servicio	0,1	9	7	7	9	9				100%		0	0	0	9	0	0	0	0	0,9	0
	Errores de mantenimiento /	1	9	7	7	9	9				30%		0	0	0	2,7	0	0	0	0	2,7	0

	actualización de programas (software)																					
SW4	Errores del administrador	0,1	3	1	1	3	2		50%	50%	20%		0	0,5	0,5	0,6	0	0	0,05	0,05	0,06	0
	Errores de configuración	0,1	3	1	1	3	2		60%	60%	25%		0	0,6	0,6	0,75	0	0	0,06	0,06	0,08	0
	Difusión de software dañino	0,1	3	1	1	3	2		30%	30%	25%		0	0,3	0,3	0,75	0	0	0,03	0,03	0,08	0
	Análisis de tráfico	0,1	3	1	1	3	2		30%				0	0,3	0	0	0	0	0,03	0	0	0
	Errores de monitorización	0,1	3	1	1	3	2	20%				20%	0,6	0	0	0	0,4	0,06	0	0	0	0,04
	Acceso no autorizado	0,1	3	1	1	3	2		40%		40%		0	0,4	0	1,2	0	0	0,04	0	0,12	0
	Denegación del servicio	0,1	3	1	1	3	2				100%		0	0	0	3	0	0	0	0	0,3	0
	Errores de mantenimiento / actualización de programas (software)	1	3	1	1	3	2				30%		0	0	0	0,9	0	0	0	0	0,9	0
SW5	Errores del administrador	0,1	3	3	3	6	2		50%	50%	20%		0	1,5	1,5	1,2	0	0	0,15	0,15	0,12	0
	Errores de configuración	0,1	3	3	3	6	2		60%	60%	25%		0	1,8	1,8	1,5	0	0	0,18	0,18	0,15	0
	Difusión de software dañino	0,1	3	3	3	6	2		30%	30%	25%		0	0,9	0,9	1,5	0	0	0,09	0,09	0,15	0
	Análisis de tráfico	0,1	3	3	3	6	2		30%				0	0,9	0	0	0	0	0,09	0	0	0
	Errores de monitorización	0,1	3	3	3	6	2	20%				20%	0,6	0	0	0	0,4	0,06	0	0	0	0,04
	Acceso no autorizado	0,1	3	3	3	6	2		40%		40%		0	1,2	0	2,4	0	0	0,12	0	0,24	0
	Denegación del servicio	0,1	3	3	3	6	2				100%		0	0	0	6	0	0	0	0	0,6	0
	Errores de mantenimiento / actualización de programas (software)	1	3	3	3	6	2				30%		0	0	0	1,8	0	0	0	0	1,8	0
SW6	Errores del administrador	0,1	9	7	7	9	7		50%	50%	20%		0	3,5	3,5	1,8	0	0	0,35	0,35	0,18	0
	Errores de configuración	0,1	3	3	3	6	2		60%	60%	25%		0	1,8	1,8	1,5	0	0	0,18	0,18	0,15	0
	Difusión de software dañino	0,1	3	3	3	6	2		30%	30%	25%		0	0,9	0,9	1,5	0	0	0,09	0,09	0,15	0
	Análisis de tráfico	0,1	3	3	3	6	2		30%				0	0,9	0	0	0	0	0,09	0	0	0
	Errores de monitorización	0,1	3	3	3	6	2	20%				20%	0,6	0	0	0	0,4	0,06	0	0	0	0,04
	Acceso no autorizado	0,1	3	3	3	6	2		40%		40%		0	1,2	0	2,4	0	0	0,12	0	0,24	0
	Denegación del servicio	0,1	3	3	3	6	2				100%		0	0	0	6	0	0	0	0	0,6	0
	Errores de mantenimiento / actualización de programas (software)	1	3	3	3	6	2				30%		0	0	0	1,8	0	0	0	0	1,8	0
SW7	Errores de mantenimiento / actualización de programas (software)	1	3	7	7	7	2		60%		60%		0	3,5	0	3,5	0	0	4,2	0	4,2	0
	Manipulación de la configuración	0,01	3	7	7	7	2		50%		50%		0	3,5	0	3,5	0	0	0,04	0	0,04	0
	Errores del administrador	0,1	3	7	7	7	2		50%		50%		0	3,5	0	3,5	0	0	0,35	0	0,35	0
	Errores de configuración	0,1	3	7	7	7	2		50%		50%		0	3,5	0	3,5	0	0	0,35	0	0,35	0
SW8	Errores de mantenimiento / actualización de programas (software)	1	3	7	7	7	2		60%		60%		0	3,5	0	3,5	0	0	4,2	0	4,2	0
	Manipulación de la configuración	0,01	3	7	7	7	2		50%		50%		0	3,5	0	3,5	0	0	0,04	0	0,04	0
	Errores del administrador	0,1	3	7	7	7	2		50%		50%		0	3,5	0	3,5	0	0	0,35	0	0,35	0
	Errores de configuración	0,1	3	7	7	7	2		50%		50%		0	3,5	0	3,5	0	0	0,35	0	0,35	0
SW9	Errores de mantenimiento / actualización de programas (software)	1	7	7	7	7	7		80%		80%		0	3,5	0	3,5	0	0	5,6	0	5,6	0
	Manipulación de la configuración	0,01	7	7	7	7	7		50%		50%		0	3,5	3,5	3,5	0	0	0,04	0,04	0,04	0
	Errores del administrador	0,1	7	7	7	7	7		50%		50%		0	3,5	3,5	3,5	0	0	0,35	0,35	0,35	0
	Errores de configuración	0,1	7	7	7	7	7		50%		50%		0	3,5	3,5	3,5	0	0	0,35	0,35	0,35	0
SW10	Errores del administrador	0,1	1	1	3	3	1		50%	50%	20%		0	0,5	1,5	0,6	0	0	0,05	0,15	0,06	0
	Errores de configuración	0,1	1	1	3	3	1		60%	60%	25%		0	0,6	1,8	0,75	0	0	0,06	0,18	0,08	0

	Difusión de software dañino	0,1	1	1	3	3	1		30%	30%	25%		0	0,3	0,9	0,75	0	0	0,03	0,09	0,08	0
	Análisis de tráfico	0,1	1	1	3	3	1		30%				0	0,3	0	0	0	0	0,03	0	0	0
	Errores de monitorización	0,1	1	1	3	3	1	20%				20%	0,2	0	0	0	0,2	0,02	0	0	0	0,02
	Acceso no autorizado	0,1	1	1	3	3	1		40%		40%		0	0,4	0	1,2	0	0	0,04	0	0,12	0
	Denegación del servicio	0,1	1	1	3	3	1				100%		0	0	0	3	0	0	0	0	0,3	0
	Errores de mantenimiento / actualización de programas (software)	1	1	1	3	3	1				30%		0	0	0	0,9	0	0	0	0	0,9	0
SW11	Errores del administrador	0,1	1	6	9	7	7		50%	50%	20%		0	3	4,5	1,4	0	0	0,3	0,45	0,14	0
	Errores de configuración	0,1	3	3	3	6	2		60%	60%	25%		0	1,8	1,8	1,5	0	0	0,18	0,18	0,15	0
	Difusión de software dañino	0,1	3	3	3	6	2		30%	30%	25%		0	0,9	0,9	1,5	0	0	0,09	0,09	0,15	0
	Análisis de tráfico	0,1	3	3	3	6	2		30%				0	0,9	0	0	0	0	0,09	0	0	0
	Errores de monitorización	0,1	3	3	3	6	2	20%				20%	0,6	0	0	0	0,4	0,06	0	0	0	0,04
	Acceso no autorizado	0,1	3	3	3	6	2		40%		40%		0	1,2	0	2,4	0	0	0,12	0	0,24	0
	Denegación del servicio	0,1	3	3	3	6	2				100%		0	0	0	6	0	0	0	0	0,6	0
	Errores de mantenimiento / actualización de programas (software)	1	3	3	3	6	2				30%		0	0	0	1,8	0	0	0	0	1,8	0
SW12	Errores del administrador	0,1	3	1	3	3	3		50%	50%	20%		0	0,5	1,5	0,6	0	0	0,05	0,15	0,06	0
	Errores de configuración	0,1	3	1	3	3	3		40%	40%	25%		0	0,4	1,2	0,75	0	0	0,04	0,12	0,08	0
	Acceso no autorizado	0,1	3	1	3	3	3		40%		40%		0	0,4	0	1,2	0	0	0,04	0	0,12	0
	Errores de monitorización	0,1	3	1	3	3	3	20%				20%	0,6	0	0	0	0,6	0,06	0	0	0	0,06
	Errores de mantenimiento / actualización de programas (software)	1	3	1	3	3	3				30%		0	0	0	0,9	0	0	0	0	0,9	0
	Manipulación de la configuración	0,01	3	1	3	3	3		60%	60%	50%		0	0,6	1,8	1,5	0	0	0,01	0,02	0,02	0
	Análisis de tráfico	0,1	3	1	3	3	3		30%				0	0,3	0	0	0	0	0,03	0	0	0
SW13	Errores del administrador	0,1	3	1	3	3	3		50%	50%	20%		0	0,5	1,5	0,6	0	0	0,05	0,15	0,06	0
	Errores de configuración	0,1	3	1	3	3	3		40%	40%	25%		0	0,4	1,2	0,75	0	0	0,04	0,12	0,08	0
	Acceso no autorizado	0,1	3	1	3	3	3		40%		40%		0	0,4	0	1,2	0	0	0,04	0	0,12	0
	Errores de monitorización	0,1	3	1	3	3	3	20%				20%	0,6	0	0	0	0,6	0,06	0	0	0	0,06
	Errores de mantenimiento / actualización de programas (software)	1	3	1	3	3	3				30%		0	0	0	0,9	0	0	0	0	0,9	0
	Manipulación de la configuración	0,01	3	1	3	3	3		60%	60%	50%		0	0,6	1,8	1,5	0	0	0,01	0,02	0,02	0
	Análisis de tráfico	0,1	3	1	3	3	3		30%				0	0,3	0	0	0	0	0,03	0	0	0
SW14	Errores del administrador	0,1	7	5	7	7	7		50%	50%	20%		0	2,5	3,5	1,4	0	0	0,25	0,35	0,14	0
	Errores de configuración	0,1	7	5	7	7	7		40%	40%	25%		0	2	2,8	1,75	0	0	0,2	0,28	0,18	0
	Acceso no autorizado	0,1	7	5	7	7	7		40%		40%		0	2	0	2,8	0	0	0,2	0	0,28	0
	Errores de monitorización	0,1	7	5	7	7	7	20%				20%	1,4	0	0	0	1,4	0,14	0	0	0	0,14
	Errores de mantenimiento / actualización de programas (software)	1	7	5	7	7	7				30%		0	0	0	2,1	0	0	0	0	2,1	0
	Manipulación de la configuración	0,01	7	5	7	7	7		60%	60%	50%		0	3	4,2	3,5	0	0	0,03	0,04	0,04	0
	Análisis de tráfico	0,1	7	5	7	7	7	70%	30%			70%	4,9	1,5	0	0	4,9	0,49	0,15	0	0	0,49
A1	Errores del administrador	1	2	2	2	2	2	50%	50%	20%		50%	1	1	0,4	0	1	1	1	0,4	0	1
	Errores de los usuarios	1	2	2	2	2	2		30%	20%			0	0,6	0,4	0	0	0	0,6	0,4	0	0
	Acceso no autorizado	0,01	2	2	2	2	2		40%	40%			0	0,8	0,8	0	0	0	0,01	0,01	0	0
	Alteración de la información	0,1	2	2	2	2	2			20%			0	0	0,4	0	0	0	0	0,04	0	0

	Introducción de información incorrecta	1	2	2	2	2	2			40%			0	0	0,8	0	0	0	0	0,8	0	0
	Vulnerabilidades de los programas (software)	1	2	2	2	2	2		40%	40%		40%	0	0,8	0,8	0	0,8	0	0,8	0,8	0	0,8
	Destrucción de información	0,01	2	2	2	2	2				100%		0	0	0	2	0	0	0	0	0,02	0
	Divulgación de información	0,01	2	2	2	2	2		100%				0	2	0	0	0	0	0,02	0	0	0
	Intercepción de información (escucha)	0,01	2	2	2	2	2		70%				0	1,4	0	0	0	0	0,01	0	0	0
	Corrupción de la información	0,01	2	2	2	2	2		50%	50%			0	1	1	0	0	0	0,01	0,01	0	0
A2	Errores del administrador	1	2	2	2	2	2	50%	50%	20%		50%	1	1	0,4	0	1	1	1	0,4	0	1
	Errores de los usuarios	1	2	2	2	2	2		30%	20%			0	0,6	0,4	0	0	0	0,6	0,4	0	0
	Acceso no autorizado	0,01	2	2	2	2	2		40%	40%			0	0,8	0,8	0	0	0	0,01	0,01	0	0
	Alteración de la información	0,1	2	2	2	2	2			20%			0	0	0,4	0	0	0	0	0,04	0	0
	Introducción de información incorrecta	1	2	2	2	2	2			40%			0	0	0,8	0	0	0	0	0,8	0	0
	Vulnerabilidades de los programas (software)	1	2	2	2	2	2		40%	40%		40%	0	0,8	0,8	0	0,8	0	0,8	0,8	0	0,8
	Destrucción de información	0,01	2	2	2	2	2				100%		0	0	0	2	0	0	0	0	0,02	0
	Divulgación de información	0,01	2	2	2	2	2		100%				0	2	0	0	0	0	0,02	0	0	0
	Intercepción de información (escucha)	0,01	2	2	2	2	2		70%				0	1,4	0	0	0	0	0,01	0	0	0
	Corrupción de la información	0,01	2	2	2	2	2		50%	50%			0	1	1	0	0	0	0,01	0,01	0	0
A3	Errores del administrador	1	7	9	9	9	7	20%	20%	20%		40%	1,4	1,8	1,8	0	2,8	1,4	1,8	1,8	0	2,8
	Errores de los usuarios	1	7	9	9	9	7		30%	20%			0	2,7	1,8	0	0	0	2,7	1,8	0	0
	Acceso no autorizado	0,01	7	9	9	9	7		40%	40%			0	3,6	3,6	0	0	0	0,04	0,04	0	0
	Alteración de la información	0,1	7	9	9	9	7			20%			0	0	1,8	0	0	0	0	0,18	0	0
	Introducción de información incorrecta	1	7	9	9	9	7			60%			0	0	3,6	0	0	0	0	5,4	0	0
	Denegación de servicio	1	7	9	9	9	7				60%		0	0	0	3,6	0	0	0	0	5,4	0
	Vulnerabilidades de los programas (software)	1	7	9	9	9	7		60%	60%		60%	0	3,6	3,6	0	3,15	0	5,4	5,4	0	4,2
	Destrucción de información	0,01	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,09	0
	Divulgación de información	0,01	7	9	9	9	7		100%				0	9	0	0	0	0	0,09	0	0	0
	Intercepción de información (escucha)	0,01	7	9	9	9	7		70%				0	6,3	0	0	0	0	0,06	0	0	0
	Corrupción de la información	0,01	7	9	9	9	7		50%	50%			0	4,5	4,5	0	0	0	0,05	0,05	0	0
D1	Fuego	0,01	10	10	10	10	10				100%		0	0	0	10	0	0	0	0	0,1	0
	Daños por agua	0,01	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,09	0
	Desastres naturales	0,01	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,09	0
	Condiciones inadecuadas de temperatura y/o humedad	0,01	7	9	9	9	7				100%		0	0	0	9	0	0	0	0	0,09	0
	Escapes de información	1	7	9	9	9	7		50%				0	4,5	0	0	0	0	4,5	0	0	0
	Alteración de la información	0,01	7	9	9	9	7		50%	80%			0	4,5	7,2	0	0	0	0,05	0,07	0	0
	Perdida o robo	0,01	7	9	9	9	7		100%	100%			0	9	9	0	0	0	0,09	0,09	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
	Destrucción de información	0,01	7	9	9	9	7			100%			0	0	9	0	0	0	0	0,09	0	0
	Divulgación de información	0,01	7	9	9	9	7		100%				0	9	0	0	0	0	0,09	0	0	0
D2	Destrucción de información	0,01	7	9	9	9	7	50%			50%	50%	3,5	0	0	4,5	3,5	0,04	0	0	0,05	0,04
	Alteración de la información	0,01	7	9	9	9	7	50%		50%	50%	50%	3,5	0	4,5	4,5	3,5	0,04	0	0,05	0,05	0,04

D3	Destrucción de información	0,01	7	9	9	9	7	50%			50%	50%	3,5	0	0	4,5	3,5	0,04	0	0	0,05	0,04
	Alteración de la información	0,01	7	9	9	9	7	50%		50%	50%	50%	3,5	0	4,5	4,5	3,5	0,04	0	0,05	0,05	0,04
D4	Escapes de información	0,1	4	4	4	4	4		100%				0	4	0	0	0	0	0,4	0	0	0
	Alteración de la información	0,1	4	4	4	4	4	100%	80%	100%		100%	4	3,2	4	0	4	0,4	0,32	0,4	0	0,4
	Introducción de información incorrecta	1	4	4	4	4	4			80%			0	0	3,2	0	0	0	0	3,2	0	0
	Destrucción de información	0,01	4	4	4	4	4			100%	100%		0	0	4	4	0	0	0	0,04	0,04	0
D5	Escapes de información	0,1	4	4	4	4	4		100%				0	4	0	0	0	0	0,4	0	0	0
	Alteración de la información	0,01	4	4	4	4	4	100%	80%	100%		100%	4	3,2	4	0	4	0,04	0,03	0,04	0	0,04
	Introducción de información incorrecta	1	4	4	4	4	4			80%			0	0	3,2	0	0	0	0	3,2	0	0
	Destrucción de información	0,01	4	4	4	4	4			100%	100%		0	0	9	9	0	0	0	0,09	0,09	0
D6	Escapes de información	0,1	9	9	9	9	9		100%				0	9	0	0	0	0	0,9	0	0	0
	Alteración de la información	0,01	9	9	9	9	9	100%	80%	100%		100%	9	7,2	9	0	9	0,09	0,07	0,09	0	0,09
	Introducción de información incorrecta	1	9	9	9	9	9			80%			0	0	7,2	0	0	0	0	7,2	0	0
	Destrucción de información	0,01	9	9	9	9	9			100%	100%		0	0	9	9	0	0	0	0,09	0,09	0
	Divulgación de información	0,01	9	9	9	9	9		100%				0	3	0	0	0	0	0,03	0	0	0
D7	Errores de reencaminamiento	0,01	4	3	4	4	3				100%		0	0	0	4	0	0	0	0	0,04	0
	Destrucción de información	0,01	4	3	4	4	3			100%	100%		0	0	4	4	0	0	0	0,04	0,04	0
	Alteración de la información	0,01	4	3	4	4	3			100%			0	0	4	0	0	0	0	0,04	0	0
D8	Errores de reencaminamiento	0,01	4	3	4	4	3				100%		0	0	0	4	0	0	0	0	0,04	0
	Destrucción de información	0,01	4	3	4	4	3			100%	100%		0	0	4	4	0	0	0	0,04	0,04	0
	Alteración de la información	0,01	4	3	4	4	3			100%			0	0	10	0	0	0	0	0,1	0	0
D9	Errores de reencaminamiento	0,01	10	7	10	10	7				100%		0	0	0	10	0	0	0	0	0,1	0
	Destrucción de información	0,01	10	7	10	10	7			100%	100%		0	0	10	10	0	0	0	0,1	0,1	0
	Alteración de la información	0,1	10	7	10	10	7			100%			0	0	10	0	0	0	0	1	0	0
D10	Errores de reencaminamiento	0,1	4	3	4	4	3				100%		0	0	0	4	0	0	0	0	0,4	0
	Destrucción de información	0,01	4	3	4	4	3			100%	100%		0	0	4	4	0	0	0	0,04	0,04	0
	Alteración de la información	0,01	4	3	4	4	3			100%			0	0	4	0	0	0	0	0,04	0	0
D11	Errores de reencaminamiento	0,1	4	3	4	4	3				100%		0	0	0	4	0	0	0	0	0,4	0
	Destrucción de información	0,01	4	3	4	4	3			100%	100%		0	0	4	4	0	0	0	0,04	0,04	0
	Alteración de la información	0,01	4	3	4	4	3			100%			0	0	4	0	0	0	0	0,04	0	0
D12	Fallos de servicios de comunicación	1	10	7	10	10	7				80%		0	0	0	10	0	0	0	0	8	0
	Acceso de personal no autorizado	1	10	7	10	10	7		80%				0	5,6	0	10	0	0	0	0	0	0
	Destrucción de información	0,01	10	7	10	10	7			100%	100%		0	0	10	10	0	0	0	0,1	0,1	0
	Alteración de la información	0,01	10	7	10	10	7			100%			0	0	10	0	0	0	0	0,1	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
D14	Alteración de la información	0,01	7	4	7	7	4	50%	100%	100%			3,5	4	7	0	0	0,04	0,04	0,07	0	0
	Destrucción de información	0,01	7	4	7	7	4	100%		100%			7	0	7	0	0	0,07	0	0,07	0	0

D15	Destrucción de información	0,1	7	7	9	9	4			70%			0	0	6,3	0	0	0	0	0,63	0	0
	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
	Destrucción de información	0,01	4	3	4	4	3				100%		0	0	0	4	0	0	0	0	0,04	0
	Alteración de la información	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	1	4	3	4	4	3			100%	100%		0	0	4	4	0	0	0	4	4	0
	Destrucción de información	0,01	4	3	4	4	3				100%		0	0	0	4	0	0	0	0	0,04	0
	Alteración de la información	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	1	10	7	10	10	7			100%	100%		0	0	10	10	0	0	0	10	10	0
	Destrucción de información	0,01	10	7	10	10	7				100%		0	0	0	10	0	0	0	0	0,1	0
	Alteración de la información	0,1	10	7	10	10	7			100%	100%		0	0	10	10	0	0	0	1	1	0
D19	Destrucción de información	0,01	7	4	9	9	4				100%		0	0	0	9	0	0	0	0	0,09	0
	Alteración de la información	0,01	7	4	9	9	4			100%	100%		0	0	9	9	0	0	0	0,09	0,09	0
D20	Destrucción de información	0,01	4	6	7	6	4					50%	0	0	0	0	2	0	0	0	0	0,02
	Alteración de la información	0,01	4	6	7	6	4					50%	0	0	0	0	2	0	0	0	0	0,02
D21	Destrucción de información	0,01	4	6	7	6	4					50%	0	0	0	0	2	0	0	0	0	0,02
	Alteración de la información	0,01	4	6	7	6	4					50%	0	0	0	0	2	0	0	0	0	0,02
D22	Destrucción de información	0,01	4	4	9	7	4			100%	100%		0	0	9	7	0	0	0	0,09	0,07	0
	Alteración de la información	0,01	4	4	9	7	4			100%	100%		0	0	9	7	0	0	0	0,09	0,07	0
D23	Destrucción de información	0,01	9	6	9	6	9	100%		100%	100%	100%	9	0	9	6	9	0,09	0	0,09	0,06	0,09
	Vulnerabilidades de los programas (software)	1	9	6	9	6	9	80%		80%		80%	9	0	9	0	9	7,2	0	7,2	0	7,2
R1	Denegación de servicio	0,01	9	9	9	10	9				100%		0	0	0	10	0	0	0	0	0,1	0
R2	Denegación de servicio	0,01	9	9	9	10	9				100%		0	0	0	10	0	0	0	0	0,1	0
S1	Denegación de servicio	0,01	9	9	9	10	9				100%		0	0	0	10	0	0	0	0	0,1	0
S2	Denegación de servicio	0,1	4	3	4	4	3				100%		0	0	0	4	0	0	0	0	0,4	0
S3	Denegación de servicio	0,01	9	4	9	9	4				100%		0	0	0	9	0	0	0	0	0,09	0
S4	Denegación de servicio	0,01	7	7	9	9	9	100%			75%	100%	7	0	0	6,75	9	0,07	0	0	0,07	0,09
S5	Denegación de servicio	0,01	6	9	6	7	6				100%		0	0	0	7	0	0	0	0	0,07	0
E1	Acceso no autorizado	0,01	6	9	9	6	6		100%	100%	100%		0	9	9	6	0	0	0,09	0,09	0,06	0
	Robo	0,01	6	9	9	6	6		100%		50%		0	9	0	3	0	0	0,09	0	0,03	0
E2	Destrucción	0,01	9	10	10	10	7				100%		0	0	0	10	0	0	0	0	0,1	0
	Acceso no autorizado	0,01	9	10	10	10	7		100%	100%			0	10	10	0	0	0	0,1	0,1	0	0

	Robo	0,01	9	10	10	10	7		100%		50%		0	10	0	5	0	0	0,1	0	0,05	0
P1	Indisponibilidad del personal	1	9	9	0	9	0				50%		0	0	0	4,5	0	0	0	0	4,5	0
	Fugas de información	0,01	9	9	0	9	0		50%				0	4,5	0	0	0	0	0,05	0	0	0
	Suplantación de la identidad del usuario	0,1	9	9	0	9	0	25%	50%		50%		2,25	4,5	0	4,5	0	0,23	0,45	0	0,45	0
	Abuso de privilegios de acceso	0,01	9	9	0	9	0	50%	25%				4,5	2,25	0	0	0	0,05	0,02	0	0	0
	Ingeniería social	0,1	9	9	0	9	0		25%				0	2,25	0	0	0	0	0,23	0	0	0
P2	Indisponibilidad del personal	0,01	4	4	0	4	0				50%		0	0	0	2	0	0	0	0	0,02	0
	Fugas de información	0,01	4	4	0	4	0		50%				0	2	0	0	0	0	0,02	0	0	0
	Suplantación de la identidad del usuario	0,01	4	4	0	4	0	25%	50%		50%		1	2	0	2	0	0,01	0,02	0	0,02	0
	Abuso de privilegios de acceso	0,01	4	4	0	4	0	50%	25%				2	1	0	0	0	0,02	0,01	0	0	0
	Ingeniería social	0,1	4	4	0	4	0		25%				0	1	0	0	0	0	0,1	0	0	0
P3	Indisponibilidad del personal	0,01	4	4	0	4	0				50%		0	0	0	2	0	0	0	0	0,02	0
	Fugas de información	0,01	4	4	0	4	0		50%				0	2	0	0	0	0	0,02	0	0	0
	Suplantación de la identidad del usuario	0,01	4	4	0	4	0	25%	50%		50%		1	2	0	2	0	0,01	0,02	0	0,02	0
	Abuso de privilegios de acceso	0,01	4	4	0	4	0	50%	25%				2	1	0	0	0	0,02	0,01	0	0	0
	Ingeniería social	0,1	4	4	0	4	0		25%				0	1	0	0	0	0	0,1	0	0	0
P4	Indisponibilidad del personal	0,01	6	6	0	6	0				50%		0	0	0	3	0	0	0	0	0,03	0
	Fugas de información	0,01	6	6	0	6	0		50%				0	3	0	0	0	0	0,03	0	0	0
	Suplantación de la identidad del usuario	0,01	6	6	0	6	0	25%	50%		50%		1,5	3	0	3	0	0,02	0,03	0	0,03	0
	Abuso de privilegios de acceso	0,01	6	6	0	6	0	50%	25%				3	1,5	0	0	0	0,03	0,02	0	0	0
	Ingeniería social	0,1	6	6	0	6	0		25%				0	1,5	0	0	0	0	0,15	0	0	0
P5	Indisponibilidad del personal	1	7	7	0	7	0				50%		0	0	0	3,5	0	0	0	0	3,5	0
	Fugas de información	0,01	7	7	0	7	0		50%				0	3,5	0	0	0	0	0,04	0	0	0
	Suplantación de la identidad del usuario	0,01	7	7	0	7	0	25%	50%		50%		1,75	3,5	0	3,5	0	0,02	0,04	0	0,04	0
	Abuso de privilegios de acceso	0,01	7	7	0	7	0	50%	25%				3,5	1,75	0	0	0	0,04	0,02	0	0	0
	Ingeniería social	0,1	7	7	0	7	0		25%				0	1,75	0	0	0	0	0,18	0	0	0
P6	Indisponibilidad del personal	0,01	4	4	0	4	0				50%		0	0	0	2	0	0	0	0	0,02	0
	Fugas de información	0,01	4	4	0	4	0		50%				0	2	0	0	0	0	0,02	0	0	0
	Suplantación de la identidad del usuario	0,01	4	4	0	4	0	25%	50%		50%		1	2	0	2	0	0,01	0,02	0	0,02	0
	Abuso de privilegios de acceso	0,01	4	4	0	4	0	50%	25%				2	1	0	0	0	0,02	0,01	0	0	0
	Ingeniería social	0,1	4	4	0	4	0		25%				0	1	0	0	0	0	0,1	0	0	0
P7	Indisponibilidad del personal	0,01	4	4	0	4	0				50%		0	0	0	2	0	0	0	0	0,02	0
	Fugas de información	0,01	4	4	0	4	0		50%				0	2	0	0	0	0	0,02	0	0	0
	Suplantación de la identidad del usuario	0,01	4	4	0	4	0	25%	50%		50%		1	2	0	2	0	0,01	0,02	0	0,02	0
	Abuso de privilegios de acceso	0,01	4	4	0	4	0	50%	25%				2	1	0	0	0	0,02	0,01	0	0	0
	Ingeniería social	0,1	4	4	0	4	0		25%				0	1	0	0	0	0	0,1	0	0	0
P8	Indisponibilidad del personal	1	8	8	0	8	0				50%		0	0	0	4	0	0	0	0	4	0

	Fugas de información	0,01	8	8	0	8	0		50%				0	4	0	0	0	0	0,04	0	0	0
	Suplantación de la identidad del usuario	0,01	8	8	0	8	0	25%	50%		50%		2	4	0	4	0	0,02	0,04	0	0,04	0
	Abuso de privilegios de acceso	0,01	8	8	0	8	0	50%	25%				4	2	0	0	0	0,04	0,02	0	0	0
	Ingeniería social	0,1	8	8	0	8	0		25%				0	2	0	0	0	0	0,2	0	0	0

Tabla 15: Resumen Riesgo residual

3.9. Resultados

En la Tabla 15 se muestra el resumen de los resultados obtenidos y los riesgos calculados que superan el máximo permitido se encuentran resaltados en rosado, para prestar especial atención a ellos y realizar las acciones necesarias para reducirlos.

4. FASE 4. PROPUESTAS DE PROYECTOS

4.1. Introducción

El principal objetivo de ésta fase consiste en proponer diversos proyectos para implementar las salvaguardas identificadas durante el análisis de riesgos realizado previamente y las acciones de mejora y/o documentación necesaria para alcanzar el nivel de cumplimiento requerido de los requisitos definidos en la norma ISO/IEC27001 y los controles propuestos por la ISO/IEC27002.

4.2. Propuestas

En la sección **Objetivos/ Controles/ Amenazas** se tendrá la siguiente clasificación:

Objetivos
Controles
Amenazas

Nota: Las amenazas incluyen una columna adicional para incluir el activo

4.2.1. Proyecto 1: Ajuste de políticas y normas de seguridad de la información existentes

Área Responsable	Área de seguridad de la información	
Áreas involucradas	Todas las áreas definidas en el alcance	
Tiempo de ejecución	2 meses	
Objetivos/ Controles/Amenazas		
N°	**Descripción**	**Activo**
1	TODOS LOS CONTROLES ASOCIADOS A LA NORMA ISO/IEC 27002	
1	Destrucción de información	Código fuente
2	Alteración de la información	Código fuente
Actividades		
N°	**Actividad**	**Responsable**
P1_1	Oficializar la creación del comité de seguridad de la información y definir claramente sus responsabilidades	Área de seguridad de la información
P1_2	Asignar oficialmente los activos de información identificados en la etapa de gestión de riesgos a los responsables que correspondan	Todas las áreas definidas en el alcance
P1_3	Incluir normas para fortalecer la política de uso de dispositivos móviles	Área de seguridad de la información
P1_4	Crear las políticas de seguridad necesarias para dar cumplimiento a los requisitos establecidos en la norma ISO/IEC27001 y los	Área de seguridad de la información

	controles de la norma ISO/IEC27002	
P1_5	Crear las políticas y normas necesarias para garantizar el desarrollo seguro de la aplicación	Área de seguridad de la información
P1_6	Fortalecer las políticas existentes mediante la creación y ajuste de normas	Área de seguridad de la información
P1_7	Incluir la evaluación de los indicadores propuestos en el presente proyecto	Área de seguridad de la información

Tabla 16: Proyecto 1. Ajuste a políticas

4.2.2. Proyecto 2: Creación y ajuste de procedimientos

Área Responsable	Área de procesos	
Áreas involucradas	Todas las áreas definidas en el alcance	
Tiempo de ejecución	3 meses	
Objetivos/ Controles/Amenazas		
N°	Descripción	
1	Revisar procedimientos a seguir como contingencia ante problemas presentados en procesos específicos	
2	Revisar procedimientos a seguir como contingencia ante la no disponibilidad de personal	
3	Validar y/o ajustar el procedimiento relacionado con la asignación y eliminación de personas por concepto de rotación o retiro de personal, el cual debe ser oportuno	
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	
A.6.1.3	Contacto con las autoridades	
A.6.1.4	Contacto con grupos de interés especial	
A.6.1.5	Seguridad de la información en la gestión de proyectos	
A.7.1.1	Investigación de antecedentes	
A.7.1.2	Términos y condiciones de contratación	
A.7.3.1	Cese o cambio de puesto de trabajo	
1	Denegación de servicio	
2	Indisponibilidad del personal	Administrador del CAAG, Personal de Tecnología, Desarrolladores
3	Encaminamiento de mensajes	Correos automáticos generados por SAAG (Producción)
Actividades		
N°	**Actividad**	**Responsable**
P2_1	Diseñar un procedimiento de mejora continua para las políticas de seguridad	Área de procesos
P2_2	Ajustar los procedimientos relacionados con la gestión de proyectos con el objetivo de involucrar las políticas y/o normas de seguridad que apliquen	Área de procesos
P2_3	Revisar y ajustar el procedimiento existente para socializar las políticas de seguridad de la información	Área de procesos
P2_4	Revisar y optimizar el procedimiento para la asignación y eliminación de privilegios a usuarios involucrando al	Área de procesos

	administrador de usuarios del aplicativo	
P2_5	Crear procedimiento encargado de revisar periódicamente las políticas de seguridad validando el cumplimiento de las mismas y realizando las acciones de mejora	Área de procesos
P2_6	Revisar el procedimiento existente para realizar auditorías internas y adaptarlo para que corresponda con los requisitos	Área de procesos
P2_7	Revisar el procedimiento existente para gestión de indicadores e incluir los indicadores que fueron propuestos	Área de procesos

Tabla 17: Proyecto 2. Ajuste a procedimientos

4.2.3. Proyecto 3: Actualización de la clasificación de información

Área Responsable	Área de Desarrollo, área de Seguridad de la información, área de Tecnología	
Áreas involucradas	Todas las áreas definidas en el alcance	
Tiempo de ejecución	3 semanas	
Objetivos/ Controles/Amenazas		
N°	Descripción	
A.8.1.1	Inventario de activos	
A.8.1.2	Propiedad de los activos	
A.8.2.1	Directrices de clasificación	
A.8.2.2	Etiquetado y manejo de información	
A.8.2.3	Manipulación de activos	
A.8.1.3	Uso aceptable de los activos	
Actividades		
N°	**Actividad**	**Responsable**
P3_1	Creación y/o actualización de diccionario de datos del aplicativo	Área de Desarrollo
P3_2	Clasificación de datos del aplicativo utilizando el diccionario de datos suministrado	Área de Seguridad de la información
P3_3	Implementar las medidas de protección necesarias para proteger la información más sensible	Área de Tecnología
P3_4	Incluir normas necesarias para garantizar el mantenimiento del proceso de clasificación de información	Área de seguridad de la información

Tabla 18: Proyecto 3. Clasificación de la información

4.2.4. Proyecto 4: Acciones de mejora de infraestructura

Área Responsable	Área de Tecnología
Áreas involucradas	Todas las áreas definidas en el alcance
Tiempo de ejecución	6 meses
Objetivos/ Controles/Amenazas	
N°	Descripción
1	Reducir la probabilidad de caída del sistema por agotamiento de recursos
2	Validar posibles causas de los fallos presentados y realizar los ajustes necesarios
A.12.10.1	Registro de auditorías
A.12.10.2	Monitoreo del uso del sistema

A.12.10.3	Protección de la información del registro	
A.12.10.4	Registros del administrador y del operador	
A.12.10.5	Registro de fallas	
1	Caída del sistema por agotamiento de recursos	Servidor de BD (Desarrollo, pruebas, producción), Servidor de aplicaciones(Desarrollo, pruebas, producción)
2	Fallos de servicios de comunicación	Servidor de BD (Desarrollo, pruebas, producción)
3	Errores de mantenimiento / actualización de programas (software)	Servidor de aplicaciones(Desarrollo, pruebas, producción)
4	Corte del suministro eléctrico	Equipos de computo de usuarios de SAAG
5	Avería de origen Físico o lógico	Equipo de computo (repositorio)
6	Fallos de servicios de comunicación	Equipo de computo (repositorio)

Actividades		
N°	**Actividad**	**Responsable**
P4_1	Definir contacto con los fabricantes de los sistemas operativos utilizados en los activos de información	Área de Tecnología
P4_2	Implementar un SIEM (Security Information and Event Management) que facilite la centralización y monitoreo basado en los logs o MONITOR	Área de Tecnología, Desarrollo
P4_3	Revisar informes generados por las herramientas de monitoreo para el aplicativo e informar al área de desarrollo para avanzar en su solución	Área de Tecnología
P4_4	Revisar y monitorear los servidores para buscar posibles casusas de la caída de servicios	Área de Tecnología
P4_5	Validar viabilidad para contar con planta de suministro de energía en el CAAG	Área de Tecnología
P4_6	Validar viabilidad, tiempo y recursos para la migración de servidor del aplicativo a uno que tenga soporte	Área de Tecnología y desarrollo
P4_7	Evaluar viabilidad, tiempo y recursos requeridos para asignación de servidor que sirva de repositorio y que sea custodiado por tecnología	Área de Tecnología

Tabla 19: Proyecto 4. Acciones de mejora de infraestructura

4.2.5. Proyecto 5: Optimización del aplicativo

Área Responsable	Área de Desarrollo, área de Tecnología
Áreas involucradas	Todas las áreas definidas en el alcance
Tiempo de ejecución	2 meses

Objetivos/ Controles/Amenazas	
N°	Descripción
1	Revisar los informes generados por tecnología relacionados con las herramientas de monitoreo del sistema e incidentes de seguridad

2	Definir planes de acción según las conclusiones de la actividad previa	
1	Caída del sistema por agotamiento de recursos	Servidor de ambientes
2	Errores de los usuarios	Código ejecutable (Desarrollo, pruebas, producción)
3	Introducción de información incorrecta	Base de Datos (Desarrollo, pruebas, producción)
4	Vulnerabilidades de los programas (software)	Logs
5	Encaminamiento de mensajes	Correos automáticos generados por SAAG (Producción)
6	Introducción de información incorrecta	Base de Datos (Desarrollo, pruebas, producción)
7	Fallos de servicios de comunicación	Archivos de salida por SAAG (Producción)
Actividades		
N°	**Actividad**	**Responsable**
P5_1	Teniendo en cuenta los informes de vulnerabilidades generados por tecnología definir los planes de acción y mejora	Área de Desarrollo
P5_2	Creación de procesos automáticos para eliminar archivos obsoletos generados	Área de Desarrollo
P5_3	Creación de malla de control-m para la realización automática de procedimientos realizados por operadores mediante la ejecución de bats.	Área de Desarrollo, pruebas
P5_4	Validar cuales son los casos más frecuentes de introducción de información errada para que se ajuste el aplicativo y se puedan reducir	Área de Desarrollo
P5_5	Generación e instalación de certificado SSL en el servidor de aplicaciones	Área de Tecnología
P5_6	Ajustar el aplicativo para el uso de protocolo seguro	Área de Desarrollo
P5_7	Validar la configuración de los correos existente y que esté de la mano con la rotación de personal	Área de procesos y Área de Desarrollo

Tabla 20: Proyecto 5. Optimización del aplicativo

4.2.6. Proyecto 6: Socialización de políticas de seguridad

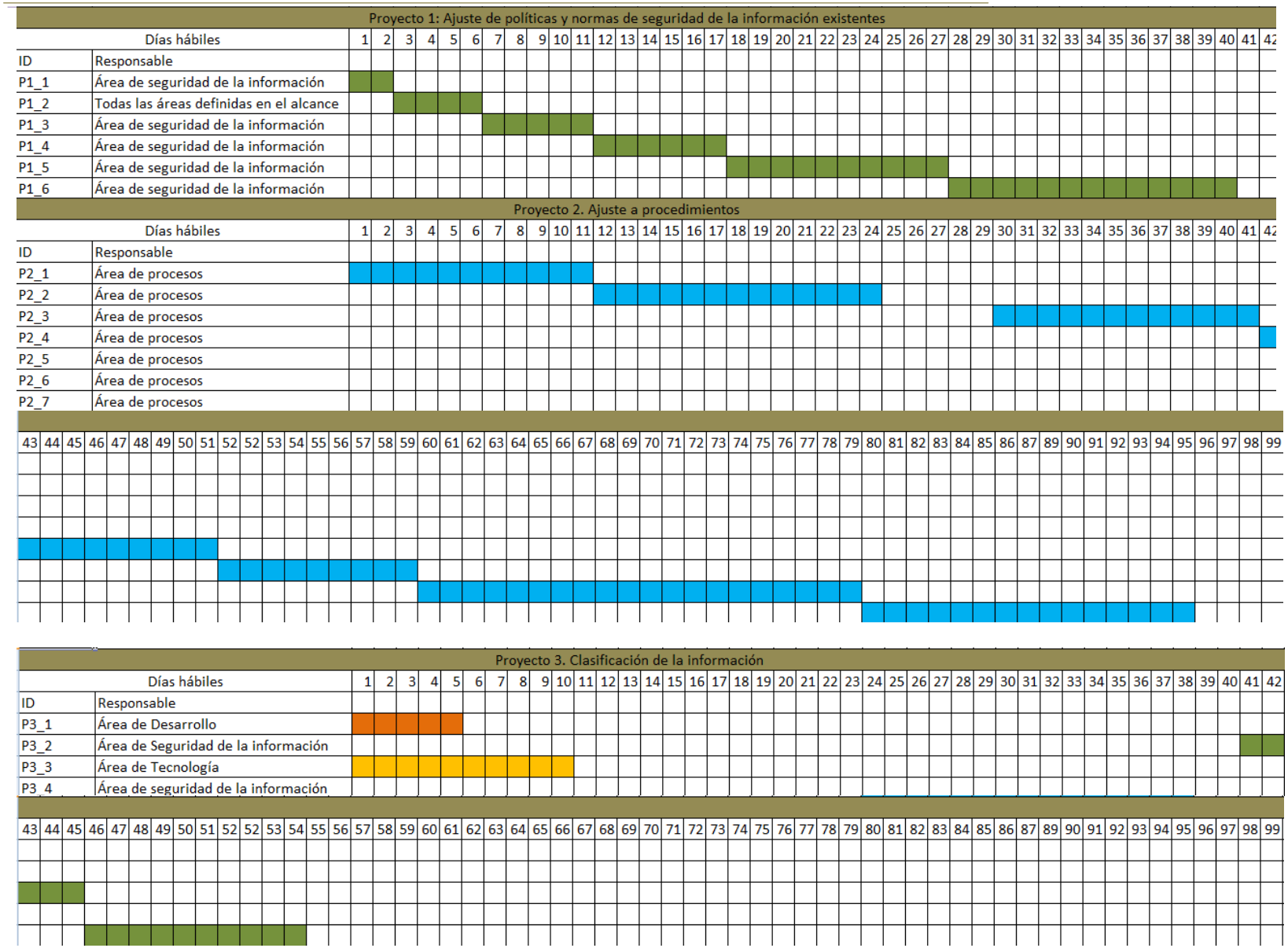
Área Responsable	Área de seguridad de la información	
Áreas involucradas	Todas las áreas definidas en el alcance	
Tiempo de ejecución	2 meses	
Objetivos/ Controles/Amenazas		
N°	Descripción	
1	Socializar las políticas y normas de seguridad existentes, entre el personal indicado en el alcance	
Actividades		
N°	**Actividad**	**Responsable**

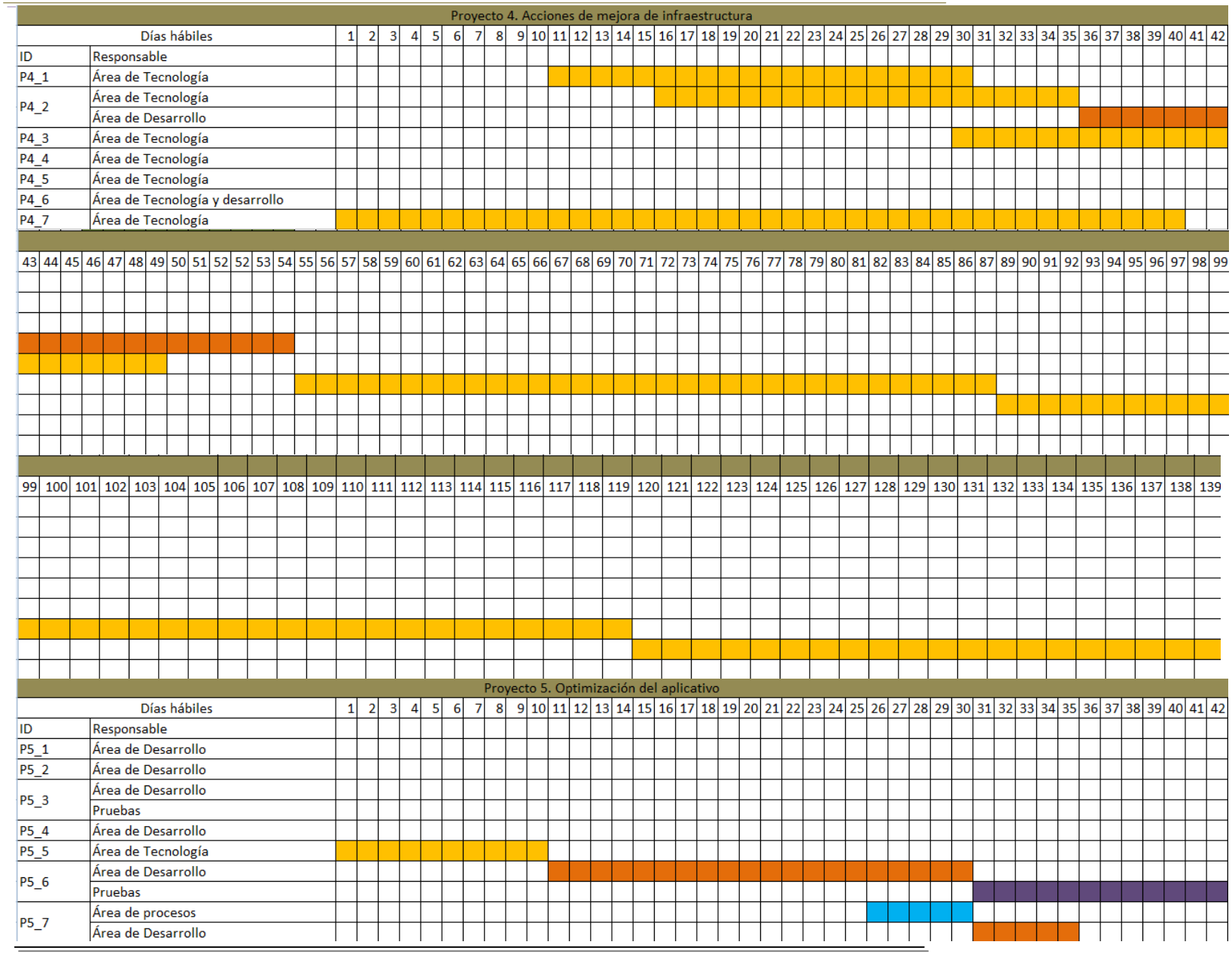
P6_1	Crear plan de comunicación efectiva	Área de seguridad de la información
P6_2	Desarrollarlo haciendo uso de los recursos necesarios (intranet, comunicados, etc.)	Área de seguridad de la información

Tabla 21: Proyecto 6: Socialización de políticas de seguridad

4.3. Resultados

A continuación se muestran los diagramas de GANTT correspondientes a cada uno de los proyectos propuestos con la proyección de tiempos que se ajusta según la disponibilidad del personal involucrado, se tienen en cuenta para la asignación de tiempos días hábiles para su estimación. **NOTA:** Se ha dado prioridad máxima para la asignación de recursos


Proyecto 1: Ajuste de políticas y normas de seguridad de la información existentes
Días hábiles
ID
Responsable
P1_1 Área de seguridad de la información
P1_2 Todas las áreas definidas en el alcance
P1_3 Área de seguridad de la información
P1_4 Área de seguridad de la información
P1_5 Área de seguridad de la información
P1_6 Área de seguridad de la información
Proyecto 2. Ajuste a procedimientos
Días hábiles
ID
Responsable
P2_1 Área de procesos
P2_2 Área de procesos
P2_3 Área de procesos
P2_4 Área de procesos
P2_5 Área de procesos
P2_6 Área de procesos
P2_7 Área de procesos
Proyecto 3. Clasificación de la información
Días hábiles
ID
Responsable
P3_1 Área de Desarrollo
P3_2 Área de Seguridad de la información
P3_3 Área de Tecnología
P3_4 Área de seguridad de la información


Proyecto 4. Acciones de mejora de infraestructura
Días hábiles
ID
Responsable
P4_1 Área de Tecnología
P4_2 Área de Tecnología
Área de Desarrollo
P4_3 Área de Tecnología
P4_4 Área de Tecnología
P4_5 Área de Tecnología
P4_6 Área de Tecnología y desarrollo
P4_7 Área de Tecnología
Proyecto 5. Optimización del aplicativo
Días hábiles
ID
Responsable
P5_1 Área de Desarrollo
P5_2 Área de Desarrollo
P5_3 Área de Desarrollo
Pruebas
P5_4 Área de Desarrollo
P5_5 Área de Tecnología
P5_6 Área de Desarrollo
Pruebas
P5_7 Área de procesos
Área de Desarrollo

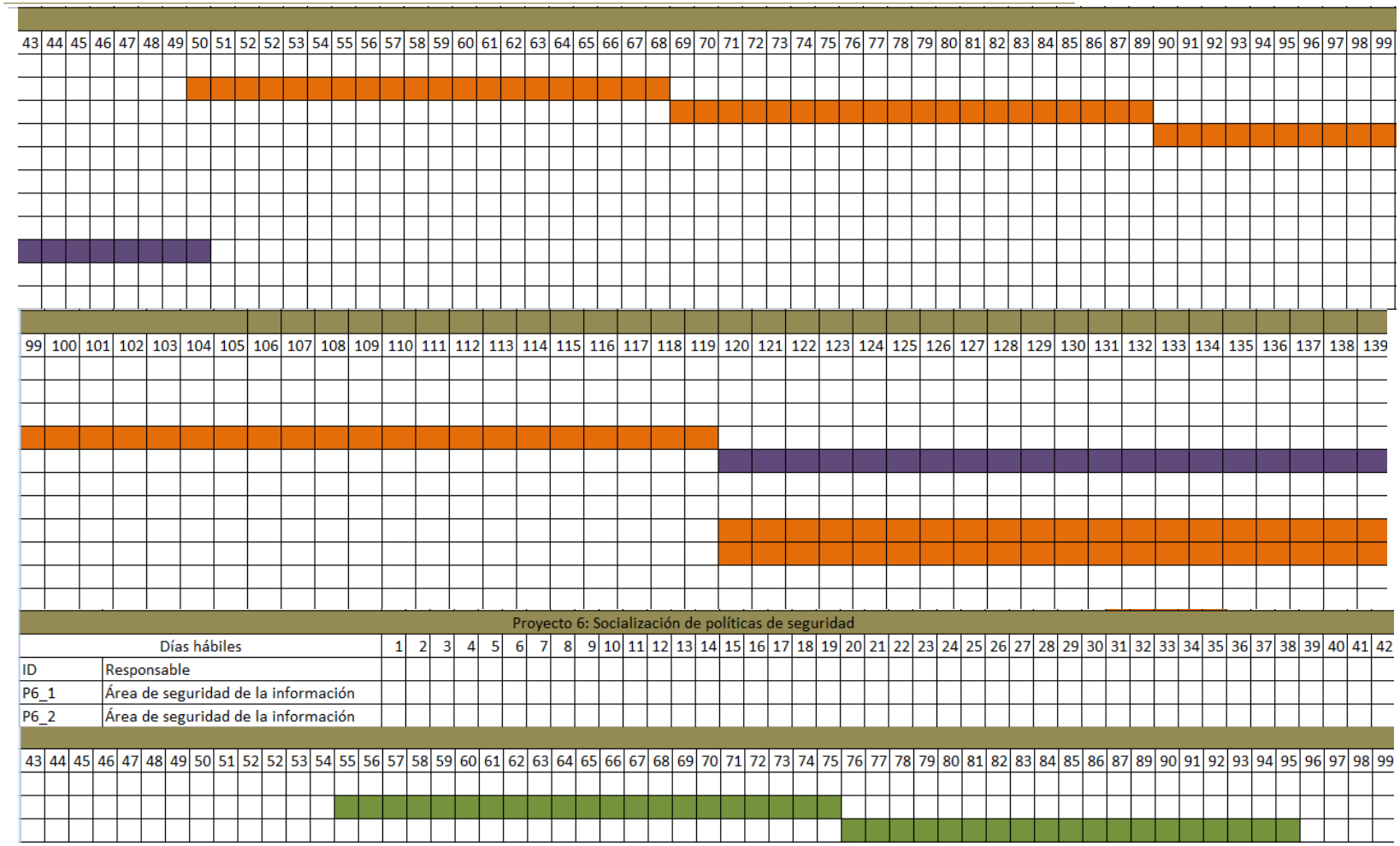


Figura 10: Cronograma proyectos

5. FASE 5. AUDITORÍA DE CUMPLIMIENTO

5.1. Introducción

La compañía que ha servido como caso de estudio ha sido evaluada previamente en función de sus activos de información y como resultado de ello se han identificado una serie de salvaguardas que podrán reducir la cantidad y el impacto de las amenazas identificadas. Esto ha servido de insumo a la fase anterior para proponer proyectos que puedan implementar dichas salvaguardas en la organización y a su vez, se han incluido otras propuestas para reducir las falencias de la compañía en otros aspectos, lo cual permite acercarnos más al cumplimiento de los requisitos definidos en la norma ISO/IEC 27001: 2013 y a las buenas prácticas incluidas en la norma ISO/IEC 27002:2013. Pues bien, en ésta fase el objetivo principal consiste precisamente en identificar el nivel de cumplimiento que hemos alcanzado a partir de los cambios generados por los proyectos propuestos, lo cual implica realizar una auditoría de cumplimiento. Al realizar la auditoría se utilizará la Declaración de aplicabilidad que incluye el listado de documentos que servirán como evidencia de la implantación de los controles, en caso de no tenerlos se dejará la respectiva indicación.

5.2. Metodología

Como se menciona previamente, en ésta fase identificaremos los niveles de cumplimiento y para ello será necesario:

PASO 1: Evaluar en cada control el grado de madurez alcanzado en cuanto a la implementación del SGSI (Sistema de Gestión de seguridad de la información) y asignar el porcentaje de

efectividad que corresponda de acuerdo a los niveles considerados en el modelo de madurez de la capacidad (CMM) que se indican a continuación:

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	L0	Inexistente	- Carencia completa de cualquier proceso reconocible. - No se ha reconocido siquiera que existe un problema a resolver.
10%	L1	Inicial /Ad-hoc	- Estado inicial donde el éxito de las actividades de los procesos - Se basa la mayoría de las veces en el esfuerzo personal. - Los procedimientos son inexistentes o localizados en áreas concretas. - No existen plantillas definidas a nivel corporativo.
50%	L2	Reproducible, pero intuitivo	- Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. - Se normalizan las buenas prácticas en base a la experiencia y al método. - No hay comunicación o entrenamiento formal, las responsabilidades que dan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	L3	Proceso definido	-La organización entera participa en el proceso. -Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	L4	Gestionado y medible	- Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. - Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	L5	Optimizado	- Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 22: Niveles de madurez CMM

PASO 2: Consolidar porcentaje de efectividad por cada dominio sacando un promedio en función de los controles incluidos.

5.3. Evaluación de la madurez

El desarrollo de los proyectos propuestos permite elevar los niveles de madurez de los controles alcanzados durante el análisis diferencial realizado al iniciar el proyecto y en ésta parte se verá el incremento de estos niveles en función de los resultados de los proyectos.

NOTA: Vamos a asumir que los proyectos se han ejecutado en su totalidad.

Dominio: Política de seguridad

Actualmente, existe una política que incluye las políticas y normas necesarias para dar cumplimiento a los controles definidos en la norma ISO/IEC 27002 en general, se ajusta a las necesidades del banco, cuenta con un proceso de mejora continua y se han involucrado los indicadores necesarios para su evaluación. Las responsabilidades de cada área se encuentran definidas por las normas incluidas en la política.

N	Descripción	Estado	%
A.5	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**	**L3**	**90%**
A 5.1	Orientación de la dirección para la gestión de la seguridad de la información		
A.5.1.1	Políticas para la seguridad de la información	L3	90%
A.5.1.2	Revisión de las políticas para la seguridad de la información	L3	90%

Tabla 23: Evaluación de la madurez |Política de seguridad

Dominio: Organización de la seguridad de la información.

Los activos de información han sido identificados claramente y a cada uno fue asignado uno o más responsables, cuenta con procedimiento para realizar contacto con autoridades pero falta incluir ajustes en relación al proceso existente para contactarse con entidades de interés especial. Adicional a esto fue incluida recientemente una política para asegurar que en los proyectos relacionados con el alcance del SGSI se involucren los temas de seguridad que correspondan.

N	Descripción	Estado	%
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**L2**	**85%**
A.6.1	Organización de la seguridad de la Información	L3	87%
A.6.1.1	Roles y responsabilidades para la seguridad de la información	L3	92%
A.6.1.2	Separación de deberes	L3	90%
A.6.1.3	Contacto con las autoridades	L3	90%
A.6.1.4	Contacto con grupos de interés especial	L2	70%
A.6.1.5	Seguridad de la información en la gestión de proyectos	L2	85%
A.6.2	Dispositivos móviles y teletrabajo	L3	90%
A 6.2.1	Política para dispositivos móviles	L3	90%
A 6.2.2	Teletrabajo	L3	90%

Tabla 24: Evaluación de la madurez |Organización de la seguridad de la información

Dominio: Seguridad en los recursos humanos

La compañía cuenta con claros procedimientos definidos y de conocimiento general al interior de la organización en relación al incumplimiento de políticas definidas y acciones a lugar en cada caso. A su vez se tiene un cuidadoso manejo en relación a la vinculación de los empleados, su contratación y su capacitación en cuanto a generalidades y al cumplimiento de las políticas y normas establecidas que correspondan.

N	Descripción	Estado	%
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**	**L3**	**91%**
A.7.1	Antes de la contratación	L4	95%
A.7.1.1	Investigación de antecedentes.	L4	95%
A.7.1.2	Términos y condiciones de contratación	L4	95%
A.7.2	Durante de la contratación	L3	90%
A.7.2.1	Responsabilidades de gestión	L3	90%
A.7.2.2	Concienciación, educación y capacitación en segur. de la información	L3	90%
A.7.2.3	Proceso disciplinario	L2	85%
A.7.3	Cese o cambio de puesto de trabajo	L3	90%
A.7.3.1	Cese o cambio de puesto de trabajo	L3	90%

Tabla 25: Evaluación de la madurez |Seguridad en los recursos humanos

Dominio: Gestión de activos

Cuenta con inventario de los activos en relación al alcance del SGSI, los cuales se encuentran clasificados, tienen asignado personal responsable y cuenta con restricciones de acceso físico y lógico. La clasificación y etiquetado de información ha sido realizado en uso de un proceso diseñado específicamente para esto. El trámite de asignación y devolución de activos corresponde a un proceso diseñado y documentado.

N	Descripción	Estado	%
A.8	**GESTIÓN DE ACTIVOS**	**L3**	**90%**
A.8.1	Responsabilidad sobre los activos	L3	90%
A.8.1.1	Inventario de activos	L3	90%
A.8.1.2	Propiedad de los activos	L3	90%
A.8.1.3	Uso aceptable de los activos	L3	90%
A.8.1.4	Devolución de activos	L3	90%
A.8.2	Clasificación de la información	L3	90%
A.8.2.1	Directrices de clasificación	L3	90%
A.8.2.2	Etiquetado y manejo de información	L3	90%
A.8.2.3	Manipulación de activos	L3	90%

Tabla 26: Evaluación de la madurez | Gestión de activos

Dominio: Control de acceso

Cuenta con política y las correspondientes normas para dar cumplimiento a los controles definidos en el dominio y adicional a esto el personal ha sido informado debidamente y capacitado para dar cumplimiento a éstas.

N	Descripción	Estado	%
A.9	**CONTROL DE ACCESO**	**L3**	**90%**
A.9.1	Requisitos de negocio para el control de accesos	L4	95%
A.9.1.1	Política de control de acceso	L4	95%
A.9.2	Gestión de acceso de usuario	L3	90%
A.9.2.1	Registro de usuarios	L3	90%
A.9.2.2	Gestión de privilegios	L3	90%
A.9.2.3	Gestión de contraseñas para usuario	L3	90%
A.9.2.4	Revisión de los derechos de acceso de los usuarios	L3	90%

A.9.3	Responsabilidades del usuario.	L3	90%
A.9.3.1	Uso de contraseñas	L3	90%
A.9.3.2	Equipo de usuario desatendido	L3	90%
A.9.3.3	Política de escritorio despejado y de pantalla despejada	L3	90%
A.9.4	Control de acceso a sistemas y aplicaciones	L3	90%
A.9.4.1	Política de uso de los servicios de red	L3	90%
A.9.4.2	Autenticación de usuarios para conexiones externas	L3	90%
A.9.4.3	Identificación de los equipos en las redes	L3	90%
A.9.4.4	Protección de los puertos de configuración y diagnóstico remoto	L3	90%
A.9.4.5	Separación en las redes	L3	90%
A.9.4.6	Control de conexión a las redes	L3	90%
A.9.4.7	Control de enrutamiento en la red	L3	90%
A.9.5.1	Procedimientos de ingreso seguro	L3	90%
A.9.5.2	Identificación y autenticación de usuarios	L3	90%
A.9.5.3	Sistema de gestión de contraseñas	L3	90%
A.9.5.4	Uso de las utilidades del sistema	L3	90%
A.9.5.5	Tiempo de inactividad de la sesión	L3	90%
A.9.5.6	Limitación del tiempo de conexión	L3	90%
A.9.6.1	Restricción de acceso a la información	L3	90%
A.9.6.2	Aislamiento de sistemas sensibles	L3	90%
A.9.7.1	Computación y comunicaciones móviles	L3	90%
A.9.7.2	Trabajo remoto	L3	90%
A.10	**CIFRADO**	L3	**90%**
A.10.1	Controles criptográficos.	L3	90%
A.10.1.1	Política de uso de los controles criptográficos	L3	90%
A.10.1.2	Gestión de claves	L3	90%
A.13	**SEGURIDAD EN LAS TELECOMUNICACIONES**	L3	90%
A.13.1	Gestión de la seguridad en las redes	L3	90%
A.13.1.1	Controles de red	L3	90%
A.13.1.2	Mecanismos de seguridad asociados a servicios en red	L3	90%
A.13.1.3	Segregación de redes	L3	90%
A.13.2	Intercambio de información con partes externas	L3	90%
A.13.2.1	Políticas y procedimientos de intercambio de información	L3	90%
A.13.2.2	Acuerdos de intercambio	L3	90%
A.13.2.3	Mensajería electrónica	L3	90%
A.13.2.4	Acuerdos de confidencialidad y secreto	L3	90%

Tabla 27: Evaluación de la madurez | Control de acceso

Dominio: Seguridad física y ambiental

En general, la compañía cuenta con protocolos de acceso a las instalaciones acordes con la necesidad de protección de activos de información. Como resultado de los proyectos recientemente ejecutados se tiene documentación al día y cuenta con procesos actualizados y documentados al respecto. De igual manera, cuenta con procesos diseñados cuidadosamente para la instalación y mantenimiento de equipos e instalaciones tecnológicas y de suministro.

N	Descripción	Estado	%
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL**	**L3**	**90%**
A.11.1	Requisitos de negocio para el control de acceso	L3	90%
A.11.1.1	Perímetro de seguridad física	L3	90%
A.11.1.2	Controles de acceso físico	L3	92%
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	L3	93%
A.11.1.4	Protección contra amenazas externas y ambientales	L3	90%
A.11.1.5	Trabajo en áreas seguras	L3	90%
A.11.1.6	Áreas de carga, despacho y acceso público	L3	90%
A.11.2	Seguridad de los equipos	L3	90%
A.11.2.1	Emplazamiento y protección de equipos	L3	90%
A.11.2.2	Instalaciones de suministro	L3	92%
A.11.2.3	Seguridad del cableado	L3	93%
A.11.2.4	Mantenimiento de los equipos	L3	90%
A.11.2.5	Salida de activos fuera de las dependencias de la empresa	L3	90%
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	L3	90%
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	L3	90%
A.11.2.8	Equipo informático de usuario desatendido	L3	90%
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	L4	95%

Tabla 28: Evaluación de la madurez | Seguridad física y ambiental

Dominio: Gestión de comunicaciones y operaciones

En general cuenta con las políticas y normas necesarias para cumplimiento a los controles relacionados con el dominio. A nivel de infraestructura cuenta con:

Ambientes segregados (Desarrollo, pruebas y producción)

Ante posible corte del servicio de internet se tiene contrato del servicio con 2 líneas de compañía distinta

Las instalaciones con servicios críticos cuentan con un SAI (Sistema de alimentación ininterrumpida) en general se utiliza SAI UPS Line Interactive, pero para los dispositivos más críticos cuentan un SAI de tipo UPS On – Line

Se tienen herramientas para monitoreo de red, base de datos, etc.

El aplicativo para Web Service se encuentra instalado en servidor balanceado

Los servidores se encuentran instalados y ubicados en cumplimiento de las normas

Se realizan backups de la información según indicaciones de procedimiento relacionado

Dependiendo del cargo que tenga el usuario de un equipo tendrá limitaciones de acceso a páginas de internet y bloqueo de puertos USB

Todos equipo de la compañía cuenta con su respectivo antivirus de versión actualizada

La distribución de red asociada al aplicativo cuenta con firewall

Los relojes de los equipos de la compañía se encuentran sincronizados

N	Descripción	Estado	
A.12	**GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES**	**L3**	**90%**
A.12.1	Responsabilidades y procedimientos de operación	L3	90%
A.12.1.1	Documentación de los procedimientos de operación	L3	90%
A.12.1.2	Gestión del cambio	L3	90%
A.12.1.3	Gestión de capacidades	L3	90%
A.12.1.4	Separación de entornos de desarrollo, prueba y producción	L3	92%
A.12.2	Protección contra código malicioso	L3	90%
A.12.2.1	Controles contra el código malicioso	L3	90%
A.12.2.2	Monitoreo y revisión de los servicios por terceras partes	L3	90%
A.12.3	Copias de seguridad.	L3	90%
A.12.3.1	Respaldo de la información	L2	80%
A.12.4	Registro de actividad y supervisión	L3	90%
A.12.4.1	Registro y gestión de eventos de actividad	L3	90%
A.12.4.2	Protección de los registros de información	L3	90%
A.12.4.3	Registros de actividad del operador y administrador del sistema	L3	90%
A.12.4.4	Sincronización de relojes	L3	90%

A.12.5	Control de software en explotación	L3	90%
A.12.5.1	Instalación del software en sistemas en producción	L3	90%
A.12.6	Gestión de la vulnerabilidad técnica	L3	90%
A.12.6.1	Gestión de las vulnerabilidades técnicas	L3	90%
A.12.6.2	Restricciones en la instalación de software	L3	90%
A.12.7	Consideraciones de las auditorías de los sistemas de información.	L3	90%
A.12.7.1	Controles de auditoría de los sistemas de información.	L3	90%

Tabla 29: Evaluación de la madurez | Gestión de comunicaciones y operaciones

Dominio: Adquisición, desarrollo y mantenimiento de Sistemas de Información

En general cuenta con las políticas y normas necesarias para cumplimiento a los controles relacionados con el dominio. Es necesario considerar una segunda fase para el proyecto 2: Ajuste a procedimientos, dado que el enfoque que se ha dado a los procedimientos no corresponde 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.

N	Descripción	Estado	%
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**	**L3**	**90%**
A.14.1	Requisitos de seguridad de los sistemas de información	L3	90%
A.14.1.1	Análisis y especificación de los requisitos de seguridad	L2	80%
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	L3	90%
A.14.1.3	Protección de las transacciones por redes telemáticas	L3	90%
A.14.2	Seguridad en los procesos de desarrollo y soporte	L3	90%
A.14.2.1	Política de desarrollo seguro de software	L3	90%
A.14.2.2	Procedimientos de control de cambios en los sistemas	L3	90%
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L3	90%
A.14.2.4	Restricciones a los cambios en los paquetes de software	L3	90%
A.14.2.5	Uso de principios de ingeniería en protección de sistemas	L3	90%
A.14.2.6	Seguridad en entornos de desarrollo	L3	90%
A.14.2.7	Externalización del desarrollo de software	L3	90%
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	L3	90%
A.14.2.9	Pruebas de aceptación.	L3	90%

A.14.3	Datos de prueba	L3	90%
A.14.3.1	Protección de los datos utilizados en pruebas	L3	90%
A.15	**RELACIONES CON SUMINISTRADORES**		
A.15.1	Seguridad de la información en las relaciones con suministradores.		
A.15.1.1	Política de seguridad de la información para suministradores	N/A	
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	N/A	
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	N/A	
A.15.2	Gestión de la prestación del servicio por suministradores		
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros	N/A	
A.15.2.2	Gestión de cambios en los servicios prestados por terceros	N/A	

Tabla 30: Evaluación de la madurez | Adquisición, desarrollo y mantenimiento de Sistemas de Información

Dominio: Gestión de incidentes

En general la compañía cuenta con herramientas para registro y reporte de incidentes presentados, dependiendo de la criticidad se debe dar solución en límite de tiempo definido o esperar a un ajuste por requerimiento que involucre la solicitud completa para su desarrollo. Esto para incidentes en general, pero los incidentes de seguridad son manejados de forma diferente, son reportados en general por personal de tecnología que se encarga de monitorear los sistemas por correo electrónico certificado, la asignación y respuesta también se realiza por éste medio. La compañía cuenta con procesos específicos asociados a éstas actividades.

También se involucran indicadores de gestión y tiempos de respuesta.

N	Descripción	Estado	%
A.16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**	**L3**	**91%**
A.16.1	Gestión de incidentes de seguridad de la información y mejoras	L3	91%
A.16.1.1	Responsabilidades y procedimientos	L3	90%
A.16.1.2	Notificación de los eventos de seguridad de la información	L4	95%
A.16.1.3	Notificación de puntos débiles de la seguridad	L3	90%
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	L3	90%

A.16.1.5	Respuesta a los incidentes de seguridad	L3	90%
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	L3	90%
A.16.1.7	Recopilación de evidencias	L3	90%

Tabla 31: Evaluación de la madurez | Gestión de incidentes

Dominio: Gestión de continuidad de negocio

El banco cuenta con un Plan de continuidad del negocio (BCP - Business Continuity Plan), se encuentra implementado desde hace más de 5 años, se realizan simulacros para validar su eficacia. En relación con la seguridad de la información se realizaron ajustes hace poco para involucrar continuidad de negocio en relación con aspectos de seguridad pero no se tiene una cobertura de 100% para ellos.

N	Descripción	Estado	%
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**	**L3**	**88%**
A.17.1	Continuidad de la seguridad de la información	L3	86%
A.17.1.1	Inclusión de la seguridad de la inf. En el proceso de gestión de la continuidad del negocio	L3	90%
A.17.1.2	Continuidad del negocio y evaluación de riesgos	L3	90%
A.17.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la inf.	L3	90%
A.17.1.4	Estructura para la planificación de la continuidad del negocio	L2	80%
A.17.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	L2	80%
A.17.2	Redundancias	L3	90%
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	L3	90%

Tabla 32: Evaluación de la madurez | Gestión de continuidad de negocio

Dominio: Cumplimiento

N	Descripción	Estado	%
A.18	**CUMPLIMIENTO**	**L3**	**90%**
A.18.1	Cumplimiento de los requisitos legales y contractuales	L3	90%
A.18.1.1	Identificación de legislación aplicable	L3	93%
A.18.1.2	Derechos de propiedad intelectual (DPI)	L3	92%
A.18.1.3	Protección de los registros de la organización	L3	92%
A.18.1.4	Protección de los datos y privacidad de la información personal	L3	92%

A.18.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	L3	90%
A.18.1.6	Regulación de los controles criptográficos.	L2	80%
A.18.2	Revisiones de la seguridad de la información	L3	90%
A.18.2.1	Revisión independiente de la seguridad de la información	L3	90%
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	L3	90%
A.18.2.3	Comprobación del cumplimiento	L3	90%

Tabla 33: Evaluación de la madurez | Cumplimiento

5.4. Presentación de resultados

Anexo 5: Informe Auditoría Interna

5.5. Resultados

En el siguiente gráfico se observa una evolución considerable de la implementación de los controles que hacen parte de la norma ISO/IEC27002

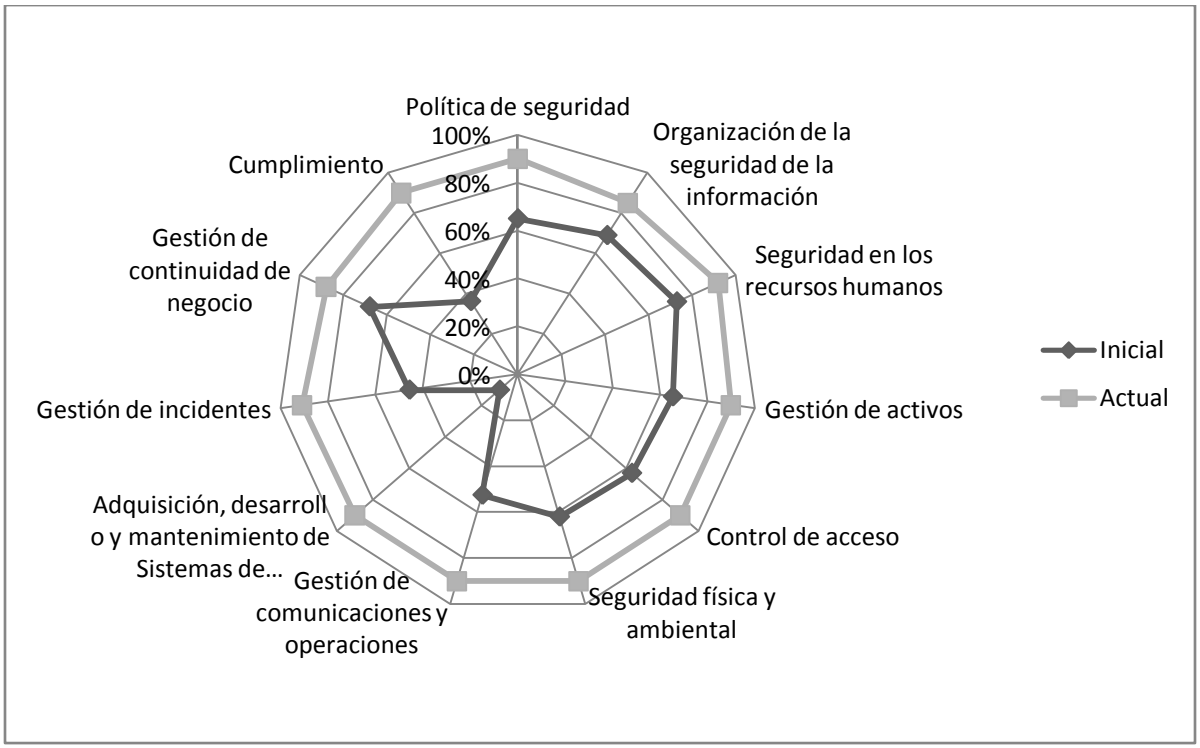


Figura 11: Comparación de dominios para evaluación de madurez inicial y actual

6. FASE 6. PRESENTACIÓN DE RESULTADOS Y ENTREGA DE INFORME

6.1. Introducción

Ésta última fase corresponde a la consolidación de resultados y conclusiones obtenidas a lo largo del proyecto, así como su presentación. Por supuesto, habrá lugar a las recomendaciones necesarias para continuar mejorando el SGSI generado.

6.2. Objetivos de la fase

Realizar una consolidación de los resultados, conclusiones y recomendaciones obtenidas

Generar los entregables necesarios como resultado del proyecto

Realizar una presentación oficial de los resultados obtenidos durante el proyecto que involucre su correspondiente análisis

6.3. Entregables

6.3.1. Resumen ejecutivo

El presente proyecto ha sido realizado con el objetivo de crear un Plan de implementación de la ISO/IEC 27001:2013, el proceso de creación se llevó a cabo en 5 fases principales y se han ido realizando entregas parciales que corresponden a cada una de ellas. En la primera fase 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. En la segunda etapa se recopilan política, procedimientos y documentos existentes, así como documentos creados para dar cumplimiento a requisitos establecidos como punto de partida. La tercera 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. 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. 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. 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.

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, normas y por supuesto realizar propuestas mucho más acertadas
- 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

6.3.2. Memoria de Proyecto

Revisar documento adjunto TFM_MISTIC_Memoria

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

ANEXO 1: POLÍTICA DE SEGURIDAD

A. 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. [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 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. [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]

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

B. 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, hallazgos y observaciones	Representante de la junta directiva, Auditor Líder	Consolidación de no conformidades, hallazgos y observaciones en la auditoría	Lista de asistencia

	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 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)	Funcionarios
¿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/IEC 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/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.)

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: 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.	Personal responsable según el alcance definido	Información recibida
3	CONSOLIDAR Y ANALIZAR INFORMACIÓN Teniendo en cuenta el resultado de la información recopilada en la actividad anterior, se debe verificar dicha información para	Representante de la Junta Directiva	Formato Informe de revisión por la Junta Directiva al SGSI FRJD01

	garantizar la confiabilidad.		
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: 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		Las áreas de desarrollo y	OM

	una bitácora de incidentes para el aplicativo		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	
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 vanguardia en temas de seguridad para actuar de forma preventiva	NC
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			