ESTABLECIMIENTO, E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013

TRABAJO DE FIN DE MÁSTER

RENÁN QUEVEDO GÓMEZ

UNIVERSIDAD ABIERTA DE CATALUÑA - UOC

MASTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

2015

TABLA DE CONTENIDO

1 INTRODUCCIÓN 6

2 DEFINICIÓN DE TÉRMINOS 6

3 ENFOQUE Y SELECCIÓN DE LA EMPRESA OBJETO DE ESTUDIO 7

3.1 DESCRIPCIÓN DE LA EMPRESA 7
3.2 ORGANIGRAMA 8
3.3 MAPA DE PROCESOS 9
3.4 ALCANCE DEL SGSI 9
3.5 PARTES INTERESADAS 10
3.6 SISTEMAS DE INFORMACIÓN 10
3.7 TOPOLOGÍA DE RED 10
3.8 REQUERIMIENTOS LEGALES 11

4 OBJETIVOS DEL PLAN DIRECTOR DE SEGURIDAD 11

5 ANÁLISIS DIFERENCIAL CON RESPECTO A ISO/IEC 27001 E ISO/IEC 27002. 12

5.1 NIVELES DE MADUREZ 12
5.2 METODOLOGÍA 13
5.3 RESULTADOS 13

6 SISTEMA DE GESTIÓN DOCUMENTAL 26

6.1 OBJETIVOS DEL SGSI 26
6.2 ALCANCE DEL SGSI 26
6.3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 26
6.4 PROCEDIMIENTO DE AUDITORÍAS INTERNAS 26
6.4.1 Requisitos de los Auditores Internos. 26
6.4.2 Actividades del Procedimiento. 27
6.4.3 Formatos Para la Ejecución de Auditorías Internas 27
6.5 GESTIÓN DE INDICADORES 28
6.5.1 Auditorías Realizadas al SGSI 28
6.5.2 Efectividad de las Acciones Correctivas 28
6.5.3 Gestión de Hallazgos de Auditorías 28
6.5.4 Impartición de Charlas de Concienciación 29
6.5.5 Resultados de las Tomas de Conciencia. 29
6.5.6 Incidentes Atendidos 30
6.5.7 Lecciones Aprendidas 30
6.5.8 Ejecución de Planes de Tratamiento 30
6.6 PROCEDIMIENTO REVISIÓN POR LA DIRECCIÓN 31
6.7 GESTIÓN DE ROLES Y RESPONSABILIDADES 31
6.7.1 Alta Dirección. 31
6.7.2 Director de Tecnología. 31
6.7.3 Oficial de Seguridad de la Información. 32
6.7.4 Comité de Seguridad de la Información 32
6.7.5 Coordinador de Sistemas 32
6.7.6 Ingeniero de Soporte 32
6.7.7 Ingeniero de Mantenimiento 32
6.8 METODOLOGÍA DE ANÁLISIS DE RIESGO 32
6.8.1 Inventario de Activos 32
6.8.2 Interdependencia Entre Activos 34
6.8.3 Valoración de Activos 34
6.8.4 Cálculo de Riesgos 35

6.9 DECLARACIÓN DE APLICABILIDAD 39
7 ANÁLISIS DE RIESGOS 57
7.1 INVENTARIO DE ACTIVOS 57
7.2 VALORACIÓN DE LOS ACTIVOS SUPERIORES 60
7.3 INTERDEPENDENCIA DE LOS ACTIVOS 60
7.4 RESUMEN DE VALORACIÓN 62
7.5 RIESGO INHERENTE 64
8 PROPUESTAS DE PROYECTOS 69
8.1 DESCRIPCIÓN DE LOS PROYECTOS PROPUESTOS 70
8.1.1 Creación de un área de Seguridad de la Información 70
8.1.2 Implementación de un GRC 71
8.1.3 Puesta en Producción de Políticas 72
8.1.4 Capacitación y Concienciación 73
8.1.5 Modificación del Proceso de Gestión Humana 74
8.1.6 Clasificación de la Información 75
8.1.7 Creación de un Ambiente de Pruebas y Desarrollo 76
8.1.8 Gestión de Vulnerabilidades Informáticas 77
8.1.9 Gestión de Incidentes de Seguridad de la Información 78
8.2 RIESGO RESIDUAL. 79
9 AUDITORIA DE CUMPLIMIENTO 80
9.1 DESCRIPCIÓN DE LA AUDITORÍA 80
9.2 ANÁLISIS DEL NIVEL DE MADURÉZ DE LOS CONTROLES 81
9.3 RESULTADOS DE LA AUDITORÍA 93
9.3.1 Diagrama de Radar 93
9.3.2 Hallazgos de Auditoría 93
10 CONCLUSIONES 94
11 BIBLIOGRAFÍA 95
12 ANEXOS 95
ANEXO 1 – POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA ABC S.A 96
1. OBJETIVO 96
2. ALCANCE 96
3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN 96
4. REVISIÓN 96
5. DIVULGACIÓN 96
6. POLÍTICAS DE ALTO NIVEL 96
7. POLÍTICA DE USO DE INTERNET Y CORREO ELECTRÓNICO 97
8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN TELETRABAJO 97
9. POLÍTICA DE USO ACEPTABLE DE ACTIVOS 97
10. POLÍTICA DE CONTROL DE ACCESO 97
ANEXO 2 – FORMATO PARA EL PLAN DE AUDITORÍA INTERNA 98
ANEXO 3 – FORMATO PARA EL INFORME DE AUDITORÍA INTERNA 99

1 INTRODUCCIÓN 100

1.1 OBJETO DE LA AUDITORÍA 100
1.2 ALCANCE DE LA AUDITORÍA 100
1.3 FECHA DE LA AUDITORÍA 100
1.4 LUGAR 100
1.5 ÁREAS AUDITADAS 100
1.6 EQUIPO AUDITOR 100
1.7 PERSONAL AUDITADO 100

2 HALLAZGOS DE AUDITORÍA 100

3 CONCLUSIONES 100

ANEXO 4 – FORMATO PARA EL INFORME DE ENTRADA 101

ANEXO 5 – FORMATO PARA EL INFORME DE SALIDA 104

ANEXO 6 – RIESGO INHERENTE 107

ANEXO 7 – DETALLE DE LA PROPUESTA DE PROYECTOS 108

ANEXO 8 – PLAN DE AUDITORÍA INTERNA 109

ANEXO 9 – INFORME DE AUDITORÍA 110

ÍNDICE DE ILUSTRACIONES

Ilustración 1 Organigrama de ABC S.A. 8
Ilustración 2 Mapa de Procesos de ABC S.A. 9
Ilustración 3 Proceso de Gestión de Servicios de Call Center 9
Ilustración 4 Topología de Red 11
Ilustración 5 Nivel de Madurez de los Controles del Anexo A ISO 27001:2013 25
Ilustración 6 Actividades del Inventario de Activos 33
Ilustración 7 Actividades Para Calcular el Riesgo 35
Ilustración 8 Proyectos Propuestos 69
Ilustración 9 Línea de Tiempo Proyectos 70
Ilustración 10 Imágen del Diagrama de Gantt del Proyecto 70
Ilustración 11 Evolución Luego de Establecer un Area de SI 71
Ilustración 12 Evolución con la Implementación de un GRC 72
Ilustración 13 Evolución Luego de la Implementación del SGSI 73
Ilustración 14 Evolución Luego de Concienciación y Capacitación 74
Ilustración 15 Evolución Luego de Modificación Proceso Gestión Humana 75
Ilustración 16 Evolución Luego de Clasificar la Información 76
Ilustración 17 Evolución Luego de Implementar Ambientes Separados 77
Ilustración 18 Evolución Luego de Implementar Gestión de Vulnerabilidades 78
Ilustración 19 Evolución Luego de Implementar la Gestión de Incidentes 79
Ilustración 20 Nivel de Madurez De los Controles - Auditoria Interna 93
Ilustración 21 Hallazgos de Auditoría – Resúmen 94

ÍNDICE DE TABLAS

Tabla 1 Análisis Diferencial con Respecto a la norma ISO 27001:2013 24
Tabla 2 Resumen del Nivel de Madurez de Cada Grupo de Controles 25

Tabla 3 Ejemplo de Tabla de Inventario de Activos 33
Tabla 4 Ejemplo Tabla de Interdependencias 34
Tabla 5 Valoración de las Dimensiones de Seguridad 35
Tabla 6 Ejemplo Valoración Activos Superiores 35
Tabla 7 Ejemplo Tabla Valoración de Activos 35
Tabla 8 Amenazas Propuestas por Magerit 37
Tabla 9 Valores de Probabilidad de Ocurrencia 37
Tabla 10 Valores Posibles Para el Impacto 38
Tabla 11 Tabla Para el Cálculo del Riesgo 38
Tabla 12 Fragmento de la Matriz Final del Análisis de Riesgo - Ejemplo 39
Tabla 13 Declaración de Aplicabilidad 57
Tabla 14 Inventario de Activos 59
Tabla 15 Activos Superiores de ABC S.A 60
Tabla 16 Dependencia de los Activos 62
Tabla 17 Resumen de Valoración 64
Tabla 18 Valor de los Riesgos más Altos Para Cada Activo 66
Tabla 19 Riesgos No Aceptables 68
Tabla 20 Amenazas que Generan Riesgos no Aceptables 69
Tabla 21 Creación de un Area de SI 71
Tabla 22 Cronograma Implementación de un GRC 72
Tabla 23 Cronograma Puesta en Producción de Políticas 73
Tabla 24 Cronograma Capacitación y Concienciación 74
Tabla 25 Cronograma Modificación Proceso Gestión Humana 75
Tabla 26 Cronograma Clasificación de la Información 76
Tabla 27 Cronograma Implementación Ambiente de Desarrollo 76
Tabla 28 Cronograma Gestión de Vulnerabilidades 77
Tabla 29 Cronograma Gestión de Incidentes 78
Tabla 30 Riesgo Residual Luego del Plan de Tratamiento de Riesgos 80
Tabla 31 Detalle de Resultados de Auditoría 93

1 INTRODUCCIÓN

Este documento, constituye la memoria técnica correspondiente al Trabajo de Fin del Máster Interuniversitario de las Tecnologías de Información y Comunicaciones (MISTIC) de la UOC.

El Trabajo de Fin de Master (TFM) consistió en la "Elaboración de un Plan de Implementación de la norma ISO 27001 en su versión 2013" para una empresa real cuyo nombre, sin embargo se omite por efectos de confidencialidad. En este orden de ideas, durante todo el documento la empresa será nombrada como **ABC S.A.**

2 DEFINICIÓN DE TÉRMINOS

Acción Correctiva: Acción para eliminar la causa de una no conformidad y prevenir la recurrencia.

Análisis de Brecha: Análisis del estado actual de cumplimiento que tiene una organización con respecto a un estándar definido, por ejemplo la norma ISO 27001:2013. Para el caso particular de un análisis de brecha sobre la norma ISO 2701:2013 se evalúa el estado de cumplimiento de 7 cláusulas de la norma así como los 114 controles especificados en su anexo A. También es conocido como análisis diferencial o "Gap Analysis".

Auditoría: Proceso independiente, documentado y sistemático para obtener evidencia de auditoría y evaluarla objetivamente para determinar el grado en el que un criterio de auditoría es cumplido.

Ataque: Intento de destruir, exponer, deshabilitar, alterar, o lograr acceso no autorizado o de hacer un uso no autorizado de un activo.

Control de Acceso: Medios para asegurar que el acceso a los activos es autorizado y restringido de acuerdo a los requerimientos del negocio y de la seguridad.

Confidencialidad: Propiedad de la información de que no sea revelada y se haga disponible a individuos, entidades o procesos no autorizados.

Competencia: Habilidad para aplicar conocimiento y aptitudes para conseguir un resultados establecidos.

Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de ser accesible y utilizable bajo demanda por una entidad autorizada.

Información: Conjunto de datos que tienen sentido, y que son considerados un activo más dentro de las organizaciones.

Información Documentada: Información que requiere ser controlada y mantenida por una organización y el medio en el cual está contenida.

Integridad: Propiedad de exactitud y completitud.

Mejora Continua: Actividad recurrente para mejorar el desempeño.

Norma ISO 27001:2013: Es la versión del año 2013 de la norma ISO 27001 que "proporciona los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información."

Norma ISO 27002:2013: Es la versión del año 2013 de la norma ISO 27002 que "está diseñada para que las organizaciones la usen como un marco de referencia para seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de la Seguridad de la Información".

Partes Interesadas: Personas u organizaciones que pueden ser, son, o consideran ellas mismas que son afectadas por una decisión o actividad.

Seguridad de la Información: La Seguridad de la Información incluye tres dimensiones principales: Confidencialidad, Disponibilidad e Integridad. La Seguridad de la información involucra la aplicación y gestión de las medidas apropiadas de seguridad que tengan en cuenta un amplio rango de amenazas. La seguridad de la información es alcanzada por medio de la implementación de un conjunto aplicable de controles, seleccionados por medio de un proceso de gestión de riesgos y gestionados usando un Sistema de Gestión de Seguridad de la Información, incluyendo políticas, procesos, procedimientos, estructuras organizacionales, software o hardware para proteger los activos de información identificados.

Sistema de Gestión: Conjunto de elementos que interactúan y se interrelacionan para establecer políticas y objetivos y los procesos para alcanzar dichos objetivos.

Triagge: Actividad dentro del procedimiento de respuesta a incidentes en la cual se analiza el evento para detectar si es o no un incidente de seguridad, adicionalmente si el evento efectivamente es un incidente, este se clasifica de acuerdo a su criticidad con el fin de tomar las decisiones correspondientes para su adecuado tratamiento.

Vulnerabilidad: Debilidad en un activo o control que puede ser explotada por una o más amenazas.

3 ENFOQUE Y SELECCIÓN DE LA EMPRESA OBJETO DE ESTUDIO

3.1 Descripción de la Empresa

ABC S.A. Es una empresa Española dedicada a la prestación de servicios de tecnología que se ha enfocado en 3 líneas de negocio diferentes:

- Factoría de Software.
- Gestión de procesos de negocio.
- Servicios de "Call Center".

ABC S.A. fue fundada en España en el año 2005 y ha cubierto desde entonces clientes del sector bancario, telecomunicaciones y gobierno, principalmente vendiéndoles su servicio de "Call Center".

Las otras dos líneas de negocio, Factoría de software y Gestión de Procesos de Negocio, también han generado negocios pero en una menor medida.

En el año 2012 **ABC S.A.** expandió su operación e inauguró una sede en Bogotá Colombia, enfocada en la oferta de los servicios de "Call Center" y Gestión de procesos de negocios, desde entonces ha captado importantes clientes en el sector gobierno y bancario.

ABC S.A. Colombia, a la fecha cuenta con 3 grandes clientes del sector bancario los cuales han firmado un contrato por 5 años para la prestación del servicio de Atención al Cliente. Por medio de este servicio el Call Center de **ABC S.A Colombia** pone toda la infraestructura física y tecnológica y el personal necesario para recibir las peticiones, quejas y reclamos de los clientes de cada banco.

Dentro de su estrategia corporativa **ABC S.A. Colombia**, pretende ampliar la cobertura de clientes del sector bancario en un 200% en los próximos dos años y reconoce como parte decisiva en su visión a mediano plazo implementar un sistema de gestión de la seguridad de la información, esto para ofrecer a sus clientes confianza en sus procesos misionales.

3.2 Organigrama

El siguiente diagrama muestra el organigrama actualizado de **ABC S.A**

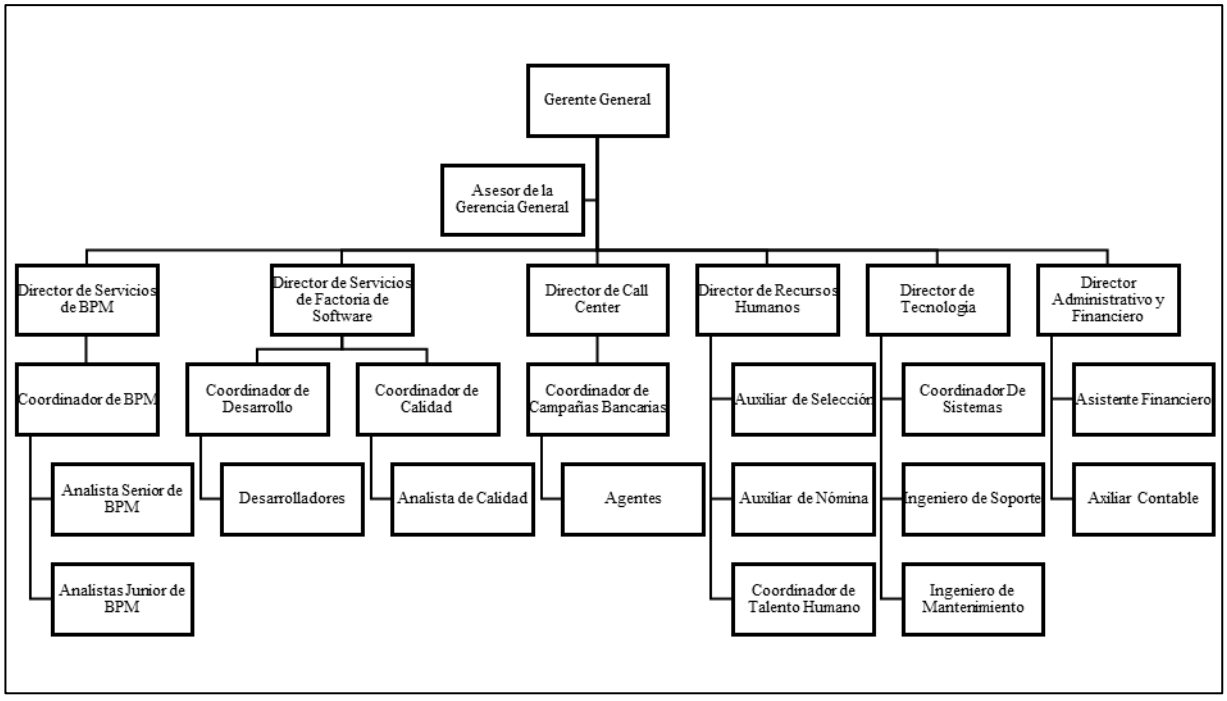


Ilustración 1 Organigrama de ABC S.A.

3.3 Mapa de Procesos

La empresa ha desarrollado su mapa de procesos misionales de la siguiente manera:

Ilustración 2 Mapa de Procesos de ABC S.A.

Compuesto por 2 procesos estratégicos, 3 procesos misionales y 3 procesos de apoyo. Cada uno de ellos descrito dentro del manual de calidad de **ABC S.A.**

3.4 Alcance del SGSI

La alta dirección de **ABC S.A. Colombia** ha delimitado el alcance del Sistema de Gestión de Seguridad de la Información a los sistemas de información que apoyan el proceso de **"Gestión de Servicios de Call Center"** debido a la criticidad del mismo para el negocio, los beneficios comerciales y de reconocimiento en el mercado, y a la generación de confianza por parte de los clientes.

Dicho proceso está compuesto por 6 procedimientos como se describe en la siguiente gráfica:

Ilustración 3 Proceso de Gestión de Servicios de Call Center

3.5 Partes Interesadas

Para el alcance definido del SGSI de **ABC S.A** se reconocen las siguientes partes interesadas:

- La alta dirección de **ABC S.A**
- El director del área de Call Center como dueño del proceso.
- Los clientes que contratan el servicio de "Call Center".
- Los usuarios finales del servicio, por ejemplo: los clientes de los diferentes bancos que han contratado el servicio con **ABC S.A.**
- Las áreas que prestan los servicios de apoyo: Gestión del Recurso Humano, Gestión Administrativa y Financiera, Gestión de la tecnología.

3.6 Sistemas de Información

Los siguientes son los sistemas de información que apoyan el proceso de Gestión de Call Center:

- E-Client: Es un software desarrollado por el área de Tecnología de **ABC S.A** que se utiliza para la gestión de información de los clientes, se integra con la planta de telefonía de VoIP de **ABC S.A** para la asignación, grabación, seguimiento y auditoría de las llamadas. Adicionalmente tiene un módulo publicado en internet por medio del cual los clientes (Bancos) pueden consultar estadísticas de sus campañas. Este Software es el sistema de información principal del negocio.
- Request Tracker: Sistema de información utilizado para la gestión de Tickets, en este queda el registro de peticiones, quejas o reclamos de los clientes, las acciones que cada uno de los agentes de call center realiza sobre el ticket, el estado del ticket, etc.

3.7 Topología de Red

La red de datos de **ABC S.A** cuenta con un firewall para filtrar el tráfico entrante y saliente y entre redes internas. Esta arquitectura permite separar las redes de usuarios de las redes de servidores y el establecimiento de una zona desmilitarizada (DMZ) donde se ubica un servidor de correo y web, y de una red dedicada para servidores de servicios internos como Directorio Activo, Servidor de Antivirus y servidores de Aplicaciones.

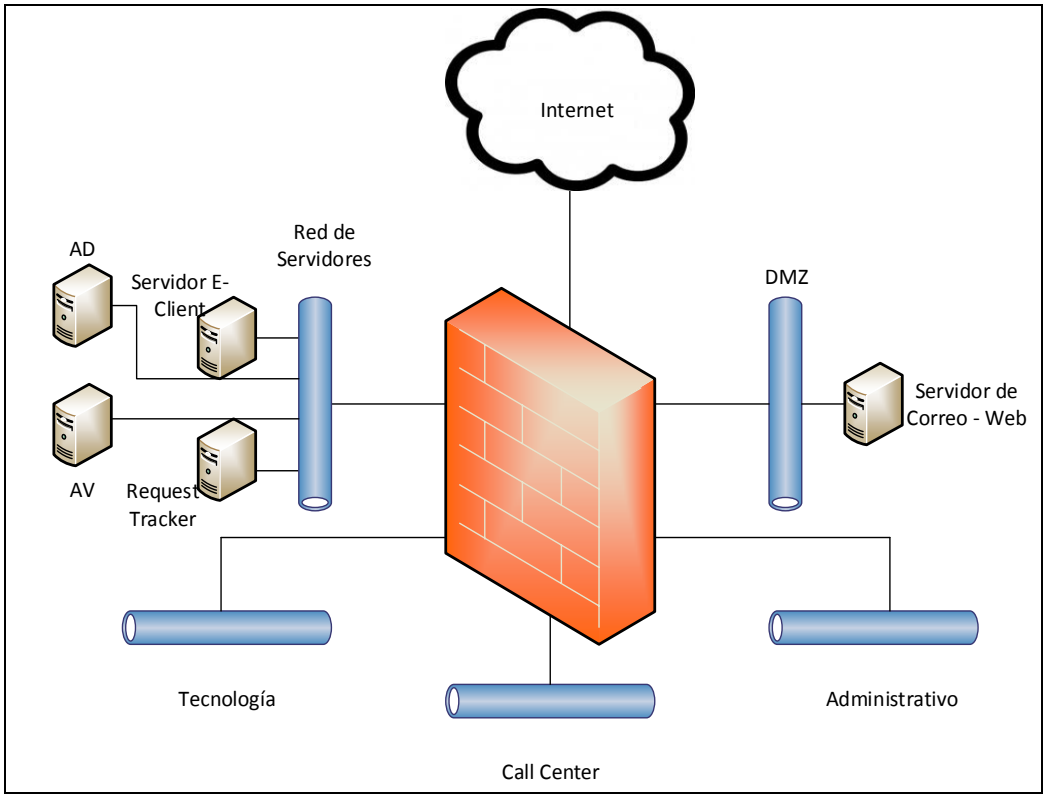


Ilustración 4 Topología de Red

3.8 Requerimientos Legales

De manera particular y teniendo en cuenta que los clientes objetivo para el servicio de "call center" son clientes Bancarios, **ABC S.A** está obligada a cumplir con las siguientes leyes y estándares:

- Ley de protección de Datos Personales
- Ley de Habeas Data
- PCI-DSS (Payment Card Industry- Data Security Standard)

Las dos primeras leyes debido a que, por la naturaleza de la actividad, se almacenan bases de datos personales de los clientes de los bancos, por otro lado también se almacenan números de tarjetas de crédito de los clientes, motivo por el cual deben tenerse en cuenta algunos de los requerimientos de seguridad del Estándar de Seguridad PCI.

4 OBJETIVOS DEL PLAN DIRECTOR DE SEGURIDAD

- Generar confianza por parte de los clientes de **ABC S.A** en el proceso de Call Center.
- Establecer, implementar y mantener un Sistema de Gestión de Seguridad de la Información para el proceso de "Gestión de Call Center" de **ABC S.A**

- Proteger Confidencialidad, Integridad y Disponibilidad de la información que hace parte del proceso de Gestión de Call Center.
- Identificar los riesgos asociados a la información que se almacena, produce, transmite y/o procesa en el proceso de "Gestión de Call Center" de **ABC S.A**
- Implementar un proceso de mejora continua en la protección de la información y la identificación y tratamiento de riesgos asociados a ella.
- Establecer un nivel de riesgo aceptable aprobado por la alta dirección y los propietarios del riesgo congruente con la estrategia corporativa.

5 ANÁLISIS DIFERENCIAL CON RESPECTO A ISO/IEC 27001 E ISO/IEC 27002.

La norma NTC-ISO-IEC 27001 en su versión 2013 proporciona los requerimientos para establecer, implementar, mantener y mejorar (de manera continua) un SGSI. Este análisis diferencial determinó el nivel de madurez de cada una de las cláusulas y cada uno de los controles pertenecientes a la norma mencionada con el fin de establecer el estado actual de cumplimiento de cada uno de ellos.

5.1 Niveles de Madurez

Los niveles de madurez utilizados para la realización del análisis de brecha fueron los establecidos en el marco COBIT en su versión 4.1, y se definen a continuación:

0 - Inexistente: El control no ha sido implementado o falla para lograr su objetivo de control.

2 - Inicial: La organización reconoce un problema que debe ser tratado. No existen procesos estandarizados sino procedimientos particulares aplicados a casos individuales.

3 – Reproducible Pero Intuitivo: Se desarrollan procesos para ser aplicados por personas diferentes entendiendo las mismas tareas. No hay una comunicación ni entrenamiento formal y la responsabilidad recae sobre los individuos. Excesiva confianza en el conocimiento de los individuos, por tanto, los errores son comunes.

4 – Proceso Definido: Los procesos se definen, documentan y se comunican a través de entrenamiento formal. Es obligatorio el cumplimiento de los procesos y por tanto la posibilidad de detectar desviaciones es alta. Los procedimientos por si mismos no son sofisticados pero se formalizan las prácticas existentes.

5 -Administrado: Existen mediciones y monitoreo sobre el cumplimiento de los procedimientos. Los procedimientos están bajo constante mejoramiento y proveen buenas prácticas. Normalmente requiere de herramientas automatizadas para la medición.

6 -Optimizado: Los procesos se refinan a nivel de buenas prácticas con base en los resultados del mejoramiento continuo y los modelos de madurez de otras empresas. Normalmente se cuenta con herramientas automatizadas de work flow.

5.2 Metodología

Para el establecimiento del nivel de madurez de cada uno de los controles y cláusulas, se realizaron entrevistas con los dueños de la información, administradores de los sistemas de información e infraestructura tecnológica y representantes de la alta dirección. La información obtenida se complementó con la revisión de los procesos y procedimientos que hacen parte del mapa de procesos de la organización.

5.3 Resultados

La siguiente tabla contiene la valoración del nivel de madurez de cada uno de los 144 controles de la norma ISO 27001:2013 y de sus 7 cláusulas, usando los niveles descritos anteriormente y proporcionando un breve resumen de la justificación de dicha valoración.

Sección	Control	Estado		Descripción
A.5	Políticas de Seguridad	0%		
A.5.1	Orientación de la Dirección para la gestión de la seguridad de la información	0%		
A.5.1.1	Políticas para la seguridad de la información	0%	Inexistente	ABC S.A no ha definido una política de seguridad de la Información
A.5.1.2	Revisión de las políticas para la seguridad de la información	0%	Inexistente	ABC S.A no ha definido una política de seguridad de la Información, por lo tanto no se ha revisado.
A.6	Organización de la Seguridad de la Información	10%		
A.6.1	Organización Interna	20%		
A.6.1.1	Roles y Responsabilidades de Seguridad de la Información	0%	Inexistente	En la organización no se han definido roles y responsabilidades de seguridad de la información, se asignó la responsabilidad de la implementación al área de Tecnología pero no hay una asignación oficial a nivel de contrato, responsabilidades del cargo, etc.
A.6.1.2	Separación de deberes	0%	Inexistente	No se ha definido un área o rol con la autoridad requerida para el gobierno de la seguridad de la información.
A.6.1.3	Contacto con las autoridades	10%	Inicial / Ad Hoc	El área de Call Center ha tenido contacto con Bomberos, Policía, alcaldias locales, etc, pero esto no se ha documentado ni procedimentado.

Sección	Control	Estado		Descripción
A.6.1.4	Contacto con grupos de interés especial	90%	Proceso Definido	Se tiene definido contacto con los fabricantes de sistemas operativos, productos de desarrollo de software y software comercial para recibir por medio de listas de correo la notificación de nuevas vulnerabilidades informáticas y actualizaciones de seguridad críticas.
A.6.1.5	Seguridad de la información en la gestión de proyectos	0%	Inexistente	No se han incluido hasta ahora requerimientos de seguridad para la gestión de proyectos.
A.6.2	Dispositivos móviles y teletrabajo	0%		
A.6.2.1	Política para dispositivos móviles	0%	Inexistente	No existe una política ni medidas de seguridad para dispositivos móviles.
A.6.2.2	Teletrabajo	0%	Inexistente	No existe una política ni medidas de seguridad para Teletrabajo a pesar de que el teletrabajo si está autorizado y se realiza en la organización.
A.7	Seguridad de los Recursos Humanos	17%		
A.7.1	Antes de asumir el empleo	45%		
A.7.1.1	Selección	90%	Proceso Definido	Dentro del proceso de Gestión Humana se encuentra el Procedimiento de selección de personal que contempla la revisión de antecedentes en las bases de datos de la Dijin, Procuraduría y Contraloria. Adicionalmente se tiene establecido en el procedimiento de contratación la realización de visitas domiciliarias y polígrafo
A.7.1.2	Términos y condiciones del empleo	0%	Inexistente	Los acuerdos contractuales con empledos y contratistas no establecen sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	Durante el empleo	7%		
A.7.2.1	Responsabilidades de la dirección	10%	Inicial / Ad Hoc	La alta dirección ha programado exporádicamente charlas de concienciación en donde se solicita al personal seguir ciertas normas básicas de seguridad pero no se ha profundizado en las responsabilidades de cada empleado para el cumplimiento de políticas, leyes, normas, etc.
A.7.2.2	Concienciación sobre la seguridad de la información, la educación y la formación	0%	Inexistente	No se ha realizado concienciación formal sobre seguridad de la información.
A.7.2.3	Proceso disciplinario	10%	Inicial / Ad Hoc	Dentro del contrato laboral existe una cláusula de confidencialidad en donde se menciona una sanción penal en caso de divu lgar información confidencial de la compañía. Sin embargo esto no aplica para el caso de contratos por prestación de servicios o de contratistas.
A.7.3	Terminación y cambio de empleo	0%		

Sección	Control	Estado		Descripción
A.7.3.1	Terminación o cambio de responsabilidades de empleo	0%	Inexistente	No se han definido las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo.
A.8	Gestión de Activos	14%		
A.8.1	Responsabilidad de los activos	35%		
A.8.1.1	Inventario de Activos	50%	Reproducible Pero Intuitivo	El área de tecnología cuenta con un inventario actualizado de los activos de información relacionados con los sistemas de información que apoyan el proceso de Gestión de Call Center. Sin embargo no hay un procedimiento formal para actualizarlo periódicamente o cuando ingrese un nuevo activo al proceso.
A.8.1.2	Propietario de los activos	0%	Inexistente	A pesar de que existe el inventario de activos, estos no tienen asociado un propietario.
A.8.1.3	Uso aceptable de los activos	0%	Inexistente	No se han identificado ni documentado las reglas para el uso aceptable de información.
A.8.1.4	Devolución de los activos	90%	Proceso Definido	Dentro del procedimiento de entrega de cargo que hace parte del proceso de Gestion del Recurso Humano se tiene definido como requisito la expedición de un paz y salvo de parte de los procesos relacionados con el empleo que incluye la devolución de activos.
A.8.2	Clasificación de la información	3%		
A.8.2.1	Clasificación de la información	10%	Inicial / Ad Hoc	Se han adelantado campañas de concienciación con respecto al carácter confidencial de los datos personales, sin embargo esto no está definido formalmente
A.8.2.2	Etiquetado de la información	0%	Inexistente	No se realiza etiquetado de información
A.8.2.3	Manejo de activos	0%	Inexistente	No se han desarrollado procedimientos para el manejo de activos de acuerdo con la clasificación de la información.
A.8.3	Manejo de medios	3%		
A.8.3.1	Gestión de medios removibles	0%	Inexistente	No hay un procedimiento para la gestión de medios removibles.
A.8.3.2	Disposición de los medios	10%	Inicial / Ad Hoc	El área de Tecnología hace un borrado seguro a bajo nivel de los discos duros de los equipos que son devueltos, o luego que cambian de responsable o custodio. Sin embargo esta práctica no está documentada ni sustentada en un procedimiento.
A.8.3.3	Transferencia de medios físicos	0%	Inexistente	No existe un procedimiento de protección para los medios que contienen información y son transportados. La organización transporta cintas con copias de respaldo a un sitio de un tercero.
A.9	Control de accesos	31%		
A.9.1	Requisitos del negocio para el control de acceso	5%		

Sección	Control	Estado		Descripción
A.9.1.1	Política de control de acceso	10%	Inicial / Ad Hoc	Existe una política de control de acceso a las intalaciones de acuerdo con el rol de cada empleado. Sin embargo la política de control de acceso no se extiende al acceso a la información en los sistemas de información y está desactualizada.
A.9.1.2	Acceso a redes y servicios en red	0%	Inexistente	La red de la organización se encuentra segmentada de tal manera que la información se encuentra aislada de acuerdo al principio de necesidad de conocer, adicionalmente los puertos de red que no están en uso se encuentran deshabilitados. Sin embargo esta segmentación no se encuentra documentada ni procedimentada.
A.9.2	Gestión de acceso de usuarios	67%		
A.9.2.1	Registro y cancelación del registro de usuarios	100%	Optimizado	Todos los sistemas de información están integrados con el directorio activos de la organización, el proceso de dada de alta y de baja de personal desde Gestión Humana contempla la dehabilitación de usuarios y/o permisos en el caso de finalización del contrato o de cambio de área.
A.9.2.2	Suministro de acceso de usuarios	100%	Optimizado	Todos los sistemas de información están integrados con el directorio activos de la organización, el proceso de dada de alta y de baja de personal desde Gestión Humana contempla la dehabilitación de usuarios y/o permisos en el caso de finalización del contrato o de cambio de área.
A.9.2.3	Gestión de derechos de acceso privilegiado	10%	Inicial / Ad Hoc	Solamente el administrador del dominio puede dar de alta un usuario con privilegios. Sin embargo esto no tiene un control adicional ni está documentado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	90%	Proceso Definido	Está definido que al crear una contraseña, se crea una contraseña temporal que expira en el primer inicio de sesión y obliga al usuario a cambiarla.
A.9.2.5	Revisión de los derechos de acceso de usuarios	0%	Inexistente	Los propietarios de los activos no revisan los derechos de acceso de los usuarios a intervalos regulares.
A.9.2.6	Retiro o ajuste de los de derechos de acceso	100%	Optimizado	Todos los sistemas de información están integrados con el directorio activos de la organización, el proceso de dada de alta y de baja de personal desde Gestión Humana contempla la dehabilitación de usuarios y/o permisos en el caso de finalización del contrato o de cambio de área.
A.9.3	Responsabilidades de los usuarios	10%		
A.9.3.1	Uso de información de autenticación secreta	10%	Inicial / Ad Hoc	Al momento de entregar la contraseña, se entrega un texto con las responsabilidades y deberes del usuario para con la contraseña.
A.9.4	Control de acceso al sistema y aplicaciones	42%		

Sección	Control	Estado		Descripción
A.9.4.1	Restricciones de acceso a la información	10%	Inicial / Ad Hoc	El acceso a la información de los sistemas de información tiene un control de acceso RBAC que además está integrado con el directorio activo. Sin embargo todavía no hay una política de control de acceso que lo sustente.
A.9.4.2	Procedimiento de ingreso seguro	50%	Reproducible Pero Intuitivo	El acceso está integrado con el directorio activo. Sin embargo no se hacen mediciones sobre este control.
A.9.4.3	Sistema de gestión de contraseñas	100%	Optimizado	El directorio activo lo provee.
A.9.4.4	Uso de programas utilitarios privilegiados	50%	Reproducible Pero Intuitivo	El software antivirus usado en la organización permite bloquear este tipo de programas.
A.9.4.5	Control de acceso a códigos fuente de programas	0%	Inexistente	Los códigos fuente están en los equipos de los desarrolladores, sin embargo el único control de acceso es la contraseña del sistema operativo.
A.10	Criptografía	0%		
A.10.1	Controles criptográficos	0%		
A.10.1.1	Política de uso de controles criptográficos	0%	Inexistente	No se usan controles criptográficos.
A.10.1.2	Gestión de llaves	0%	Inexistente	No se usan controles criptográficos.
A.11	Seguridad física y del entorno	50%		
A.11.1	Áreas seguras	48%		
A.11.1.1	Perímetro de seguridad física	50%	Reproducible Pero Intuitivo	Se encuentran definidos los perímetros de seguridad para agentes de call center, centros de procesamiento de datos, etc.
A.11.1.2	Controles de acceso físicos	50%	Reproducible Pero Intuitivo	Se cuenta con biometria y tarjetas de proximidad, sin embargo esto no está documentado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	50%	Reproducible Pero Intuitivo	Se cuenta con biometria y tarjetas de proximidad, sin embargo esto no está documentado.
A.11.1.4	Protección contra las amenazas externas y ambientales	50%	Reproducible Pero Intuitivo	Se cuenta con sistemas de prevención de incendio. Se han desarrollado campañas de prevención de desastres y se tiene implementado un procedimiento de DRP.
A.11.1.5	Trabajo en áreas seguras	0%	Inexistente	No existen procedimientos diseñados para el trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga	90%	Proceso Definido	El único punto de despacho y carga es el de recepción de correspondencia que se encuentra aislado
A.11.2	Equipos	51%		

Sección	Control	Estado		Descripción
A.11.2.1	Ubicación y protección de equipos	90%	Proceso Definido	XXXXX S:A cuenta con un CPD con una arquitectura que cumple con las buenas prácticas en la materia, solamente se tiene acceso a el por medio de biométricos y tarjetas de proximidad. Para el caso de los computadores personales no se tiene implementada ninguna protección.
A.11.2.2	Servicios de suministro	50%	Reproducible Pero Intuitivo	Se cuenta con UPS suficientes para dar autonomía a los servidores así como redes reguladas de energía.
A.11.2.3	Seguridad del cableado	90%	Proceso Definido	Todo el edificio cuenta con cableado estructurado certificado
A.11.2.4	Mantenimiento de los equipos	0%	Inexistente	No se cuenta con un contrato de mantenimiento para los equipos ni hace parte de las tareas del área de sistemas.
A.11.2.5	Retiro de activos	90%	Proceso Definido	El personal de vigilancia tiene la instrucción de verificar la salida de elementos, estos solo pueden salir si están registrados o si se ha expedido una orden de salida por parte del área administrativa y financiera.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	0%	Inexistente	No se ha implementado ninguna medida de seguridad para proteger los equipos que salen de las instalaciones como es el caso de los computadores portátiles.
A.11.2.7	Disposición segura o reutilización de equipos	50%	Reproducible Pero Intuitivo	El área de tecnología tiene la costumbre de hacer un borrado a bajo nivel de los discos duros de equipos de personal que se retira de la compañía o en el caso de reasignación de equipos.
A.11.2.8	Equipo de usuario desatendido	90%	Proceso Definido	Desde el directorio activo se tiene configurado un bloqueo de sesión luego de 3 minutos de inactividad. Esto no está documentado.
A.11.2.9	Política de escritorio limpio y pantalla limpia	0%	Inexistente	No existe una política de escritorio y pantalla limpio.
A.12	Seguridad de las operaciones	18%		
A.12.1	Procedimientos operacionales y responsabilidades	0%		
A.12.1.1	Procedimientos de operación documentados	10%	Inicial / Ad Hoc	Se tienen escritos algunos procedimientos de operación , sin embargo esto no está estandarizado ni se cubre la totalidad de la operación que hace parte del alcance del SGSI
A.12.1.2	Gestión de cambios	0%	Inexistente	No hay un procedimiento de gestión de cambios establecido. Los cambios se ejecutan por demana y bajo la discreción del administrador de los activos.
A.12.1.3	Gestión de la capacidad	0%	Inexistente	No se de definido un plan de capacidad ni se ha tenido en cuenta el posible crecimiento de la organización, tampoco se monitorean parámetros como espacio, consumo de memoria o de procesamiento.

Sección	Control	Estado		Descripción
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	0%	Inexistente	A pesar de que se hace desarrollo seguro al interior de la organización, no se encuentra una separación de ambientes, el desarrollo se hace en las estaciones de trabajo de los desarrolladores y luego se carga en el ambiente de producción.
A.12.2	Protección contra códigos maliciosos	90%		
A.12.2.1	Controles contra códigos maliciosos	90%	Proceso Definido	Se tiene implementada una solución de antivirus centralizada y administrada por el área de tecnología, esto cubre los servidores y equipos de escritorio.
A.12.3	Copias de respaldo	10%		
A.12.3.1	Respaldo de la información	10%	Inicial / Ad Hoc	Se toman copias de respaldo de los servidores de producción de manera exporádica, estas copias de respaldo se almacenan en cintas que son transportadas y almacenadas en las instalaciones de un tercero.
A.12.4	Registro y seguimiento	23%		
A.12.4.1	Registro de eventos	0%	Inexistente	No se tiene configuado el registro de eventos de usuario. La configuración de logs en servidores y equipos de escritorio corresponde a la configuración por defecto
A.12.4.2	Protección de la información de registro	0%	Inexistente	No se tiene configuado el registro de eventos de usuario. La configuración de logs en servidores y equipos de escritorio corresponde a la configuración por defecto
A.12.4.3	Registros del administrador y del operador	0%	Inexistente	No se tiene configuado el registro de eventos del administrador y del operador. La configuración de logs en servidores y equipos de escritorio corresponde a la configuración por defecto
A.12.4.4	Sincronización del relojes	90%	Proceso Definido	El controlador de dominio y todos los servidores están integrados con un NTP público de la Superintendencia de Industria y Comercio de Colombia quién fija la hora legal colombiana.
A.12.5	Control de software operacional	0%		
A.12.5.1	Instalación de software en sistemas operativos	0%	Inexistente	El control de acceso basado en roles implementado por medio del directorio activo impide la instalación de software por parte de usuarios estándar.
A.12.6	Gestión de la vulnerabilidad técnica	0%		
A.12.6.1	Gestión de las vulnerabilidades técnicas	0%	Inexistente	Hasta el momento la organización no ha realizado análisis de vulnerabilidades y no tiene implementado un procedimiento de gestión de vulnerabilidades técnicas.
A.12.6.2	Restricciones sobre la instalación de software	0%	Inexistente	El control de acceso basado en roles implementado por medio del directorio activo impide la instalación de software por parte de usuarios estándar.

Sección	Control	Estado		Descripción
A.12.7	Consideraciones sobre auditorías de sistemas de información	0%		
A.12.7.1	Controles de auditoría de sistemas de información	0%	Inexistente	Hasta el momento, la organización no realiza auditorías sobre los sistemas de información, tampoco se tiene un proceso documentado para realizarlo.
A.13	Seguridad en las comunicaciones	26%		
A.13.1	Gestión de la seguridad de las redes	50%		
A.13.1.1	Controles de redes	90%	Proceso Definido	Se cuenta con una segmentación de redes , adicionalmente los puertos que no están en uso se encuentran deshabilitados.
A.13.1.2	Seguridad de los servicios de red	10%	Inicial / Ad Hoc	No se han identificado formalmente los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de los servicios de red.
A.13.1.3	Separación en las redes	50%	Reproducible Pero Intuitivo	Se encuentra una separación de redes dependiendo del área de negocio. Esto sin embargo no está documentado.
A.13.2	Transferencia de información	3%		
A.13.2.1	Políticas y procedimientos de transferencia de información	0%	Inexistente	No se han definido políticas y procedimientos de transferencia de información.
A.13.2.2	Acuerdos sobre transferencia de información	0%	Inexistente	No se han definido acuerdos para la transferencia segura de información entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	0%	Inexistente	No se han definido controles para la protección de la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	10%	Inicial / Ad Hoc	Se cuenta con una cláusula de confidencialidad en los contratos laborales y de prestación de servicios de los empleados, sin embargo este no ha sido revisado desde su creación, hace alrededor de 6 años. No se tienen definidos acuerdos de confidencialidad con clientes ni con terceros.
A.14	Adquisición, desarrollo y mantenimiento de sistemas	21%		
A.14.1	Requisitos de seguridad de los sistemas de información	63%		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	50%	Reproducible Pero Intuitivo	Todos los desarrolladores han sido capacitados en técnicas de desarrollo seguro y han recibido una solicitud expresa pero no formal de procurar realizar un desarrollo seguro de los sistemas.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	50%	Reproducible Pero Intuitivo	Se implementó el protocolo SSL para el módulo público del software E-Client, para el acceso remoto se utilizan VPN seguras. Estos controles no están documentados ni procedimentados.

Sección	Control	Estado		Descripción
A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones	90%	Proceso Definido	Se definió como estándar (no documentado) el uso de VPN para las conexiones con clientes, y proveedores.
A.14.2	Seguridad en los procesos de desarrollo y de soporte	1%		
A.14.2.1	Política de desarrollo seguro	10%	Inicial / Ad Hoc	A pesar de que el grupo de desarrollo ha sido capacitado en temas de desarrollo seguro. No se ha formalizado una política de desarrollo seguro.
A.14.2.2	Procedimientos de control de cambios en sistemas	0%	Inexistente	No se han documentado ni establecido procedimientos de control de cambios dentro del ciclo de desarrollo seguro de los sistemas.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	0%	Inexistente	La organización no cuenta con un área de pruebas que realice pruebas antes de realizar cambios en las plataformas de operación. Los cambios se aplican de acuerdo al criterio de los desarrolladores.
A.14.2.4	Restricciones en los cambios a los paquetes de software	0%	Inexistente	Los cambios no son controlados, no hay controles implementados que impidan que un desarrollador haga un cambio sobre sistemas de producción sin un debido proceso de análisis. Se hace como buena práctica de los desarrolladores.
A.14.2.5	Principios de construcción de los sistemas seguros	0%	Inexistente	A pesar de que el grupo de desarrollo ha sido capacitado en temas de desarrollo seguro. No se ha formalizado una política de desarrollo seguro.
A.14.2.6	Ambiente de desarrollo seguro	0%	Inexistente	No existe un ambiente de desarrollo, todos los desarrollos se ejecutan en los computadores de los desarrolladores desde donde tienen acceso incluso al ambiente de producción, a internet y a correo electrónico.
A.14.2.7	Desarrollo contratado externamente	0%	Inexistente	No existe una supervisión de la actividad de desarrollo seguro de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas	0%	Inexistente	No se realizan pruebas de funcionalidad de la seguridad durante el desarrollo.
A.14.2.9	Pruebas de aceptación de sistemas	0%	Inexistente	No se han establecido programas de prueba para la aceptación de los sisetmas de información nuevos, nuevos módulos o actualizaciones de los existentes.
A.14.3	Datos de prueba	0%		
A.14.3.1	Protección de los datos de prueba	0%	Inexistente	No existe una separación de los datos de prueba que puedan ser protegidos.
A.15	Relaciones con los proveedores	13%		
A.15.1	Seguridad de la información en las relaciones con proveedores	0%		

Sección	Control	Estado		Descripción
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	0%	Inexistente	No se han acordado ni documentado los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de información.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	0%	Inexistente	No hay acuerdos explícitos sobre los requisitos de seguridad de la información pertinentes con cada proveedore que pueda tener acceso, procesar, almacenar, comunicar o suminstrar componetnes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	0%	Inexistente	Dentro de los acuerdos con proveedores no se incluyen requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2	Gestión de la prestación de servicios de proveedores	25%		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	50%	Reproducible Pero Intuitivo	Se tienen programadas reuniones de seguimiento periódicas con los proveedores para discutir aspectos relacionados con la prestación del servicio, esto como buena práctica que no está documentada.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	0%	Inexistente	No se hace una gestión de cambios en el suminitro de servicios, los cambios que los proveedores deban hacer quedan a discreción suya y solamente informan a la organización.
A.16	Gestión de incidentes de seguridad de la información	0%		
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	0%		
A.16.1.1	Responsabilidades y procedimientos	0%	Inexistente	No se gestionan los incidentes, cuando ocurre un incidente se trata por demanda dependiendo de las áreas afectadas, la criticidad y la disponibilidad del personal.
A.16.1.2	Reporte de eventos de seguridad de la información	0%	Inexistente	No se gestionan los incidentes, cuando ocurre un incidente se trata por demanda dependiendo de las áreas afectadas, la criticidad y la disponibilidad del personal.
A.16.1.3	Reporte de debilidades de seguridad de la información	0%	Inexistente	No se ha definido una matriz de comunicación ni canales adecuados para que los empleados puedan repotar posibles incidentes de seguridad.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	0%	Inexistente	No se gestionan los incidentes, cuando ocurre un incidente se trata por demanda dependiendo de las áreas afectadas, la criticidad y la disponibilidad del personal.
A.16.1.5	Respuesta a incidentes de seguridad de la información	0%	Inexistente	No se gestionan los incidentes, cuando ocurre un incidente se trata por demanda dependiendo de las áreas afectadas, la criticidad y la disponibilidad del personal.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	0%	Inexistente	Cuando se han tratado los incidentes presentados no se han hecho sesiones de lecciones aprendidas ni se ha alimentado una base de datos de incidentes.

Sección	Control	Estado		Descripción
A.16.1.7	Recopilación de evidencia	0%	Inexistente	No existe un procedimiento relacionado con la recopilación de evidencia.
A.17	Aspectos de la seguridad de la información de la gestión de continuidad de negocio	67%		
A.17.1	Continuidad de seguridad de la información	38%		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	10%	Inicial / Ad Hoc	La organización tiene desarrollado un un Plan de continuidad de negocio en donde tiene en cuenta ciertos controles de seguridad de acuerdo con el criterio del área de tecnología.
A.17.1.2	Implantación de la continuidad de la seguridad de la información	10%	Inicial / Ad Hoc	Si bien existe el BCP, este no detallad de manera explícita procesos, procedimientos y controles para mantener la seugridad de la información durante una situación adversa. Los controles implementados han sido elegidos por el área de tecnología.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	95%	Gestionado y Medible	El plan de continuidad de negocio es verificado a intervalos regulares, se tienen programadas pruebas de escritorio y en paralelo para el BCP
A.17.2	Redundancias	95%		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	95%	Gestionado y Medible	La organización cuenta con un centro alterno de procesamiento de datos que tiene estaciones de trabajo para proporcionar el mínimo servicio aceptable para el negocio en caso de contingencia. Los servicios de este centro alterno incluyen los relacionados con el alcance del SGSI y son probados de manera periódica.
A.18	Cumplimiento	26%		
A.18.1	Cumplimiento de requisitos legales y contractuales	48%		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	90%	Proceso Definido	El área Administrativa y financiera cuenta con un asesor jurídico que dentro de sus responsabilidades tiene la de mantener actualizado el inventario de normas y leyes aplicables a la organización.
A.18.1.2	Derechos de propiedad intelectual (DPI)	50%	Reproducible Pero Intuitivo	La instalación de software en los equipos es controlada por medio de políticas del directorio activo, todo software que es instalado debe ser aprobado por el área de sistemas quien hace una validación de las respectivas licencias.
A.18.1.3	Protección de registros	50%	Reproducible Pero Intuitivo	Los registros propios del proceso de Gestión de Call center son almacenados en un servidor de archivos aislado de la red y con acceso restringido.
A.18.1.4	Privacidad y protección de información de datos personales	50%	Reproducible Pero Intuitivo	La organización da cumplimiento a la ley de protección de datos personales por medio de diferentes controles administrativos y técnicos. Sin embargo no se ha definido una revisión de este control.
A.18.1.5	Reglamentación de controles criptográficos	0%	Inexistente	Actualmente la organización no usa controles criptográficos.

Sección	Control	Estado		Descripción
A.18.2	Revisiones de seguridad de la información	3%		
A.18.2.1	Revisión independiente de la seguridad de la información	0%	Inexistente	Dentro de los planes de auditoría no se ha planificado la revisión de los aspectos de seguridad de la información.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	10%	Inicial / Ad Hoc	Los directores hicieron una primera revisión del cumplimiento de las normas de seguridad apropiadas por parte de los procesos y procedimientos de la organización, esta es apenas la primera revisión y de donde sale la iniciativa de la implementación del SGSI.
A.18.2.3	Revisión del cumplimiento técnico	0%	Inexistente	No se hacen revisiones de los sistemas de información para determinar el cumplimiento con las políticas y normas de seguridad de la información
C	Clausulas ISO27001:2013	27%		
C.4	Contexto de la Organización	90%	Proceso Definido	La organización ya ha definido su contexto de acuerdo a los objetivos estratégicos de negocio y a las partes interesadas.
C.5	Liderazgo	50%	Reproducible Pero Intuitivo	La alta dirección ha demostrado su compromiso con el SGSI al asignar recursos para la implementación del SGSI.
C.6	Planificación	0%	Inexistente	La organización no ha llevado a cabo una valoración y tratamiento de riesgos de seguridad de la información ni ha hecho un análisis de oportunidades y amenazas.
C.7	Soporte	50%	Reproducible Pero Intuitivo	La organización asignó para el año 2015 un presupuesto suficiente para cubrir el establecimiento e implementación del SGSI, sin embargo este es el primer esfuerzo de la organización hasta el momento en este tema. Se han planeado además jornadas de toma de conciencia con respecto a la seguridad de la información.
C.8	Operación	0%	Inexistente	Hasta el momento no se han planificado, implementado y controlado los procesos necesarios para cumplir los requisitos de seguridad de la información. No se han desarrollado aún planes para cumplir con los objetivos de la seguridad.
C.9	Evaluación del desempeño	0%	Inexistente	Hasta el momento no se han definido métricas para medir la eficacia del sistema de gestión, no se a incluido la seguridad de la información dentro de los planes de auditoría ni se han hecho revisiones por parte de la dirección.
C.10	Mejora	0%	Inexistente	Dado que la implementación del SGSI hasta el momento inicia, no se tienen registros ni acciones relacionadas con no conformidades y acciones correctivas.

Tabla 1 Análisis Diferencial con Respecto a la norma ISO 27001:2013

La siguiente gráfica muestra el nivel de madurez general de cada una de las secciones del anexo A de la norma ISO 27001:2013

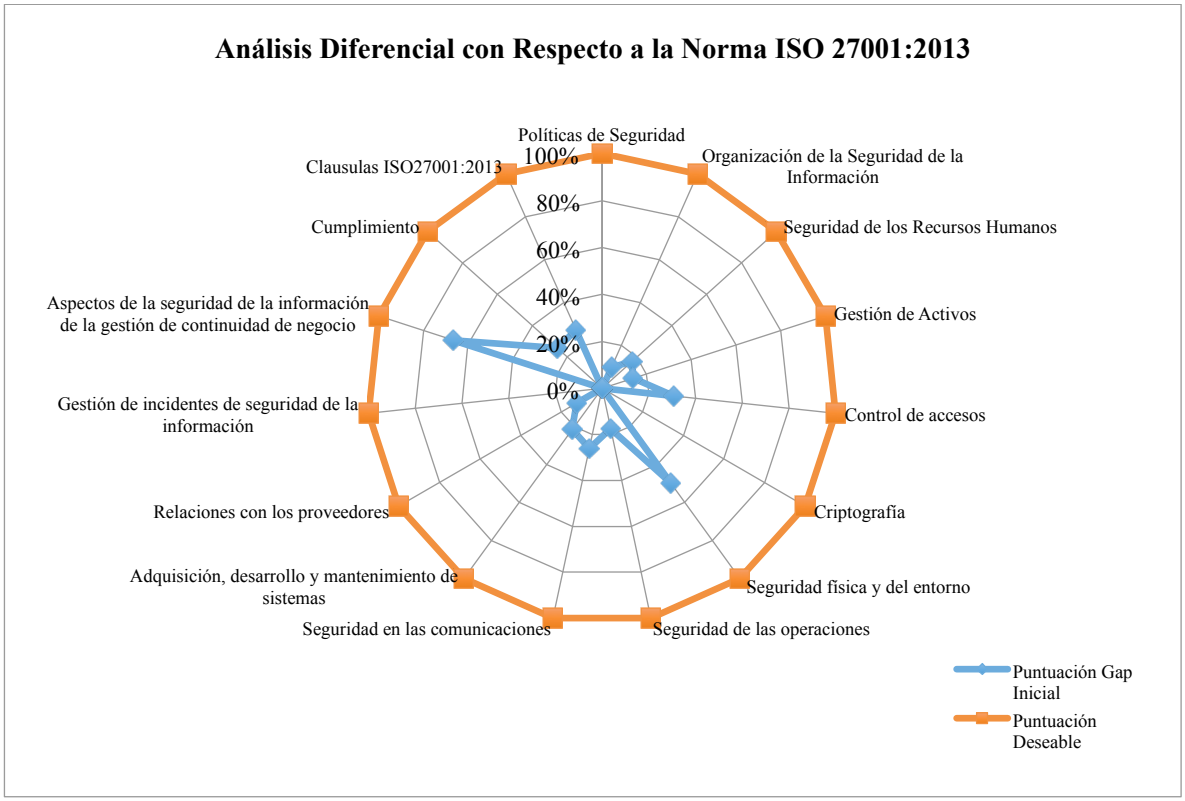


Ilustración 5 Nivel de Madurez de los Controles del Anexo A ISO 27001:2013

Cuyos valores fueron obtenidos de promediar el nivel de madurez de cada uno de los controles que componen cada sección, el resumen de este promedio puede verse en la siguiente tabla:

Sección	Título	Nivel de Maduez
A.5	Políticas de Seguridad	0%
A.6	Organización de la Seguridad de la Información	10%
A.7	Seguridad de los Recursos Humanos	17%
A.8	Gestión de Activos	14%
A.9	Control de accesos	31%
A.10	Criptografía	0%
A.11	Seguridad física y del entorno	50%
A.12	Seguridad de las operaciones	18%
A.13	Seguridad en las comunicaciones	26%
A.14	Adquisición, desarrollo y mantenimiento de sistemas	21%
A.15	Relaciones con los proveedores	13%
A.16	Gestión de incidentes de seguridad de la información	0%
A.17	Aspectos de la seguridad de la información de la gestión de continuidad de negocio	67%
A.18	Cumplimiento	26%
C	Cláusulas	27%

Tabla 2 Resumen del Nivel de Madurez de Cada Grupo de Controles

6 SISTEMA DE GESTIÓN DOCUMENTAL

A continuación se presentan los documentos que hacen parte del SGSI de **ABC S.A**

6.1 Objetivos del SGSI

a) Tomar las acciones necesarias para que el Sistema de Gestión de Seguridad de la Información mejore continuamente.
b) Gestionar los incidentes de seguridad de la información de tal manera que el impacto a la organización se minimice en caso de que se materialice un riesgo.
c) Crear conciencia en funcionarios, directivos, proveedores y contratistas con respecto a la Seguridad de la Información.
d) Proteger la confidencialidad, integridad, y disponibilidad de la información que almacenen, procesen, transporten, generen o accedan los activos de información de la organización, dando prioridad a aquellos que hagan parte del alcance del SGSI.

6.2 Alcance del SGSI

El alcance del Sistema de Gestión de Seguridad de la Información son los sistemas de información que apoyan el proceso de **"Gestión de Servicios de Call Center"**, los cuales se especifican a continuación:

- E-Client
- Request Tracker
- Correo Electrónico

6.3 Política de Seguridad de la Información

La política de Seguridad de la Información de **ABC S.A** se encuentra desarrollada en el anexo 1 de la presente memoria técnica.

6.4 Procedimiento de Auditorías Internas

El SGSI será auditado con una periodicidad anual, dichas auditorías internas serán ejecutadas por un tercero idóneo teniendo en cuenta que **ABC S.A** no cuenta con un área de auditoría interna; los terceros contratados para la ejecución de auditorías internas serán gestionados por la dirección de tecnología y deberán cumplir con los siguientes requisitos.

6.4.1 Requisitos de los Auditores Internos.

El auditor encargado de ejecutar la auditoría, ya sea contratado como persona natural o por medio de una empresa debe demostrar como mínimo y sin limitarse a:

- Título profesional como Ingeniero de Sistemas, Electrónico, de Telecomunicaciones o afines.
- 3 años de experiencia en auditorías de sistemas.
- Haber participado en por lo menos 3 auditorías de Sistemas de Gestión de Seguridad con respecto a la norma ISO 27001 en el rol de auditor o auditor líder.
- Demostrar experiencia en consultoría, asesoría y/o auditoría en temas relacionados con Seguridad de la Información para el sector bancario.

6.4.2 Actividades del Procedimiento.

Para la ejecución de auditorías deben tenerse en cuenta las siguientes actividades:

a. Planeación de la Auditoría

   La oficina de sistemas evaluará propuestas de mínimo 3 proveedores que cumplan el papel de auditores internos para el SGSI **ABC S.A** Y se encargará de elegir el proveedor idóneo para dicha tarea. Debe tenerse en cuenta que el perfil auditor cumpla con experiencia en la realización de auditorías a este tipo de sistemas.

   La elección del proveedor deberá hacerse con 1 mes de antelación al inicio de la auditoría.

b. Ejecución de la Auditoría

   Todas las auditorías internas del SGSI de **ABC S.A** deberán seguir las siguientes actividades:

   i. Reunión de Inicio.

   ii. Revisión de documentación por parte de la empresa auditora.

   iii. Planeación y programación de entrevistas.

   iv. Ejecución de auditoría en Sitio.

   v. Generación de Informe.

   vi. Presentación de Resultados y Reunión de Cierre.

c. Gestión de Hallazgos y Mejora Continua.

   Una vez finalizada la auditoría se deberá comunicar a las partes interesadas y a la alta dirección los hallazgos de la misma y generar el plan de acción relacionado. Dicho plan de acción deberá contemplar de manera obligatoria, y sin limitarse a, las siguientes características:

   - Determinación de la causa raíz de los hallazgos.
   - Planteamiento de las acciones Correctivas
   - Análisis de la efectividad de la eficacia de acciones correctivas de anteriores auditorías.

6.4.3 Formatos Para la Ejecución de Auditorías Internas

Para la ejecución de auditorías internas, el proveedor seleccionado deberá basarse en los siguientes modelos de Plan de Auditoría, e Informe de Auditoría.

6.4.3.1 Formato Para el Plan de Auditoría

El plan de auditoría deberá desarrollarse de acuerdo al formato presentado en el Anexo 2 de este documento.

6.4.3.2 Formato Para el Informe de Auditoría

El informe de auditoría deberá presentarse siguiendo el formato presentado en el Anexo 3 de este documento.

6.5 Gestión de Indicadores

Para la evaluación del desempeño del SGSI se plantean los siguientes indicadores:

6.5.1 Auditorías Realizadas al SGSI

Descripción: Medición del porcentaje de cumplimiento de ejecución de auditorías internas. Cualquier valor diferente al 100% no es aceptable por que generará una no conformidad.

Este indicador ayuda a medir el cumplimiento del objetivo 6.1. a).

Fórmula de Medición:

$$\frac{\#\ Auditorías\ Realizadas}{\#\ Auditorias\ Programadas}\ X\ 100\%$$

Frecuencia de Medición: Anual

Objetivo: 100%

Umbral: <100%

Responsable: Dirección de Sistemas

6.5.2 Efectividad de las Acciones Correctivas

Descripción: Medición del porcentaje de efectividad de las acciones correctivas tomadas para eliminar la causa raíz de las no conformidades encontradas como hallazgos de las auditorías internas al SGSI.

Este indicador ayuda a medir el cumplimiento del objetivo 6.1. a).

Fórmula de Medición:

$$\frac{\#\ Acciones\ Correctivas\ Que\ Eliminaron\ Causas\ Raiz}{\#\ Acciones\ Correctivas\ Implementadas}\ X\ 100\%$$

Frecuencia de Medición: Semestral

Objetivo: 100%

Umbral: <90%

Responsable: Dirección de Sistemas

6.5.3 Gestión de Hallazgos de Auditorías

Descripción: Con este indicador se mide la gestión sobre los hallazgos de auditoría. Se espera detectar la causa raíz de cada uno de los hallazgos con el fin de prevenir recurrencia

Este indicador ayuda a medir el cumplimiento del objetivo 6.1. a).

Fórmula de Medición:

$$\frac{\#\ Causas\ Raiz\ Identificadas}{\#\ Hallazgos\ de\ Auditoría}\ X\ 100\%$$

Frecuencia de Medición: Semestral

Objetivo: 100%

Umbral: <90%

Responsable: Dirección de Sistemas

6.5.4 Impartición de Charlas de Concienciación

Descripción: Este indicador mide el porcentaje de ejecución de charlas de concienciación programadas.

Este indicador ayuda a medir el cumplimiento del objetivo 6.1. c).

Fórmula de Medición:

$$\frac{\#\ Charlas\ de\ Concienciación\ Dictadas}{\#\ Charlas\ de\ Concienciación\ Programadas}\ X\ 100\%$$

Frecuencia de Medición: Bimensual

Objetivo: 100%

Umbral: <80%

Responsable: Dirección de Recursos Humanos

6.5.5 Resultados de las Tomas de Conciencia.

Descripción: Este indicador mide el resultado del puntaje obtenido en las encuestas de toma de conciencia realizadas luego de cada charla de concienciación dictada.

Este indicador ayuda a medir el cumplimiento del objetivo 6.1. c).

Fórmula de Medición:

$$\frac{\sum Calificación\ Obtenida\ por\ Cada\ Encuestado}{\#\ Total\ de\ Encuestados}$$

Frecuencia de Medición: Bimensual

Objetivo: 8/10

Umbral: 6/10

Responsable: Dirección de Recursos Humanos

6.5.6 Incidentes Atendidos

Descripción: Este indicador mide el porcentaje de incidentes de seguridad de la información que fueron atendidos con respecto al número de incidentes reportados.

Este indicador ayuda a medir el cumplimiento del objetivo 6.1. b).

Fórmula de Medición:

$$\frac{\#\ Incidentes\ Gestionados}{\#\ Incidentes\ Reportados}\ X\ 100\%$$

Frecuencia de Medición: Trimestral

Objetivo: 100%

Umbral: 95%

Responsable: Dirección de Tecnología.

6.5.7 Lecciones Aprendidas

Descripción: Este indicador mide la realización de reuniones de lecciones aprendidas luego de la atención de un incidente de seguridad.

Este indicador ayuda a medir el cumplimiento del objetivo 6.1. b).

Fórmula de Medición:

$$\frac{\#\ Reuniones\ de\ Lecciones\ Aprendidas}{\#\ Incidentes\ Gestionados}\ X\ 100\%$$

Frecuencia de Medición: Trimestral

Objetivo: 100%

Umbral: 90%

Responsable: Dirección de Tecnología.

6.5.8 Ejecución de Planes de Tratamiento

Descripción: Se mide el porcentaje de ejecución de los planes de tratamiento de riesgos ejecutados.

Este indicador ayuda a medir el cumplimiento del objetivo 6.1. d).

Fórmula de Medición:

$$\frac{\#\ Planes\ de\ Tratamiento\ Ejecutados}{\#\ Planes\ de\ Tratamiento\ Propuestos}\ X\ 100\%$$

Frecuencia de Medición: Trimestral

Objetivo: 100%

Umbral: 90%

Responsable: Dirección de Tecnología.

6.6 Procedimiento Revisión por la Dirección

El SGSI de **ABC S.A** establece que se debe realizar una revisión anual por parte de la dirección, para tal fin deberá aplicarse el siguiente proceso:

a. Recolección de Información: El encargado de seguridad de la información deberá recolectar la siguiente información previa a la revisión por la alta dirección:
    i. Resultados de las auditorías internas.
    ii. Métricas de desempeño del SGSI.
    iii. Resultado del Tratamiento de las no conformidades.
    iv. Resumen ejecutivo de los incidentes de seguridad del último año, incluyendo las lecciones aprendidas.
    v. Estado de los planes de tratamiento de riesgos
b. Preparación del Informe de Entrada: El encargado de seguridad de la información deberá preparar un informe de entrada previo a la revisión por parte de la dirección, para esto deberá utilizar el formato especificado en el Anexo 4 de este documento.
c. Convocatoria a la Reunión de Revisión: El encargado de seguridad de la información convoca a la alta dirección y a los propietarios del riesgo para la respectiva revisión Anual.
d. Reunión de Revisión: en la reunión de revisión se analizan los resultados de la información levantada en el numeral a) de este proceso con el fin de determinar las acciones de mejora continua adecuadas para el SGSI de **ABC S.A**
e. Generación de Informe de Salida: todos los temas discutidos y decisiones tomadas en la reunión de revisión deben registrarse en un informe de salida, de acuerdo al formato que se encuentra en el Anexo 5 de este documento.

6.7 Gestión de Roles y Responsabilidades

Los siguientes son los Roles que tienen alguna responsabilidad en el mantenimiento y/o mejora continua del SGSI de ABC S.A:

6.7.1 Alta Dirección.

Deberá aprobar las políticas de seguridad de la información, demostrar su compromiso en el establecimiento, implementación, mantenimiento y mejora continua del SGSI de ABC S.A. Será responsabilidad también de la alta dirección asignar los roles, responsabilidades y autoridades suficientes para la debida protección de la información y deberá participar activamente en las revisiones anuales del SGSI.

6.7.2 Director de Tecnología.

Será responsabilidad del director de tecnología gestionar la implementación de los controles técnicos asociados al SGSI, aprobar y revisar el procedimiento de respuesta a

incidentes de seguridad de la información y coordinar el grupo de respuesta a incidentes de seguridad.

6.7.3 Oficial de Seguridad de la Información.

Será responsabilidad del Oficial de Seguridad: Garantizar que los procesos y procedimientos necesarios para el SGSI sean establecidos, implementados y mantenidos, gestionar la toma de conciencia sobre seguridad de la información en todos los niveles de la organización, gestionar la medición de las métricas de desempeño del SGSI y comunicarla oportunamente a la Alta Dirección, gestionar la debida instrucción y formación para los propietarios de los riesgos con el fin de que entiendan sus responsabilidades con el SGSI de **ABC S.A** y las ejecuten.

6.7.4 Comité de Seguridad de la Información

Es responsabilidad del comité de seguridad generar las políticas general y específicas de la seguridad de la información, aprobar la metodología de análisis de riesgo o los cambios sobre ella que se requieran dentro del proceso de mejora continua, asesorar a la alta dirección en la toma de decisiones con respecto al nivel de riesgo aceptable de ABC S.A. Analizar las lecciones aprendidas que se desprenden de la gestión de incidentes de seguridad de la información, y los indicadores establecidos para medir la eficacia del cumplimiento de los objetivos de seguridad de la información.

6.7.5 Coordinador de Sistemas

El coordinador de sistemas tendrá bajo su responsabilidad la implementación de los controles técnicos definidos dentro de los planes de tratamiento de riesgo, para esto deberá delegar apropiadamente las tareas requeridas dentro de su equipos.

6.7.6 Ingeniero de Soporte

Es el encargado de implementar los controles de acceso lógicos a los activos de información que hacen parte del alcance del SGSI y todos aquellos controles técnicos adicionales que el Coordinador de Sistemas disponga.

6.7.7 Ingeniero de Mantenimiento

Es el encargado de implementar los controles relacionados con la toma de copias de respaldo de los activos de información que hacen parte del alcance del SGSI y todos aquellos controles técnicos adicionales que el Coordinador de Sistemas disponga.

6.8 Metodología de Análisis de Riesgo

El análisis de riesgo de **ABC S.A** estará compuesto de cuatro etapas fundamentales:

- Inventario de Activos
- Interdependencias de Activos
- Valoración de Activos
- Cálculo del Riesgo

6.8.1 Inventario de Activos

Esta fase tiene como objetivo listar, clasificar e identificar el propietario de todos los activos de información que hacen parte de el proceso o servicio que se va a analizar.

De esta manera, el inventario de activos estará compuesto de 3 actividades como se muestra en la siguiente gráfica:

Ilustración 6 Actividades del Inventario de Activos

6.8.1.1 Listado de Activos

En esta primera actividad se listarán todos los activos de información, entendiendo como activo de información cualquier dato, servicio, aplicación, equipo, soporte de información, equipamento auxiliar, red de comunicación, instalación, clave criptográfica, o persona que almacene, manipule, procese, transporte, o genere información relacionada con el proceso, servicio o sistema de información objeto de análisis.

Debe tenerse en cuenta que esta lista es exhaustiva, es decir, deben indentificarse todos los activos que participan en el proceso.

6.8.1.2 Clasificación de Activos

Una vez se cuente con el listado completo de activos de información estos deberán ser clasificados de acuerdo a las siguientes categorías:

- Servicios
- Aplicaciones Informáticas
- Equipos Informáticos
- Soportes de Información
- Equipamiento Auxiliar
- Redes de Comunicaciones
- Instalaciones
- Personas

Estas categorías corresponden exactamente a las estipuladas por la metodología Magerit – versión 3.0, libro II – "Catálogo de Elementos".

6.8.1.3 Asignación de propietario

En esta actividad, ya habiendo obtenido una lista clasificada de activos, se deberá asignar un propietario a cada activo de información.

De esta manera, al finalizar el inventario de activos deberá contarse con una tabla que tendrá la siguiente estructura (la información contenida se presenta a manera de ejemplo):

Categoría	Activo	Propietario
Hardware	Servidor de Bases de Datos	Director de Tecnología
Datos	Base de Datos de Clientes	Director de Call Center

Tabla 3 Ejemplo de Tabla de Inventario de Activos

6.8.2 Interdependencia Entre Activos

Para determinar la interdependencia entre los activos, se tendrá en cuenta lo que define la metodología Magerit: "los activos vienen a formar árboles o grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en la estructura o "*superiores"* depende de los activos que se encuentran mas abajo, o "*inferiores"*...Se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de segu-ridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras pala-bras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. Informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores "

En este sentido, deberán primero determinarse, dentro del inventario ya realizado, los activos que tienen la característica de *no ser activos inferiores para ningún otro activo que haga parte del inventario*.

Llamaremos a este conjunto de activos, S que se identifica como:

$$S = \{ x \mid x > y, \forall y \in A\}$$

Donde A es el conjunto de activos e "y" un elemento de A.

Puede observarse que S es un subconjunto de A, este subconjunto de activos será utilizado para asignar a cada uno de los activos de A su activo superior, viéndo la interdependencia como un arbol o grafo podemos resumir, que a cada activo del inventario se le asignará su correspondiente nodo superior o raiz principal a la que pertenece.

Una vez terminado el análisis de interdependencias, se obtendrá una tabla como la siguiente:

Categoria	Activo	Activo Superior
Hardware	Servidor de Correo	Correos Electrónicos
Hardware	Firewall	Atención al Cliente

Tabla 4 Ejemplo Tabla de Interdependencias

6.8.3 Valoración de Activos

6.8.3.1 Valoración de Activos Superiores

Ya teniento el inventario de activos y sus interdependencias, se debe proceder a asignar un valor para cada activo que pertenezca al conjunto S de activos superiores, para lo cual se utilizará lo descrito en la metodología Magerit, libro III, numeral 2.1, es decir se deberá asignar un valor a cada activo en las siguientes dimensiones:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad
- Trazabilidad

Teniendo en cuenta la siguiente escala de valoración para cada una de las dimensiones:

Valor	Criterio
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Tabla 5 Valoración de las Dimensiones de Seguridad

Para efectos prácticos se construirá una tabla que contenga la totalidad de los activos superiores y se asignará a cada uno de ellos un valor del rango 1-10 en cada una de sus 5 dimensiones de seguridad, de manera que al final deberá obtenerse una tabla como la que se describe a continuación:

Categoria	Activo (Perteneciente a S)	A	C	I	D	T
Hardware	Correos Electrónicos	10	8	10	6	7
Hardware	Atención al Cliente	6	6	5	10	6

Tabla 6 Ejemplo Valoración Activos Superiores

6.8.3.2 Valoración General de Activos.

Para la valoración de la totalidad de los activos, se tendrá como regla que el valor de los activos superiores deberá acumularse en los activos inferiores, es decir que el valor de cada activo será el valor de su activo superior.

De esta manera deberá completarse una como la que se muestra en el siguiente ejemplo:

Categoria	Activo	Activo Superior	A	C	I	D	T
Hardware	Servidor de Correo	Correos Electrónicos	10	8	10	6	7
Hardware	Firewall	Atención al Cliente	6	6	5	10	6
Hardware	Router de Internet	Atención al Cliente	6	6	5	10	6

Tabla 7 Ejemplo Tabla Valoración de Activos

Dicha tabla representará la valoración final de los activos de información de ABC S.A.

6.8.4 Cálculo de Riesgos

Para el cálculo del riesgo se llevarán a cabo las siguientes etapas:

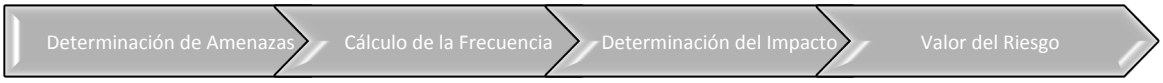


Ilustración 7 Actividades Para Calcular el Riesgo

6.8.4.1 Determinación de Amenazas

En esta actividad se listarán las posibles amenazas que pueden afectar cada uno de los activos que hacen parte del inventario. Se tendrán en cuenta situaciones como accidentes, errores, amenazas intencionales y no intencionales de acuerdo a lo establecido en el catalogo de amenazas del libro 2 de Magerit.

La siguiente tabla resume las amenazas propuestas por Magerit y su clasificación:

Tipo de Amenaza	Amenaza
Desastres Naturales	Fuego
	Daños Por Agua
	Desastres Naturales
De Origen Industrial	Fuego
	Daños Por Agua
	Desastres Industriales
	Contaminación Mecánica
	Contaminación Electromagnética
	Avería de Orígen Físico o Lógico
	Corte del Suministro Eléctrico
	Condiciones Inadecuadas de Temperatura o Humedad
	Fallo de Servicios de Comunicaciones
	Interrupción de Otros Servicios y Suministros Esenciales
	Degradación de los Soportes de Almacenamiento de la Información
	Emanaciones Electromagnéticas
Errores y Fallos No Intencionados	Errores de los Usuarios
	Errores del Administrador
	Errores de Monitorización
	Errores de Configuración
	Deficiencias en la Organización
	Difusión de Software Dañino
	Errores de Re-encaminamiento
	Errores de Secuencia
	Escapes de Información
	Alteración Accidental de la Información
	Destrucción de Información
	Fugas de Información
	Vulnerabilidades de los Programas
	Errores de Mantenimiento/ Actualización de Programas
	Errores de Mantenimiento / Actualización de Equipos
	Caida del Sistema por agotamiento de Recursos
	Pérdida de Equipos
	Indisponibilidad del Personal
Ataques Intencionados	Manipulación de los Registros de Actividad

Tipo de Amenaza	Amenaza
	Manipulación de la Configuración
	Suplantación de la Identidad de Usuario
	Abuso de Privilegios de Acceso
	Uso no Previsto
	Difusión de software Dañino
	Re-encaminamiento de Mensajes
	Alteración de Secuencia
	Acceso no Autorizado
	Análisis de Tráfico
	Repudio
	Interceptación de Información
	Modificación Delierada de la Información
	Destrucción de Información
	Divulgación de Información
	Manipulación de Programas
	Manipulación de los Equipos
	Denegación de Servicio
	Robo
	Ataque Destructivo
	Ocupación Enemiga
	Indisponibilidad del Personal
	Extorsión
	Ingenieria Social

Tabla 8 Amenazas Propuestas por Magerit

6.8.4.2 Cálculo de la Frecuencia

Una vez listadas todas las amenazas que pueden afectar los activos de ABC S.A. se debe determinar la frecuencia de ocurrencia de cada amenaza de acuerdo a la siguiente tabla:

Probabilidad de Ocurrencia		
Cualitativo	**Ocurrencia**	**Probabilidad Anual**
MA	183	0,501369863
A	24	0,065753425
M	12	0,032876712
B	6	0,016438356
MB	1	0,002739726

Tabla 9 Valores de Probabilidad de Ocurrencia

Para el caso de ABC S.A. se tendrá en cuenta la ocurrencia anual de cada amenaza, por ejemplo una frecuencia calificada como Muy Alta (MA) representará una ocurrencia de 183 veces al año lo que dará un valor cualitativo de Probabilidad Anual de 0,5.

6.8.4.3 Determinación del Impacto

Luego de determinar las posibles amenazas y su frecuencia, deberá estimarse el impacto que tendrá dicha amenaza sobre cada una de las dimensiones de seguridad de cada activo, de acuerdo a la siguiente escala:

Impacto
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%

Tabla 10 Valores Posibles Para el Impacto

6.8.4.4 Valor del Riesgo

Para el cálculo del valor del riesgo, se usará la siguiente Ecuación:

$$Riesgo = Valor\ del\ Activo\ en\ Cada\ Dimensión\ X\ Impacto\ X\ Frecuencia$$

a. Análisis de Riesgo Intrínseco o Inherente.
   Una vez realizado el análisis de amenazas se calculará el riesgo intrínseco de acuerdo a la siguiente fórmula:

$$Riesgo\ Inherente = Valor\ del\ Activo\ X\ Vulnerabilidad\ X\ Impacto$$

Es importante resaltar que exisitirá un valor de riesgo por cada dimensión de seguridad, de esta manera se encontrarán 5 valores de riesgo para cada activo como se muestra en la siguiente tabla:

	Frecuencia	Activo				
		A	C	I	D	T
Amenaza		Valor - Autenticidad	Valor - Confidencialidad	Valor Integridad	Valor Disponibilidad	Valor Trazabilidad
Nombre de la Amenaza	Valor de la Frecuencia	Valor Impacto (%)	Valor Impacto (%)	Valor Impacto (%)	Valor Impacto (%)	Valor Impacto (%)
		Valor de Riesgo	**Valor de Riesgo**	**Valor de Riesgo**	**Valor de Riesgo**	**Valor de Riesgo**

Tabla 11 Tabla Para el Cálculo del Riesgo

Finalmente deberá obtenerse una matriz con los activos en las columnas y las amenazas en las filas en donde cada intersección estará compuesta por la estructura presentada en la tabla anterior.

El siguiente es un fragmento a modo de ejemplo de la matriz final resultante del análisis de riesgo.

Tipo de Amenaza	Amenaza	Frecuencia	Servidor de Directorio Activo					Servidor de E-Client				
			A	C	I	D	T	A	C	I	D	T
			6	6	5	10	6	7	10	10	10	7
Desastres Naturales	Fuego	MB	0%	0%	0%	100%	0%	0%	0%	0%	100%	0%
			0	**0**	**0**	**0,027**	**0**	**0**	**0**	**0**	**0,027**	**0**
	Daños Por Agua	MB	0%	0%	0%	100%	0%	0%	0%	0%	100%	0%
			0	**0**	**0**	**0,027**	**0**	**0**	**0**	**0**	**0,027**	**0**
	Desastres Naturales	MB	0%	0%	0%	100%	0%	0%	0%	0%	100%	0%
			0	**0**	**0**	**0,027**	**0**	**0**	**0**	**0**	**0,027**	**0**

Tabla 12 Fragmento de la Matriz Final del Análisis de Riesgo - Ejemplo

6.9 Declaración de Aplicabilidad

La siguiente tabla muestra la declaración de aplicabilidad del SGSI de **ABC S.A**.

Sección	Control	Aplica	Justificación
A.5	Políticas de Seguridad		
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	Aplica	La alta dirección ha reconocido la necesidad de definir, aprobar, publicar y comunicar a los empleados, terceros y contratistas, políticas para la seguridad de la información.
A.5.1.2	Revisión de las políticas para la seguridad de la información	Aplica	ABC S.A. Reconoce la necesidad de revisar periódicamente las políticas de seguridad de la información como un factor de éxito en la mejora continua del SGSI.
A.6	Organización de la Seguridad de la Información		
A.6.1	Organización Interna		

A.6.1.1	Roles y Responsabilidades de Seguridad de la Información.	Aplica	Hasta el momento, ABC S.A. no había asignado Roles y Responsabilidades de Seguridad de la Información. La organización reconoce esta necesidad para poder gestionar todos los aspectos de la seguridad de la información.
A.6.1.2	Separación de deberes	Aplica	Por la naturaleza y criticidad del negocio de ABC S.A. se reconoce como necesario evitar la modificación no intencional o no autorizada de los activos de la organización.
A.6.1.3	Contacto con las autoridades	Aplica	La naturaleza de los fraudes y ataques al sector bancario muestran la necesidad de ABC S.A. de estar en contacto con autoridades como la policía, Grupos de Respuesta a Emergencias (CERT), etc.
A.6.1.4	Contacto con grupos de interés especial	Aplica	La tecnología utilizada para los procesos misionales de ABC S.A. puede ser vulnerable a nuevos ataques, es necesario pertenecer a grupos de interés especial como por ejemplo los boletines de seguridad de los fabricantes.
A.6.1.5	Seguridad de la información en la gestión de proyectos	Aplica	Dentro del alcance del SGSI se adelantan proyectos como el desarrollo de software misional, razón por la cual deben tenerse en cuenta los aspectos de seguridad de la información en la gestión de proyectos.
A.6.2	Dispositivos móviles y teletrabajo		
A.6.2.1	Política para dispositivos móviles	Aplica	El uso de dispositivos móviles para acceder a la información que hace parte del SGSI ha tomado auge en

			ABC S.A. y está autorizada por la alta dirección. Es necesario por lo tanto establecer una política para dispositivos móviles.
A.6.2.2	Teletrabajo	Aplica	El teletrabajo está autorizado e incluye el acceso a activos de información que hacen parte del SGSI, se requiere por lo tanto establecer una política que soporte las medidas de seguridad que se requieren para proteger la información.
A.7	Seguridad de los Recursos Humanos		
A.7.1	Antes de asumir el empleo		
A.7.1.1	Selección	Aplica	Los empleados y contratistas tendrán acceso a información confidencial por lo que este control es necesario.
A.7.1.2	Términos y condiciones del empleo	Aplica	Los empleados y contratistas tendrán acceso a información confidencial por lo que este control es necesario.
A.7.2	Durante el empleo		
A.7.2.1	Responsabilidades de la dirección	Aplica	La alta dirección reconoce que la Información es responsabilidad de todos el personal que interactúa con ella, por lo tanto reconoce la necesidad de comunicar a todo el personal la necesidad y obligatoriedad de proteger la información de acuerdo a lo establecido en las políticas.
A.7.2.2	Concienciación sobre la seguridad de la información, la educación y la formación	Aplica	ABC S.A. entiende como necesario generar conciencia en el personal como factor de éxito en la protección de la seguridad de la información.
A.7.2.3	Proceso disciplinario	Aplica	Este control aplica para ABC S.A. Teniendo en cuenta la criticidad de la información que maneja el personal de Call Center y los empleados en general.

A.7.3	Terminación y cambio de empleo		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Aplica	Este control aplica para ABC S.A. Teniendo en cuenta la criticidad de la información que maneja el personal de Call Center y los empleados en general. Adicionalmente se ha visto una alta rotación en el personal operativo por lo que este control se hace fundamental.
A.8	Gestión de Activos		
A.8.1	Responsabilidad de los activos		
A.8.1.1	Inventario de Activos	Aplica	Esto hace parte de la metodología de análisis de riesgo aprobada por ABC S.A.
A.8.1.2	Propietario de los activos	Aplica	Esto hace parte de la metodología de análisis de riesgo aprobada por ABC S.A.
A.8.1.3	Uso aceptable de los activos	Aplica	ABC S.A. reconoce como necesario establecer reglas para el uso aceptable de activos.
A.8.1.4	Devolución de los activos	Aplica	Los activos de información de propiedad de ABC S.A. Deben ser utilizados solamente para fines laborales y en caso de terminación de contrato laboral deben ser devueltos a la organización.
A.8.2	Clasificación de la información		
A.8.2.1	Clasificación de la información	Aplica	Teniendo en cuenta que la información que maneja ABC S.A. incluye datos personales y potencialmente confidenciales como números de productos bancarios, esta debe ser clasificada con el fin de poder determinar adecuadamente el manejo que debe dársele.
A.8.2.2	Etiquetado de la información	Aplica	Con el fin de poder dar un manejo adecuado a la

			información, esta debe ser etiquetada de acuerdo a los niveles de clasificación definidos en la política de Clasificación de Información.
A.8.2.3	Manejo de activos	Aplica	Con el fin de que todo el personal dé el manejo adecuado a los activos de información de acuerdo a su clasificación, deben implementarse procedimientos que dejen claro este manejo.
A.8.3	Manejo de medios		
A.8.3.1	Gestión de medios removibles	Aplica	El uso de dispositivos removibles está autorizado por lo cual es indispensable proteger de manera adecuada la información que contienten.
A.8.3.2	Disposición de los medios	Aplica	Por la naturaleza del negocio de ABC S.A., existe una alta rotación de tecnologías, incluyendo el hecho de que los equipos de escritorio son arrendados, se requiere un procedimiento formal para la disposición segura de los medios.
A.8.3.3	Transferencia de medios físicos	No aplica	Dentro de los procesos que hacen parte del alcance del SGSI no se realiza transferencia de medios físicos.
A.9	Control de accesos		
A.9.1	Requisitos del negocio para el control de acceso		
A.9.1.1	Política de control de acceso	Aplica	Teniendo en cuenta que la información que maneja ABC S.A. debe ser clasificada en diferentes niveles, es indispensable que el acceso a la misma esté basado en el principio de “necesidad de conocer”.

A.9.1.2	Acceso a redes y servicios en red	Aplica	Es necesario para proteger la Información de ABC S.A. proveer acceso a los recursos de red y servicios solamente a las personas o procesos que lo requieran para el correcto funcionamiento del negocio.
A.9.2	Gestión de acceso de usuarios		
A.9.2.1	Registro y cancelación de usuarios	Aplica	Existe una alta rotación de personal en las áreas, este control aplica para la operación de ABC S.A.
A.9.2.2	Suministro de acceso de usuarios	Aplica	Teniendo en cuenta que los usuarios tienen distintos niveles de acceso a la información, este control es requerido para proteger la información.
A.9.2.3	Gestión de derechos de acceso privilegiado	Aplica	ABC S.A. administra sus propios activos y sistemas de información, esto hace que se requiera gestionar los derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Aplica	ABC S.A. reconoce la información secreta de autenticación como un activo crítico de información, razón por la cual decide implementar este control.
A.9.2.5	Revisión de los derechos de acceso de usuarios	Aplica	Este control se requiere como una segunda validación al proceso de registro y cancelación de usuarios
A.9.2.6	Retiro o ajuste de los de derechos de acceso	Aplica	Se requiere remover los derechos de acceso a la información a usuarios que terminan su contrato laboral o que cambian de función dentro de la organización.
A.9.3	Responsabilidades de los usuarios		
A.9.3.1	Uso de información de autenticación secreta	Aplica	ABC S.A. utiliza usuarios y contraseñas para acceder a los sistemas y reconoce la información secreta de autenticación como un activo

			crítico de información, razón por la cual decide implementar este control.
A.9.4	Control de acceso al sistema y aplicaciones		
A.9.4.1	Restricciones de acceso a la información	Aplica	Se requiere para proteger los activos de información dentro del alcance del SGSI que se cumpla el principio de "necesidad de acceder".
A.9.4.2	Procedimiento de ingreso seguro	Aplica	ABC S.A. reconoce este control como una implementación válida para proteger la información de accesos no autorizados y para lograr trazabilidad del acceso de usuarios a los sistemas de información.
A.9.4.3	Sistema de gestión de contraseñas	Aplica	Es requerido que se use un sistema de gestión contraseñas con el fin de garantizar la calidad de las mimas, por otro lado ABC S.A. cuenta con un Directorio Activo por medio del cual se puede implementar una gestión robusta de contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	Aplica	ABC S.A. Reconoce como indispensable este control para proteger la información y los registros de acceso.
A.9.4.5	Control de acceso a códigos fuente de programas	Aplica	Este control aplica teniendo en cuenta que ABC S.A. realiza desarrollos internos para sistemas de información que hacen parte del alcance del SGSI.
A.10	Criptografía		
A.10.1	Controles criptográficos		
A.10.1.1	Política de uso de controles criptográficos	Aplica	Este control aplica ya que se usa el protocolo https para el acceso seguro a las aplicaciones web.
A.10.1.2	Gestión de llaves	Aplica	Este control aplica ya que se usa el protocolo https para el acceso seguro a las

			aplicaciones web.
A.11	Seguridad física y del entorno		
A.11.1	Áreas seguras		
A.11.1.1	Perímetro de seguridad física	Aplica	Toda la operación que hace parte del alcance del SGSI, se realiza en oficinas físicas de propiedad e ABC S.A. De tal manera que la mayoría de los activos de información se encuentran físicamente en dichas oficinas.
A.11.1.2	Controles de acceso físicos	Aplica	Toda la operación que hace parte del alcance del SGSI, se realiza en oficinas físicas de propiedad e ABC S.A. De tal manera que la mayoría de los activos de información se encuentran físicamente en dichas oficinas.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Aplica	Toda la operación que hace parte del alcance del SGSI, se realiza en oficinas físicas de propiedad e ABC S.A. De tal manera que la mayoría de los activos de información se encuentran físicamente en dichas oficinas.
A.11.1.4	Protección contra las amenazas externas y ambientales	Aplica	Toda la operación que hace parte del alcance del SGSI, se realiza en oficinas físicas de propiedad e ABC S.A. De tal manera que la mayoría de los activos de información se encuentran físicamente en dichas oficinas.
A.11.1.5	Trabajo en áreas seguras	Aplica	Toda la operación que hace parte del alcance del SGSI, se realiza en oficinas físicas de propiedad e ABC S.A. De tal manera que la mayoría de los activos de información se encuentran físicamente en dichas oficinas.
A.11.1.6	Áreas de despacho y carga	Aplica	Toda la operación que hace parte del alcance del SGSI, se realiza en oficinas físicas de

			propiedad e ABC S.A. De tal manera que la mayoría de los activos de información se encuentran físicamente en dichas oficinas.
A.11.2	Equipos		
A.11.2.1	Ubicación y protección de equipos	Aplica	La mayor parte de la información que hace parte del alcance del SGSI se maneja por medio de equipos de cómputo o servidores. Este control debe ser implementado.
A.11.2.2	Servicios de suministro	Aplica	La mayor parte de la información que hace parte del alcance del SGSI se maneja por medio de equipos de cómputo o servidores. Este control debe ser implementado.
A.11.2.3	Seguridad del cableado	Aplica	La mayor parte de la información que hace parte del alcance del SGSI se maneja por medio de equipos de cómputo o servidores. Este control debe ser implementado.
A.11.2.4	Mantenimiento de los equipos	Aplica	La mayor parte de la información que hace parte del alcance del SGSI se maneja por medio de equipos de cómputo o servidores. Este control debe ser implementado.
A.11.2.5	Retiro de activos	Aplica	La mayor parte de la información que hace parte del alcance del SGSI se maneja por medio de equipos de cómputo o servidores. Este control debe ser implementado.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Aplica	Este control aplica ya que el personal técnico tiene acceso remoto a los activos de ABC S.A. y trabajan con equipos portátiles que pueden llevar

			fuera de las instalaciones de ABC S.A.
A.11.2.7	Disposición segura o reutilización de equipos	Aplica	Por la naturaleza del negocio de ABC S.A., existe una alta rotación de tecnologías, incluyendo el hecho de que los equipos de escritorio son arrendados, se requiere un procedimiento formal para la disposición segura de los medios.
A.11.2.8	Equipo de usuario desatendido	Aplica	Este control aplica ya que una buena parte de la información que hace parte del SGSI es accedida desde los equipos de usuarios.
A.11.2.9	Política de escritorio limpio y pantalla limpia	Aplica	Este control aplica ya que una buena parte de la información que hace parte del SGSI es accedida desde los equipos de usuarios.
A.12	Seguridad de las operaciones		
A.12.1	Procedimientos operacionales y responsabilidades		
A.12.1.1	Procedimientos de operación documentados	Aplica	Todas las actividades operacionales son ejecutadas por el personal de ABC S.A. Por esto se reconoce como necesaria la implementación de este control.
A.12.1.2	Gestión de cambios	Aplica	La naturaleza del negocio hace que labores de mantenimiento, instalación de parches, nuevas versiones de software y hardware, etc. sean llevadas a cabo. Se requiere en aras de proteger la disponibilidad que este control sea implementado.
A.12.1.3	Gestión de la capacidad	Aplica	Dado que la información está soportada y apoyada por equipos tecnológicos, y que se espera un crecimiento en cuanto a la cantidad de clientes, este control es necesario.

A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Aplica	Este control aplica teniendo en cuenta que se hacen desarrollos internos.
A.12.2	Protección contra códigos maliciosos		
A.12.2.1	Controles contra códigos maliciosos	Aplica	Los sistemas operativos utilizados para la operación normal de ABC S.A. Son susceptibles a contaminación por códigos maliciosos, este control, por lo tanto, es requerido.
A.12.3	Copias de respaldo		
A.12.3.1	Respaldo de la información	Aplica	Este control se reconoce como indispensable ante la respuesta a posibles incidentes de seguridad de la información.
A.12.4	Registro y seguimiento		
A.12.4.1	Registro de eventos	Aplica	Es un requerimiento del negocio tener trazabilidad de la actividad de los usuarios sobre sus activos de información.
A.12.4.2	Protección de la información de registro	Aplica	Es un requerimiento del negocio tener trazabilidad de la actividad de los usuarios sobre sus activos de información.
A.12.4.3	Registros del administrador y del operador	Aplica	Es un requerimiento del negocio tener trazabilidad de la actividad de los usuarios sobre sus activos de información.
A.12.4.4	Sincronización del relojes	Aplica	Para efectos legales, la hora de los dispositivos informáticos debe estar sincronizada con la hora legal colombiana, dicha hora es provista por el servidor NTP de la Superintendencia de Industria y Comercio.
A.12.5	Control de software operacional		
A.12.5.1	Instalación de software en sistemas operativos	Aplica	ABC S.A. reconoce que los sistemas operativos deben protegerse para evitar contaminación por malware,

			implantación de nuevas vulnerabilidades, o inactivación de controles técnicos.
A.12.6	Gestión de la vulnerabilidad técnica		
A.12.6.1	Gestión de las vulnerabilidades técnicas	Aplica	Los productos de software utilizados para la operación de ABC S.A. son productos que están expuestos, por naturaleza, a múltiples vulnerabilidades y que requieren ser gestionadas.
A.12.6.2	Restricciones sobre la instalación de software	Aplica	ABC S.A. reconoce que la instalación no controlada de software puede ocasionar contaminación por malware, implantación de nuevas vulnerabilidades, o inactivación de controles técnicos.
A.12.7	Consideraciones sobre auditorías de sistemas de información		
A.12.7.1	Controles de auditoría de sistemas de información	Aplica	La realización de auditorías técnicas es una necesidad reconocida por la organización, por lo tanto este control es necesario para prevenir indisponibilidad de la operación.
A.13	Seguridad en las comunicaciones		
A.13.1	Gestión de la seguridad de las redes		
A.13.1.1	Controles de redes	Aplica	Todos los servicios que hacen parte del alcance del SGSI de ABC S.A. utilizan una red de datos interna administrada por la organización. Es necesaria la implementación de este control.
A.13.1.2	Seguridad de los servicios de red	Aplica	Todos los servicios que hacen parte del alcance del SGSI de ABC S.A. utilizan una red de datos interna administrada por la organización. Es necesaria la implementación de este control.

A.13.1.3	Separación en las redes	Aplica	Dado que ABC S.A. cuenta con infraestructura tecnológica que hace parte y apoya los servicios que hacen parte del alcance del SGSI, es necesario implementar una correcta segregación de redes, que establezca varias capas de seguridad (pej, presentación, aplicación y datos).
A.13.2	Transferencia de información		
A.13.2.1	Políticas y procedimientos de transferencia de información	Aplica	Dentro de la operación de ABC S.A. suele transferirse información por correo electrónico, con clientes y proveedores, este control requiere ser implementado.
A.13.2.2	Acuerdos sobre transferencia de información	Aplica	Dentro de la operación de ABC S.A. suele transferirse información por correo electrónico, con clientes y proveedores, este control requiere ser implementado.
A.13.2.3	Mensajería electrónica	Aplica	Dentro de la operación de ABC S.A. suele transferirse información por correo electrónico, con clientes y proveedores, este control requiere ser implementado.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Aplica	Este control aplica para los empleados y contratistas que trabajan para ABC S.A.
A.14	Adquisición, desarrollo y mantenimiento de sistemas		
A.14.1	Requisitos de seguridad de los sistemas de información		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Aplica	Aplica ya el alcance del SGSI cubre precisamente los sistemas de información de ABC S.A.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Aplica	Este control aplica dado que se tienen publicados servicios en internet.
A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones	Aplica	Este control debe implementarse teniendo en cuenta el tipo de información que ABC S.A maneja.

A.14.2	Seguridad en los procesos de desarrollo y de soporte		
A.14.2.1	Política de desarrollo seguro	Aplica	Aplica ya que uno de los sistemas misionales que además hace parte del alcance del SGSI es desarrollado y mantenido internamente.
A.14.2.2	Procedimientos de control de cambios en sistemas	Aplica	Aplica ya que uno de los sistemas misionales que además hace parte del alcance del SGSI es desarrollado y mantenido internamente.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Aplica	Aplica ya que uno de los sistemas misionales que además hace parte del alcance del SGSI es desarrollado y mantenido internamente y dentro de ese mantenimiento se desarrollan nuevas versiones y parches.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Aplica	Aplica ya que uno de los sistemas misionales que además hace parte del alcance del SGSI es desarrollado y mantenido internamente.
A.14.2.5	Principios de construcción de los sistemas seguros	Aplica	Aplica ya que uno de los sistemas misionales que además hace parte del alcance del SGSI es desarrollado y mantenido internamente.
A.14.2.6	Ambiente de desarrollo seguro	Aplica	Aplica ya que uno de los sistemas misionales que además hace parte del alcance del SGSI es desarrollado y mantenido internamente.
A.14.2.7	Desarrollo contratado externamente	No Aplica	Este control no aplica porque no se contrata desarrollo por terceros.
A.14.2.8	Pruebas de seguridad de sistemas	Aplica	Aplica ya que uno de los sistemas misionales que además hace parte del alcance del SGSI es desarrollado y mantenido internamente.
A.14.2.9	Pruebas de aceptación de sistemas	Aplica	Aplica ya que uno de los sistemas misionales que además hace parte del alcance del SGSI es desarrollado y

			mantenido internamente.
A.14.3	Datos de prueba		
A.14.3.1	Protección de los datos de prueba	Aplica	Este control aplica ya que en los ambientes de desarrollo se requieren hacer pruebas y en muchos casos se usa información de producción en dichas pruebas.
A.15	Relaciones con los proveedores		
A.15.1	Seguridad de la información en las relaciones con proveedores		
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Aplica	Este control debe ser implementado porque en el flujo de información que hace parte de los servicios incluidos en el alcance del SGSI participan varios proveedores que en mayor o menor medida pueden llegar a acceder a información.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Aplica	Este control debe ser implementado porque en el flujo de información que hace parte de los servicios incluidos en el alcance del SGSI participan varios proveedores que en mayor o menor medida pueden llegar a acceder a información.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Aplica	Este control debe ser implementado porque en el flujo de información que hace parte de los servicios incluidos en el alcance del SGSI participan varios proveedores que en mayor o menor medida pueden llegar a acceder a información.
A.15.2	Gestión de la prestación de servicios de proveedores		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Aplica	Este control debe ser implementado porque en el flujo de información que hace parte de los servicios incluidos en el alcance del

			SGSI participan varios proveedores que en mayor o menor medida pueden llegar a acceder a información.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	Aplica	Este control debe ser implementado porque en el flujo de información que hace parte de los servicios incluidos en el alcance del SGSI participan varios proveedores que en mayor o menor medida pueden llegar a acceder a información. Adicionalmente, algunos de ellos, como es el caso de los Proveedores de Servicios de Internet, los cambios sobre su infraestructura pueden afectar la disponibilidad de los servicios de ABC S.A.
A.16	Gestión de incidentes de seguridad de la información		
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información		
A.16.1.1	Responsabilidades y procedimientos	Aplica	La alta dirección reconoce la necesidad de gestionar los incidentes de seguridad para mitigar el impacto de los riesgos que no serán tratados. En este sentido es necesario establecer responsabilidades y procedimientos al respecto.
A.16.1.2	Reporte de eventos de seguridad de la información	Aplica	La alta dirección reconoce la necesidad de gestionar los incidentes de seguridad para mitigar el impacto de los riesgos que no serán tratados. En este sentido es establecer las vías para reportar los eventos de seguridad de la información, estas vías o medios deben ser debidamente comunicados a todas las partes interesadas.
A.16.1.3	Reporte de debilidades de seguridad de la información	Aplica	Dentro de la gestión de incidentes, es necesario que todo el personal esté debidamente capacitado y

			concienciado para reconocer y reportar las posibles debilidades de seguridad de la información.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Aplica	La alta dirección reconoce que es necesaria la evaluación de eventos de seguridad que puedan convertirse en incidentes y su tratamiento adecuado.
A.16.1.5	Respuesta a incidentes de seguridad de la información	Aplica	ABC S.A. reconoce este control como necesario para mitigar el impacto que se desprende de los incidentes de seguridad de la información.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Aplica	Este control es aplicable para la organización en el sentido que esta reconoce la revisión de lecciones aprendidas como un factor de éxito en la mejora continua del SGSI.
A.16.1.7	Recopilación de evidencia	Aplica	Este control se reconoce como necesario pues es un requerimiento particular de los clientes Bancarios.
A.17	Aspectos de la seguridad de la información de la gestión de continuidad de negocio		
A.17.1	Continuidad de seguridad de la información		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Aplica	Por requerimiento de los clientes bancarios y como parte de la estrategia corporativa se ha requerido implementar planes de continuidad de negocio. En este sentido ABC S.A. Reconoce como necesario planificar la continuidad de la seguridad de la información en momentos de emergencia, crisis o contingencia.
A.17.1.2	Implantación de la continuidad de la seguridad de la información	Aplica	Por requerimiento de los clientes bancarios y como parte de la estrategia corporativa se ha requerido implementar planes de

			continuidad de negocio. En este sentido ABC S.A. Reconoce como necesario implantación de la continuidad de la seguridad de la información en momentos de emergencia, crisis o contingencia.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Aplica	Por requerimiento de los clientes bancarios y como parte de la estrategia corporativa se ha requerido implementar planes de continuidad de negocio. En este sentido ABC S.A. Reconoce como necesario verificar, revisar y evaluar de la continuidad de la seguridad de la información en momentos de emergencia, crisis o contingencia.
A.17.2	Redundancias		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Aplica	Dado el componente tecnológico que hace parte de los servicios misionales de ABC S.A. es requerido que se implemente este control
A.18	Cumplimiento		
A.18.1	Cumplimiento de requisitos legales y contractuales		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Aplica	Aplica y es necesaria su implementación. ABC S.A. quiere realizar todas su operaciones de acuerdo a los requisitos legales que le apliquen.
A.18.1.2	Derechos de propiedad intelectual (DPI)	Aplica	Aplica por estrategia de negocio y porque lo exige la Ley de Derechos de Autor.
A.18.1.3	Protección de registros	Aplica	Por exigencia de los clientes y por capacidad de reacción ante posibles incidentes que requieran interacción judicial. Se decide implementar este control.

A.18.1.4	Privacidad y protección de información de datos personales	Aplica	Aplica por estrategia de negocio y porque lo exige la Ley de Protección de Datos Personales.
A.18.1.5	Reglamentación de controles criptográficos	Aplica	Aplica, para ABC S.A. es estratégico estar alineado con cualquier reglamentación. Ley o buena práctica que trabaje en pro de la protección de su información.
A.18.2	Revisiones de seguridad de la información		
A.18.2.1	Revisión independiente de la seguridad de la información	Aplica	Las auditorías internas al SGSI son reconocidas como una necesidad dentro de la mejora continua del mismo.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Aplica	Aplica y es necesaria su implementación. ABC S.A. quiere realizar todas su operaciones de acuerdo a los requisitos legales que le apliquen.
A.18.2.3	Revisión del cumplimiento técnico	Aplica	Se reconoce como necesaria hacer una revisión del cumplimiento de los requerimientos en seguridad para los sistemas de información, ABC S.A. reconoce este control como necesario y debe ser incluido dentro de los planes de auditoría periódicas.

Tabla 13 Declaración de Aplicabilidad

7 ANÁLISIS DE RIESGOS

El análisis de riesgo fue ejecutado de acuerdo a lo establecido en la metodología de análisis de riesgo, detallada en el numeral 6.8 de esta memoria.

7.1 Inventario de Activos

La siguiente tabla contiene el inventario de activos que están dentro del alcance del SGSI de ABC S.A. De acuerdo a lo establecido en la metodología de análisis de riesgo propuesta para la organización.

Categoría	Activo	Propietario
Hardware	Servidor de Directorio Activo	Director de Tecnología
Hardware	Servidor de E-Client	Director de Tecnología
Hardware	Servidor de Antivirus	Director de Tecnología

Categoría	Activo	Propietario
Hardware	Servidor de Request Tracker	Director de Tecnología
Hardware	Servidor de Correo	Director de Tecnología
Hardware	Firewall	Director de Tecnología
Hardware	Router de Internet	Director de Tecnología
Hardware	Switch de Core	Director de Tecnología
Hardware	PCs de Agentes de Call Center	Director de Tecnología
Hardware	Pcs de Empleados Administrativos	Director de Tecnología
Hardware	Portátiles de Empleados de Tecnología	Director de Tecnología
Hardware	Portátiles de la Alta Dirección	Director de Tecnología
Aplicación	Sofware de Directorio Activo (Active Directory de Microsoft)	Director de Tecnología
Aplicación	Software E-Client	Director de Tecnología
Aplicación	Software Antivirus	Director de Tecnología
Aplicación	Software de Correo Electrónico	Director de Tecnología
Aplicación	Software Servidor Web	Director de Tecnología
Aplicación	Sistema Operativo del Directorio Activo	Director de Tecnología
Aplicación	Sistema Operativo del Servidor de Antivirus	Director de Tecnología
Aplicación	Sistema Operativo del Servidor E-Client	Director de Tecnología
Aplicación	Sistema Operativo del Servidor de Request Tracker	Director de Tecnología
Aplicación	Sistema Operativo de los Pc de agentes de Call Center	Director de Tecnología
Servicios	Canal de Internet	Director de Tecnología
Instalaciones	Centro de Cómputo	Director de Tecnología
Aplicación	Motor de Base de Datos de Request Tracker	Director de Tecnología
Aplicación	Motor de Base de Datos de E-client	Director de Tecnología
Soportes de Información	Cintas con Copias de Respaldo	Director de Tecnología
Personas	Proveedor de almacenamiento de Cintas	Director de Tecnología
Datos	Copias de Respaldo de Request Tracker	Director de Call Center
Datos	Copias de Respaldo de E-client	Director de Call Center
Datos	Base de Datos de E-client	Director de Call Center
Datos	Base de datos de Request Tracker	Director de Call Center
Datos	Información del Directorio Activo	Director de Call Center

Categoría	Activo	Propietario
Datos	Correos Electrónicos	Director de Call Center
Aplicación	Cliente de Correo Electrónico	Director de Tecnología
Datos	Código Fuente de E-client	Director de Call Center
Instalaciones	Oficinas de ABC S.A.	Director Administrativo y Financiero
Personas	Agentes de Call Center	Director de Call Center
Personas	Coordinador de Campañas Bancarias	Director de Call Center
Personas	Director de Call Center	Gerente General
Personas	Ingeniero de Mantenimiento	Director de Tecnología
Personas	Ingeniero de Soporte	Director de Tecnología
Personas	Coordinador de Sistemas	Director de Tecnología
Personas	Director de Tecnología	Gerente General
Personas	Coordinador de Talento Humano	Director de Recursos Humanos
Personas	Auxiliar de Nómina	Director de Recursos Humanos
Personas	Auxiliar de Selección	Director de Recursos Humanos
Personas	Director de Recursos Humanos	Gerente General
Personas	Desarrolladores	Director de Servicios de Factoría de Software
Personas	Coordinador de Desarrollo	Director de Servicios de Factoría de Software
Personas	Director de Servicios de Factoría de Software	Gerente General
Servicios	Internet	Director de Tecnología
Red	Red de Call Center	Director de Tecnología
Red	Red de Tecnología	Director de Tecnología
Red	Red de Área Administrativa	Director de Tecnología
Red	Red de Servidores	Director de Tecnología
Red	DMZ	Director de Tecnología
Equipamiento Auxiliar	Cableado Estructurad	Director de Tecnología
Equipamiento Auxiliar	Aire Acondicionado Centro de Cómputo	Director de Tecnología
Equipamiento Auxiliar	Biométrico de Acceso al Centro de Cómputo	Director de Tecnología
Equipamiento Auxiliar	Sistema Antiincendios	Director de Tecnología

Tabla 14 Inventario de Activos

7.2 Valoración de los Activos Superiores

La siguiente tabla enumera por extensión los activos superiores de ABC S.A. y les asigna un valor en cada una de sus dimensiones de seguridad de acuerdo a lo establecido en la metodología de riesgo aprobada por la organización.

Categoria	Activo	Dimensiones de Seguridad				
		A	C	I	D	T
Datos	Copias de Respaldo de Request Tracker	5	7	10	6	5
Datos	Copias de Respaldo de E-client	5	10	10	6	5
Datos	Base de Datos de E-client	7	10	10	10	7
Datos	Base de datos de Request Tracker	7	7	10	5	7
Datos	Correos Electrónicos	10	8	10	6	7
Datos	Código Fuente de E-client	4	3	8	2	3
Servicios	Atención al Cliente	6	6	5	10	6

Tabla 15 Activos Superiores de ABC S.A.

7.3 Interdependencia de los Activos

La siguiente tabla muestra el activo superior correspondiente a cada uno de los activos del inventario, tal y como lo pide la metodología de análisis de riesgo y de la cual se dio un ejemplo en la tabla 4 de este documento.

Categoria	Activo	Activo Superior
Hardware	Servidor de Directorio Activo	Atención al Cliente
Hardware	Servidor de E-Client	Base de Datos de E-client
Hardware	Servidor de Antivirus	Base de Datos de E-client
Hardware	Servidor de Request Tracker	Base de datos de Request Tracker
Hardware	Servidor de Correo	Correos Electrónicos
Hardware	Firewall	Atención al Cliente
Hardware	Router de Internet	Atención al Cliente
Hardware	Switch de Core	Atención al Cliente
Hardware	PCs de Agentes de Call Center	Atención al Cliente
Hardware	Pcs de Empleados Administrativos	Atención al Cliente
Hardware	Portátiles de Empleados de Tecnología	Base de Datos de E-client
Hardware	Portátiles de la Alta Dirección	Atención al Cliente
Aplicación	Sofware de Directorio Activo (Active Directory de Microsoft)	Atención al Cliente
Aplicación	Software E-Client	Base de Datos de E-client
Aplicación	Software Antivirus	Base de Datos de E-client
Aplicación	Software de Correo Electrónico	Correos Electrónicos
Aplicación	Software Servidor Web	Atención al Cliente

Categoria	Activo	Activo Superior
Aplicación	Sistema Operativo del Directorio Activo	Atención al Cliente
Aplicación	Sistema Operativo del Servidor de Antivirus	Base de Datos de E-client
Aplicación	Sistema Operativo del Servidor E-Client	Base de Datos de E-client
Aplicación	Sistema Operativo del Servidor de Request Tracker	Base de Datos de E-client
Aplicación	Sistema Operativo de los Pc de agentes de Call Center	Atención al Cliente
Red	Canal de Internet	Atención al Cliente
Instalaciones	Centro de Cómputo	Base de Datos de E-client
Aplicación	Motor de Base de Datos de Request Tracker	Base de datos de Request Tracker
Aplicación	Motor de Base de Datos de E-client	Base de Datos de E-client
Soportes de Información	Cintas con Copias de Respaldo	Copias de Respaldo de E-client
Personas	Proveedor de almacenamiento de Cintas	Copias de Respaldo de E-client
Datos	Copias de Respaldo de Request Tracker	Copias de Respaldo de Request Tracker
Datos	Copias de Respaldo de E-client	Copias de Respaldo de E-client
Datos	Base de Datos de E-client	Base de Datos de E-client
Datos	Base de datos de Request Tracker	Base de datos de Request Tracker
Datos	Correos Electrónicos	Correos Electrónicos
Aplicación	Cliente de Correo Electrónico	Correos Electrónicos
Datos	Código Fuente de E-client	Código Fuente de E-client
Instalaciones	Oficinas de ABC S.A.	Atención al Cliente
Personas	Agentes de Call Center	Base de Datos de E-client
Personas	Coordinador de Campañas Bancarias	Base de Datos de E-client
Personas	Director de Call Center	Base de Datos de E-client
Personas	Ingeniero de Mantenimiento	Atención al Cliente
Personas	Ingeniero de Soporte	Base de Datos de E-client
Personas	Coordinador de Sistemas	Base de Datos de E-client
Personas	Director de Tecnología	Base de Datos de E-client
Personas	Coordinador de Talento Humano	Base de Datos de E-client
Personas	Auxiliar de Nómina	Atención al Cliente
Personas	Auxiliar de Selección	Base de Datos de E-client
Personas	Director de Recursos Humanos	Copias de Respaldo de E-client

Categoria	Activo	Activo Superior
Personas	Desarrolladores	Base de Datos de E-client
Personas	Coordinador de Desarrollo	Base de Datos de E-client
Personas	Director de Servicios de Factoria de Software	Código Fuente de E-client
Red	Internet	Atención al Cliente
Red	Red de Call Center	Atención al Cliente
Red	Red de Tecnología	Atención al Cliente
Red	Red de Área Administrativa	Atención al Cliente
Red	Red de Servidores	Atención al Cliente
Red	DMZ	Atención al Cliente
Equipamiento Auxiliar	Cableado Estructurad	Atención al Cliente
Equipamiento Auxiliar	Aire Acondicionado Centro de Cómputo	Atención al Cliente
Equipamiento Auxiliar	Biométrico de Acceso al Centro de Cómputo	Atención al Cliente
Equipamiento Auxiliar	Sistema Antiincendios	Atención al Cliente
Servicios	Atención al Cliente	Atención al Cliente

Tabla 16 Dependencia de los Activos

7.4 Resumen de Valoración

Habiendo recopilado los activos de información, la dependencia entre ellos y el valor acumulado en cada dimensión de la seguridad, se obtuvo la siguiente tabla de valoración de activos de ABC S.A.

Categoria	Activo	A	C	I	D	T
Hardware	Servidor de Directorio Activo	6	6	5	10	6
Hardware	Servidor de E-Client	7	10	10	10	7
Hardware	Servidor de Antivirus	7	10	10	10	7
Hardware	Servidor de Request Tracker	7	7	10	5	7
Hardware	Servidor de Correo	10	8	10	6	7
Hardware	Firewall	6	6	5	10	6
Hardware	Router de Internet	6	6	5	10	6
Hardware	Switch de Core	6	6	5	10	6
Hardware	PCs de Agentes de Call Center	6	6	5	10	6
Hardware	Pcs de Empleados Administrativos	6	6	5	10	6
Hardware	Portátiles de Empleados de Tecnología	7	10	10	10	7
Hardware	Portátiles de la Alta Dirección	6	6	5	10	6
Aplicación	Sofware de Directorio Activo (Active Directory de Microsoft)	6	6	5	10	6
Aplicación	Software E-Client	7	10	10	10	7

Categoria	Activo	A	C	I	D	T
Aplicación	Software Antivirus	7	10	10	10	7
Aplicación	Software de Correo Electrónico	10	8	10	6	7
Aplicación	Software Servidor Web	6	6	5	10	6
Aplicación	Sistema Operativo del Directorio Activo	6	6	5	10	6
Aplicación	Sistema Operativo del Servidor de Antivirus	7	10	10	10	7
Aplicación	Sistema Operativo del Servidor E-Client	7	10	10	10	7
Aplicación	Sistema Operativo del Servidor de Request Tracker	7	10	10	10	7
Aplicación	Sistema Operativo de los Pc de agentes de Call Center	6	6	5	10	6
Red	Canal de Internet	6	6	5	10	6
Instalaciones	Centro de Cómputo	7	10	10	10	7
Aplicación	Motor de Base de Datos de Request Tracker	7	7	10	5	7
Aplicación	Motor de Base de Datos de E-client	7	10	10	10	7
Soportes de Información	Cintas con Copias de Respaldo	5	10	10	6	5
Personas	Proveedor de almacenamiento de Cintas	5	10	10	6	5
Datos	Copias de Respaldo de Request Tracker	5	7	10	6	5
Datos	Copias de Respaldo de E-client	5	10	10	6	5
Datos	Base de Datos de E-client	7	10	10	10	7
Datos	Base de datos de Request Tracker	7	7	10	5	7
Datos	Correos Electrónicos	10	8	10	6	7
Aplicación	Cliente de Correo Electrónico	10	8	10	6	7
Datos	Código Fuente de E-client	4	3	8	2	3
Instalaciones	Oficinas de ABC S.A.	6	6	5	10	6
Personas	Agentes de Call Center	7	10	10	10	7
Personas	Coordinador de Campañas Bancarias	7	10	10	10	7
Personas	Director de Call Center	7	10	10	10	7
Personas	Ingeniero de Mantenimiento	6	6	5	10	6
Personas	Ingeniero de Soporte	7	10	10	10	7
Personas	Coordinador de Sistemas	7	10	10	10	7
Personas	Director de Tecnología	7	10	10	10	7
Personas	Coordinador de Talento Humano	7	10	10	10	7
Personas	Auxiliar de Nómina	6	6	5	10	6
Personas	Auxiliar de Selección	7	10	10	10	7
Personas	Director de Recursos Humanos	5	10	10	6	5

Categoria	Activo	A	C	I	D	T
Personas	Desarrolladores	7	10	10	10	7
Personas	Coordinador de Desarrollo	7	10	10	10	7
Personas	Director de Servicios de Factoria de Software	4	3	8	2	3
Red	Internet	6	6	5	10	6
Red	Red de Call Center	6	6	5	10	6
Red	Red de Tecnología	6	6	5	10	6
Red	Red de Área Administrativa	6	6	5	10	6
Red	Red de Servidores	6	6	5	10	6
Red	DMZ	6	6	5	10	6
Equipamiento Auxiliar	Cableado Estructurad	6	6	5	10	6
Equipamiento Auxiliar	Aire Acondicionado Centro de Cómputo	6	6	5	10	6
Equipamiento Auxiliar	Biométrico de Acceso al Centro de Cómputo	6	6	5	10	6
Equipamiento Auxiliar	Sistema Antiincendios	6	6	5	10	6
Servicios	Atención al Cliente	6	6	5	10	6

Tabla 17 Resumen de Valoración

7.5 Riesgo Inherente

Para cada activo se calculó el riesgo en cada una de sus dimensiones de acuerdo a lo establecido en la metodología de riesgo, dada la extensión de la matriz definitiva de análisis de riesgo, se presenta en el anexo 6 y a continuación se presentan los aspectos relevantes que resultaron del análisis:

La siguiente tabla muestra el mayor valor de riesgo que tiene cada uno de los activos en cada una de sus dimensiones:

Etiquetas de fila	A	C	D	I	T
Agentes de Call Center	0	0,16	5,01	0,16	0,00
Aire Acondicionado Centro de Cómputo	0	0,10	0,53	0,08	0,00
Atención al Cliente	0	2,41	4,01	0,50	0,10
Auxiliar de Nómina	0	0,10	4,01	0,08	0,00
Auxiliar de Selección	0	0,16	4,01	0,16	0,00
Base de Datos de E-client	0	0,66	0,66	0,66	0,00
Base de datos de Request Tracker	0	0,46	0,33	0,66	0,00
Biométrico de Acceso al Centro de Cómputo	0	0,10	0,33	0,08	0,00
Cableado Estructurado	0	0,10	0,33	0,08	0,00
Canal de Internet	0	0,20	0,66	0,16	0,00
Centro de Cómputo	0	0,33	0,33	0,33	0,00
Cintas con Copias de Respaldo	0	1,50	2,11	3,51	0,00

Cliente de Correo Electrónico	0	0,53	0,39	0,66	0,00
Código Fuente de E-client	0	0,20	0,13	0,53	0,00
Coordinador de Campañas Bancarias	0	0,16	5,01	0,16	0,00
Coordinador de Desarrollo	0	0,16	2,51	0,16	0,00
Coordinador de Sistemas	0	0,16	5,01	0,16	0,00
Coordinador de Talento Humano	0	0,16	4,01	0,16	0,00
Copias de Respaldo de E-client	0	0,66	0,39	0,66	0,00
Copias de Respaldo de Request Tracker	0	0,46	0,39	0,66	0,00
Correos Electrónicos	0	3,21	0,90	2,01	0,00
Desarrolladores	0	0,16	2,51	0,16	0,00
Director de Call Center	0	0,16	5,01	0,16	0,00
Director de Recursos Humanos	0	0,16	2,41	0,16	0,00
Director de Servicios de Factoria de Software	0	0,05	0,50	0,13	0,00
Director de Tecnología	0	0,16	5,01	0,16	0,00
DMZ	0	0,39	0,66	0,33	0,00
Firewall	0	0,39	0,66	0,33	0,00
Ingeniero de Mantenimiento	0	0,10	5,01	0,08	0,00
Ingeniero de Soporte	0	0,16	5,01	0,16	0,00
Internet	0	0,39	0,66	0,33	0,00
Motor de Base de Datos de E-client	0	0,66	0,66	0,66	0,00
Motor de Base de Datos de Request Tracker	0	0,46	0,33	0,66	0,00
Oficinas de ABC S.A.	0	0,20	0,33	0,16	0,00
PCs de Agentes de Call Center	0	0,28	0,46	0,23	0,00
Pcs de Empleados Administrativos	0	0,28	0,46	0,23	0,00
Portátiles de Empleados de Tecnología	0	0,46	0,46	0,46	0,00
Portátiles de la Alta Dirección	0	0,28	0,46	0,23	0,00
Proveedor de almacenamiento de Cintas	0	0,00	3,01	0,00	0,00
Red de Área Administrativa	0	0,39	0,66	0,33	0,00
Red de Call Center	0	0,39	0,66	0,33	0,00
Red de Servidores	0	0,39	0,66	0,33	0,00
Red de Tecnología	0	0,39	0,66	0,33	0,00
Router de Internet	0	0,39	0,66	0,33	0,00
Servidor de Antivirus	0	0,66	0,66	0,66	0,00
Servidor de Correo	0	0,53	0,39	0,66	0,00
Servidor de Directorio Activo	0	2,37	0,66	0,33	0,00
Servidor de E-Client	0	0,66	0,66	0,66	0,00
Servidor de Request Tracker	0	0,46	0,33	0,66	0,00
Sistema Antiincendios	0	0,10	0,66	0,08	0,00
Sistema Operativo de los Pc de agentes de Call Center	0	0,90	3,51	0,75	0,00
Sistema Operativo del Directorio Activo	0	0,39	0,66	0,33	0,00
Sistema Operativo del Servidor de Request Tracker	0	0,53	0,53	0,53	0,00

Sistema Operativo del Servidor de Antivirus	0	0,53	0,53	0,53	0,00
Sistema Operativo del Servidor E-Client	0	0,53	0,53	0,53	0,00
Software Servidor Web	0	0,39	0,66	0,33	0,00
Software Antivirus	0	0,66	0,66	0,66	0,00
Software de Correo Electrónico	0	1,20	0,60	2,01	0,00
Software E-Client	0	3,51	1,50	3,51	0,00
Sofware de Directorio Activo (Active Directory de Microsoft)	0	0,60	1,00	0,50	0,00
Switch de Core	0	0,39	0,66	0,33	0,00

Tabla 18 Valor de los Riesgos más Altos Para Cada Activo

La alta dirección ha aprobado como nivel de riesgo aceptable aquellos riesgos que tengan un valor menor o igual a MEDIO, es decir que tengan una valoración numérica menor o igual a 3.

De la tabla anterior se obtuvieron los riesgos que están por fuera del nivel de riesgo aceptable (mayores a 3) y se correlacionaron con la tabla del anexo 6 para conocer la amenaza que los genera, la siguiente tabla muestra los riesgos que están fuera del nivel de riesgo aceptable y que deben, por lo tanto, ser tratados.

Agentes de Call Center	
Amenaza	Deficiencias en la Organización
Dimensión	Disponibilidad
Riesgo	5
Propietario del Riesgo	Director de Call Center
Coordinador de Campañas Bancarias	
Amenaza	Deficiencias en la Organización
Dimensión	Disponibilidad
Riesgo	5
Propietario del Riesgo	Director de Call Center
Director de Call Center	
Amenaza	Deficiencias en la Organización
Dimensión	Disponibilidad
Riesgo	5
Propietario del Riesgo	Gerente General
Ingeniero de Mantenimiento	
Amenaza	Deficiencias en la Organización
Dimensión	Disponibilidad
Riesgo	5
Propietario del Riesgo	Director de Tecnología
Ingeniero de Soporte	
Amenaza	Deficiencias en la Organización

Dimensión	Disponibilidad
Riesgo	5
Propietario del Riesgo	Director de Tecnología
Coordinador de Sistemas	
Amenaza	Deficiencias en la Organización
Dimensión	Disponibilidad
Riesgo	5
Propietario del Riesgo	Director de Tecnología
Director de Tecnología	
Amenaza	Deficiencias en la Organización
Dimensión	Disponibilidad
Riesgo	5
Propietario del Riesgo	Gerente General
Coordinador de Talento Humano	
Amenaza	Deficiencias en la Organización
Dimensión	Disponibilidad
Riesgo	4
Propietario del Riesgo	Director de Talento Humano
Auxiliar de Talento Humano	
Amenaza	Deficiencias en la Organización
Dimensión	Disponibilidad
Riesgo	4
Propietario del Riesgo	Director de Talento Humano
Auxiliar de Selección	
Amenaza	Deficiencias en la Organización
Dimensión	Disponibilidad
Riesgo	4
Propietario del Riesgo	Director de Talento Humano
Atención al Cliente	
Amenaza	Errores de los Usuarios
Dimensión	Disponibilidad
Riesgo	4
Propietario del Riesgo	Director de Call Center
Correos Electrónicos	
Amenaza	Errores de los Usuarios
Dimensión	Confidencialidad
Riesgo	3
Propietario	Director de Tecnología

del Riesgo	
Proveedor de Almacenamiento de Cintas	
Amenaza	Deficiencias en la Organización
Dimensión	Disponibilidad
Riesgo	3
Propietario del Riesgo	Director de Tecnología
Cintas con Copias de Respaldo	
Amenaza	Errores de los Usuarios
Dimensión	Integridad
Riesgo	3
Propietario del Riesgo	Director de Tecnología
Sistema Operativo de los Pc de Agentes de Call Center	
Amenaza	Errores de los Usuarios
Dimensión	Disponibilidad
Riesgo	3
Propietario del Riesgo	Director de Tecnología
Software E-Client	
Amenaza	Errores de los Usuarios
Dimensión	Confidencialidad, Integridad
Riesgo	3
Propietario del Riesgo	Director de Tecnología

Tabla 19 Riesgos No Aceptables

Puede verse que los riesgos que están fuera del nivel aceptable por ABC S.A. son generados por 2 amenazas:

- Deficiencias en la Organización
- Errores de los Usuarios

Vale la pena entonces recordar la descripción de dichas amenazas, en la siguiente tabla se encuentra la descripición dada en la Metodología Magerit 3.0 (Libro II, Catálogo de Elementos):

Amenaza	Descripción	Tipos de Activos	Dimensiones
Deficiencias en la Organización	Cuando no está claro quién tiene que hacer exáctamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones Descoordinadas, Errores por omisión, etc.	Personal	Disponibilidad

Amenaza	Descripción	Tipos de Activos	Dimensiones
Errores de los Usuarios	Equivocaciones de personas cuando usan los servicios, datos, etc.	Datos/Información Claves Criptográficas Servicios Aplicaciones Soportes de Información	Integridad Confidencialidad Disponibilidad

Tabla 20 Amenazas que Generan Riesgos no Aceptables

8 PROPUESTAS DE PROYECTOS

Para la reducción del nivel de riesgo y para establecer un esquema de mejora continua de acuerdo a los requerimientos de la norma ISO 27001:2013, se plantean 9 proyectos que se consideran prioritarios.

Podemos clasificar los proyectos planteados en dos grupos, el primero, compuesto por aquellos proyectos propuestos para reducir el nivel de riesgo a niveles aceptables, de esta manera modificarán el valor de aquellos riesgos que se encontraron fuera del nivel de riesgo aceptable de ABC S.A y que se detallaron en la tabla 19; y un segundo grupo conformado por aquellos proyectos que se plantean para mejorar los niveles de seguridad de ABC S.A y entrar en cumplimiento con la norma ISO 27001:2013. Si bien, estos proyectos del segundo grupo reducirán el actual nivel de riesgo, no serán tratados como parte del plan de tratamiento de riesgos.

La siguiente gráfica detalla los proyectos que pertenecen a cada uno de los grupos.

Ilustración 8 Proyectos Propuestos

Algunos de estos proyectos podrían llegar a ejecutarse en paralelo, pero teniendo en cuenta la limitación de recursos se plantea una ejecución en serie de los 9 proyectos con el fin de evitar sobrecargas de trabajo a aquellos roles cuya participación es indispensable en todos los proyectos. Por otro lado, debe mencionarse, que el orden planteado responde a lo que se considera prioritario para ABC S.A.

El siguiente gráfico muestra, en un una línea de tiempo, los proyectos planteados y su orden de ejecución:

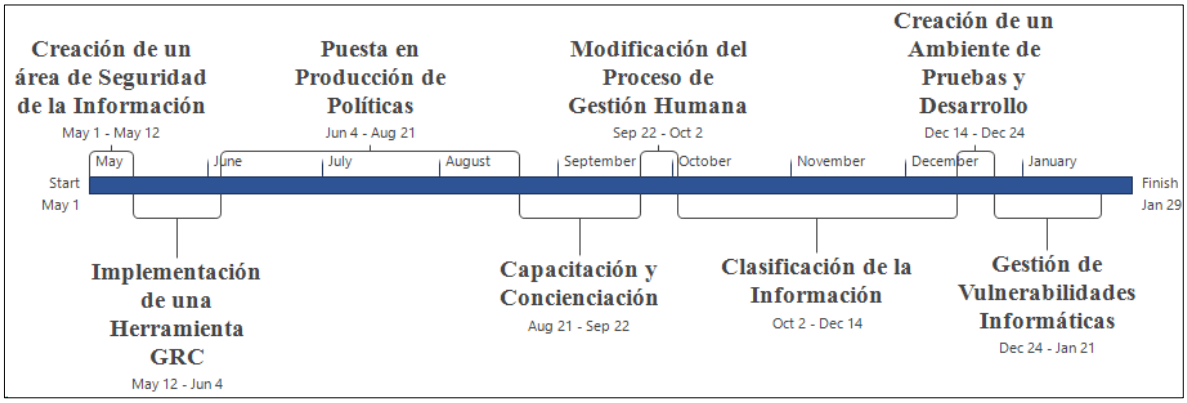
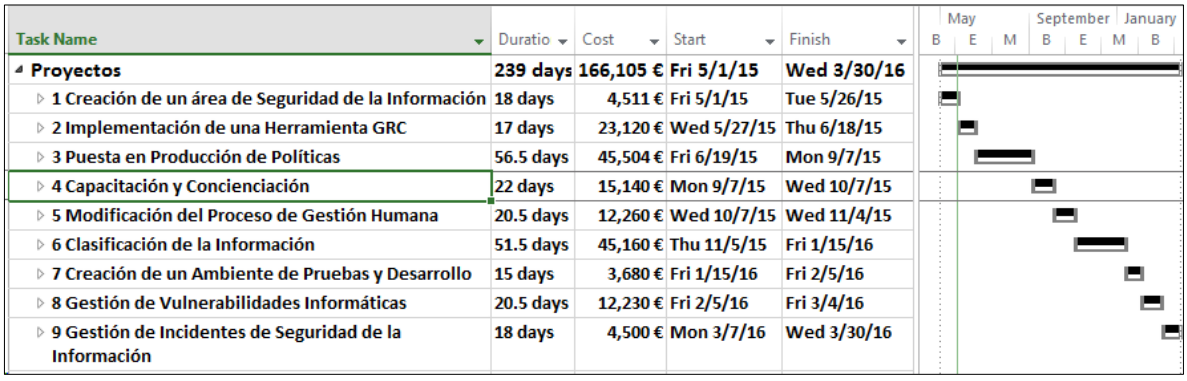


Ilustración 9 Línea de Tiempo Proyectos

El diagrama completo de Gantt puede observarse en el anexo 7 que contiene todo el detalle del proyecto, trabajado en la herramienta Microsoft Project®, sin embargo, en la siguiente gráfica puede verse el diagrama de Gantt incluendo los 9 proyectos sin el detalle de sus actividades:



Task Name	Duratio	Cost	Start	Finish
Proyectos	239 days	166,105 €	Fri 5/1/15	Wed 3/30/16
1 Creación de un área de Seguridad de la Información	18 days	4,511 €	Fri 5/1/15	Tue 5/26/15
2 Implementación de una Herramienta GRC	17 days	23,120 €	Wed 5/27/15	Thu 6/18/15
3 Puesta en Producción de Políticas	56.5 days	45,504 €	Fri 6/19/15	Mon 9/7/15
4 Capacitación y Concienciación	22 days	15,140 €	Mon 9/7/15	Wed 10/7/15
5 Modificación del Proceso de Gestión Humana	20.5 days	12,260 €	Wed 10/7/15	Wed 11/4/15
6 Clasificación de la Información	51.5 days	45,160 €	Thu 11/5/15	Fri 1/15/16
7 Creación de un Ambiente de Pruebas y Desarrollo	15 days	3,680 €	Fri 1/15/16	Fri 2/5/16
8 Gestión de Vulnerabilidades Informáticas	20.5 days	12,230 €	Fri 2/5/16	Fri 3/4/16
9 Gestión de Incidentes de Seguridad de la Información	18 days	4,500 €	Mon 3/7/16	Wed 3/30/16

Ilustración 10 Imágen del Diagrama de Gantt del Proyecto

8.1 Descripción de los Proyectos Propuestos

8.1.1 Creación de un área de Seguridad de la Información

Objetivo: Crear un area independiente del area de tecnología con las autoridades y responsabilidades suficientes para la gestión y gobierno de la seguridad de la información de ABC S.A.

Cronograma y Costos:

Tarea	Duración	Costo
Creación de un área de Seguridad de la Información	**18 days**	**4,511 €**
Revisión de Requerimientos	3 days	2,736 €
Aprobación	2 days	840 €
Asignación de Autoridades y Responsabilidades	2 days	400 €
Selección de Personal	10 days	175 €
Entrada en Producción	1 day	360 €
Area en Funcionamiento	0 days	0 €

Tabla 21 Creación de un Area de SI

Evolución en los Dominios de la Norma:

Una vez finalizado este proyecto, el nivel de madurez de los dominos de seguridad se verá modificado como lo presenta la siguiente gráfica:

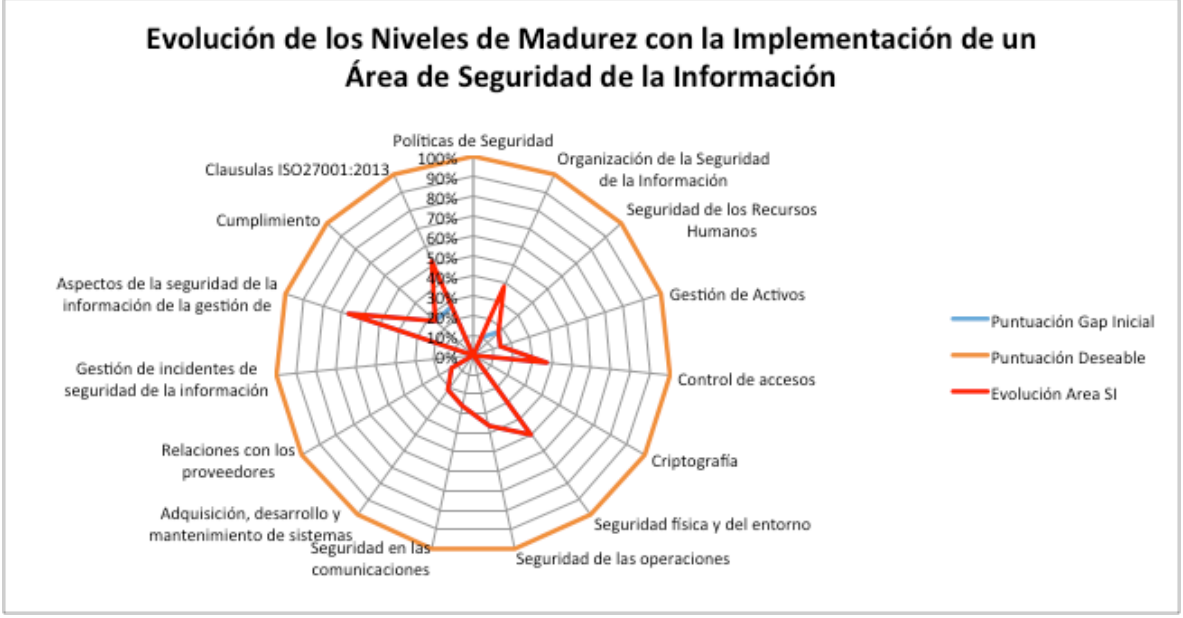


Ilustración 11 Evolución Luego de Establecer un Area de SI

8.1.2 Implementación de un GRC

Objetivo: Implementar una herramienta de Gestión Riesgo y Cumplimiento con el fin de facilitar la gestión del riesgo, la creación y revisión de políticas, la documentación y administración del SGSI y la gestión de incidentes de seguridad de la información.

Cronograma y Costos:

Tarea	Duración	Costo
Implementación de una Herramienta GRC	**17 days**	**23,120 €**
Estudio de Mercado	8 hrs	1,040 €
Selección de Proveedores	8 hrs	720 €
Adquisición de la Herramienta	16 hrs	640 €

Puesta en Producción de la Herramienta	24 hrs	3,120 €
Capacitación en la Herramienta	40 hrs	8,800 €
Parametrización de la Herramienta	40 hrs	8,800 €
Grc en Producción	0 days	0 €

Tabla 22 Cronograma Implementación de un GRC

Evolución en los Dominios de la Norma:

Una vez finalizado este proyecto, el nivel de madurez de los dominos de seguridad se verá modificado como lo presenta la siguiente gráfica:

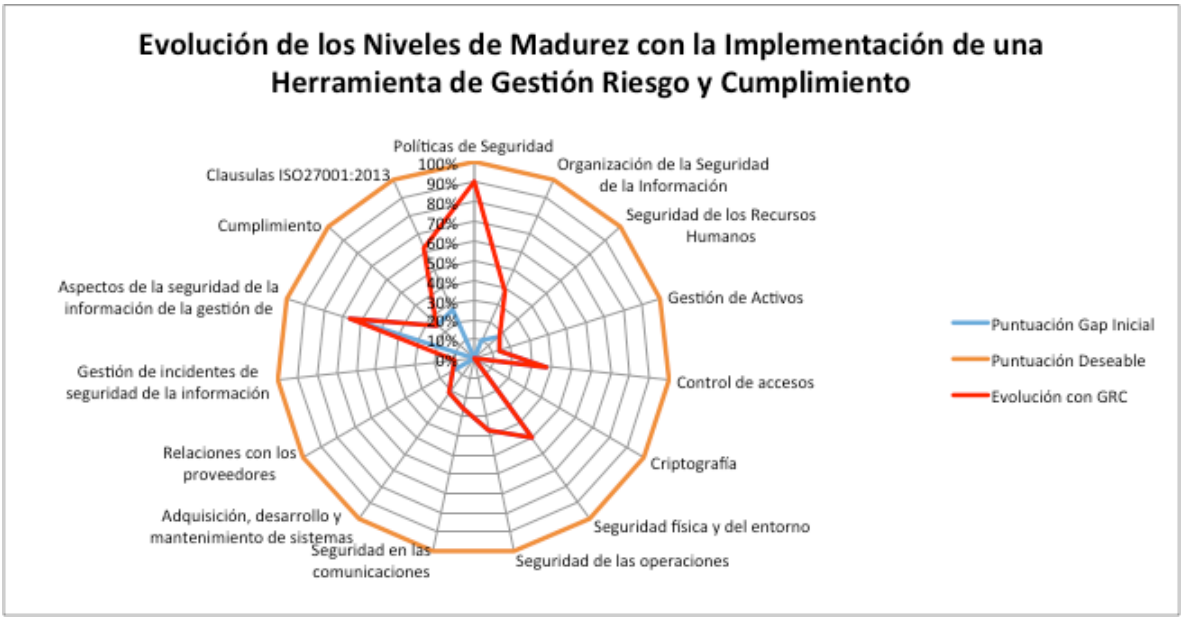


Ilustración 12 Evolución con la Implementación de un GRC

8.1.3 Puesta en Producción de Políticas

Objetivo: Revisar, aprobar y poner en producción la política general de seguridad de la información, las políticas específicas, la metodología de análisis de riesgo, los indicadores de medición, y en general todos los documentos, procedimientos y políticas establecidos en la etapa de planeación del SGSI.

Tarea	Duración	Costo
Puesta en Producción de Políticas	**56.5 days**	**45,504 €**
Revisión de la Política General por Parte de la Alta Dirección	24 hrs	15,840 €
Aprobación de la Política General	4 hrs	480 €
Publicación de la Política General	16 hrs	3,680 €
Publicación y Divulgación de las políticas específicas	320 hrs	14,400 €
Revisión y Aprobación de la Metodología de Riesgo	16 hrs	1,840 €
Revisión y Aprobación de los Indicadores del Sistema	16 hrs	1,824 €

Revisión y Aprobación de Formatos de Apoyo	16 hrs	2,240 €
Carga del sistema en la herramienta GRC	40 hrs	5,200 €
Políticas en Producción	0 days	0 €

Tabla 23 Cronograma Puesta en Producción de Políticas

Evolución en los Dominios de la Norma:

Una vez finalizado este proyecto, el nivel de madurez de los dominos de seguridad se verá modificado como lo presenta la siguiente gráfica:

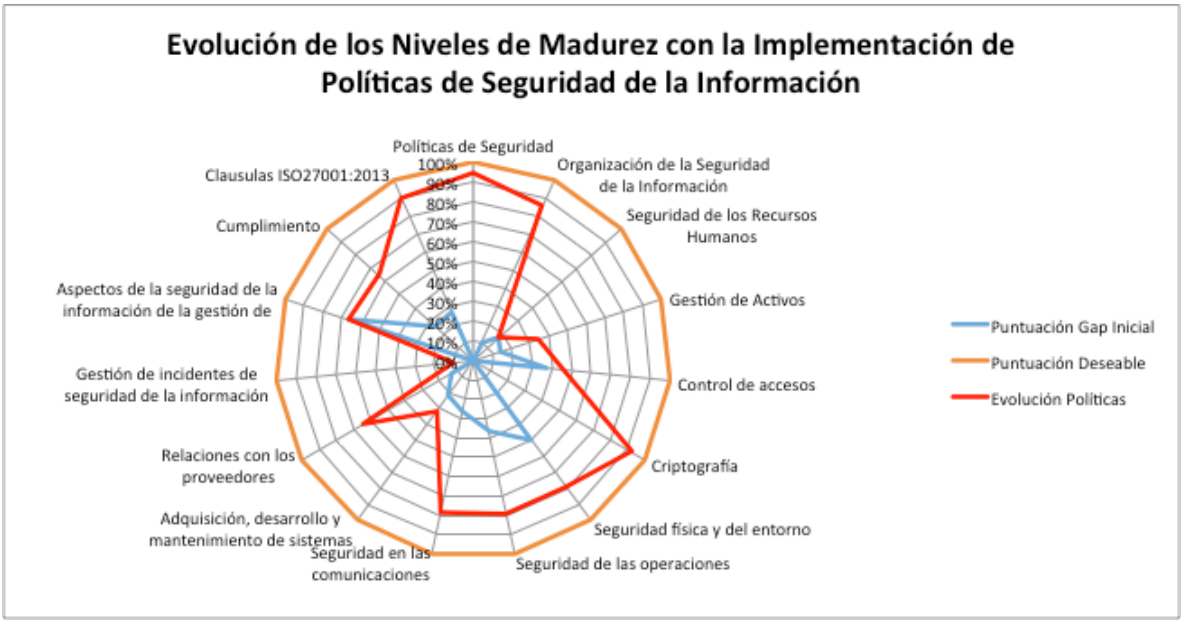


Ilustración 13 Evolución Luego de la Implementación del SGSI

8.1.4 Capacitación y Concienciación

Objetivo: Generar conciencia de manera continua en los empleados, proveedores, contratistas y terceros con respecto a la posición de la seguridad de la información de ABC S.A. Generar también el conocimiento necesario en el personal interno encargado de gestionar diferentes aspectos de la seguridad de la información, tal como: Auditoría interna en ISO 27001:2013, Gestión de Riesgos, Gestión de Vulnerabilidades, Atención de Incidentes, entre otros.

Cronograma y Costos:

Tarea	Duración	Costo
Capacitación y Concienciación	**22 days**	**15,140 €**
Generación de Contenido para Charlas de Concienciación	20 hrs	2,600 €
Manufactura de material de Campañas	4 hrs	160 €
Charlas de concienciación al Personal de Sistemas	8 hrs	320 €
Charlas de Concienciación a Funcionarios en General	40 hrs	1,600 €
Charlas de Concienciación a Directivos	4 hrs	360 €

Charlas de Concienciación a Proveedores	10 hrs	900 €
Charlas de Concienciación a Contratistas	10 hrs	400 €
Pruebas de Ingeniería Social	40 hrs	3,600 €
Capacitación en Auditoría Interna sobre Iso 27001:2013	40 hrs	5,200 €
Personal Capacitado	0 days	0 €

Tabla 24 Cronograma Capacitación y Concienciación

Evolución en los Dominios de la Norma:

Una vez finalizado este proyecto, el nivel de madurez de los dominos de seguridad se verá modificado como lo presenta la siguiente gráfica:

Ilustración 14 Evolución Luego de Concienciación y Capacitación

8.1.5 Modificación del Proceso de Gestión Humana

Objetivo: Modificar los procedimientos asociados al Proceso de Gestión Humana con el fin de incluir dentro de los contratos del personal, contratistas, proveedores, y terceros los requerimientos de seguridad de la información de acuerdo a lo establecido en el SGSI de ABC S.A.

Cronograma y Costos:

Tarea	Duración	Costo
Modificación del Proceso de Gestión Humana	**20.5 days**	**12,260 €**
Revisión del Proceso Actual	10 days	6,320 €
Alineación con los requerimientos de ISO 27001	20 hrs	2,800 €
Generación de Otrosi a contratos laborales	5 days	1,700 €
Firma por parte de los empleados	8 hrs	0 €

Firma por parte de Contratistas	8 hrs	0 €
Auditoría De Cumplimiento	16 hrs	1,440 €
Proceso Modificado	0 days	0 €

Tabla 25 Cronograma Modificación Proceso Gestión Humana

Evolución en los Dominios de la Norma:

Una vez finalizado este proyecto, el nivel de madurez de los dominos de seguridad se verá modificado como lo presenta la siguiente gráfica:

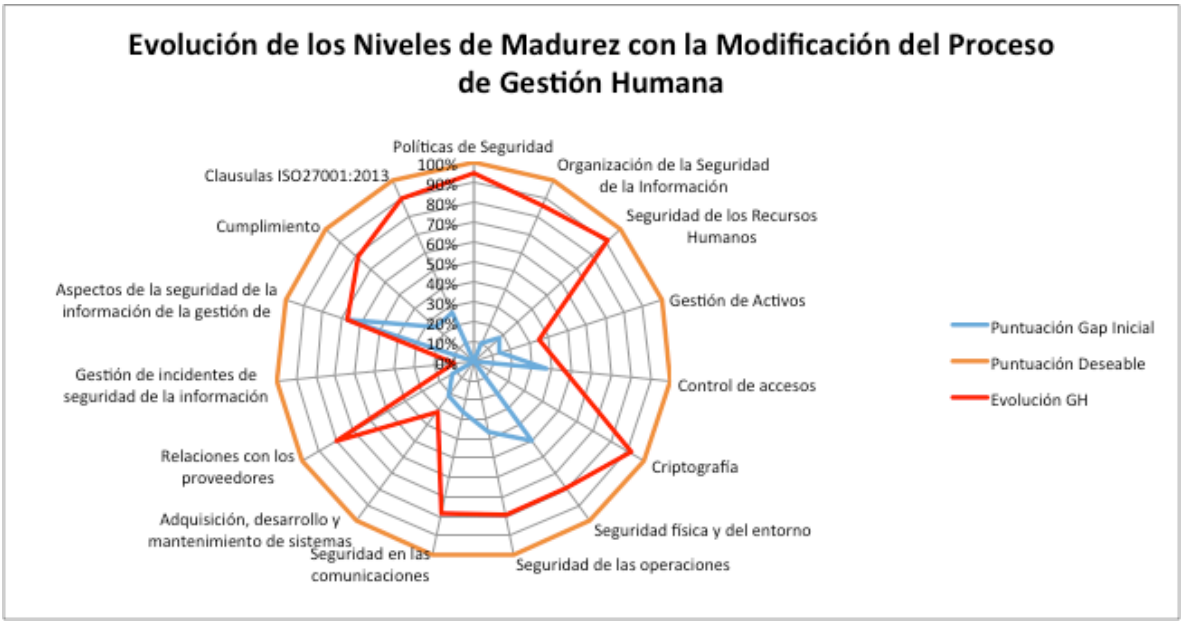


Ilustración 15 Evolución Luego de Modificación Proceso Gestión Humana

8.1.6 Clasificación de la Información

Objetivo: Clasificar la Información de acuerdo a lo establecido en la política de clasificación de información de ABC S.A., etiquetar la información de acuerdo a la clasificación establecida e implementar la guía de tratamiento de información de acuerdo.

Cronograma y Costos:

Tarea	Duración	Costo
Clasificación de la Información	**51.5 days**	**45,160 €**
Revisión de Posibles Ajustes a la Política de Clasificación de la Información	16 hrs	2,080 €
Oficialización de la Política de Seguridad de la Información	4 hrs	480 €
Divulgación de la política	16 hrs	2,240 €
Generación de guías de etiquetado de información	20 hrs	1,700 €
Generación de guías de tratamiento de información	20 hrs	1,700 €
Divulgación de guías de etiquetado y tratamiento	16 hrs	2,240 €

Etiquetado de Información	320 hrs	34,720 €
Información Clasificada	0 days	0 €

Tabla 26 Cronograma Clasificación de la Información

Evolución en los Dominios de la Norma:

Una vez finalizado este proyecto, el nivel de madurez de los dominos de seguridad se verá modificado como lo presenta la siguiente gráfica:

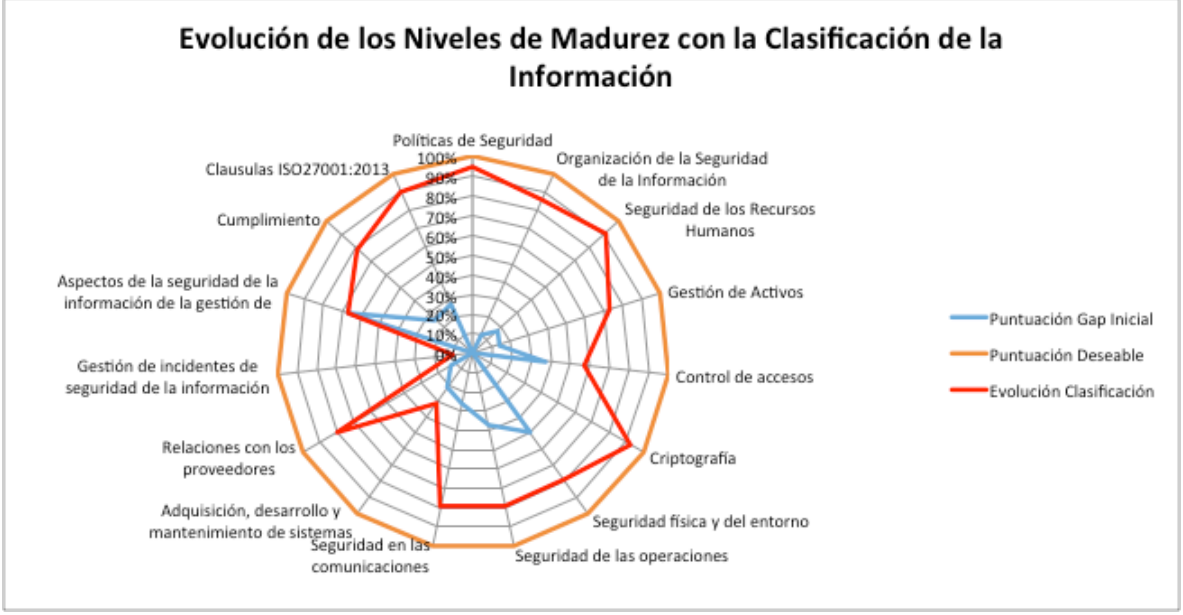


Ilustración 16 Evolución Luego de Clasificar la Información

8.1.7 Creación de un Ambiente de Pruebas y Desarrollo

Objetivo: Crear los ambientes de pruebas y desarrollo, separados del ambiente de producción.

Cronograma y Costos:

Tarea	Duración	Costo
Creación de un Ambiente de Pruebas y Desarrollo	**15 days**	**3,680 €**
Diseño de Red	16 hrs	1,440 €
Levantamiento de Especificaciones	8 hrs	280 €
Petición y Análisis de Cotizaciones	8 hrs	280 €
Instalación de los ambientes	10 days	1,400 €
Pruebas sobre los ambientes	8 hrs	280 €
Ambientes Instalados	0 days	0 €

Tabla 27 Cronograma Implementación Ambiente de Desarrollo

Evolución en los Dominios de la Norma:

Una vez finalizado este proyecto, el nivel de madurez de los dominos de seguridad se verá modificado como lo presenta la siguiente gráfica:

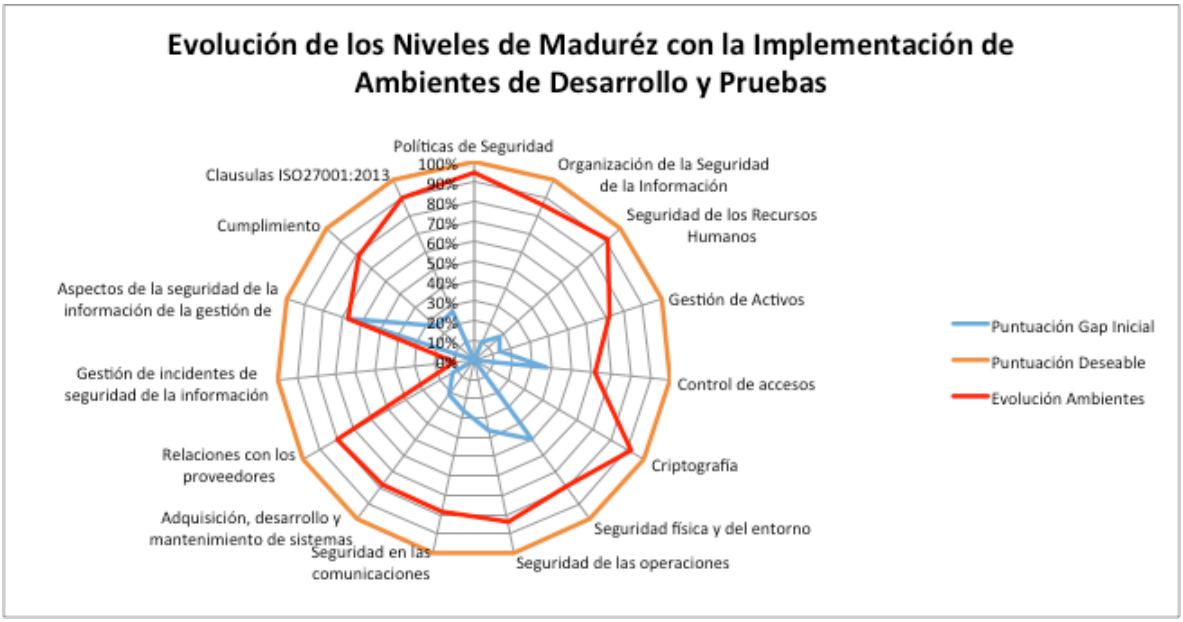


Ilustración 17 Evolución Luego de Implementar Ambientes Separados

8.1.8 Gestión de Vulnerabilidades Informáticas

Objetivo: Implementar un proceso de gestión continuca de vulnerabilidades informáticas, basado en una herramienta de análisis de vulnerabilidades gestionada por el área de sistemas de ABC S.A.

Cronograma y Costos:

Tarea	Duración	Costo
Gestión de Vulnerabilidades Informáticas	**20.5 days**	**12,230 €**
Selección de Herramientas	24 hrs	2,400 €
Provisionamiento de la Herramienta Seleccionada	20 hrs	2,000 €
Instalación de la Herramienta	16 hrs	1,440 €
Capacitación al Personal Interno	40 hrs	3,600 €
Configuración Inicial	8 hrs	180 €
Afinamiento	20 hrs	450 €
Programación de Escaneos Anuales	20 hrs	2,000 €
Personalización de reportes	16 hrs	160 €
Herramienta en Producción	0 days	0 €

Tabla 28 Cronograma Gestión de Vulnerabilidades

Evolución en los Dominios de la Norma:

Una vez finalizado este proyecto, el nivel de madurez de los dominos de seguridad se verá modificado como lo presenta la siguiente gráfica:

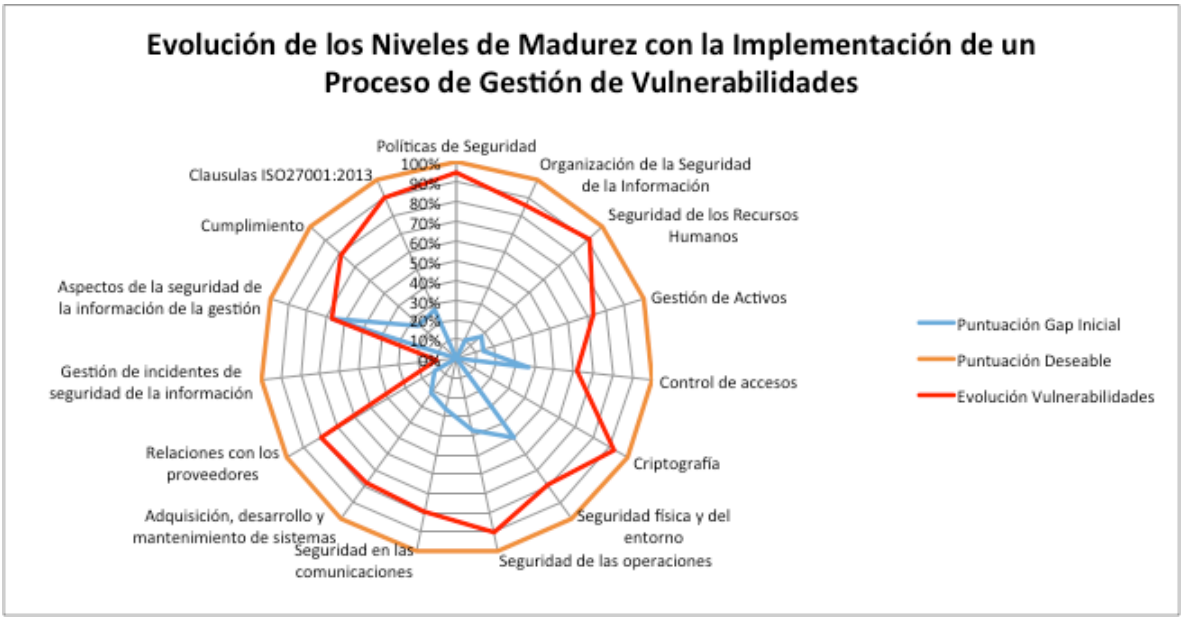


Ilustración 18 Evolución Luego de Implementar Gestión de Vulnerabilidades

8.1.9 Gestión de Incidentes de Seguridad de la Información

Objetivos: Tercerizar un servicio de monitoreo y correlación de eventos de seguridad de la información en modalidad 7x24x365 y el apoyo experto en la gestión de incidentes de seguridad de la información.

Cronograma y Costos:

Tarea	Duración	Costo
Gestión de Incidentes de Seguridad de la Información	**18 days**	**4,500 €**
Generación de un estudio de mercado	5 days	2,200 €
Creación de una solicitud de Ofertas	3 days	1,320 €
Selección de Proveedores	10 days	980 €
Inicio del Servicio Annual	0 hrs	0 €

Tabla 29 Cronograma Gestión de Incidentes

Evolución en los Dominios de la Norma:

Una vez finalizado este proyecto, el nivel de madurez de los dominos de seguridad se verá modificado como lo presenta la siguiente gráfica:

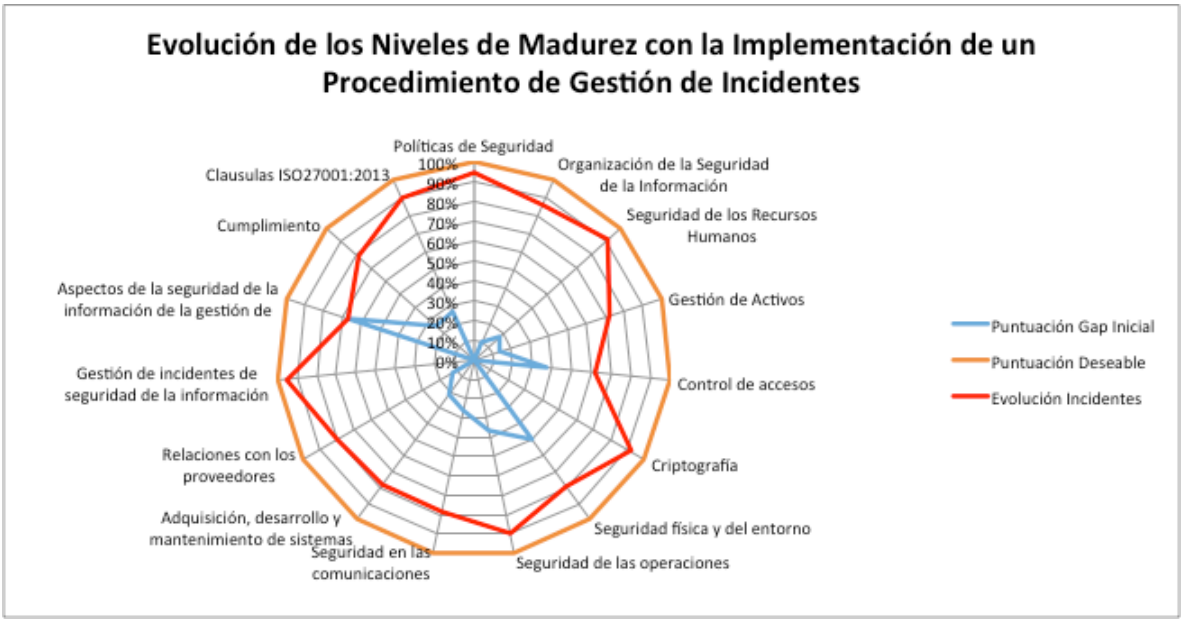


Ilustración 19 Evolución Luego de Implementar la Gestión de Incidentes

8.2 Riesgo Residual.

El objetivo fundamental del plan de tratamiento de riesgos es "tratar" los riesgos que dentro del análisis de riesgo están en niveles no aceptables para la organización, en el caso particular de ABC S.A., son aquellos que están en un nivel mayor o igual a 3 y que se encuentran detallados en la tabla 19 de este documento.

Se estima que el plan de tratamiento de riesgos modifique los niveles de riesgo como se muestra en la siguiente tabla:

Amenaza	Activo	Propietario del Riesgo	Dimensión de la Seguridad Afectada	Riesgo Inherente	Riesgo Residual
Deficiencias de la Organización	Agentes de Call Center	Director de Call Center	Disponibilidad	5	2.5
Deficiencias de la Organización	Coordinador de Campañas Bancarias	Director de Call Center	Disponibilidad	5	2.5
Deficiencias de la Organización	Director de Call Center	Gerente General	Disponibilidad	5	2.5
Deficiencias de la Organización	Ingeniero de Mantenimiento	Director de Tecnología	Disponibilidad	5	2.5
Deficiencias de la Organización	Ingeniero de Soporte	Director de Tecnología	Disponibilidad	5	2.5

Amenaza	Activo	Propietario del Riesgo	Dimensión de la Seguridad Afectada	Riesgo Inherente	Riesgo Residual
Deficiencias de la Organización	Coordinador de Sistemas	Director de Tecnología	Disponibilidad	5	2.5
Deficiencias de la Organización	Coordinador de Talento Humano	Director de Talento Humano	Disponibilidad	4	2
Deficiencias de la Organización	Auxiliar de Talento Humano	Director de Talento Humano	Disponibilidad	4	2
Deficiencias en la Organización	Auxiliar de Selección	Director de Talento Humano	Disponibilidad	4	2
Errores de los Usuarios	Atención al Cliente	Director de Call Center	Disponibilidad	4	2
Errores de los Usuarios	Correos Electrónicos	Director de Tecnología	Confidencialidad	3	2
Deficiencias en la Organización	Proveedor de Almacenamiento de Cintas	Director de Tecnología	Disponibilidad	3	2
Errores de los Usuarios	Cintas con Copias de Respaldo	Director de Tecnología	Integridad	3	2
Errores de los Usuarios	Sistema Operativo de los PC de Agentes de Call Center	Director de Tecnología	Disponibilidad	3	2
Errores de los Usuarios	Software E-Client	Director de Tecnología	Confidencialidad, Integridad	3	2

Tabla 30 Riesgo Residual Luego del Plan de Tratamiento de Riesgos

9 AUDITORIA DE CUMPLIMIENTO

9.1 Descripción de la Auditoría

Los días 18,19,20, y 21 de mayo de 2015 se realizó la primer auditoría interna del SGSI de ABC S.A. de acuerdo a lo establecido en el "Procedimiento de Auditorías Internas", el informe final y el plan de esta auditoría se incluye en los Anexos 8 y 9 de esta memoria "Informe de Auditoría Interna", sin embargo a continuación se detalla el nivel de madurez de los controles de la norma ISO 27001 encontrados durante la auditoría y un resúmen ejecutivo de los resultados.

9.2 Análisis del Nivel de Maduréz de los Controles

La siguiente tabla muestra el detalle de la evaluación del nivel de madurez de cada uno de los 144 controles y las 7 cláusulas de la norma ISO 27001:2013, de acuerdo a lo encotrado en la auditoría interna.

Para la definición del nivel de madurez de los controles se utilizaron los mismos niveles que se han tenido en cuenta para el análisis diferencial y para el análisis de evolución con la implementación de los proyectos propuestos, y que están definidos en el numeral 5.1 de esta memoria: Inexistente, Inicial, Repetible pero Intuitivo, Proceso Definido, Optimizado, Automatizado.

Sección	Control	Resultados Auditoria 1		Estado	Observaciones
A.5	Políticas de Seguridad	93%			
A.5.1	Orientación de la Dirección para la gestión de la seguridad de la información	93%			
A.5.1.1	Políticas para la seguridad de la información	95%	Gestionado y Medible	En Cumplimiento	Ya se definieron, aprobaron y divulgaron las políticas de Seguridad de la Información.
A.5.1.2	Revisión de las políticas para la seguridad de la información	90%	Proceso Definido	Observación	Hasta el momento no se han realizado revisiones a las Políticas de Seguridad de la información dado que el SGSI es reciente, sin embargo está definido que dichas reuniones deben hacerse de manera periódica.
A.6	Organización de la Seguridad de la Información	82%			
A.6.1	Organización Interna	74%			
A.6.1.1	Roles y Responsabilidades de Seguridad de la Información	90%	Proceso Definido	En Cumplimiento	Dentro de la Implementación del SGSI, ABC S.A. Definió un área de Seguridad de la Información y está en proceso de implementación. De manera temporal, la alta dirección asignó la Responsabilidad de gestionar la seguridad de la información en la Dirección de Tecnología.
A.6.1.2	Separación de deberes	90%	Proceso Definido	Observación	Dentro de la Implementación del SGSI, ABC S.A. Definió un área de Seguridad de la Información y está en proceso de implementación. De manera temporal, la alta dirección asignó la Responsabilidad de gestionar la seguridad de la información en la Dirección de Tecnología.
A.6.1.3	Contacto con las autoridades	10%	Inicial / Ad Hoc	No Conformidad Menor	No se encuentra evidencia suficiente de que exista un contacto con las autoridades ni procedimientos que especifiquen en qué momento y quién debe contactar a las autoridades y cómo deben ser reportados los incidentes de seguridad a tiempo.

Sección	Control	Resultados Auditoria 1		Estado	Observaciones
A.6.1.4	Contacto con grupos de interés especial	90%	Proceso Definido	Oportunidad de Mejora	Teniendo en cuenta que la organización tiene planeada la tercerización de la atención de incidentes de seguridad, puede evaluarse la posibilidad de exigir a los posibles proveedores que hagan parte de un CERT reconocido por FIRTS.
A.6.1.5	Seguridad de la información en la gestión de proyectos	90%	Proceso Definido	En Cumplimiento	Dentro de las responsabilidades de la nueva area de Seguridad de la Información Planteada para ABC S.A. Se encuetra garantizar que se tengan en cuenta los requerimientos de Seguridad de la Información en nuevos proyectos.
A.6.2	Dispositivos móviles y teletrabajo	90%			
A.6.2.1	Política para dispositivos móviles	90%	Proceso Definido	Observación	Al momento de la Auditoría esta política no había entrado en producción, sin embargo está dentro de las políticas específicas definidas del SGSI.
A.6.2.2	Teletrabajo	90%	Proceso Definido	Observación	Al momento de la Auditoría esta política no había entrado en producción, sin embargo está dentro de las políticas específicas definidas del SGSI.
A.7	Seguridad de los Recursos Humanos	90%			
A.7.1	Antes de asumir el empleo	90%			
A.7.1.1	Selección	90%	Proceso Definido	En Cumplimiento	Dentro del proceso de Gestión Humana se encuentra el Procedimiento de selección de personal que contempla la revisión de antecedentes en las bases de datos de la Dijin, Procuraduría y Contraloria. Adicionalmente se tiene establecido en el procedimiento de contratación la realización de visitas domiciliarias y polígrafo
A.7.1.2	Términos y condiciones del empleo	90%	Proceso Definido	Observación	Este control aún no está implementado, sin embargo, ABC S.A. Tiene dentro de sus planes de tratamiento de riesgo definido un proyecto que se llama: "Modificación del Proceso de Gestión Humana" que contempla la modificación de contratos y el proceso de contratación en general para incluir los requerimientos de seguridad antes, durante y luego del empleo. Este proyecto le da alcance a los contratos de proveedores y terceros.
A.7.2	Durante el empleo	90%			

Sección	Control	Resultados Auditoria 1		Estado	Observaciones
A.7.2.1	Responsabilidades de la dirección	90%	Proceso Definido	Observación	Este control aún no está implementado, sin embargo, ABC S.A. Tiene dentro de sus planes de tratamiento de riesgo definido un proyecto que se llama: "Modificación del Proceso de Gestión Humana" que contempla la modificación de contratos y el proceso de contratación en general para incluir los requerimientos de seguridad antes, durante y luego del empleo. Este proyecto le da alcance a los contratos de proveedores y terceros. Existe además un proyecto dentro del plan de tratamiento de riesgos llamado "Concienciación y Capacitación" que tiene como objetivo aumentar el nivel de concienciación de todo el personal y generar el conocimiento necesario para la gestión de la seguridad de la información.
A.7.2.2	Concienciación sobre la seguridad de la información, la educación y la formación	90%	Proceso Definido	Observación	Este control aún no está implementado, sin embargo, ABC S.A. Tiene dentro de sus planes de tratamiento de riesgo definido un proyecto que se llama: "Concienciación y Capacitación" que tiene como objetivo aumentar el nivel de concienciación de todo el personal y generar el conocimiento necesario para la gestión de la seguridad de la información.
A.7.2.3	Proceso disciplinario	90%	Proceso Definido	Observación	Este control aún no está implementado, sin embargo, ABC S.A. Tiene dentro de sus planes de tratamiento de riesgo definido un proyecto que se llama: "Modificación del Proceso de Gestión Humana" que contempla la modificación de contratos y el proceso de contratación en general para incluir los requerimientos de seguridad antes, durante y luego del empleo. Este proyecto le da alcance a los contratos de proveedores y terceros. Existe además un proyecto dentro del plan de tratamiento de riesgos llamado "Concienciación y Capacitación" que tiene como objetivo aumentar el nivel de concienciación de todo el personal y generar el conocimiento necesario para la gestión de la seguridad de la información.
A.7.3	Terminación y cambio de empleo	90%			
A.7.3.1	Terminación o cambio de responsabilidades de empleo	90%	Proceso Definido	Observación	Este control aún no está implementado, sin embargo, ABC S.A. Tiene dentro de sus planes de tratamiento de riesgo definido un proyecto que se llama: "Modificación del Proceso de Gestión Humana" que contempla la modificación de contratos y el proceso de contratación en general para incluir los requerimientos de seguridad antes, durante y luego del empleo. Este proyecto le da alcance a los contratos de proveedores y terceros.
A.8	Gestión de Activos	79%			
A.8.1	Responsabilidad de	58%			

Sección	Control	Resultados Auditoria 1		Estado	Observaciones
	los activos				
A.8.1.1	Inventario de Activos	50%	Reproducible Pero Intuitivo	Oportunidad de Mejora	Este control se aplica de manera intuitiva sin embargo es recomendable que se procedimente para que sea repetible, se pueda gestionar y medir y posiblemente posteriormente automatizar.
A.8.1.2	Propietario de los activos	0%	Inexistente	No Conformidad Menor	No se ha asignado un propietario a los activos
A.8.1.3	Uso aceptable de los activos	90%	Proceso Definido	Observación	Las políticas general y específicas dentro del establecimiento del SGSI de ABC S.A. Contemplan el uso aceptable de activos, sin embargo el sistema no ha terminado de ser implementado. Haceparte de los proyectos dentro del plan de tratamiento de riesgos.
A.8.1.4	Devolución de los activos	90%	Proceso Definido	En Cumplimiento	Dentro del procedimiento de entrega de cargo que hace parte del proceso de Gestion del Recurso Humano se tiene definido como requisito la expedición de un paz y salvo de parte de los procesos relacionados con el empleo que incluye la devolución de activos.
A.8.2	Clasificación de la información	90%			
A.8.2.1	Clasificación de la información	90%	Proceso Definido	Observación	Dentro del plan de tratamiento de riesgos se tiene planificado un proyecto de clasificación de información que contempla este control.
A.8.2.2	Etiquetado de la información	90%	Proceso Definido	Observación	Dentro del plan de tratamiento de riesgos se tiene planificado un proyecto de clasificación de información que contempla este control.
A.8.2.3	Manejo de activos	90%	Proceso Definido	Observación	Dentro del plan de tratamiento de riesgos se tiene planificado un proyecto de clasificación de información que contempla este control.
A.8.3	Manejo de medios	90%			
A.8.3.1	Gestión de medios removibles	90%	Proceso Definido	Observación	Dentro del plan de tratamiento de riesgos se tiene planificado un proyecto de clasificación de información que contempla este control.
A.8.3.2	Disposición de los medios			No aplica	Está exlcuido de la declaración de aplicabilidad.
A.8.3.3	Transferencia de medios físicos	90%	Proceso Definido	Observación	Dentro del plan de tratamiento de riesgos se tiene planificado un proyecto de clasificación de información que contempla este control.
A.9	Control de accesos	61%			
A.9.1	Requisitos del negocio para el control de acceso	90%			
A.9.1.1	Política de control de acceso	90%	Proceso Definido	Observación	Dentro de la implementación del SGI, en su esquema documental, se planteó una política específica de control de acceso, al momento de la auditoría no está implementada pero hace parte de lo planeado por la dirección.

Sección	Control	Resultados Auditoria 1		Estado	Observaciones
A.9.1.2	Acceso a redes y servicios en red	90%	Proceso Definido	Observación	Dentro de la implementación del SGI, en su esquema documental, se planteó una política específica de control de acceso, al momento de la auditoría no está implementada pero hace parte de lo planeado por la dirección.
A.9.2	Gestión de acceso de usuarios	67%			
A.9.2.1	Registro y cancelación del registro de usuarios	100%	Optimizado	En Cumplimiento	Todos los sistemas de información están integrados con el directorio activos de la organización, el proceso de dada de alta y de baja de personal desde Gestión Humana contempla la dehabilitación de usuarios y/o permisos en el caso de finalización del contrato o de cambio de área.
A.9.2.2	Suministro de acceso de usuarios	100%	Optimizado	En Cumplimiento	Todos los sistemas de información están integrados con el directorio activos de la organización, el proceso de dada de alta y de baja de personal desde Gestión Humana contempla la dehabilitación de usuarios y/o permisos en el caso de finalización del contrato o de cambio de área.
A.9.2.3	Gestión de derechos de acceso privilegiado	10%	Inicial / Ad Hoc	No Conformidad Menor	Esto se ha venido haciendo bajo necesidad y de acuerdo al criterio del administrador de dominio, esto debe procedimentarse para garantizar que los derechos de acceso son restringidos y controlados.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	90%	Proceso Definido	En Cumplimiento	Está definido que al crear una contraseña, se crea una contraseña temporal que expira en el primer inicio de sesión y obliga al usuario a cambiarla.
A.9.2.5	Revisión de los derechos de acceso de usuarios	0%	Inexistente	No Conformidad Menor	No se ha contemplado en ninguna política la revisión de los derechos de acceso de maera periódica, esto debe ser definido e implementado. Puede considerarse la inclusión de este control dentro de la política de control de acceso que está planeada para ser implementada.
A.9.2.6	Retiro o ajuste de los de derechos de acceso	100%	Optimizado	En Cumplimiento	Todos los sistemas de información están integrados con el directorio activos de la organización, el proceso de dada de alta y de baja de personal desde Gestión Humana contempla la dehabilitación de usuarios y/o permisos en el caso de finalización del contrato o de cambio de área.
A.9.3	Responsabilidades de los usuarios	10%			
A.9.3.1	Uso de información de autenticación secreta	10%	Inicial / Ad Hoc	Oportunidad de Mejora	Para lograr aumentar el nivel de madurez de este control se recomienda incluirlo en una política específica y dentro del temario de concienciación y capacitación.
A.9.4	Control de acceso al sistema y aplicaciones	76%			

Sección	Control	Resultados Auditoria 1		Estado	Observaciones
A.9.4.1	Restricciones de acceso a la información	90%	Proceso Definido	Observación	La implementación de la política de control de acceso en conjunto con la integración de directorio activo dan cumplimiento a este control, sin embargo la implementación de la política está en curso por lo que no se considera aún el control en cumplimiento.
A.9.4.2	Procedimiento de ingreso seguro	50%	Reproducible Pero Intuitivo	Oportunidad de Mejora	Se recomienta implementar un procedimiento que permita medir y mejorar este control.
A.9.4.3	Sistema de gestión de contraseñas	100%	Optimizado	En Cumplimiento	El directorio activo lo provee.
A.9.4.4	Uso de programas utilitarios privilegiados	50%	Reproducible Pero Intuitivo	Oportunidad de Mejora	La revisión y gestión de la consola centralizada del antivirus se hace solamente por demanda y a criterio del administrador, es aconsejable madurar este control por medio de un procedimiento y guías de revisión y gestión de la consola de antivirus u otras herramientas de apoyo.
A.9.4.5	Control de acceso a códigos fuente de programas	90%	Proceso Definido	Observación	Esto quedará implementado luego del proyecto de "implementación de ambientes de pruebas y desarrollo".
A.10	Criptografía	93%			
A.10.1	Controles criptográficos	93%			
A.10.1.1	Política de uso de controles criptográficos	95%	Gestionado y Medible	Observación	Está política está incluida dentro de las políticas específicas que hacen parte de la estructura documental del SGSI
A.10.1.2	Gestión de llaves	90%	Proceso Definido	Observación	Está política está incluida dentro de las políticas específicas que hacen parte de la estructura documental del SGSI
A.11	Seguridad física y del entorno	82%			
A.11.1	Áreas seguras	83%			
A.11.1.1	Perímetro de seguridad física	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas específicas del SGSI en donde se contempló una política de seguridad Física
A.11.1.2	Controles de acceso físicos	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas específicas del SGSI en donde se contempló una política de seguridad Física
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas específicas del SGSI en donde se contempló una política de seguridad Física
A.11.1.4	Protección contra las amenazas externas y ambientales	50%	Reproducible Pero Intuitivo	Oportunidad de Mejora	Se ha implementado este control por demanda, sin embargo no hay una revisión periódica ni se encuentra definido formalmente.
A.11.1.5	Trabajo en áreas seguras	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas específicas del SGSI en donde se contempló una política de seguridad Física
A.11.1.6	Áreas de despacho y carga	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas específicas del SGSI en donde se contempló una política de seguridad Física
A.11.2	Equipos	81%			

Sección	Control	Resultados Auditoria 1		Estado	Observaciones
A.11.2.1	Ubicación y protección de equipos	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas específicas del SGSI en donde se contempló una política de seguridad Física
A.11.2.2	Servicios de suministro	50%	Reproducible Pero Intuitivo	Oportunidad de Mejora	Se cuenta con UPS suficientes para dar autonomía a los servidores así como redes reguladas de energía. Sin embargo no está definido formalmente el mantenimiento y gestión de estos equipos.
A.11.2.3	Seguridad del cableado	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas específicas del SGSI en donde se contempló una política de seguridad Física
A.11.2.4	Mantenimiento de los equipos	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas específicas del SGSI en donde se contempló una política de seguridad Física
A.11.2.5	Retiro de activos	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas específicas del SGSI en donde se contempló una política de seguridad Física
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas específicas del SGSI en donde se contempló una política de seguridad Física
A.11.2.7	Disposición segura o reutilización de equipos	50%	Reproducible Pero Intuitivo	Oportunidad de Mejora	El área de tecnología tiene la costumbre de hacer un borrado a bajo nivel de los discos duros de equipos de personal que se retira de la compañía o en el caso de reasignación de equipos. Sin embargo no está formalizado.
A.11.2.8	Equipo de usuario desatendido	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas específicas del SGSI en donde se contempló una política de seguridad Física
A.11.2.9	Política de escritorio limpio y pantalla limpia	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas específicas del SGSI en donde se contempló una política de seguridad Física
A.12	Seguridad de las operaciones	90%			
A.12.1	Procedimientos operacionales y responsabilidades	90%			
A.12.1.1	Procedimientos de operación documentados	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas y procedimientos en donde se incluyen los procedimientos operativos.
A.12.1.2	Gestión de cambios	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas y procedimientos en donde se incluye una política de gestión de cambios.
A.12.1.3	Gestión de la capacidad	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas y procedimientos en donde se incluyen una política de gestión de la capacidad
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de implementación de ambientes separados de desarrollo y pruebas

Sección	Control	Resultados Auditoria 1		Estado	Observaciones
A.12.2	Protección contra códigos maliciosos	90%			
A.12.2.1	Controles contra códigos maliciosos	90%	Proceso Definido	Oportunidad de Mejora	Se tiene implementada una solución de antivirus centralizada y administrada por el área de tecnología, esto cubre los servidores y equipos de escritorio. Sin embargo no está formalizada su gestión y medición de desempeño.
A.12.3	Copias de respaldo	90%			
A.12.3.1	Respaldo de la información	90%	Proceso Definido	Observación	La implementación de este control está incluida dentro del proyecto de políticas y procedimientos en donde se incluyen una política de toma de copias de respaldo.
A.12.4	Registro y seguimiento	90%			
A.12.4.1	Registro de eventos	90%	Proceso Definido	Observación	Se tiene contemplado dentro del proyecto de implementación de políticas y procedimientos que incluye una política y procedimientos de registro y protecció de eventos.
A.12.4.2	Protección de la información de registro	90%	Proceso Definido	Observación	Se tiene contemplado dentro del proyecto de implementación de políticas y procedimientos que incluye una política y procedimientos de registro y protecció de eventos.
A.12.4.3	Registros del administrador y del operador	90%	Proceso Definido	Observación	Se tiene contemplado dentro del proyecto de implementación de políticas y procedimientos que incluye una política y procedimientos de registro y protecció de eventos.
A.12.4.4	Sincronización del relojes	90%	Proceso Definido	Oportunidad de Mejora	Está implementado pero se aconseja que se formalice su implementación y se inicien mediciones de efectividad del mismo.
A.12.5	Control de software operacional	90%			
A.12.5.1	Instalación de software en sistemas operativos	90%	Proceso Definido	En Cumplimiento	Está implementado con políticas de grupo desde el Directorio Activo.
A.12.6	Gestión de la vulnerabilidad técnica	90%			
A.12.6.1	Gestión de las vulnerabilidades técnicas	90%	Proceso Definido	Observación	Dentro del plan de tratamiento de riesgos existe un proyecto de implementación de una herramienta de gestión de vulnerabilidades.
A.12.6.2	Restricciones sobre la instalación de software	90%	Proceso Definido	En Cumplimiento	Está implementado con políticas de grupo desde el Directorio Activo.
A.12.7	Consideraciones sobre auditorías de sistemas de información	90%			
A.12.7.1	Controles de auditoría de sistemas de información	90%	Proceso Definido	En Cumplimiento	Queda Definido con la nueva implementación del SGSI, esta auditoría hace parte de dicha definición.
A.13	Seguridad en las	83%			

Sección	Control	Resultados Auditoria 1		Estado	Observaciones
	comunicaciones				
A.13.1	Gestión de la seguridad de las redes	77%			
A.13.1.1	Controles de redes	90%	Proceso Definido	En Cumplimiento	Se cuenta con una segmentación de redes , adicionalmente los puertos que no están en uso se encuentran deshabilitados.
A.13.1.2	Seguridad de los servicios de red	90%	Proceso Definido	Observación	Está contemplado dentro de los planes de tratamiento de riesgo, particularmente en la política de control de acceso.
A.13.1.3	Separación en las redes	50%	Reproducible Pero Intuitivo	Oportunidad de Mejora	Ha sido implementado por necesidad, sin embargo no está formalizado ni documentado.
A.13.2	Transferencia de información	90%			
A.13.2.1	Políticas y procedimientos de transferencia de información	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.13.2.2	Acuerdos sobre transferencia de información	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.13.2.3	Mensajería electrónica	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.14	Adquisición, desarrollo y mantenimiento de sistemas	81%			
A.14.1	Requisitos de seguridad de los sistemas de información	63%			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	50%	Reproducible Pero Intuitivo	En Cumplimiento	Todos los desarrolladores han sido capacitados en técnicas de desarrollo seguro y han recibido una solicitud expresa pero no formal de procurar realizar un desarrollo seguro de los sistemas.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	50%	Reproducible Pero Intuitivo	En Cumplimiento	Se implementó el protocolo SSL para el módulo público del software E-Client, para el acceso remoto se utilizan VPN seguras. Estos controles no están documentados ni procedimentados.
A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones	90%	Proceso Definido	En Cumplimiento	Se definió como estándar (no documentado) el uso de VPN para las conexiones con clientes, y proveedores.
A.14.2	Seguridad en los procesos de desarrollo y de soporte	90%			
A.14.2.1	Política de desarrollo seguro	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.14.2.2	Procedimientos de control de cambios en sistemas	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo

Sección	Control	Resultados Auditoria 1		Estado	Observaciones
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.14.2.4	Restricciones en los cambios a los paquetes de software	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.14.2.5	Principios de construcción de los sistemas seguros	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.14.2.6	Ambiente de desarrollo seguro	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.14.2.7	Desarrollo contratado externamente			No aplica	Está excluido en la Declaración de Aplicabilidad
A.14.2.8	Pruebas de seguridad de sistemas	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.14.2.9	Pruebas de aceptación de sistemas	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.14.3	Datos de prueba	90%			
A.14.3.1	Protección de los datos de prueba	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.15	Relaciones con los proveedores	90%			
A.15.1	Seguridad de la información en las relaciones con proveedores	90%			
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.15.2	Gestión de la prestación de servicios de proveedores	90%			
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.15.2.2	Gestión de cambios en los servicios de los proveedores	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo

Sección	Control	Resultados Auditoria 1		Estado	Observaciones
A.16	Gestión de incidentes de seguridad de la información	90%			
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	90%			
A.16.1.1	Responsabilidades y procedimientos	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.16.1.2	Reporte de eventos de seguridad de la información	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.16.1.3	Reporte de debilidades de seguridad de la información	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.16.1.4	Evaluación de eventos de seguridad y decisiones sobre ellos	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.16.1.5	Respuesta a incidentes de seguridad de la información	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.16.1.7	Recopilación de evidencia	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.17	Aspectos de la seguridad de la información de la gestión de continuidad de negocio	67%			
A.17.1	Continuidad de seguridad de la información	38%			
A.17.1.1	Planificación de la continuidad de la seguridad de la información	10%	Inicial / Ad Hoc	Oportunidad de Mejora	La organización tiene desarrollado un un Plan de continuidad de negocio en donde tiene en cuenta ciertos controles de seguridad de acuerdo con el criterio del área de tecnología.
A.17.1.2	Implantación de la continuidad de la seguridad de la información	10%	Inicial / Ad Hoc	Oportunidad de Mejora	Si bien existe el BCP, este no detallad de manera explícita procesos, procedimientos y controles para mantener la seugridad de la información durante una situación adversa. Los controles implementados han sido elegidos por el área de tecnología.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la	95%	Gestionado y Medible	En Cumplimiento	El plan de continuidad de negocio es verificado a intervalos regulares, se tienen programadas pruebas de escritorio y en paralelo para el BCP

Sección	Control	Resultados Auditoria 1		Estado	Observaciones
	información				
A.17.2	Redundancias	95%			
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	95%	Gestionado y Medible	En Cumplimiento	La organización cuenta con un centro alterno de procesamiento de datos que tiene estaciones de trabajo para proporcionar el mínimo servicio aceptable para el negocio en caso de contingencia. Los servicios de este centro alterno incluyen los relacionados con el alcance del SGSI y son probados de manera periódica.
A.18	Cumplimiento	78%			
A.18.1	Cumplimiento de requisitos legales y contractuales	66%			
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	90%	Proceso Definido	En Cumplimiento	El área Administrativa y financiera cuenta con un asesor jurídico que dentro de sus responsabilidades tiene la de mantener actualizado el inventario de normas y leyes aplicables a la organización.
A.18.1.2	Derechos de propiedad intelectual (DPI)	50%	Reproducible Pero Intuitivo	En Cumplimiento	La instalación de software en los equipos es controlada por medio de políticas del directorio activo, todo software que es instalado debe ser aprobado por el área de sistemas quien hace una validación de las respectivas licencias.
A.18.1.3	Protección de registros	50%	Reproducible Pero Intuitivo	En Cumplimiento	Los registros propios del proceso de Gestión de Call center son almacenados en un servidor de archivos aislado de la red y con acceso restringido.
A.18.1.4	Privacidad y protección de información de datos personales	50%	Reproducible Pero Intuitivo	En Cumplimiento	La organización da cumplimiento a la ley de protección de datos personales por medio de diferentes controles administrativos y técnicos. Sin embargo no se ha definido una revisión de este control.
A.18.1.5	Reglamentación de controles criptográficos	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.18.2	Revisiones de seguridad de la información	90%			
A.18.2.1	Revisión independiente de la seguridad de la información	90%	Proceso Definido	En Cumplimiento	Quedó definido dentro del proceso de Auditoría al SGSI
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	90%	Proceso Definido	En Cumplimiento	Su implementación está en curso dentro de los planes de tratamiento de riesgo
A.18.2.3	Revisión del cumplimiento técnico	90%	Proceso Definido	En Cumplimiento	Quedó definido dentro del proceso de Auditoría al SGSI
C	Clausulas ISO27001:2013	90%			

Sección	Control	Resultados Auditoria 1		Estado	Observaciones
C.4	Contexto de la Organización	90%	Proceso Definido	En Cumplimiento	Se está en cumplimiento teniendo en cuenta el establecimiento e implementación del SGSI
C.5	Liderazgo	90%	Proceso Definido	En Cumplimiento	Se está en cumplimiento teniendo en cuenta el establecimiento e implementación del SGSI
C.6	Planificación	90%	Proceso Definido	En Cumplimiento	Se está en cumplimiento teniendo en cuenta el establecimiento e implementación del SGSI
C.7	Soporte	90%	Proceso Definido	En Cumplimiento	Se está en cumplimiento teniendo en cuenta el establecimiento e implementación del SGSI
C.8	Operación	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo y propuestas de proyectos
C.9	Evaluación del desempeño	90%	Proceso Definido	En Cumplimiento	Se está en cumplimiento teniendo en cuenta el establecimiento e implementación del SGSI
C.10	Mejora	90%	Proceso Definido	Observación	Su implementación está en curso dentro de los planes de tratamiento de riesgo y propuestas de proyectos

Tabla 31 Detalle de Resultados de Auditoría

9.3 Resultados de la Auditoría

9.3.1 Diagrama de Radar

La siguiente ilustración representa el diagrama de radar de los niveles de madurez encontrado en la auditoría interna para cada uno de los controles y cláusulas de la norma:

Ilustración 20 Nivel de Madurez De los Controles - Auditoria Interna

9.3.2 Hallazgos de Auditoría

A continuación se muestra una gráfica con las estadísticas de los hallazgos de auditoría, cabe resaltar que no se encontraron No Conformidades Mayores en la auditoría.

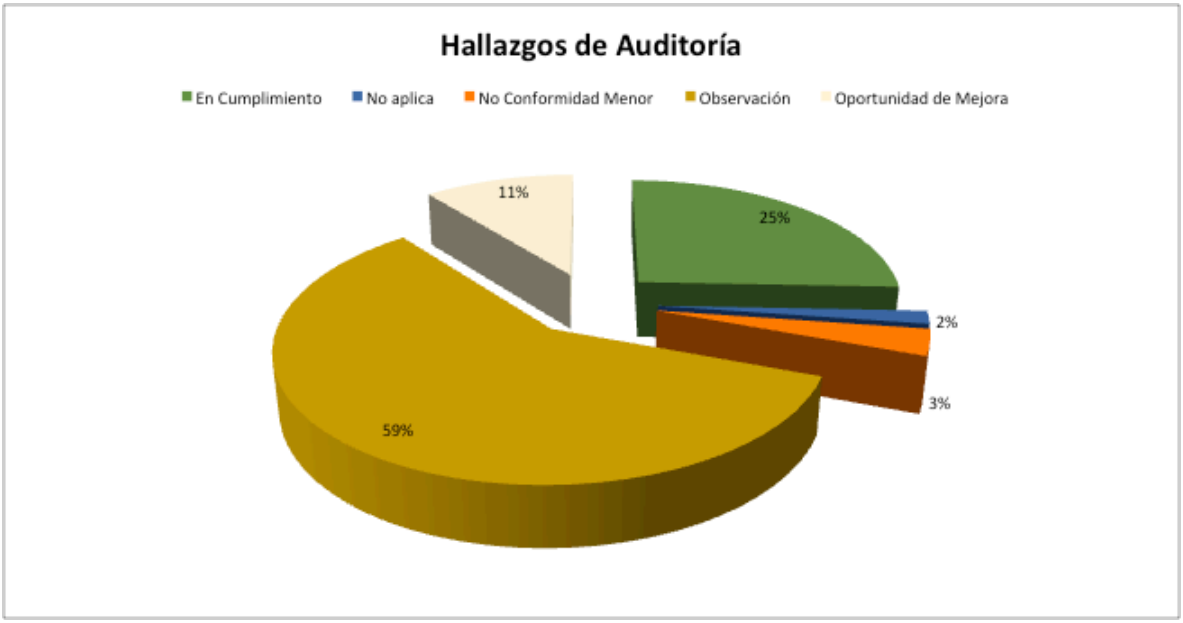


Ilustración 21 Hallazgos de Auditoría – Resúmen

Como puede verse en la Gráfica, el 59% de los hallazgos corresponden a observaciones, todas ellas se generaron por el hecho de que ABC S.A. se encuentra en etapa de implementación de proyectos enfocados a dar cumplimiento a los controles de la norma y a reducir el riesgo a un nivel aceptable, teniendo en cuenta que estos controles están en etapa de implementación no fueron catalogados como no conformidades, se espera que en la siguiente auditoría, se vea reflejado el nivel de implementación de los controles de acuerdo a lo establecido en los proyectos propuestos.

Se encontraron 4 No Conformidades menores que corresponden al 3%, 2 controles no aplican de acuerdo a la declaración de aplicabilidad, 13 oportunidades de mejora que corresponden al 11% de los hallazgos y 31 controles en cumplimiento que equivalen a un 25% del total de los hallazgos.

10 CONCLUSIONES

- Luego del análisis de diferencial se encuentra que 9 de las 14 secciones de controles del anexo A de la norma se encuentran en un nivel de madurez inexistente, 4 en un nivel de madurez inicial y 1 en un nivel de madurez repetible, de acuerdo a los niveles definidos en COBIT 4.1
- Por otro lado, de las 7 cláusulas de la norma, 4 se encuentran en un nivel inexistente, 2 en nivel repetible y 1 en nivel definido.
- Los resultados del análisis diferencial son coherentes teniendo en cuenta que **ABC S.A** no había asignado recursos anteriormente a los aspectos de seguridad de la información y estos no habían sido reconocidos como parte de la estrategia corporativa.

- Con respecto a la declaración de Aplicabilidad, ABC S.A. ha decidido excluir los controlores A.8.3.3 y A.14.2.7 correspondientes a "Transferencia de Medios Físicos" y "Desarrollo Externo" respectivamente.
- ABC S.A. ha definido como nivel de riesgo aceptable el valor "3" en una escala de 1 a 5.
- Una vez realizado el análisis de riesgo inherente para ABC S.A. se encontraron 16 riesgos por fuera del valor de riesgo aceptable.
- Con el fin de mejorar el nivel de riesgo y entrar en cumplimiento con la norma ISO 27001 en su versión 2013, ABC S.A. ha programado la ejecución de 9 proyectos que se consideran prioritarios y fundamentales. El Costo total de dichos proyectos es de € 165.105, y tienen una duración estimada de 239 días.
- Dentro de la auditoría realizada al Sistema de Gestión de Seguridad de la Información de ABC S.A. realizada entre el 18 y 21 de mayo de 2015, no se encontraron no conformidades mayores, se encontraron 4 conformidades menores y 13 oportunidades de mejora.
- Como observación general debe decirse que debido al estado inicial del SGSI, el 59% de los controles de la norma se encuentran en estado de implementación dentro de lo establecido por ABC S.A en su plan de tratamiento de Riesgos, en esta auditoría inicial no se catalogan como no conformidades pero debe tenerse en cuenta que en futuras auditorías al sistema se espera que el nivel de madurez de dichos controles ya haya aumentado.

11 BIBLIOGRAFÍA

Cruz Allende Daniel, Garre Gui Silvia. (2011). *Sistema de Gestión de Seguridad de la Información – Material Docente de la UOC* (1ª. ed.). Barcelona: Eureca Media, SL.

ISO/IEC. (2014). 27000 *Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary* (3a. ed.).

ISO/IEC. (2013). 27001 *Information Technology – Security Techniques – Information Security Management Systemas – Requirements* (2a. ed.).

ISO/IEC. (2013). 27002 *Information Technology – Security Techniques – Code of Practice for Information Security Controls* (2a. ed.).

Ministerio de Hacienda y Administraciones Públicas, Gobierno de España. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información versión 3.*

12 ANEXOS

ANEXO 1 – POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA ABC S.A

1. Objetivo

Presentar a los funcionarios, contratistas, terceros, clientes y directivos de **ABC S.A** los estatutos que establece la alta dirección de la compañía con respecto a la Seguridad de la Información que se almacena, procesa, genera o transmite dentro de sus procesos de misionales, estratégicos y de negocio.

2. Alcance

Esta política aplica para la sede en Bogotá de **ABC S.A**, de ahora en adelante **ABC S.A** y abarca a todos los empleados, contratistas, personal freelance, proveedores, y en general a cualquier persona natural o jurídica que interactue en los procesos de creación, almacenamiento, transmisión, tratamiento o acceso a la información de **ABC S.A.**

3. Política General de Seguridad de la Información

La alta dirección de **ABC S.A** reconoce la información como uno de sus principales activos, por lo tanto, se compromete con:

- La protección de la Integridad, Confidencialidad y Disponibilidad de la misma.
- Garantizar la provisión de los recursos, tecnológicos, humanos y económicos necesarios para la adecuada protección y manejo de la información.
- Asignar las responsabilidades y autoridades adecuadas a cada rol de la organización con respecto a los aspectos de la seguridad de la información.

Y establece que todos los roles que participan en los procesos de la compañía tanto misionales como estratégicos y de apoyo deben conocer y cumplir con la debida diligencia las autoridades y responsabilidades asignadas a su cargo con respecto a la protección de la seguridad de la información.

4. Revisión

Esta política será revisada anualmente con el fin de modificarla de acuerdo a las acciones de mejora continua que se detecten como necesarias durante el proceso de monitoreo del Sistema de Gestión de Seguridad de la Información.

5. Divulgación

Esta política debe ser divulgada a todas las partes interesadas y se debe garantizar que todas ellas la comprenda y apliquen de manera adecuada.

6. Políticas de Alto Nivel

Las siguientes políticas de alto nivel tienen como objetivo desarrollar la política general de seguridad de la información en aspectos más específicos.

7. Política de Uso de Internet y Correo Electrónico

Tanto Internet como el Correo Electrónico corporativo son considerados recursos que la organización pone a disposición de sus colaboradores para facilitar el desempeño de sus funciones. Como tal, estos deben ser utilizados de manera adecuada teniendo como premisa proteger la información de **ABC S.A**

La navegación en internet desde la red de datos de **ABC S.A** debe ser utilizada solamente para temas laborales, no está permitida la navegación para fines personales, por ningún motivo se permite el acceso a sitios web que puedan contener código malicioso o que puedan representar un riesgo para la seguridad de la información.

8. Política de Seguridad de la Información en Teletrabajo

Todos aquellos roles que por la naturaleza de sus funciones deban trabajar en modo remoto, deben ceñirse a las mismas políticas de seguridad que aplican para la red interna de **ABC S.A** Esto incluye garantizar que el equipo que usan para acceder a los sistemas de información esté libre de software mal intencionado, y debe cumplir con los requisitos mínimos de seguridad de la información.

9. Política de Uso Aceptable de Activos

Todas las partes interesadas que dentro de sus labores tengan interacción alguna con los activos de información de **ABC S.A** deben usarlos para los fines relacionados con su labor y protegerlos de acuerdo a las políticas de seguridad de la compañía y al principio de debida diligencia. No es permitido usar los activos de información de la compañía para fines diferentes a los que están designados.

10. Política de Control de Acceso

El acceso a los sistemas de información y en general a la información en cualquier medio que esté almacenado, deberá regirse por el principio de “Necesidad de Conocer”, es decir, solamente deberán acceder a ella las personas, o sistemas que por sus labores o funciones necesiten hacerlo.

ANEXO 2 – FORMATO PARA EL PLAN DE AUDITORÍA INTERNA

Objetivo de la auditoría: ____

Alcance: ____

Auditores: ____

Fecha de inicio de la auditoría (dd/mm/aa): __________ **Fecha de finalización de la auditoría (dd/mm/aa):** __________

Normatividad relacionada: ____

Tabla de actividades						
Fecha	**Hora**	**Lugar**	**Auditor**	**Actividad**	**Documentación relacionada**	**Responsable ABC S.A.**

ANEXO 3 – FORMATO PARA EL INFORME DE AUDITORÍA INTERNA

INFORME DE AUDITORIA INTERNA SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

<FECHA>

ABC S.A

1 INTRODUCCIÓN

1.1 Objeto de la Auditoría

1.2 Alcance de la Auditoría

1.3 Fecha de la Auditoría

1.4 Lugar

1.5 Áreas Auditadas

1.6 Equipo Auditor

1.7 Personal Auditado

2 HALLAZGOS DE AUDITORÍA

HALLAZGOS DE LA AUDITORÍA				
ID	Hallazgo	Numeral(es) de la Norma Relacionado(s)	Descripción	Tipo de hallazgo (No Conformidad Mayor, No Conformidad Menor, Recomendación)

3 CONCLUSIONES

FIN DEL INFORME

ANEXO 4 – FORMATO PARA EL INFORME DE ENTRADA

INFORME DE ENTRADA
1. Resumen de la Revisión Anterior

2. Resumen Ejecutivo de Indicadores

2.1. Auditorías realizadas al SGSI

2.2. Efectividad de las Acciones Correctivas

2.3. Gestión de Hallazgos de Auditorías

2.4. Impartición de Charlas de Concienciación

2.5. Resultados de las Tomas de Conciencia

2.6. Incidentes Atendidos	2.7. Lecciones Aprendidas

2.8. Ejecución de Planes de Tratamiento

3. Resumen ejecutivo de Hallazgos de Auditoría

4. Resumen Ejecutivo de la Gestión de Incidentes de Seguridad

ANEXO 5 – FORMATO PARA EL INFORME DE SALIDA

INFORME DE SALIDA

1. Fecha de Reunión: _____

2. Asistentes a la Reunión de Revisión:

3. Resultados de la Revisión de Indicadores:

4. Resultados de la Revisión de la Política de Seguridad de la Información:

5. Resultados de la Revisión del Alcance del SGSI:

6. Resultados de la Revisión del Nivel de Riesgo Aceptable:

7. Conclusiones:

ANEXO 6 – RIESGO INHERENTE

El Anexo 6 consite en una tabla en formato Excel que contiene el análisis de riesgo inherente para los activos de información de ABC S.A. que hacen parte del alcance del SGSI.

Para los cálculos se tuvo en cuenta el valor del activo en cada una de sus dimensiones de seguridad:

- Autenticidad
- Confidencialidad
- Integridad
- Disponibilidad
- Trazabilidad

ANEXO 7 – DETALLE DE LA PROPUESTA DE PROYECTOS

En el archivo anexo puede verse el consolidado de proyectos propuestos incluyendo su duración, costo, perfiles estimados e interdependencia entre sus tareas. Se adjunta también el proyecto completo en formato pdf, pero debe tenerse en cuenta que en este formato no se cuenta con toda la información disponible en Mircrosoft Project.

ANEXO 8 – PLAN DE AUDITORÍA INTERNA

Para la realización de la auditoría interna del SGSI, se realizó un plan de auditoría tal y como lo pide el “Procedimiento de Auditorías Internas” y de acuerdo al formato establecido en el Aneo 4 de esta memoria.

ANEXO 9 – INFORME DE AUDITORÍA

El Anexo 9 contiene el informe de la auditoría interna realizada al SGSI de ABC S.A. entre el 18 y el 21 de mayo de 2015, dicho informe fué elaborado de acuerdo a lo establecido en el procedimiento de auditorías internas de la organización.