SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS TRES PROCESOS MISIONALES DE LA CORPORACIÓN AUTÓNOMA REGIONAL DE RISARALDA (CARDER)

PROYECTO

JUAN GUILLERMO ESPINOSA BETANCUR

RAFAEL SANTIAGO GARCÍA GALLO

ALEXANDER GIRALDO RESTREPO

UNIVERSIDAD AUTÓNOMA DE MANIZALES

FACULTAD DE INGENIERÍA

MAESTRÍA EN GESTIÓN Y DESARROLLO DE PROYECTOS DE SOFTWARE

(COHORTE IV)

2016

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS TRES PROCESOS MISIONALES DE LA CORPORACIÓN AUTÓNOMA REGIONAL DE RISARALDA (CARDER).

JUAN GUILLERMO ESPINOSA BETANCUR

RAFAEL SANTIAGO GARCÍA GALLO

ALEXANDER GIRALDO RESTREPO

PRESENTADO A:

CARLOS VILLAMIZAR R.

UNIVERSIDAD AUTÓNOMA DE MANIZALES

FACULTAD DE INGENIERÍA

MAESTRÍA EN GESTIÓN Y DESARROLLO DE PROYECTOS DE SOFTWARE

(COHORTE IV)

2016

TABLA DE CONTENIDO

TABLA DE CONTENIDO 3

LISTA DE TABLAS 8

INTRODUCCIÓN. 10

1. REFERENTE CONTEXTUAL. 11

1.1. DESCRIPCIÓN DEL ÁREA PROBLEMÁTICA 11

1.2. ANTECEDENTES 12

1.3. JUSTIFICACIÓN. 16

1.4. PROBLEMA DE INVESTIGACIÓN 18

1.5. OBJETIVOS 18

OBJETIVO GENERAL. 18

OBJETIVOS ESPECÍFICOS 18

1.6. RESULTADO ESPERADO. 19

2. ESTRATEGIA METODOLÓGICA 20

2.1. METODOLOGÍA. 20

2.2. PLANEAR 21

2.3. HACER 24

2.4. PRESUPUESTO. 25

3. DESARROLLO. 26

3.1. REFERENTE TEÓRICO. 26

3.1.1. MARCO INSTITUCIONAL 26

3.1.2. GOBIERNO EN LÍNEA 28

3.1.3. MARCO LEGAL 30

3.1.4. MARCO DE REFERENCIA 33

3.2. PLANEACIÓN DEL SGSI 48

3.2.1. DEFINICIÓN DEL ALCANCE DEL SGSI 48

3.2.2. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LA CARDER 48

EXPLICACIÓN DEL OBJETIVO DEL DIAGNÓSTICO. 50

REVISIÓN PRELIMINAR DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN EXISTENTE 51

PRESENTACIÓN DE LOS CONTROLES DE ISO 27001 A SER EVALUADOS 51

A5. POLÍTICA DE SEGURIDAD. 58

A6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. 58

A7. SEGURIDAD DE RECURSO HUMANO. 59

A8. GESTIÓN DE ACTIVOS. 59

A9. CONTROL DE ACCESO. 59

A10. CRIPTOGRAFÍA. 59

A11. SEGURIDAD FÍSICA Y AMBIENTAL. 59

A12. GESTIÓN DE COMUNICACIONES Y OPERACIONES. 59

A13. SEGURIDAD DE LAS COMUNICACIONES. 60

A14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN. 60

A15. RELACIONES CON LOS PROVEEDORES. 60

A16. GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN. 60

A17. GESTIÓN DE LA CONTINUIDAD DE NEGOCIO. 60

A.18 CUMPLIMIENTO. 60

3.2.3. IDENTIFICACIÓN DE ACTIVOS 64

3.2.4. GESTIONAR LAS AMENAZAS, VULNERABILIDADES Y RIESGOS RESIDUALES A LOS QUE ESTÁN EXPUESTOS LOS ACTIVOS DEFINIDOS DENTRO DEL ALCANCE DEL SGSI 64

NIVEL DE RIESGO INHERENTE (NRI) 66

ESTIMACIÓN DEL NIVEL DE IMPACTO. 67

ESTIMACIÓN DE NIVEL DE PROBABILIDAD/FRECUENCIA 67

NIVEL DE SOLIDEZ (EFECTIVIDAD) DE LOS CONTROLES 74

NIVEL DE RIESGO RESIDUAL (NRR) 75

LISTADO DE IMPACTOS 76

LISTADO DE AMENAZAS 76

LISTADO DE CONTROLES 76

MAPA DE RIESGOS 76

3.2.5. DECLARACIÓN DE APLICABILIDAD 95

3.2.6. POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN. 104

3.2.7. POLITICAS DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION. 106

3.3. HACER 120

3.3.1. MÉTRICAS DE SEGURIDAD 121

3.3.2. ESTUDIO DE MERCADO 125

4. CONCLUSIONES. 131

5. RECOMENDACIONES. 132

BIBLIOGRAFÍA. 133

ANEXOS 135

ANEXO 1: IMPACTO (RIESGOS) 135

ANEXO 2: VULNERABILIDADES 135

ANEXO 3: CONTROLES 136

ANEXO 4: 138

CARDER - GESTIÓN DE RIESGOS V8.XLSX 138

LISTA DE IMÁGENES

FIGURA 1: MODELO PHVA APLICADO PARA LOS SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN..... 21
FIGURA 2: MAPA DE PROCESOS DE LA CARDER..... 26
FIGURA 3: FAMILIA ISO 27000 PARA SGSI..... 35
FIGURA 4: CONTROLES ISO 27002..... 36
FIGURA 5: MODELO MAGERIT PARA LA GESTIÓN DE RIESGOS..... 41
FIGURA 6: PROCESO PARA LA ADMINISTRACIÓN DEL RIESGO..... 46
FIGURA 7 NIVELES DE MADUREZ..... 54
FIGURA 8: ESTADO ACTUAL DE LOS CONTROLES..... 56
FIGURA 9: NIVEL DE CUMPLIMIENTO ISO 27001..... 57
FIGURA 10: NIVEL DE CUMPLIMIENTO ISO 27001..... 58
FIGURA 11: METODOLOGÍA DE ANÁLISIS DE RIESGO..... 65
FIGURA 12: ELEMENTOS CLAVE PARA ANÁLISIS DE RIESGOS..... 66
FIGURA 13. DISTRIBUCIÓN DEL NIVEL DE RIESGO RESIDUAL..... 78
FIGURA 14. DISTRIBUCIÓN DE LAS AMENAZAS..... 79
FIGURA 15. DISTRIBUCIÓN DE IMPACTOS..... 80
FIGURA 16. IMPACTOS POR PROCESO..... 81
FIGURA 17. RIESGO RESIDUAL POR PROCESO..... 82
FIGURA 18: CARTA DE ACEPTACIÓN DE LA CARDER..... 120

LISTA DE TABLAS

TABLA 1: CUADRO DE RESULTADOS Y/O PRODUCTOS ESPERADOS FORMAN PARTE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: 19
TABLA 2: PRESUPUESTO DEL PROYECTO..... 25
TABLA 3: TABLA DE IDENTIFICACIÓN DE ACTIVOS..... 64
TABLA 4: NIVELES PARA ESTIMACIÓN DEL NIVEL DE IMPACTO 67
TABLA 5: NIVELES PARA ESTIMACIÓN DE PROBABILIDAD/FRECUENCIA..... 68
TABLA 6: I1. BRECHAS EN LA CONFIDENCIALIDAD DE LA INFORMACIÓN 69
TABLA 7: I2. PÉRDIDA DE INTEGRIDAD DE LA INFORMACIÓN..... 69
TABLA 8: I3. INTERRUPCIÓN DE SERVICIOS INFORMÁTICOS QUE AFECTEN LA OPERACIÓN MISIONAL 70
TABLA 9: I4. PÉRDIDA EN LA EFECTIVIDAD DE LOS PROCESOS (RESULTADO)..... 71
TABLA 10: I5. PÉRDIDA EN LA EFICIENCIA DE LOS PROCESOS (USO DE LOS RECURSOS)..... 72
TABLA 11: I6. INFORMACIÓN NO VERAZ 72
TABLA 12: I7. SANCIONES DE TIPO LEGAL 73
TABLA 13: I8. PÉRDIDA DE CREDIBILIDAD, COMPETITIVIDAD O IMAGEN DE LA ENTIDAD..... 74
TABLA 14: ESTIMACIÓN NIVEL DE RIESGO RESIDUAL 75
TABLA 15: MAPA DE RIESGOS..... 77
TABLA 16: CRITERIOS DE ACEPTACIÓN..... 77
TABLA 17: ACTUALIZACIÓN DE MANUALES DE USUARIO..... 85
TABLA 18: ASIGNACIÓN DE ROLES Y PERMISOS..... 86

TABLA 19: IMPLEMENTACIÓN DE ARCHIVOS DE LOG 88

TABLA 20: ACTUALIZACIÓN DE LOS DOCUMENTOS DE LOS PROCEDIMIENTOS DE ADMINISTRACIÓN 89

TABLA 21: IMPLEMENTACIÓN DE BUENAS PRÁCTICAS PARA COPIAS DE RESPALDO 90

TABLA 22: SEGURIDAD DE LA INFORMACIÓN EN APLICACIONES 91

TABLA 23: CONCIENCIACIÓN 92

TABLA 24: MONITOREO DE TRÁFICO DE RED 92

TABLA 25: ALMACENAMIENTO DE DOCUMENTOS CLASIFICADOS 93

TABLA 26: DECLARACIÓN DE APLICABILIDAD 95

TABLA 27: ESTUDIO DE MERCADO 125

Introducción.

Se implementa un Sistema de Gestión de Seguridad de la Información en la Corporación Autónoma Regional de Risaralda (CARDER) para sus tres (3) procesos misionales (Gestión Ambiental Sectorial, Gestión Integral y Ordenamiento Ambiental del Territorio y Gestión Ambiental Territorial), que da importantes resultados y apoya el cumplimiento de los requerimientos del Ministerio de las Tecnologías y Comunicaciones MINTIC, establecidos en el manual 3.1 de Gobierno en Línea, y se ejecutara basándonos en las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013.

Se elaboró un diagnóstico del estado actual de la seguridad de la información en la entidad a través de un análisis de brecha. De este diagnóstico se identificaron las amenazas de seguridad de la información (causas de riesgo) y se procedió a planear e implementar el tratamiento del riesgo para aquellos escenarios que superaban el nivel de riesgo aceptado por la CARDER, se elaboró la declaración de aplicabilidad (SOA) para identificar los controles que se debían implementar, y se diseñó e implementó un nuevo modelo de seguridad de la información para la entidad, con el fin de conservar los pilares de seguridad de la información (Integridad, Confidencialidad y Disponibilidad).

También se construyó el plan de mejora al que la corporación se comprometió a monitorear y ejecutar en la medida que los recursos físicos, humanos y económicos se fueran consolidando.

1. Referente Contextual.

1.1. Descripción del área problemática

CARDER no cuenta con un modelo de seguridad de la información definido en el cual se consideren mecanismos adecuados para proteger la información, ni planes de acción para generar conciencia de la importancia del uso y salvaguarda de la información, razón por la cual se han presentado incidentes leves relacionados con divulgación de información y acceso no autorizado a la misma, lo que ha llevado a la entidad a preguntarse:

- ¿Cuál es la información más importante de la entidad?
- ¿A qué amenazas, vulnerabilidades, riesgos están expuestos los activos de información?
- ¿Cómo mitigar estos riesgos y disminuir su impacto en la entidad?

Por otra parte, desde el punto de vista de cumplimiento normativo, las entidades del orden nacional y territorial deben dar respuesta a la estrategia de gobierno en línea del Ministerio TIC, uno de cuyos componentes transversales es la implementación en 2.015 de un sistema de gestión de seguridad de la información.

Por estas razones, y, sobre todo, para la protección de los pilares de seguridad de la información (Confidencialidad, Integridad y Disponibilidad) CARDER requiere el establecimiento de Sistemas de Gestión de Seguridad de la Información que le permita gestionar los riesgos de seguridad de la información identificados con la ayuda de los controles y los procesos que la norma ISO 27001:2013 sugiere, y al mismo tiempo darle cumplimiento al manual 3.1 de gobierno en línea.

1.2. Antecedentes

De acuerdo al decreto 2482 de diciembre de 2012, el Gobierno Nacional establece los lineamientos para la integración de las políticas de gestión de Tecnologías de Información y Comunicación (TIC) a las políticas administrativas definidas en el artículo 3 del decreto; las cuales se adoptan en CARDER según acuerdo No. 005 de febrero de 2013. En el cuál se fija la creación del grupo de gobierno en línea, con el objetivo de dar cumplimiento a los requerimientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (Ministerio TIC) en el manual 3.1 de Gobierno en Línea (GEL).

Con este manual se determinan los lineamientos que deben seguir las entidades públicas y las particulares que desempeñan labores públicas; con la conciencia de avanzar tecnológicamente, haciendo énfasis en mejorar la transparencia y eficiencia en la gestión estatal, sin hacer de lado la competitividad y el buen desempeño de las empresas, los cuales se ven afectados positivamente gracias a la implementación de las buenas prácticas propuestas por los marcos que le ayudan a cumplir los objetivos organizativos. Para seguridad de la información, la buena práctica sugerida por GEL en su momento fue ISO/IEC 27001:2005, sin embargo, dicha norma fue actualizada el año en 2.013.

Cada día crece a nivel mundial la cantidad de empresas que abordan proyectos de implementación de Sistemas de Gestión de Seguridad de la Información y logran certificarse en la norma ISO27001 (según datos de ISO, al finalizar el año 2012 existían cerca de 20.000 empresas certificadas, de las cuales en Colombia había 58).

Desde hace algunos años la Corporación Autónoma Regional de Risaralda (CARDER), cuenta con un Sistema Integrado de Gestión que incluye las certificaciones en las normas NTC-ISO 9001:2008 Sistema de Gestión de Calidad, NTC-ISO 14001:2004 Sistema de Gestión

Ambiental, NTC-GP Norma Técnica en la Gestión Pública y NTC-OHSAS 18001-2007 Sistema de Gestión de Seguridad y Salud Ocupacional.

A cerca de ese tema se han realizado diferentes trabajos de investigación tanto nacional como internacionalmente, y se hace referencia a algunos de ellos.

IMPLEMENTACION DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA COMUNIDAD NUESTRA SEÑORA DE GRACIA, ALINEADO TECNOLÓGICAMENTE CON LA NORMA ISO 27001

Este trabajo es el resultado de un proyecto de investigación en la Comunidad Nuestra Señora de Gracia, de la ciudad de Bogotá, con la finalidad de implementar un SGSI en dicha institución, quienes realizaron un proceso de diagnóstico, a partir del cual concluyeron que no tenían definidas políticas y procesos adecuados para el correcto manejo de la seguridad de la información. A partir de allí elaboraron un plan piloto para elaborar políticas ajustadas a la norma ISO/IEC 27001 e implementaron un sistema de información para levantamiento de información, análisis de brechas y GAP. Por último, establecieron políticas y controles de mejoramiento de los procesos de seguridad de la información y se definieron declaraciones de aplicabilidad que fortalecieron todo el análisis de riesgos efectuado (1).

Análisis y Evaluación del Riesgo de Información: Un Caso en la Banca. Aplicación del ISO 27001:2005

Este trabajo es realizado en un Banco comercial de Perú, donde se hace una definición del alcance mediante la metodología de las elipses para un proceso particular de la entidad en cuanto a la gestión de cuentas corrientes. La gerencia del banco ante el aumento de riesgos y fraudes en el manejo de la información en muchos de sus procesos decidió la implementación de un SGSI ISO27001:2005. Este modelo fue implementado en el proceso de cuentas corrientes (2).

Diseño del Sistema de Gestión de Seguridad de la Información que Permita Apoyar la Subgerencia de Informática y Tecnología de la empresa de Telecomunicaciones de Bucaramanga Telebucaramanga S.A – E.S.P en el Proceso Certificación en ISO 27000.

Es un trabajo dirigido a la subgerencia de informática y tecnología de Telebucaramanga S.A quienes consientes de los riesgos y amenazas que corren los activos de información de la empresa quisieron diseñar e implementar un SGSI con base a la norma ISO 27000. En su proceso hicieron un proceso de diagnóstico de su estado actual con respecto a la seguridad de la información, análisis de riesgos a nivel tecnológico y de información para la detección de vulnerabilidades de alteración de la información, diseño de una política de seguridad, definición de controles a utilizar y operación del sistema (3).

Política para la seguridad de la información de la Universidad Distrital Francisco José de Caldas.

La Universidad Distrital Francisco José de Caldas enfrenta amenazas de seguridad que la lleva a un proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales. De tal manera ha definido una política de seguridad de la información que permite detallar el alcance de la misma, identificar, clasificar y valorar los activos de información, valorar la seguridad de los recursos humanos, determinar las responsabilidades del personal, valoración de seguridad física, controles de acceso, entre otras políticas (4).

Implementación del Primer Sistema de Gestión de Seguridad de la Información, en el Ecuador, Certificado bajo la Norma ISO27001:2005

Este proyecto presenta un resumen de la metodología de implementación del sistema de gestión se seguridad de información y su certificación para una empresa de servicios de telecomunicaciones. Expone en gran medida la totalidad de la metodología empleada para alcanzar este logro, y además hace un gran énfasis particular en las tareas llevadas a cabo para el análisis y evaluación del riesgo, siendo este un esfuerzo multidisciplinario y bajo un enfoque cualitativo ya que fueron considerados todos los activos con mayor facilidad. Este trabajo permitió señalar como uno de los eslabones más débiles el recurso humano de la organización, recomendando por tanto dentro del análisis y evaluación del riesgo del SGSI dar el énfasis necesario para considerar este tipo de amenazas (5).

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL GRUPO EMPRESARIAL LA OFRENDA

Proyecto presentado en la Universidad Tecnológica de Pereira (2012); donde identificaron que el grupo empresarial La Ofrenda S.A no contaba con un sistema de seguridad de la información por lo que requerían garantizar que los riesgos de la seguridad de la información fueran conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. El principal objetivo en dicho trabajo fue el diseño del sistema de gestión de seguridad de la información para el grupo empresarial la Ofrenda, para la consecución del proyecto iniciaron con la determinación de riesgos en la información, medición del nivel de impacto de dichos riesgos, construcción de planes de mitigación de riesgos, uso de herramientas tecnológicas para la gestión de la seguridad de la información y por último la aplicación de los controles de la norma ISO 27001-2013

1.3. Justificación.

El Ministerio de Tecnologías de la Información y las Comunicaciones (TIC) busca mejorar el servicio que las entidades públicas prestan a los ciudadanos con el fin de construir un estado más productivo, más transparente y más participativo generando con ello mayor eficiencia de los procesos y por ende mayor confianza en la entidad al mejorar la calidad de vida de los ciudadanos.

Por este motivo las entidades públicas prestarán servicios en línea a los ciudadanos haciendo uso de las Tecnologías de la Información y las Comunicaciones (TIC), ofreciendo así la posibilidad de realizar todo tipo de consultas y de trámites a través de Internet.

Para implementar estas medidas las entidades deben hacer pública la información y permitir el acceso a sus sistemas de información, lo cual implica tener en cuenta aspectos importantes como la veracidad de la información y la continuidad del negocio.

Al hacer pública la información, se incrementa su vulnerabilidad y aumentan las amenazas abriendo la posibilidad de que se presenten ataques, fraudes, espionaje, virus informáticos, vandalismo y sabotaje de los contenidos lo cual genera perdida de confidencialidad e integridad de la información.

El segundo aspecto a tener en cuenta es la ocurrencia de incidentes causados de forma voluntaria o involuntaria como son, los cortes eléctricos o incendios o incluso los causados por desastres naturales, como terremotos o inundaciones, los cuales interfieren en la disponibilidad de la información.

Con el objetivo de que las empresas puedan desarrollar e implementar estas condiciones, el gobierno a través de la estrategia de Gobierno en Línea y basándose en la familia de normas ISO 27000, ha creado una serie de instrumentos con lineamientos, buenas prácticas y una hoja de ruta

para la implementación de la arquitectura de la tecnología de la información (TI), que les ayudan a garantizar que la tecnología que ponen a disposición de la ciudadanía sea de valor.

La CARDER, siendo una entidad pública de gran valor para la ciudad de Pereira, desea y debe cumplir con estos lineamientos del ministerio de Tecnologías de la Información y las Comunicaciones (TIC) y a través de este proyecto se busca determinar cómo la entidad puede asegurar de forma efectiva la información generada y utilizada por los procesos misionales del negocio, sumado a la magnitud que representa dar el cumplimiento al componente de seguridad de la información de la estrategia de Gobierno en Línea, es lo que justifica el presente proyecto, el cual se va a llevar a cabo por medio del diseño y desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI).

Con ello se pretende realizar un análisis inicial del estado actual en seguridad de la información (análisis de brecha o GAP Analysis), identificar los riesgos a los que está expuesta la información y crear políticas y procedimientos de seguridad de la información con el fin de reducir el impacto causado por la falta de gestión de la seguridad de la información, minimizar las consecuencias derivadas de las situaciones de riesgo y evitar cualquier tipo de sanción que pueda ser impuesta por el incumplimiento de la estrategia de Gobierno en Línea.

Con el fin de apoyar esta estrategia, el enfoque del SGSI se centrará en los tres (3) procesos misionales, los cuales, de acuerdo al mapa de procesos de la entidad, son los procesos críticos y que proponen el punto de partida del SGSI visionando una aplicación a los demás procesos de la entidad una vez se avance en la madurez de la seguridad de la información.

También es importante fomentar la importancia del SGSI y que exista un compromiso por parte de todas las áreas y dependencias de la entidad las cuales deben formar parte activa del proceso, así como también es importante determinar los recursos económicos, físicos y humanos

que posea la entidad, ya que dependiendo a estos se determinará el tratamiento de los riesgos (mitigar, asumir, aceptar o transferir) y se asumirán compromisos con el proceso basado en la mejora continua.

1.4. Problema de investigación

¿Cómo CARDER puede asegurar de forma efectiva la información generada y utilizada por los procesos misionales del negocio y dar cumplimiento al componente de seguridad de la información de la estrategia de Gobierno en Línea?

1.5. Objetivos

Objetivo general.

Diseñar y desarrollar un Sistema de Gestión de Seguridad de la Información para los tres (3) procesos misionales de la Corporación Autónoma Regional de Risaralda (*Gestión ambiental sectorial, Gestión integral y Ordenamiento ambiental del territorio y Gestión ambiental territorial*), basados en las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013.

Objetivos específicos

- Adoptar el modelo PHVA de mejoramiento continuo para el diseño e implementación del Sistema de gestión de Seguridad de la Información, haciendo énfasis en las fases Planeación e Implementación como se detalla en el numeral 6. Estrategia Metodológica.
- Elaborar un diagnóstico de la situación actual de la seguridad de la información en la CARDER, por medio de los procesos descritos en la norma ISO/IEC 27001:2013 e ISO/IEC 27002:2013.
- Gestionar los riesgos de seguridad de la información a través de una metodología de riesgos repetible y perdurable.

- Establecer las políticas, procesos y procedimientos de seguridad necesarios para mitigar los riesgos y mejorar la seguridad de la información en la CARDER.
- Elaborar un estudio comparativo de algunas herramientas de software que sirvan para dar auto sostenibilidad al SGSI.

1.6. Resultado esperado.

En general la implementación del SGSI en CARDER contribuirá a:

1. Satisfacer las expectativas de las partes interesadas en cuanto a seguridad de la información tomando en cuenta los riesgos críticos de seguridad y la legislación vigente.
2. Brindar confianza en el cumplimiento de las normativas estatales
3. Proporcionar un fundamento sólido para una gestión de riesgos eficiente y efectiva, una mejora de procesos, una respuesta rápida a incidentes y gestión de continuidad
4. Aumentar la previsibilidad y reducir la incertidumbre en las operaciones del negocio al reducir los riesgos a niveles definibles y aceptables
5. Proteger la reputación de la organización

Y para dar cumplimiento a los objetivos del SGSI a continuación se muestra una tabla que refleja cada uno de los resultados, su beneficiario y los encargados de producir ese resultado.

Tabla 1: Cuadro de resultados y/o productos esperados forman parte del Sistema de Gestión de Seguridad de la Información:

RESULTADOS	BENEFICIARIOS	ENCARGADOS
DIAGNOSTICO CON EL ESTADO ACTUAL (ANALISIS DE BRECHA)	CARDER	Rafael Santiago García Juan Guillermo Espinosa Alexander Giraldo
INVENTARIO DE ACTIVOS QUE SE ENCUENTRAN EN EL ALCANCE DEL SGSI	CARDER	Rafael Santiago García

DOCUMENTO DE EVALUACION Y GESTION DE RIESGOS	CARDER	Juan Guillermo Espinosa Alexander Giraldo Rafael Santiago García
DECLARACION DE APLICABILIDAD	CARDER	Juan Guillermo Espinosa
MANUAL DE SEGURIDAD DE LA INFORMACIÓN (POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACION)	CARDER e interesados en general	Juan Guillermo Espinosa Alexander Giraldo Rafael Santiago García
METRICAS E INDICADORES DE SEGURIDAD DE LA INFORMACION	CARDER	Rafael Santiago García Juan Guillermo Espinosa Alexander Giraldo.
ESTUDIO COMPARATIVO DE HERRAMIENTAS	CARDER	Alexander Giraldo

2. Estrategia Metodológica

2.1. Metodología.

Para el desarrollo del proyecto y dar cumplimiento al primer objetivo, el modelo a emplearse será PHVA (Planear, Hacer, Verificar, Actuar), basado en la norma ISO/IEC 27001:2013, como se muestra en la figura 1 (aunque ISO27001:2013 no indica explícitamente la adopción del modelo de procesos PHVA, tampoco hay una restricción para su uso).

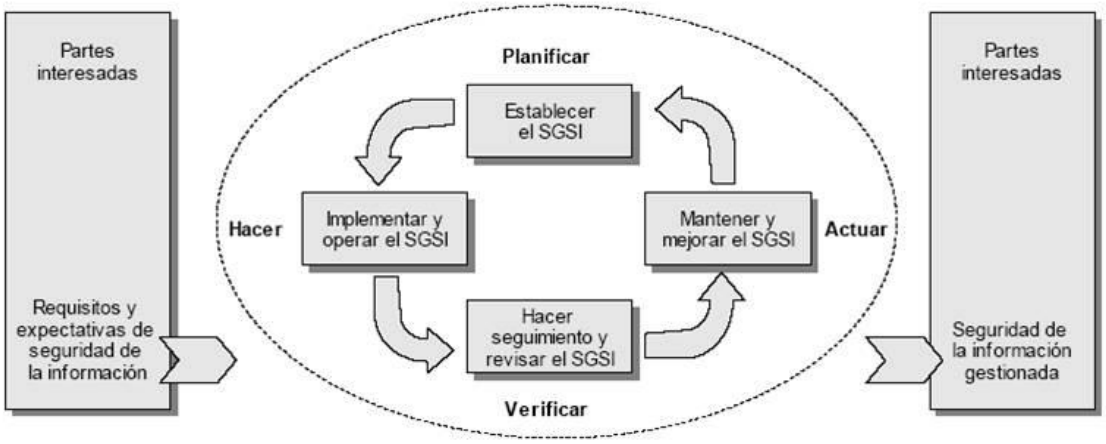


Figura 1: Modelo PHVA aplicado para los Sistemas de Gestión de Seguridad de la Información

Para la ejecución del modelo planteado y en alineamiento con el manual 3.1 de Gobierno en Línea (y los Anexos Técnicos que soportan la implementación del modelo – Anexo 13 – Fase Plan y Anexo 14 – Fase Hacer) se desarrollaran únicamente las fases de **Planear y Hacer**, considerando que para los ejecutores del proyecto es imposible éticamente realizar la evaluación del SGSI en la etapa de Verificación y de igual manera la ejecución del plan de acciones correctivas en la etapa de Actuar, pues para la implementación y la ejecución de esta etapa se considera como limitación la falta de recursos económicos ya que siendo la CARDER una entidad pública, los recursos para ejecutar proyectos se deben solicitar con un (1) año de anticipación. Igualmente, para lo concerniente a Gestión de Riesgos se utilizarán la metodología y criterios establecidos en la Guía de Administración de Riesgos del DAFP y el catálogo de amenazas de seguridad por tipo de activo identificado en MAGERIT.

2.2. Planear

La primera etapa del proyecto se centra en establecer las políticas, objetivos, procesos y procedimientos de seguridad necesarios para gestionar los riesgos y mejorar la seguridad de la

información, con el fin de entregar resultados afines a las políticas y objetivos de la organización.

Según el estándar establecido en la ISO/IEC 27001, en la fase de Planificación se incluirá lo detallado a continuación:

Definición del Alcance del SGSI.

Uno de los pasos más importantes a la hora de implementar un SGSI es definir adecuadamente el alcance. ¿Qué ámbito debe cubrir? Suele ser un tema complicado de decidir, principalmente porque un alcance global, que cubra toda la organización, no suele ser ni la opción más eficiente ni la más eficaz. Es por ello que el alcance del SGSI se centrará en los procesos misionales de CARDER.

Elaboración y documentación de un diagnóstico de la situación actual de la seguridad de la información en la CARDER.

Para esta actividad realizará un análisis de brecha, el cual nos permitirá conocer el estado actual de la entidad, conocer que áreas pueden ser mejoradas y hacer una comparación entre la actualidad y las recomendaciones de lo que se puede hacer a futuro.

Esta actividad se realizó con la ayuda de una matriz donde se listan los controles de la norma ISO 27001:2013 (anexo 2). Aquí define el estado actual que tiene el control en la organización de acuerdo a los niveles de madurez de COBIT 4.1, comentarios y recomendaciones acerca del control, si aplica o no aplica junto con su justificación y el valor asociado a cada nivel de madurez. Para recoger la información de esta matriz, se diseñará una encuesta que será aplicada a los encargados de cada proceso.

De acuerdo a la información que arroja esta matriz, se generará un informe que será entregado a la entidad donde se evidencia cual es el estado actual respecto a la seguridad de la información con respecto al ideal.

Identificación de activos de información

Aquí se realiza una clasificación y valoración para determinar la importancia del activo para la entidad; se definirán los propietarios y los procesos a los cuales pertenecen, mediante el uso de una hoja de Excel donde registramos la información del propietario del activo, el proceso al que pertenece, los niveles de integridad, confidencialidad y disponibilidad del activo, así como su importancia dentro de la entidad.

Se realizarán entrevistas con las personas involucradas en cada proceso para identificarlos, y definir la importancia que este tiene.

Gestionar los impactos (riesgos), amenazas y vulnerabilidades a las que están expuestos los activos definidos dentro del alcance del SGSI, con la ayuda de la metodología MAGERIT.

El instrumento utilizado para identificar los impactos (riesgos) se puede ver en el anexo 3, donde para cada activo de información se identifican las amenazas y las vulnerabilidades, el impacto (riesgo) más relevante para el proceso, el nivel de impacto, nivel de probabilidad y nivel de riesgo inherente; además, calcula el riesgo residual y el nivel de riesgo residual asociado. Después de haber identificado los riesgos residuales, usando el mismo instrumento, definimos cuales son los controles para que cada riesgo pueda ser mitigado.

Definir y documentar los riesgos residuales

Los escenarios de riesgos que pueden permanecer luego de realizar las acciones de mitigación, deberán clasificarse como aceptables o inaceptables para la organización y ser

puestos a consideración de la dirección a fin de ser aprobados antes continuar con la fase de implantación.

Elaborar una declaración de Aplicabilidad

Basados en el anexo 2, se obtiene la lista de controles del Anexo A de ISO27001:2013 que fueron definidos como aplicables, teniendo en cuenta aquellos controles que se van a implementar y aquellos que se van a excluir para generar el documento SOA (Statement of Aplicability) especificado en los entregables.

Definir una Política y el nuevo modelo de seguridad de la Información para CARDER

Este documento incluye políticas de seguridad detalladas y procedimientos de seguridad. Y da cumplimiento al objetivo 4

Autorización de la gerencia

Obtener la autorización de la gerencia para implementar y operar el SGSI.

2.3. Hacer

Implementar y operar la política, controles, procesos y procedimientos del SGSI. Según el estándar establecido en la ISO/IEC 27001, en la fase de Implementación se incluirá lo detallado a continuación:

- Elaboración de un plan para el tratamiento de riesgos, identificando la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información.
- Implementar el plan para el tratamiento de riesgos de tal forma que se puedan cumplir los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades.

- Implementar los controles para el tratamiento de los riesgos que fueron seleccionados en la fase de planeación, para cumplir los objetivos de control, mediante una prueba piloto.
- Definir como se medirá la eficacia de los controles o grupo de controles seleccionados, y especificar cómo se van a usar estas mediciones con el fin de valorar la eficacia de los controles para producir resultados comparables y reproducibles.
- Implementar las políticas y procedimientos de seguridad definidos de acuerdo a la Declaración de Aplicabilidad.

2.4. Presupuesto.

Tabla 2: Presupuesto del Proyecto

DETALLE	DESCRIPCIÓN	VALOR (COP)
Personal	Asesor del proyecto	
Bibliografía	Libros y normas	600.000
	Fotocopias	100.000
Viajes y viáticos	Desplazamientos a la entidad en la ciudad de Pereira	1’000.000
Documento final	Impresión	200.000
	Empastes	50.000

Nota: Se aclara que este presupuesto es únicamente para el desarrollo de este Proyecto de Maestría y no para la Implementación del SGSI.

3. Desarrollo.

3.1. Referente Teórico.

3.1.1. Marco Institucional

La Corporación Autónoma Regional de Risaralda CARDER es una entidad pública, encargada de administrar y controlar los recursos naturales del departamento de Risaralda; al ser la autoridad ambiental la corporación genera gran cantidad de información diariamente que debe ser conservada de una manera adecuada. A continuación, se presenta el Mapa de Procesos de la entidad de acuerdo al Sistema de Gestión de Calidad ISO9001.



Figura 2: Mapa de procesos de la CARDER

CARDER debe implementar y acoger el Manual de Gobierno en línea, que es el resultado de la evolución de la Estrategia de Gobierno en línea establecida mediante el Decreto 1151 del 14 de abril de 2008 y determina los lineamientos que deben seguir las entidades públicas y los particulares que desempeñan funciones públicas en la implementación de la Estrategia de Gobierno en línea en Colombia.

Dada la dinámica propia de las Tecnologías de la Información y las Comunicaciones (TIC), la información de este Manual se actualiza periódicamente, con la colaboración de las entidades públicas y de otros actores relacionados con la Estrategia, con el fin de mantener a los responsables de impulsar y desarrollar la Estrategia de Gobierno en línea en las diferentes entidades públicas:

El Decreto 2693 de 2012 está dirigido a las entidades de la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen con funciones administrativas. El Manual de Gobierno en línea vigente es la versión 3.1.

El manual 3.1 de gobierno en línea busca cumplir con seis (6) componentes que están distribuidos en elementos trasversales, información en línea, integración en línea, transacción en línea, transformación y democracia, con la implementación de estos elementos el gobierno nacional busca cambiar la manera de operar de los estados y de las entidades.

La implementación de la Estrategia de Gobierno en línea requiere que se desarrollen actividades que no están asociadas a un solo Componente, pues implican consideraciones o análisis que impactan las diferentes áreas temáticas y sirven de soporte a éstas. Por esta razón se conforma un Componente de Elementos Transversales.

En la ejecución del componente número uno (1) elementos trasversales, es necesario implementar un sistema de gestión de seguridad de la Información. Las entidades poseen en la información un activo de gran importancia que debe ser protegido, para lo cual se deben tener en cuenta los riesgos en los diferentes espacios y momentos en los que ésta se manipula. La protección de datos personales, el manejo de la reserva, la gestión segura de la tecnología son elementos cruciales en la protección de la relación del Estado con sus usuarios, razón por la cual

las entidades requieren del establecimiento de sistemas de seguridad de la información que les permitan manejar los riesgos identificados.

La entidad debe establecer su SGSI para sus procesos misionales, de igual forma, dicho sistema debe contemplar el análisis de riesgos y las medidas a implementar para mitigarlos, aceptarlos y eliminarlos.

La Corporación y sus sistemas de información están expuestos cada día a un número más elevado de amenazas, que aprovechando cualquiera de las vulnerabilidades existentes, pueden someter los activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos, estos procedimientos se encuentran explicados en el manual 3.1 de gobierno en línea y son la base para la implementación de la norma ISO 27001.

El Sistema de Gestión de la Seguridad de la Información ayuda a establecer estas políticas y procedimientos en relación a los objetivos de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo.

3.1.2. Gobierno En Línea

En Colombia, la agencia de Gobierno Electrónico (Gobierno en Línea) es la encargada de cumplir a nivel nacional con los estatutos y políticas estipuladas por el Ministerio de las Tecnologías de Información y Comunicación (MinTIC). La Estrategia Gobierno en línea,

liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones, es el conjunto de instrumentos técnicos, normativos y de política pública que promueven la construcción de un Estado más eficiente, transparente y participativo, y que, a su vez, preste mejores servicios con la colaboración de toda la sociedad mediante el aprovechamiento de la tecnología. Lo anterior con el fin de impulsar la competitividad y el mejoramiento de la calidad de vida para la prosperidad de todos los colombianos (MinTIC).

Esta estrategia cuenta con una misión, propósitos y objetivos específicos, los cuales se describen a continuación:

Visión, Propósito y Objetivos Específicos: La visión del Gobierno en línea es la de un Estado construido por y para los colombianos, mediante el aprovechamiento de las TIC, para la prosperidad del país. Esta visión parte de considerar al Estado como una construcción colectiva en el cual, las potencialidades de cada persona pueden ser puestas a disposición de los demás y, a su vez, las instituciones públicas responden de manera efectiva a los intereses de la sociedad, en lo cual las TIC juegan un rol fundamental y generan un impacto positivo sobre la gestión pública, sobre la competitividad y sobre la sociedad en su conjunto.

El propósito es el de contribuir a la construcción de un Estado más eficiente, más transparente y participativo, que presta mejores servicios con la colaboración de toda la sociedad, mediante el aprovechamiento de las TIC. Para alcanzar este propósito se definieron cuatro objetivos específicos:

- Facilitar la eficiencia y colaboración en y entre las entidades del Estado, así como con la sociedad en su conjunto, con procesos que permitan la integración de los diferentes servicios, optimizar y compartir recursos y contar con datos e información de calidad y

oportunos en las instituciones que promuevan a su vez la generación de servicios de valor agregado por parte de terceros.

- Contribuir al incremento de la transparencia en la gestión pública, con una mayor visibilidad de los asuntos públicos y facilitando al ciudadano el conocimiento de la gestión del Estado.
- Promover la participación ciudadana haciendo uso de los medios electrónicos, generando confianza en la administración pública y habilitando nuevos canales para la construcción colectiva de políticas públicas, resolución de problemas, toma de decisiones y control social.
- Fortalecer las condiciones para el incremento de la competitividad y el mejoramiento de la calidad de vida, a partir de la oferta de servicios que respondan a las necesidades de los ciudadanos y las empresas, mejorando su calidad, generando ahorros en costos y tiempos por filas y desplazamientos, con trámites más simples, donde se eliminen pasos y documentos innecesarios, se reduzcan altos costos de transacción, se habiliten múltiples canales y en últimas el ciudadano no tenga que ir de un lugar a otro como mensajero del Estado. MinTIC.

3.1.3. Marco Legal

- ***Documento Conpes 3072 de 2000***: Agenda de conectividad programa presidencial para la identificación de las necesidades de información, computacional y social en Colombia. http://www.mintic.gov.co/portal/604/articles-3498_documento.pdf
- ***Ley 962 de 2005:*** *ley* Anti-tramites, tiene como objetivo facilitar las relaciones de los particulares con la administración pública. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=17004

- ***Ley 1151 de 2007 art 6***: El cual especifica la intención del estado en promover la implementación progresiva del software en las entidades públicas y la inclusión digital. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=25932
- ***Decreto 1151 de 2008:*** Reglamenta los lineamientos de gobierno en línea y empieza a implementar la ley anti- trámites. http://programa.gobiernoenlinea.gov.co/apc-aa-files/e5203d1f18ecfc98d25cb0816b455615/decreto1151abril14de2008_1.pdf
- ***Documento Conpes 3650 de 2010:*** Implementa la agenda de conectividad. http://www.mintic.gov.co/portal/604/articles-3650_documento.pdf
- ***Ley 1450 de 2011 art. 227:*** Administración de bases de datos de acceso permanente, seguro y confiable. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43101
- ***Ley 1450 de 2011 art. 230:*** Establece el cumplimiento de la estrategia de gobierno en línea que será liderada por el MinTIC. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43101
- ***Ley 1450 de 2011 art. 232:*** Haciendo uso de las tecnologías y las comunicaciones ofrecer una oportuna, eficiente y eficaz prestación de servicio en la gestión de las entidades. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43101
- ***Decreto 2693 de 2012:*** Definir lo lineamientos, plazos términos para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones con el fin de contribuir con la construcción de un estado más eficiente más transparente y participativo que preste mejores servicios con la colaboración de toda la sociedad. Utilizar lineamientos o estándares internacionales. http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/decreto-2693-de-2012.pdf

- **Ley 527 de 1999:** Se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276
- **Decreto 1747 de 2000 art 9:** La entidad deberá contar con un equipo de personas, una infraestructura física y tecnológica y unos procedimientos y sistemas de seguridad, tal que puedan generar las firmas digitales propias y todos los servicios para los que soliciten autorización. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277
- **Ley estatutaria 1266 de 2008:** Disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488
- **Ley 1273 de 2009:** Dicta disposiciones para preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
- **Ley 1581 de 2012:** Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492
- **LEY 23 DE 1982:** Reglamenta todas las generalidades sobre las normas que protegen los derechos de autor para cualquier obra científica, literaria u artística. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431

- **LEY 44 DE 1993:** Modifica y adiciona la ley 23 de 1982. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3429.

3.1.4. Marco de Referencia

La historia de la serie 27000 de las normas ISO, estas normas fueron concebidas y anunciadas en 2005, pero su historia inicia desde mucho antes; sus principios se dan en el Departamento de Industria y Comercial del Reino Unido. Su Centro de Computación de Seguridad Comercial tenía la tarea de crear unos criterios de evaluación de la seguridad de productos de TI; y su primer estándar creado fue el ITSEC. (The ISO 27000 Directory, 2007)

ITSEC propone una serie de mediciones técnicas, a las cuales se hace referencia como funciones para "hacer cumplir" la seguridad, con el fin de llevar un control sobre los requerimientos de confidencialidad, integridad y disponibilidad; y para tener confianza de estas funciones se debe asegurar que sean correctas y efectivas. (Department of Trade and Industry, 1991)

De igual manera, fue publicado otro documento denominado DISC PD/003 el cual fue organizado en 10 secciones, cada una alineando una serie de objetivos y de controles; y a pesar de haber sido publicado a principios de 1990, su formato y contenido aún se encuentra disponible en partes de la actual norma ISO 17799/27002. El PD/003 continuó siendo desarrollado bajo la custodia del British Standard Institute, y eventualmente se convirtió en un estándar formal conocido como BS7799:1995.

El estándar BS7799 fue publicado para brindar una guía para implementar la Administración de Seguridad de la Información, y su primera revisión se realizó en abril de 1999 para empezar a integrar los nuevos desarrollos tecnológicos que se venían presentando como eran las redes y las comunicaciones; y tuvieron énfasis en áreas como el comercio electrónico, el

teletrabajo, la computación móvil, etc. En 2005 fue reemplazada y actualizada por el estándar internacional ISO/IEC 27001. (BSI Education, 2008).

ISO/IEC 27001:2005 establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la administración de la seguridad de la información en la organización. Los controles y objetivos en esta norma están implementados para suplir los requerimientos identificados por la evaluación de riesgos. (ISO, 2010)

Este estándar internacional provee a las organizaciones y a las personas una visión general de todas las familias de estándares que contempla el SGSI; una introducción a los SGSI y los términos y definiciones usados para en todas las familias de estándares. Su propósito es describir los fundamentos de los SGSI, que forman el asunto de los SGSI y define los términos relacionados.

Aplica para todo tipo de organizaciones, de cualquier tamaño (empresas comerciales, agencias gubernamentales, organizaciones sin ánimo de lucro)

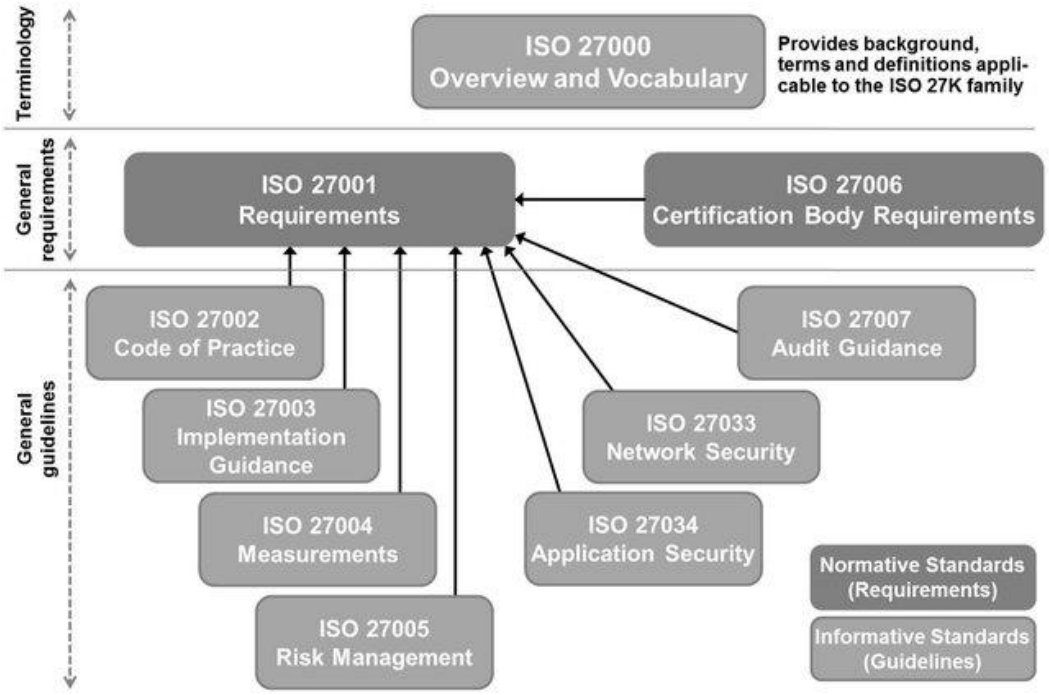


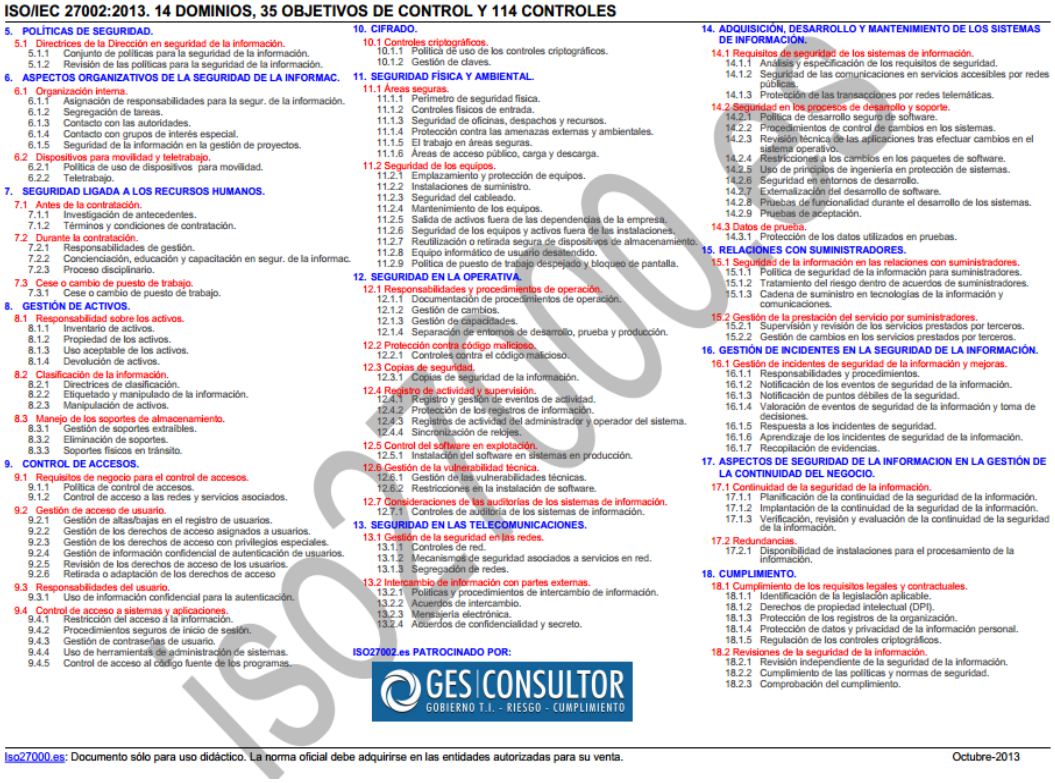
Figura 3: Familia ISO 27000 para SGSI[1]

El estándar ISO 27001 está centrado en los requerimientos para la planeación, implementación, operación y monitoreo y mejoramiento continuo de procesos orientados al SGSI. El enfoque debe estar alineado por el ciclo PHVA. La cobertura y el alcance deben ser definidos para la planeación y la implementación; los riesgos deben ser identificados y evaluados; y los objetivos de control deben ser definidos para la información y los sistemas de información. (Disterer, 2013)

El alcance del estándar ISO27002, según ISO (2005), define que:

Este Estándar Internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

Los objetivos de control y los controles de este Estándar Internacional son diseñados para ser implementados para satisfacer los requerimientos identificados por una evaluación del riesgo. Este Estándar Internacional puede servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales. (p. 13)



ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:
GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

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

15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

ISO27000

Iso27000.es: Documento sólo para uso didáctico. La norma oficial debe adquirirse en las entidades autorizadas para su venta. Octubre-2013

Figura 4: Controles ISO 27002

Para el estándar internacional ISO27003 se centra en los aspectos críticos necesarios para diseñar e implementar exitosamente un SGSI de acuerdo con ISO/IEC 27001:2005. Describe los procesos de especificación y diseño de SGSI desde el origen hasta la producción de los planes de implementación. Describe el proceso para obtener la aprobación administrativa, definir el proyecto y proveer guías en como el SGSI debe ser implementado; dando como resultado un Plan de Proyecto para la Implementación de un SGSI final. (ISO, 2010; Peltier, 2001; ISO, 2005)

Para la Norma Internacional ISO27005 proporciona directrices para la gestión de riesgos de seguridad de información en una organización, apoyando en particular los requisitos de una gestión de la seguridad de la información, evaluando los riesgos, su tratamiento, aceptación, comunicación, vigilancia, y revisión

Contenidos de la norma:

- Introducción
- Ámbito de aplicación
- Referencias normativas
- Términos y definiciones
- Estructura de la norma
- Antecedentes
- Descripción general del proceso SGSI
- Establecimiento del contexto
- Evaluación del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación de los riesgos de seguridad
- Vigilancia y revisión de los factores de riesgo

Para realizar las estrategias propuestas en lo concerniente a los riesgos se trabajó con dos instrumentos que enmarcan los pasos y procedimientos necesarios uno de ellos es MAGERIT, esta metodología habla sobre la implementación del Proceso de Gestión de Riesgos de Seguridad de la Información dentro de un marco de trabajo para que los órganos del gobierno tomen

decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. (Ministerio de Hacienda y Administraciones Públicas, 2012)

MAGERIT es conocida como la Metodología para el Análisis y Gestión de Riesgos de los Sistemas de Información, utilizada para la mitigación y control de los riesgos a los cuales se enfrentan las organizaciones al momento de la implantación y uso de las TIC.

Los principales objetivos en los cuales se enfoca MAGERIT son:

- Brindar una guía y/o metodología ordenada y segura que permita realizar un análisis sistemático de los posibles riesgos resultado del uso de las tecnologías de la información y las comunicaciones.
- Administrar y gestionar oportunamente los riesgos para realizar un tratamiento eficaz de los mismos.
- Propiciar el manejo de las TIC cumpliendo con los estándares regulatorios del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Generar conciencia práctica a los involucrados y responsables de las TIC de la organización sobre la inminente necesidad de la correcta administración de riesgos.

a. Empresas objetivo

La metodología Magerit tiene como objetivo principal la incursión en las entidades de Administración Pública, propiciando y apoyando el cumplimiento de la normatividad de TIC del estado actual para beneficio de toda la ciudadanía.

b. Descripción de las principales fases

Con base en lo que expone el autor (Gaona, 2013), la metodología Magerit dentro de sus componentes establece las siguientes fases de ejecución para la Gestión de Riesgos:

Toma de Datos. Proceso de la Información: En esta fase se determina el alcance del análisis que se realizará para la Gestión de Riesgos de Activos de los Sistemas de Información. Es importante hacer hincapié en los activos críticos de los procesos de la organización.

Dimensionamiento. Establecimiento de parámetros: Determinar los criterios bajo los cuales se definirán los niveles de análisis de la gestión de riesgos. Estos parámetros darán un enfoque de la situación real de la organización.

- Valoración de los Activos: Son los rangos económicos dentro de los cuales se contempla el activo teniendo en cuenta para su clasificación costo de adquisición, valor de reposición, valor de configuración, valor de uso del activo y el valor de pérdida de oportunidad.
- Vulnerabilidad: Frecuencia de ocurrencia de la amenaza detectada a un activo.
- Impacto: Rango de pérdida en cuanto al valor del activo posteriormente a la ocurrencia de un incidente.
- Efectividad del control de seguridad: Efectividad en las medidas tomadas para mitigar el riesgo

Análisis de activos: Identificar todos los activos que entraran dentro del sistema de gestión de riesgos de la organización y clasificarlos con base en la siguiente clasificación:

- Activos físicos.
- Activos lógicos.
- Activos de personal.
- Activos de entorno e infraestructura.
- Activos intangibles.

Análisis de amenazas: Establecer e identificar las situaciones que generan problemas de seguridad y operación para la organización. Es por esto que se las amenazas se clasifican en 4 categorías:

- Accidentes: Eventos provocados por efectos de la naturaleza.
- Errores: Eventos cometidos involuntariamente.
- Amenazas intencionales presenciales: Eventos ocasionados intencionalmente con un objetivo específico por el personal interno de la organización.
- Amenazas intencionales remotas: Eventos provocados por personas externas a la organización.

Establecimiento de vulnerabilidades

Valoración de impactos: Identificar el tipo de daño que un impacto genera en la organización. Teniendo en cuenta los resultados obtenidos de la ocurrencia de una amenaza sobre un activo y la consecuencia generada en los demás activos.

Análisis de riesgo intrínseco: Es el peor caso de riesgo posible en el cual no se haya definido de forma correcta el impacto y/o la vulnerabilidad de este.

- Riesgo Intrínseco (o Inherente): Valor del activo x Vulnerabilidad x Impacto

Influencia de salvaguardias: Definir las acciones que apoyen la mitigación del riesgo del activo en cuanto a vulnerabilidad e impacto.

- **Preventivas:** Encaminadas a la minimización de la vulnerabilidad (NV: Vulnerabilidad * % disminución de la vulnerabilidad, donde NV es la nueva vulnerabilidad definida).
- **Correctivas:** Encaminadas a minimizar el impacto que es generado sobre la amenaza. (NI: Impacto * % disminución del Impacto, donde NI es el nuevo impacto definido).

Análisis de riesgo efectivo (RE): Es el resultado del análisis que se realiza entre el Riesgo Intrínseco y las salvaguardias definidas para el riesgo, donde se utiliza la siguiente fórmula:

- **Riesgo efectivo:** Valor efectivo x Nueva vulnerabilidad x Nuevo Impacto = Valor activo x (Vulnerabilidad x % disminución de vulnerabilidad) x (Impacto x % disminución de impacto) = Riesgo intrínseco x Porcentaje de disminución de vulnerabilidad x Porcentaje de disminución de impacto.

Gestión de riesgos: Finalmente y con las demás fases ejecutadas, se determinó la gestión de riesgos que conlleva a contrarrestar (Reducir, Transferir o Aceptar los riesgos) los posibles eventos ocasionados a los activos críticos de la organización.

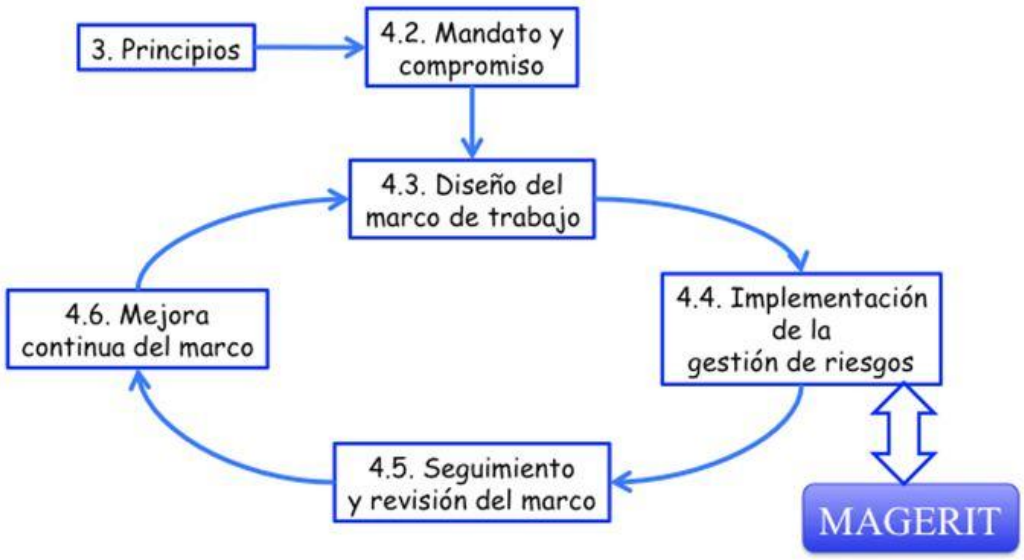


Figura 5: Modelo MAGERIT para la Gestión de Riesgos[2]

Es importante indicar que para el desarrollo del proyecto lo que se utilizó de la metodología MAGERIT fue la tipificación de activos y listados de amenazas y vulnerabilidades. Para la metodología de gestión de riesgos se siguieron los lineamientos del DAFP.

Por otro lado, encontramos el documento elaborado por El Departamento Administrativo de la Función Pública (DAFP) denominado Administración del Riesgo, que tiene como fin entregar lineamientos y aclaraciones sobre la aplicación de la metodología planteada en la guía emitida en el año 2009, esto considerando la importancia cada vez mayor, que para las entidades representa su aplicación como elemento básico en su planeación estratégica.

La administración del riesgo ayuda al conocimiento y mejoramiento de la entidad, contribuye a elevar la productividad y a garantizar la eficiencia y la eficacia en los procesos organizacionales, permitiendo definir estrategias de mejoramiento continuo, brindándole un manejo sistémico a la entidad.

La consigna es que la administración del riesgo sea incorporada en el interior de las entidades como una política de gestión por parte de la alta dirección y cuente con la participación y respaldo de todos los servidores públicos; tarea que se facilitará con la implementación de la metodología aquí presentada, la cual permite establecer mecanismos para identificar, valorar y minimizar los riesgos a los que constantemente están expuestas y poder de esta manera fortalecer el Sistema de Control Interno permitiendo el cumplimiento de los objetivos misionales y los fines esenciales del Estado.

DAFP se encarga de orientar la Política de Racionalización de Trámites y el marco normativo para su implementación, con base en las directrices que sobre la materia expida el Gobierno Nacional; brinda asesoría a los organismos y entidades con el fin de facilitarles la optimización, simplificación, estandarización o supresión de los trámites; realiza seguimiento a

los avances en el proceso de racionalización de trámites desarrollados en cada uno de los sectores y entidades de la Administración Pública.

El artículo 269 la Constitución Política establece:

> *ARTÍCULO 269. En las Entidades Públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la Ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas.*

Según la cartilla para la Administración del Riesgo de la DAFP, se plantean los siguientes objetivos (Benavides, Giraldo, Jaramillo, García, Jiménez, Sanín, 2012, p 9)

- Aumentar la probabilidad de alcanzar los objetivos y proporcionar a la administración un aseguramiento razonable con respecto al logro de los mismos
- Ser consciente de la necesidad de identificar y tratar los riesgos en todos los niveles de la entidad.
- Involucrar y comprometer a todos los servidores de las entidades de la Administración Pública en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos
- Cumplir con los requisitos legales y reglamentarios pertinentes.
- Mejorar el Gobierno.
- Proteger los recursos del Estado.
- Establecer una base confiable para la toma de decisiones y la planificación.
- Asignar y usar eficazmente los recursos para el tratamiento del riesgo.
- Mejorar la eficacia y eficiencia operativa.

- Mejorar el aprendizaje y la flexibilidad organizacional.

Es el modelo estándar de control interno para todas las entidades del estado permitiendo el diseño, desarrollo y operación del Sistema de Control Interno en las entidades, está estructurado en 3 Subsistemas, 9 componentes y 29 elementos

a. Empresas objetivo

Las empresas objetivo obedecen a las entidades de Administración Pública de orden nacional y territorial además de entidades y particulares que ejercen funciones públicas

b. Descripción de las principales fases

El proceso de administración del riesgo se hace de la siguiente forma:

Identificar el riesgo: para identificar el riesgo se deben determinar las causas teniendo en cuenta los factores internos y/o externos que la entidad haya analizado y que puedan afectar el alcance de los objetivos propuestos por la entidad. Entender la importancia del manejo del riesgo implica conocer con más detalle los siguientes conceptos:

- Nombre del proceso.
- Objetivo del proceso: Se debe transcribir el objetivo que se ha definido para el proceso al cual se le están identificando los riesgos.
- Riesgo: Representa la posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la entidad y afectar el logro de sus objetivos.
- Causas (factores internos o externos): Son los medios, las circunstancias y agentes generadores de riesgo. Los agentes generadores que se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo.
- Descripción: Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.

- Efectos: Constituyen las consecuencias de la ocurrencia del riesgo sobre los objetivos de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental. (DAFP, 2011, p 24)

Analizar el riesgo: El análisis del riesgo establece qué probabilidad de ocurrencia del riesgo y los efectos que pueda tener. El análisis del riesgo dependerá, de la información que se obtenga en la fase de identificación

Valorar el riesgo: La valoración del riesgo resulta de la confrontación de los resultados de la evaluación del riesgo con los controles que se han identificado, de esta forma se logra establecer las prioridades para su manejo y las políticas que se implementarán

Gestionar el Riesgo: Gestionar el riesgo consiste en la aplicación de los principios y metodologías propuesta en la Gestión del Riesgo con el fin de darle un correcto tratamiento al riesgo.



Figura 6: Proceso para la administración del riesgo[3]

La seguridad de la información Según la Norma ISO/IEC 27001 (2013): "Esta definida como la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad" (p.3).

Torres (2010) menciona: "El objetivo de la protección son los datos mismos y trata de evitar su pérdida y modificación no-autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo más requisitos como por ejemplo la autenticidad entre otros" (p.44), y la seguridad informática, Según Torres (2010): "… consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la

información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización" (p.37).

Posada y Gómez (2012) mencionan: "En el ámbito de las TI, es necesario analizar cómo preservar el valor del negocio a través de la seguridad que les proporcione las TI para proteger sus activos, conservar la continuidad de los servicios y recuperarlos después de un desastre". (p.11).

De acuerdo a lo establecido en la ISO/IEC 27001:2013, para que un sistema sea realmente fiable y preciso, debe contemplar las siguientes características:

Integridad: "Propiedad de salvaguardar la exactitud y estado completo de los activos". La información solamente podrá ser modificada por el personal que se designe autorizado para realizarlo.

Confidencialidad: "Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados". Lo cual conlleva a determinar que la información sólo podrá ser consultada para el personal autorizado para esto.

Disponibilidad: "Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada". La consulta de información debe ser en tiempo real y al momento que ésta precisamente se necesite.

El riesgo es definido como la probabilidad que una amenaza pueda explotar una vulnerabilidad en particular (Peltier, 2001). La gestión del riesgo, generalmente, contempla el cálculo del riesgo, la apreciación de su impacto en el negocio y la probabilidad de ocurrencia (Hiles, 2004). Luego se derivan pasos para reducir la frecuencia a un nivel considerado aceptable.

3.2. Planeación del SGSI

La primera etapa del proyecto se centró en el establecimiento de las políticas, objetivos, procesos y procedimientos de seguridad necesarios para gestionar los riesgos y mejorar la seguridad de la información. Y para dar cumplimiento a estos objetivos la norma ISO 27001 propone, como primer paso, definir el alcance del SGSI.

3.2.1. Definición del Alcance del SGSI

Definir adecuadamente el alcance del SGSI es uno de los pasos más importantes, principalmente porque debe ser global y que cubra toda la organización; Teniendo esto en cuenta, y de acuerdo a las reuniones sostenidas con el grupo de Gobierno en Línea de la CARDER se definió que los esfuerzos para la implementación del SGSI debería estar centrado en los tres (3) procesos misionales de la corporación, Gestión Ambiental Sectorial, Gestión Ambiental Territorial y Gestión Integral y Ordenamiento Ambiental del Territorio.

3.2.2. Diagnóstico de la situación actual de la CARDER

El análisis de brecha (gap analysis) de seguridad consistió en identificar el nivel de eficiencia y eficacia de los controles existentes en la organización para proteger la integridad, confidencialidad y disponibilidad de sus activos de información, mediante la ayuda de la herramienta del anexo 5 y aplicación de una encuesta (anexo 6).

El objetivo principal fue establecer un estado de la situación inicial de CARDER con respecto a la norma ISO 27001:2013 derivado de la realización del análisis de brecha (gap analysis).

Como consecuencia de dicho análisis se establecieron los siguientes puntos:

- Nivel de madurez de CARDER con respecto a la norma y en general con respecto a la seguridad de la información.

- Primera aproximación del sistema a implantar: recomendaciones de primeros controles, recolección de información que ya posea la empresa, etc.
- Cumplimiento del requisito 4.2.1 j) de la norma ISO27001:2013
- Cumplimiento del requisito “Situación Actual” Manual 3.1 Gobierno en Línea.

El análisis de brecha supone un estudio inicial de la situación de la organización contra la norma ISO 27001: 2013. Supone un análisis de la madurez de la CARDER con respecto a las cláusulas generales de la norma, así como cada uno de los controles del Anexo A de la misma. Para efectos prácticos de este informe, dado que la organización aún no ha implementado su SGSI, sino este está en proceso de diseño e implementación, se suprime el análisis de los requisitos 4 – 10 de la norma ISO27001:2013.

En este sentido la evaluación y análisis se centra en los 114 controles de los anexos de dicha norma.

Este diagnóstico ayudó a definir el punto de partida para la implantación, así como un medio para un primer acercamiento a la organización por parte del equipo, recopilar información que ya disponga CARDER y pueda ser aplicable en la implantación y poder identificar tanto los controles que ya disponen como los que todavía necesitarán implantarse.

Los puntos tratados en el análisis diferencial son los Controles del Anexo A.

- Política de Seguridad.
- Aspectos Organizativos de la Seguridad de la Información.
- Seguridad Ligada a los Recursos Humanos.
- Gestión de Activos.
- Control de Accesos.
- Criptografía

- Seguridad Física y Ambiental.
- Gestión de Comunicaciones y Operaciones.
- Seguridad de las Comunicaciones.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Relaciones con los Proveedores
- Gestión de Incidentes de la Seguridad de la Información.
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
- Cumplimiento.

El análisis de brecha ISO 27001 de CARDER se realizó a través de la ejecución de los siguientes pasos metodológicos:

- Explicación del objetivo de esta fase de la consultoría al equipo de CARDER
- Revisión preliminar del Modelo de Seguridad de la Información existente y documentos relacionados.
- Presentación de los requisitos ISO 27001 a ser evaluados
- Ejecución de entrevistas iniciales por parte del equipo de consultoría para identificar controles existentes y calificación del estado actual de implementación del control.

Explicación del Objetivo del Diagnóstico.

El equipo de trabajo explicó la metodología y resultados esperados de un análisis diferencial y de la necesidad de que este fuera realizado conjuntamente con los funcionarios de CARDER. Se estableció como objetivo de esta fase del diagnóstico determinar el estado actual de la implementación de cada uno de los catorce (14) dominios del estándar ISO 27001:2013 en la organización. Igualmente se definieron bases para establecer la Declaración de Aplicabilidad (SOA).

Revisión preliminar del Modelo de Seguridad de la Información existente

En desarrollo de esta actividad se hizo una revisión del modelo actual de seguridad de la Información establecido con base en las entrevistas realizadas y documentación allegada por los entrevistados.

Presentación de los controles de ISO 27001 a ser evaluados

Durante las diversas entrevistas el equipo de trabajo presentó el alcance de los dominios de seguridad y controles a ser evaluados y sobre estos se hicieron preguntas que permitieran identificar el estado actual de implementación, así:

Política de Seguridad: Documento en el cual se estipulan las políticas con respecto a la seguridad de la información.

Organización de la Seguridad de la Información: Estructura del área de seguridad de la información que le permita gestionar la seguridad de la información dentro de la organización: Roles, compromisos, autorizaciones, acuerdos, manejo con terceros, entre otros.

Seguridad del Recurso Humano: Procedimientos para asegurar que empleados, contratistas y terceros entienden sus responsabilidades y son idóneos para los roles a desempeñar minimizando los riesgos relacionados con personal.

Gestión de Activos: Procedimientos para la identificación de los activos de información de la entidad y los requerimientos de estos en cuanto a confidencialidad, integridad y disponibilidad.

Control de Accesos: Procedimientos y controles para garantizar que el acceso a los activos de información este restringido a personal autorizado.

Criptografía: Protección de la información mediante procedimientos criptográficos.

Seguridad Física y ambiental: Procedimientos y controles para prevenir accesos físicos no autorizados (perímetro), daños o interferencias a las instalaciones de la entidad y a su información.

Gestión de comunicaciones y operaciones: Procedimientos y controles para garantizar la correcta operación de las áreas de procesamiento de información (actividades operativas y concernientes a la plataforma tecnológica)

Seguridad de las comunicaciones: Procedimientos y controles para garantizar la operación de las áreas de procesamiento de información de forma segura

Adquisición, desarrollo y mantenimiento de Sistemas de Información: Procedimientos y controles para asegurar la inclusión de los controles de seguridad en los nuevos sistemas de información (infraestructura, aplicaciones, servicios, etc.) o por cambios a los mismos.

Relaciones con los proveedores: Procedimientos y controles para proteger la información de terceros.

Gestión de incidentes de seguridad: Procedimientos y controles que buscan que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, sean comunicados de tal manera que se tome una acción correctiva adecuada y en el momento indicado.

Aspectos de seguridad de la información en la gestión de la continuidad del negocio: Procedimientos y controles enfocados en reaccionar en contra de interrupciones de las operaciones de la entidad y en proteger los procesos críticos contra fallas mayores en los sistemas de información o desastres, y, por otro lado, asegurar que se recuperen a tiempo.

Cumplimiento: Procedimientos y controles que buscan prevenir el incumplimiento total o parcial de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

Una vez presentados los requisitos y/o controles a evaluar, se estableció qué ha hecho MRE para la implementación de cada requisito y su **nivel de madurez**.

Dentro de las diferentes metodologías para establecer el modelo de madurez se ha impuesto la Software Engineering Institute's Capability Maturity Model (CMM), la cual establece una escala de 0 (No existente) a 5 (Optimizado). Igualmente, CobiT v. 4.1 ha adoptado modelos de madurez para medir el desempeño de sus procesos, considerando los siguientes niveles:

0 No Existente: No hay procesos de control reconocidos. La organización no reconoce el problema y por ende la necesidad de su tratamiento.

1 Inicial/Ad hoc: La organización reconoce un problema que debe ser tratado. No existen procesos estandarizados sino procedimientos particulares aplicados a casos individuales.

2 Repetible 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.

3 Definidos: 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.

4 Administrados y medibles: 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.

5 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.

Un modelo de madurez es una medida que permite a una organización determinar su grado de madurez para un proceso concreto desde el nivel inexistente (0) hasta el nivel optimizado (5). El nivel de madurez proporciona una escala para referenciar las prácticas de las empresas contra los estándares y guías de la industria.

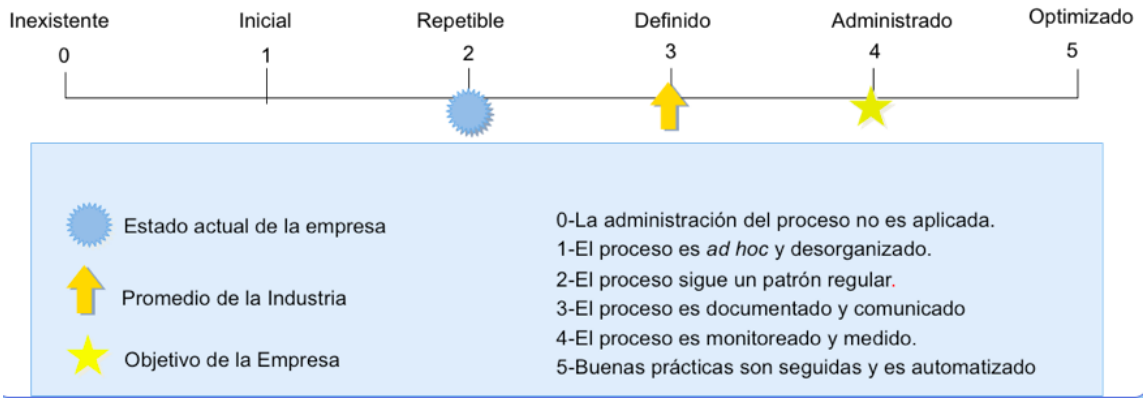


Figura 7 Niveles de Madurez.

En la figura 7 a manera de ejemplo hay una representación gráfica sobre los niveles de madurez y el comportamiento normal de las organizaciones en seguridad y control de la información La escala muestra el estado hipotético de la ubicación actual y deseada por la organización en relación con las mejores prácticas, estándares y guías de la industria.

Considerando que la norma ISO 27002:2013 recomienda la implementación de 114 controles agrupados en 14 dominios, la evaluación de estado actual de madurez por cada uno de los dominios empleó la escala referida en CobiT 4.1.:

- Inexistente (51 % de cumplimiento)
- Inicial (33 % de cumplimiento)
- Repetible (8 % de cumplimiento)
- Definido (5 % de cumplimiento)
- Administrado (3 % % de cumplimiento)
- Optimizado (0% de cumplimiento)

Para identificar el nivel de madurez en el que se encuentra cada dominio se estableció el promedio del nivel de madurez de los controles evaluados.

El Anexo A de la norma ISO 27001 propone 114 controles de seguridad agrupados en dominios y objetivos de control. Durante el análisis de brecha se ha evaluado cada uno de los controles de seguridad de dicho anexo para analizar si aplican a la entidad y en caso afirmativo establecer en qué medida estos controles están o no implantados dentro de la organización.

El estado de situación de CARDER con respecto a la implantación de los controles que contiene se puede resumir en la siguiente gráfica:

De un total de 114 controles evaluados, 113 aplican a la entidad, 58 controles están sin implementar (51%), 52 controles están parcialmente implementados (46 %), es decir, aquellos que se encuentran en los niveles 1 o 2, y 3 controles están en un nivel administrable (3 %).

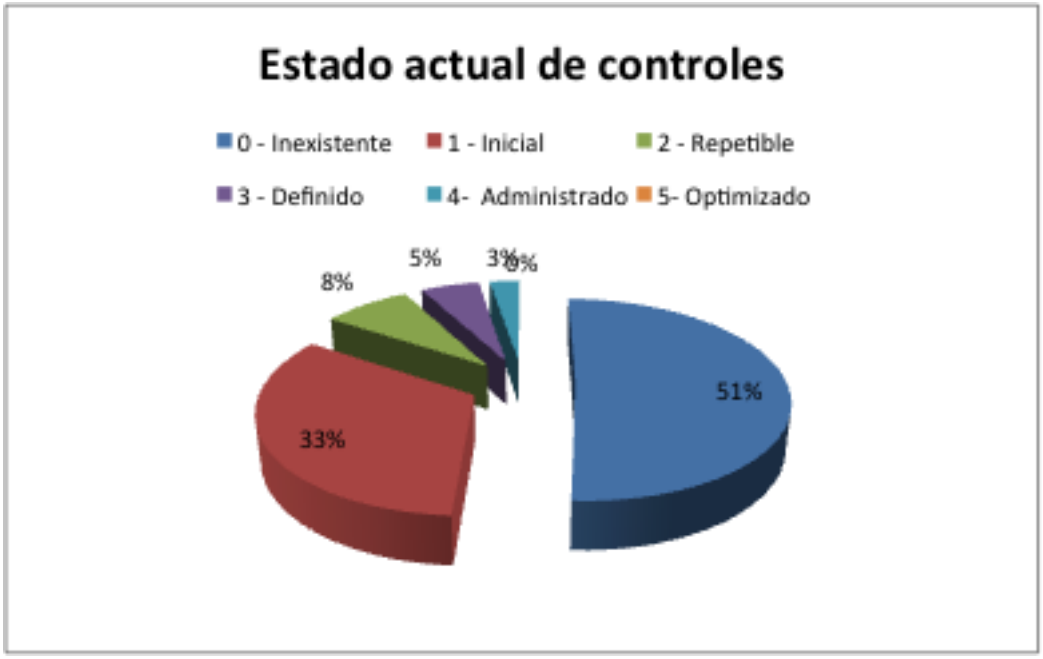


Figura 8: Estado actual de los controles

En cuanto al nivel de cumplimiento de cada uno de los dominios evaluados, se aprecia un nivel muy bajo en la mayoría de ellos.

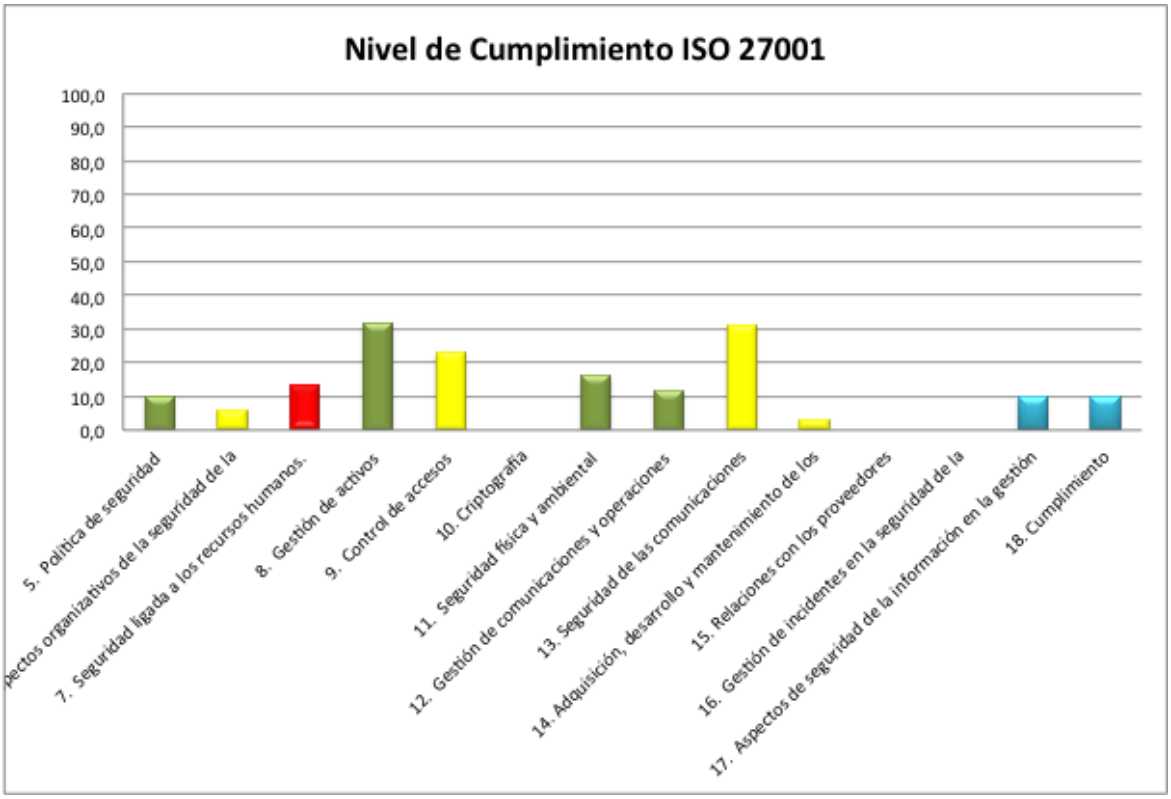


Figura 9: Nivel de Cumplimiento ISO 27001.

En la figura 9, encontramos el nivel de cumplimiento en que se encuentra cada uno de los controles que especifica la norma en la Corporación. Podemos ver que existen Dominios sin ningún avance como el número diez, (10) que hace referencia a la Criptografía, el número quince (15) Relaciones con los proveedores y la numero dieciséis (16) que se trata sobre la Gestión de incidentes en la seguridad de la información.

También podemos observar los Dominios que más nivel de cumplimiento poseen son el número ocho (8) Gestión de activos y el número trece (13) Seguridad de las comunicaciones, a pesar de ser los niveles más altos de cumplimiento, siguen siendo bajos para la evaluación general.

Finalmente, la gráfica de telaraña muestra una nueva visión del nivel de cumplimiento para cada uno de los dominios evaluados.

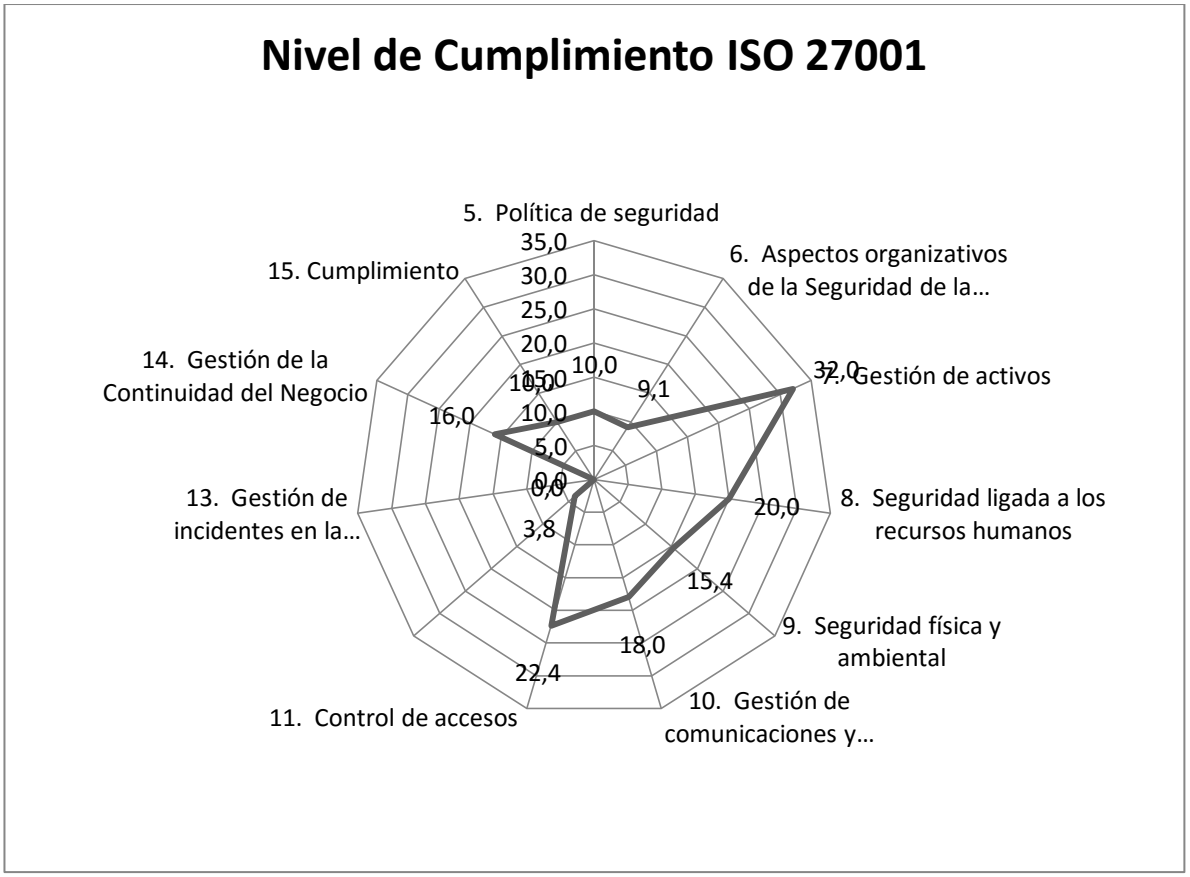


Figura 10: Nivel de Cumplimiento ISO 27001

Al revisar detalladamente el estado de cada dominio, se encuentra lo siguiente:

A5. Política de Seguridad.

CARDER dispone de una política de seguridad de la información, pero no se tienen claro en qué momento deben realizan revisiones periódicas de la misma.

A6. Organización de la seguridad de la Información.

Se evidencia un compromiso por parte de la dirección al abordar la implementación de buenas prácticas en seguridad de la información alineadas a la norma ISO27001 y al manual 3.1 de Gobierno en Línea. Sin embargo, se debe establecer un Comité de Seguridad de la Información, que tenga las funciones de promover la seguridad de la información en cada uno de

los funcionarios y contratistas de la entidad, además que realice controles de forma periódica al cumplimiento de las políticas.

A7. Seguridad de Recurso Humano.

Se evidencia un nivel de implementación para los controles de este dominio muy bajo en algunos aspectos.

A8. Gestión de Activos.

Respecto a este dominio la entidad cuenta con un avance importante, que necesita algunas mejoras para llegar al nivel que garantice la seguridad de la información.

A9. Control de Acceso.

Este dominio cuenta con un nivel apreciable de implementación en el cual se estableció que existen controles avanzados, Sin embargo, se debe considerar la importancia que tiene el manejo de las contraseñas y concientizar que este control puede mitigar algunos riesgos.

A10. Criptografía.

En este dominio la corporación no tiene ningún avance.

A11. Seguridad Física y Ambiental.

En este dominio también se evidencia un nivel de implementación inicial en casi todos los controles.

A12. Gestión de Comunicaciones y Operaciones.

En este dominio se detectó ausencia de documentación o falta de instrucción técnica que describa la implementación de muchos controles que se analizan en este dominio, pero es un control avanzado que puede crecer rápidamente.

A13. Seguridad de las Comunicaciones.

En este dominio se detectó ausencia de documentación o falta de instrucción técnica que describa la implementación de muchos controles que se analizan en este dominio, pero es un control avanzado que puede crecer rápidamente.

A14. Adquisición, desarrollo y mantenimiento de los sistemas de información.

Se aprecia un nivel muy preocupante en los controles que se implementan en este dominio y es importante plantear una metodología para reducir la brecha y cumplir con los objetivos pactados para el desarrollo del SGSI.

A15. Relaciones con los Proveedores.

En cuanto a este dominio, los controles se encuentran de una forma inexistente y es en el que la entidad debe trabajar más fuerte para cumplir con el objetivo planteado.

A16. Gestión de Incidentes de la Seguridad de la Información.

En cuanto a este dominio, los controles se encuentran de una forma inexistente y es en el que la entidad debe trabajar más fuerte para cumplir con el objetivo planteado.

A17. Gestión de la Continuidad de Negocio.

La implementación de este control se ve apoyada en el proyecto planteado por la secretaria general y oficina de T.I. (sistemas), que generaría un nivel de seguridad, confianza y respaldo a la información almacenada, garantizando la continuidad del negocio y mitigando muchos riesgos que se pueden presentar.

A.18 Cumplimiento.

Se debe trabajar en la implementación de los siguientes controles:

- Identificación de la legislación aplicable y tratamiento de datos de carácter personal conforme la ley 1581 (protección de datos personales)
- Reglamentación de controles criptográficos.

- Protección de los registros de la organización.
- Cumplimiento con las políticas y normas de seguridad.
- Controles de auditoría de los sistemas de información.
- Protección de las herramientas de auditoría de los sistemas de información.

Los controles críticos (aquellos que aún no están implementados) son los siguientes:

- 5.1.2 Revisión de la política de seguridad de la información.
- 6.1.1 Asignación de responsabilidades para la seguridad de la información.
- 6.1.2 Distribución de funciones.
- 6.1.4 Contactos con grupos de interés especiales
- 6.2.2 Trabajo remoto
- 7.1.1 Selección
- 7.1.2 Términos y condiciones laborales.
- 7.2.1 Responsabilidades de la dirección.
- 7.2.2 Educación, formación y concienciación sobre seguridad de la información.
- 7.3.1 Responsabilidades en la terminación.
- 8.2.2 Etiquetado de información
- 8.2.3 Manejo de información
- 8.3.2 Eliminación de los medios
- 9.2.4 Gestión de contraseñas para usuarios.
- 9.4.5 Control de acceso al código fuente de los programas.
- 10.1.1 Política sobre el uso de controles criptográficos.
- 10.1.2 Gestión de llaves.
- 11.1.2 Controles de acceso físico

- 11.1.3 Seguridad de oficinas, recintos e instalaciones
- 11.1.5 Trabajo en áreas seguras
- 11.1.6 Áreas de carga, despacho y acceso público.
- 11.2.1 Ubicación y protección de los equipos.
- 11.2.5 Seguridad de los equipos fuera de las instalaciones.
- 12.1.1 Documentación de los procedimientos de operación
- 12.1.2 Gestión del cambio.
- 12.1.4 Separación de las instalaciones de desarrollo, prueba y producción.
- 12.4.4 Sincronización de relojes.
- 12.6.1 Control de vulnerabilidades técnicas
- 12.7.1 Controles de auditoría de los sistemas de información.
- 13.1.3 Separación en las redes.
- 13.2.4 Acuerdos de confidencialidad.
- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 14.1.2 Seguridad de servicios de las aplicaciones en redes públicas
- 14.2.1 Política de desarrollo seguro
- 14.2.3 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.
- 14.2.6 Ambiente de desarrollo seguro
- 14.2.7 Desarrollo de software contratado externamente.
- 14.2.8 Pruebas de seguridad del sistema
- 14.2.9 Pruebas de aceptación del sistema.
- 14.3.1 Protección de los datos de prueba del sistema.

- 15.1.1 Identificación de los riesgos relacionados con las partes externas.
- 15.1.2 Consideraciones de seguridad en los acuerdos con terceras partes.
- 15.1.3 Cadena de suministro de tecnología de información y comunicación
- 15.2.1 Monitoreo y revisión de los servicios por terceras partes.
- 15.2.2 Gestión de los cambios en los servicios por terceras partes.
- 16.1.1 Responsabilidades y procedimientos
- 16.1.2 Reporte sobre eventos de seguridad de la información
- 16.1.3 Reporte sobre las debilidades de la seguridad
- 16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
- 16.1.5 Respuesta a incidentes de seguridad de la información
- 16.1.6 Aprendizaje debido a los incidentes de seguridad de la información.
- 16.1.7 Recolección de evidencia.
- 17.1.3 Verificación, evaluación y revisión de la continuidad de la seguridad de la información
- 18.1.3 Protección de los registros de la organización.
- 18.1.4 Protección de los datos y privacidad de la Información Personal.
- 18.1.5 Reglamentación de los controles criptográficos.
- 18.2.1 Revisión independiente de la seguridad de la información.
- 18.2.2 Cumplimiento con las políticas y normas de seguridad.
- 18.2.3 Verificación del cumplimiento técnico

3.2.3. Identificación de activos

La siguiente tabla muestra la herramienta de recolección de la información de los activos y la cual se encuentra detallada en el anexo 4:

Tabla 3: Tabla de identificación de activos

ID	PROCESO	SUBPROCESO	ACTIVO	TIPO ACTIVO	PROPIETARIO	UBICACIÓN	CANTIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	IMPORTANCIA ACTIVO

La escala de medición de la confidencialidad, integridad, disponibilidad e importancia del activo fue dada como BAJA, MEDIA y ALTA; y el tipo de activo (según MAGERIT) como PROCESOS, SERVICIOS, INFORMACIÓN, HARDWARE, SOFTWARE, PERSONAS, INSTALACIONES y COMUNICACIONES.

La cantidad de activos puestos a consideración fueron 110 y que fueron tomados en cuenta para el análisis de riesgos.

3.2.4. Gestionar las amenazas, vulnerabilidades y riesgos residuales a los que están expuestos los activos definidos dentro del alcance del SGSI

Para la valoración de los riesgos se utilizó la herramienta presentada en el anexo 7, la cual contempla la identificación, estimación, análisis y evaluación de riesgos y se apoya en la unificación de criterios básicos que permiten referenciar cambios adversos en el cumplimiento de objetivos del negocio y reseñar probabilidades e impactos en el evento de materialización de amenazas dentro del alcance y límites de la organización. Los resultados de este proceso constituyen la base para la toma de decisiones frente al riesgo, como la identificación de medidas de tratamiento orientadas a encauzar esfuerzos, lograr objetivos, cumplir obligaciones y evitar

pérdidas o afectaciones económicas significativas a causa de vulnerabilidades localizadas sobre los recursos críticos.

La Figura 11, ilustra el flujo de actividades asociadas al proceso de análisis y valoración de riesgos como fuente principal de datos en la identificación de opciones de tratamiento y gestión del riesgo.

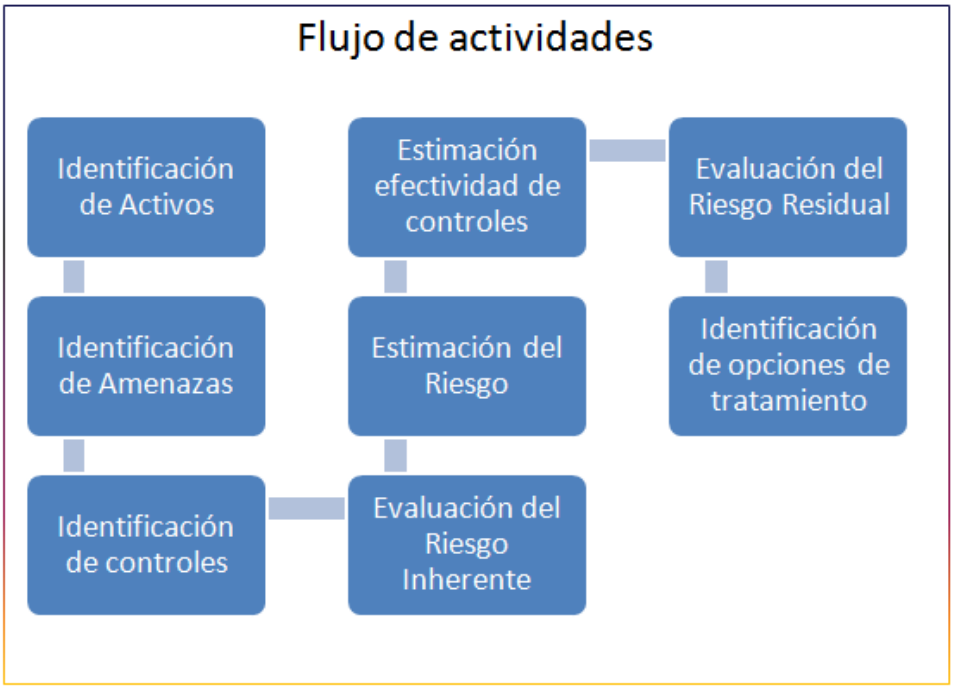


Figura 11: Metodología de Análisis de Riesgo

La metodología llevada a cabo en la CARDER comenzó con la definición del contexto mediante la ejecución de reuniones de entendimiento de los procesos de la entidad y arquitectura tecnológica del negocio, lo cual permitió identificar los activos de la entidad incluidos en el Informe Clasificación de Activos.

Posteriormente, se adoptan los criterios básicos de estimación y evaluación de riesgos y se desarrolla la recolección de información a partir de un formato Excel desarrollado que incluye

las principales amenazas por tipos de activo de acuerdo a la metodología MAGERIT con el fin de identificar amenazas potenciales y relevantes que al materializarse afecten activos de información comprometidos en la prestación de servicios de la CARDER.

Los elementos clave en la identificación, análisis y valoración de riesgos, se observan en la siguiente figura:

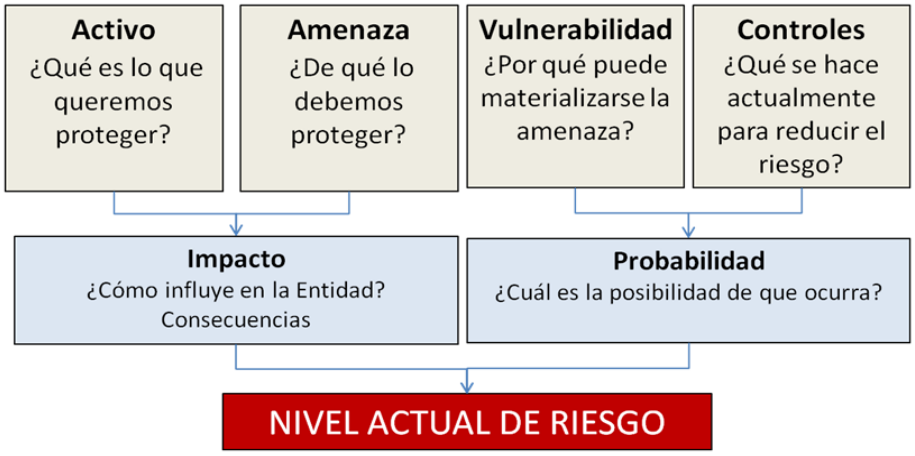


Figura 12: Elementos Clave para Análisis de Riesgos

Nivel de riesgo Inherente (NRi)

Los activos de información de cada proceso o actividad analizada son identificados y agrupados de acuerdo a sus funciones dentro de los procesos, para posteriormente ser revisados a través de un ciclo continuo de valoración de riesgos para determinar las amenazas relevantes, vulnerabilidades existentes, consecuencias de su materialización y probabilidad de ocurrencia , para establecer el riesgo inherente, y la existencia y efectividad de controles implementados que disminuyen el impacto o la probabilidad de concretar la amenaza.

Con la identificación del promedio de efectividad de controles para cada escenario de riesgo se facilita el cálculo del nivel de riesgo residual, que finalmente se emplea para establecer

aquellas fuentes de riesgo de mayor importancia debido a que podrían llegar a generar un impacto importante en la operación en caso de materializarse.

Para la determinación de criterios básicos de estimación de riesgo, se contemplan factores de probabilidad e impacto, utilizando los criterios definidos en el Manual de Riesgos (CR-M-001)

Estimación del nivel de impacto.

La siguiente tabla fue utilizada para establecer tanto cuantitativa como cualitativamente los niveles de impacto de los escenarios de riesgo evaluados.

Tabla 4: Niveles para estimación del Nivel de Impacto

Nivel Cualitativo	Nivel Cuantitativo	Criterios de evaluación de Impacto
IN	***1***	Insignificante
ME	***5***	Menor
MO	***20***	Moderado
MA	***70***	Mayor
CA	***300***	Catastrófico

Estimación de Nivel de probabilidad/frecuencia

La siguiente tabla fue utilizada para establecer tanto cuantitativa como cualitativamente los niveles de probabilidad/frecuencia de los escenarios de riesgo evaluados.

Tabla 5: Niveles para estimación de Nivel de Probabilidad/Frecuencia

Nivel Cualitativo	Nivel Cuantitativo	Criterios de evaluación de Probabilidad/Frecuencia
CC	***1,0***	**Certeza:** es la probabilidad máxima establecida, la cual se asocia con una vez cada dos mes, es decir, 6 veces en un año
MP	***0,8***	**Muy Probable**: es la probabilidad que un riesgo se presente una vez cada 5 meses
PR	***0,6***	**Probable**: es la probabilidad de que se presente el evento una vez en 7 meses,
PP	***0,4***	**Poco Probable:** es la probabilidad que un riesgo se presente una vez cada 10 meses,
RA	***0,2***	**Raro**: es la probabilidad mínima establecida, la cual se asocia con una vez al año

Se definieron 8 diferentes impactos como se hace referencia en el anexo A y para cada uno de ellos se establecieron los criterios asociados a cada nivel de impacto como se muestra a continuación

Tabla 6: I1. Brechas en la confidencialidad de la información

Nivel Cualitativo	I1. Brechas en la confidencialidad de la información
IN	**Insignificante:** cuando se accede a información pública sin catalogar los roles de usuarios.
ME	**Menor**: cuando la información no tiene definidos los estados y usuarios específicos.
MO	**Moderado**: cuando los usuarios pueden acceder a la información sin importar su rol y el estado de la información.
MA	**Mayor:** cuando la información tiene estados definidos pero es accedida.
CA	**Catastrófico**: cuando se publica información que debe ser confidencial, teniendo roles y estados de la información.

Tabla 7: I2. Pérdida de integridad de la información

Nivel Cualitativo	I2. Pérdida de integridad de la información
IN	**Insignificante:** cuando la información puede ser consultada por usuarios no autorizados.
ME	**Menor**: cuando la información puede ser vulnerada de alguna manera

MO	**Moderado**: cuando la información puede ser modificada por usuarios sin roles.
MA	**Mayor:** cuando la información puede ser borrada por usuarios sin roles.
CA	**Catastrófico**: cuando la información es robada y mal utilizada.

Tabla 8: I3. Interrupción de servicios informáticos que afecten la operación misional

Nivel Cualitativo	I3. Interrupción de servicios informáticos que afecten la operación misional
IN	**Insignificante:** Información cuya inaccesibilidad no afecta la operación de CARDER o una inaccesibilidad permanente durante 15 DÍAS podría ocasionar pérdidas NO significativas para CARDER, o terceros.
ME	**Menor**: Información cuya inaccesibilidad permanente durante 8 DIAS podría ocasionar pérdidas significativas a CARDER o a terceros.
MO	**Moderado**: Información cuya inaccesibilidad permanente durante 5 DIAS podría ocasionar pérdidas significativas a CARDER o a terceros.
MA	**Mayor:** Información cuya inaccesibilidad permanente durante 3 DIAS podría ocasionar pérdidas significativas a CARDER o a terceros.

CA	**Catastrófico**: Información cuya inaccesibilidad permanente durante 1 DIA o menos podría ocasionar pérdidas significativas a CARDER o a terceros.

Tabla 9: I4. Pérdida en la efectividad de los procesos (resultado)

Nivel Cualitativo	I4. Pérdida en la efectividad de los procesos (resultado)
IN	**Insignificante:** cuando no se ejecutan las actividades establecidas en los procesos con leve impacto operativo en procesos NO críticos.
ME	**Menor**: cuando no se ejecutan las actividades establecidas en los procesos con leve impacto operativo en procesos críticos.
MO	**Moderado**: cuando el proceso no ejecuta actividades ni controles establecidos afectando procesos NO críticos.
MA	**Mayor:** cuando se presentan no conformidades por la falta de ejecución de actividades y controles en procesos críticos.
CA	**Catastrófico**: cuando ocurren incidentes graves por la falta de ejecución de actividades o controles en procesos críticos.

Tabla 10: I5. Pérdida en la eficiencia de los procesos (uso de los recursos)

Nivel Cualitativo	I5. Pérdida en la eficiencia de los procesos (uso de los recursos)
IN	**Insignificante:** cuando las actividades ejecutadas no tienen el resultado esperado.
ME	**Menor**: cuando no se tienen herramientas para ejecutar las actividades.
MO	**Moderado**: cuando las herramientas no son las adecuadas para ejecutar la actividad.
MA	**Mayor:** cuando las herramientas o las actividades no son las correctas y no se obtienen los resultados esperados.
CA	**Catastrófico**: cuando ocurren sanciones o accidentes por que las actividades ejecutadas no cumplieron con los resultados esperados.

Tabla 11: I6. Información no veraz

Nivel Cualitativo	I6. Información no veraz
IN	**Insignificante:** cuando los funcionarios cometen errores de redacción y la información no se ha publicado.

ME	**Menor**: cuando los funcionarios recolectan en las visitas técnicas información errónea.
MO	**Moderado**: cuando los usuarios traen información errónea o incompleta.
MA	**Mayor: cuando** los funcionarios realizan procedimientos con información incompleta o errónea y es publicada.
CA	**Catastrófico**: cuando los usuarios son sancionados o perjudicados de alguna manera por publicar información errónea.

Tabla 12: I7. Sanciones de tipo legal

Nivel Cualitativo	I7. Sanciones de tipo legal
IN	**Insignificante:** requerimientos de las entidades de control.
ME	**Menor**: requerimiento de explicación de información.
MO	**Moderado**: investigación por entrega de información extemporánea
MA	**Mayor:** investigación por no entregar información a usuarios o entidades.
CA	**Catastrófico**: sanción por entrega de información extemporánea o no entregada.

Tabla 13: I8. Pérdida de credibilidad, competitividad o imagen de la entidad

Nivel Cualitativo	I8. Pérdida de credibilidad, competitividad o imagen de la entidad
IN	**Insignificante:** cuando la entidad hace requerimientos innecesarios a usuarios.
ME	**Menor**: cuando la entidad no cumple con los plazos para responder requerimientos de los usuarios.
MO	**Moderado**: cuando se cometen errores publicitarios.
MA	**Mayor:** cuando un usuario tiene conflictos con la entidad por injusticias o exceso de autoridad.
CA	**Catastrófico**: cuando la entidad tiene investigaciones, demandas o problemas legales de algún tipo.

El producto entre el nivel de impacto y el nivel de probabilidad determina el nivel de riesgo inherente en el cual se encuentra expuesto el activo de información a la amenaza y vulnerabilidad (es) considerada (s).

Nivel de Solidez (Efectividad) de los controles

Como parte del análisis fue necesario identificar y establecer la solidez (efectividad) del conjunto de controles que actualmente aportan en la mitigación de los escenarios de riesgo o aquellos que hoy en día no existen y que deberían ser implementados, para reducir la probabilidad de materialización de la amenaza o su impacto en caso de ser inminente. La calificación de la efectividad del control es realizada con base en las situaciones encontradas en la entidad y a criterio del personal entrevistado y la validación del equipo consultor.

Nivel de riesgo residual (NRr)

Para estimar el nivel de riesgo residual de cada escenario, se utilizó el siguiente análisis matemático:

NRr = (NRi) x (1 – Efc), donde NRi = Nivel de Probabilidad x Nivel de Impacto

Donde NRr representa el nivel de riegos residual, resultado de las medidas de control implementadas en el entorno de trabajo relacionado. De la misma forma NRi representa el nivel de riesgo inherente resultado de multiplicar los valores de nivel de impacto y nivel de probabilidad que se obtuvieron en el análisis inicial. El promedio de efectividad de los controles o solidez (Efc), es un promedio ponderado que matemáticamente busca la disminución del nivel de riesgo inherente. A continuación, se incluye un ejemplo de este tipo de análisis:

Tabla 14: Estimación Nivel de Riesgo Residual

Escenario	Nivel de Probabilidad (0,2 - 1)	Nivel de Impacto (1 - 300)	NRi	Nivel Riesgo Inherente	Solidez de los controles	NRr	Nivel Riesgo Residual
Amenaza "1"	**0,4**	**70**	0,4 x70 =**28**	**A**	**87,5%**	28 x (1-0,875) = **3,5**	M
Amenaza "2"	**0,4**	**1**	0,4 x1 = 0,4	**B**	**85,0%**	0,4 x (1-0,85) = **0.06**	B

En el ejemplo se puede apreciar como para el primer escenario de riesgo, situado en un nivel de Riesgo Inherente ALTO, (en el cual inicialmente NO se considerarán las medidas de

control.) la solidez (efectividad) de sus controles mitiga apropiadamente la Amenaza “1”, obteniendo un nivel de riesgo residual MEDIO. En el segundo escenario no hay variación del nivel de riesgo residual.

Listado de Impactos

El Anexo 1 muestra el listado de Impactos (riesgos) estratégicos definido.

Listado de Amenazas

El Anexo 2 muestra el listado completo de las amenazas consideradas para el análisis de riesgo con base en la metodología MAGERIT, en la cual por cada tipo de activo se listan las amenazas y vulnerabilidades frecuentes a las cuales estos están expuestos.

Listado de controles

El Anexo 3 muestra el listado de controles considerados para mitigar los riesgos. Dicho anexo incluye un código de identificación que inicia con la letra **C** más un número consecutivo y que es utilizado para hacer referencia a cada una de los controles (existentes o no) que deberían ser implementados para mitigar los riesgos identificados.

Mapa de riesgos

El mapa de riesgos permite visualizar la ubicación de los escenarios en una escala de prioridades tras haber referido los factores de probabilidad e impacto frente a una amenaza y sirve a su vez de coordenadas en los ejes principales de la matriz de riesgos para calcular la estimación final de los niveles de riesgo residual.

Tabla 15: Mapa de Riesgos

PROBABILIDAD								
	1	CON CERTEZA	CC	1	5	20	70	300
	0,8	MUY PROBABLE	MP	0,8	4	16	56	240
	0,6	PROBABLE	PR	0,6	3	12	42	180
	0,4	POCO PROBABLE	PP	0,4	2	8	28	120
	0,2	RARO	RA	0,2	1	4	14	60
				INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTROFICO
	Valor			1	5	20	70	300
		Nemónico		IN	ME	MO	MA	CA
				IMPACTO				

Los riesgos residuales son priorizados con base en el mapa de riesgos que establece cuatro niveles de criticidad “Extremo”, “Alto”, “Moderado” y “Bajo”, en los cuales se establece que Impactos (riesgos) de niveles “Extremo” y “Alto” se consideran inaceptables y deben ser tratados. Así mismo, para los niveles “Medio” y “Bajo” su tratamiento es considerado como de mejor esfuerzo, es decir, dependiendo del beneficio aportado a los objetivos de negocio y la capacidad de recursos del área afectada para emprender las acciones requeridas.

Tabla 16: Criterios de aceptación

Aceptables		Inaceptables	
	Bajo	Alta	
	Media	Extrema	

El presente documento muestra una serie de gráficos con los resultados encontrados en la etapa de evaluación de riesgos:

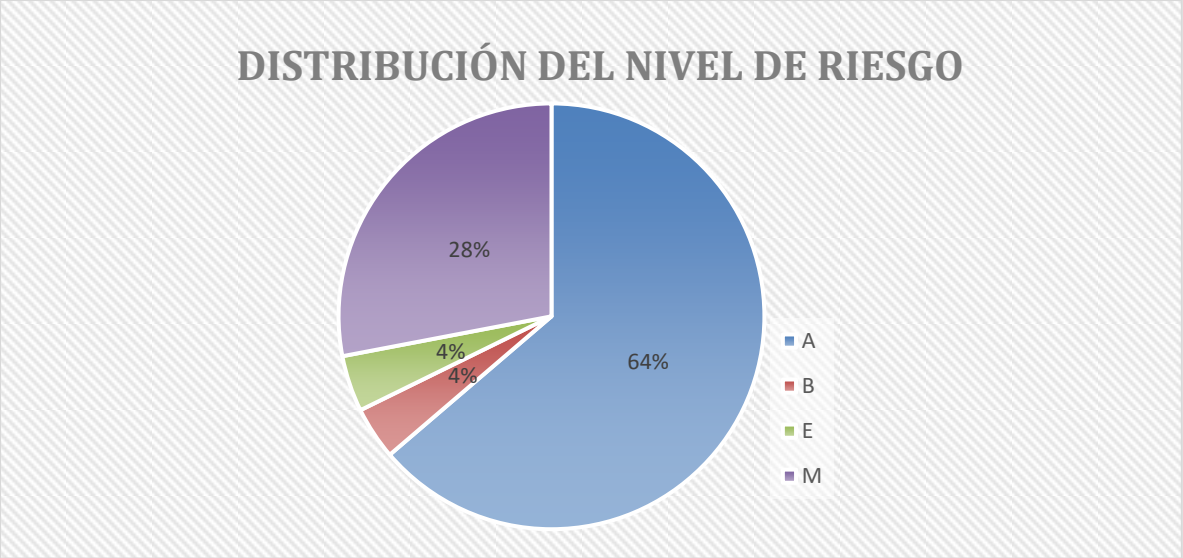


Figura 13. Distribución del Nivel de Riesgo Residual

La figura 13 indica que la mayor cantidad de escenarios de riesgos se encuentran en un nivel Alto (64%), seguidos de escenarios con un nivel de Riesgo Medio (28%). En suma, el 68% de los escenarios de riesgo evaluados requieren un gran esfuerzo para la mitigación de los mismos (niveles Alto y Extremo). Esto representa **255 escenarios,** de un total de 375, que fueron identificados por encima del nivel de riesgo aceptable.

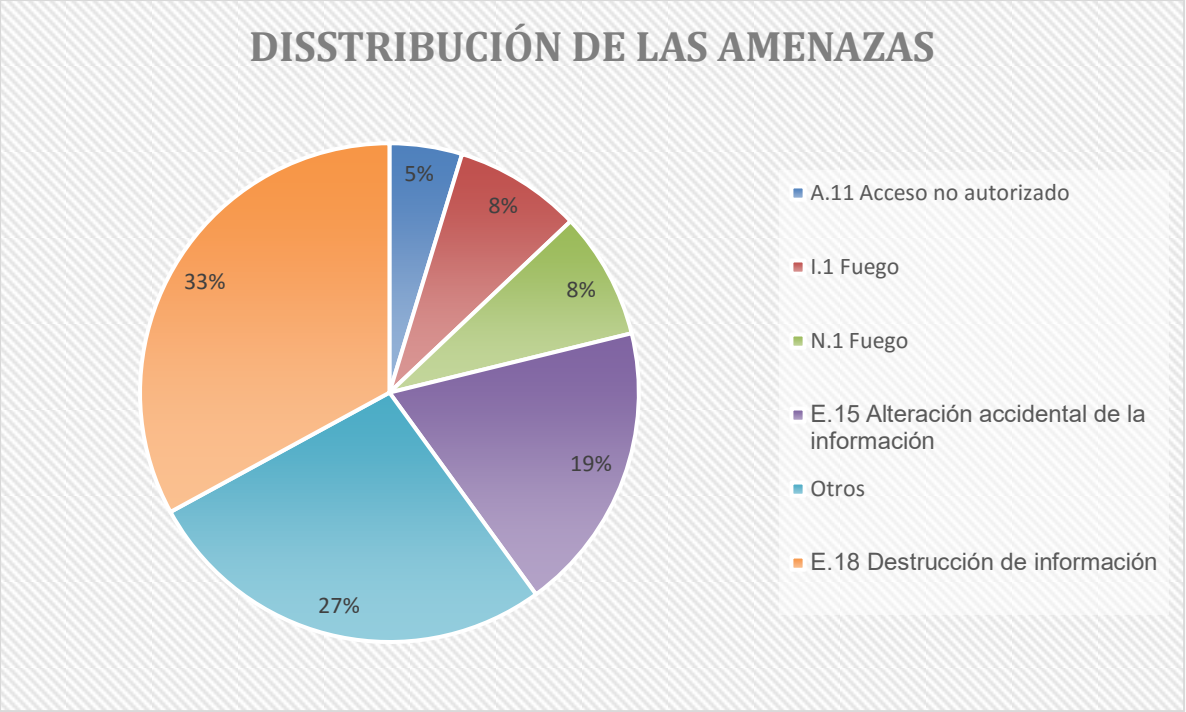


Figura 14. Distribución de las amenazas

La figura 14 nos muestra que la amenaza más latente encontrada en el análisis de riesgos es **[E.18]** Destrucción de la información, seguida de **[E.15]** Alteración accidental de la información y vemos que la amenaza de fuego se encuentra presente dado el material con el cual se encuentra construida en su mayoría las instalaciones de la entidad.

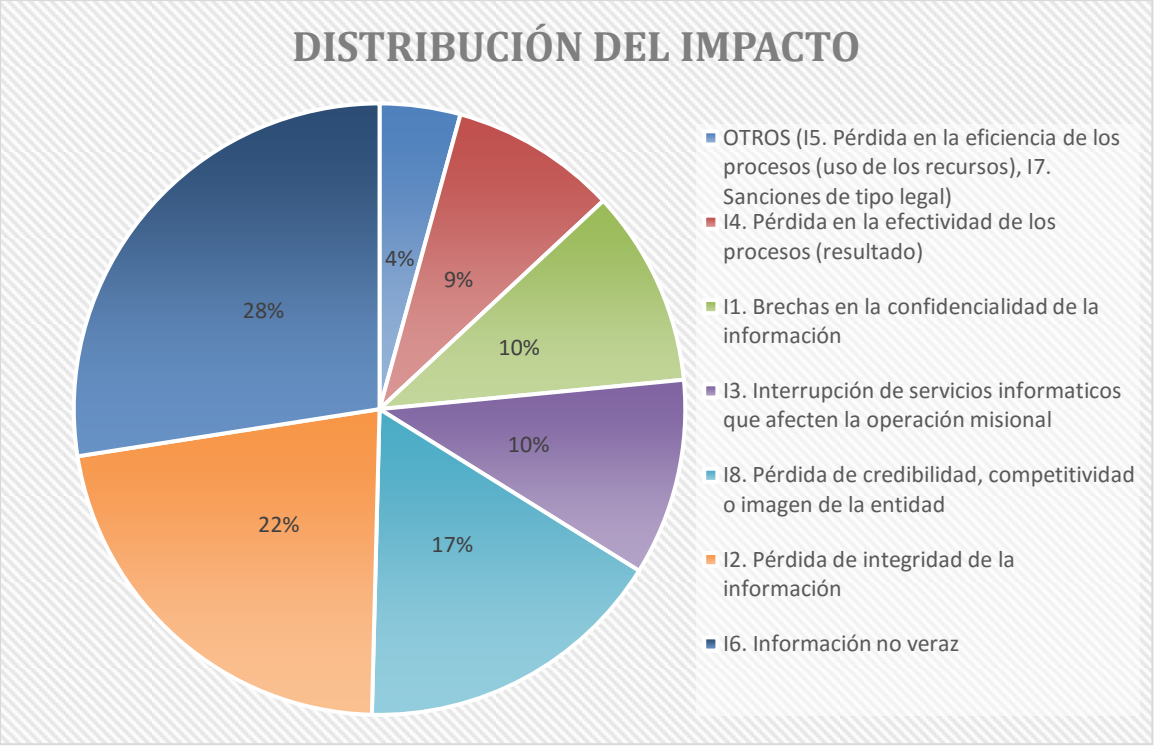


Figura 15. Distribución de impactos

Dada la distribución de las amenazas que se encuentran en la figura 14, esta figura nos muestra que los Impactos más sobresalientes son: I6. información no veraz e I2. pérdida de integridad de la información

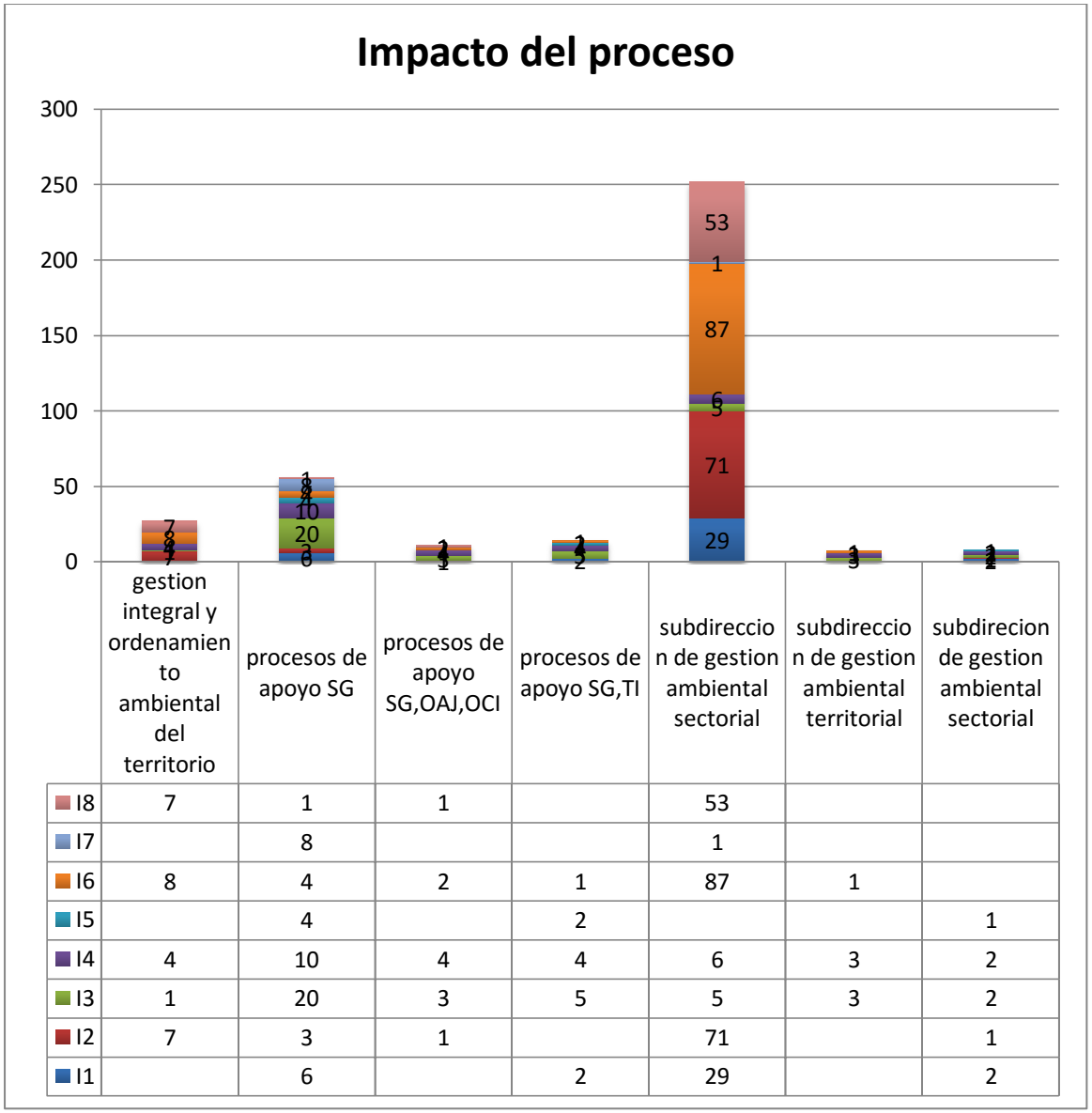


Figura 16. Impactos por proceso

Esta figura nos muestra cómo se distribuyen los impactos por proceso. El proceso de la Subdirección de gestión ambiental sectorial es el proceso con mayor cantidad de impactos identificados.

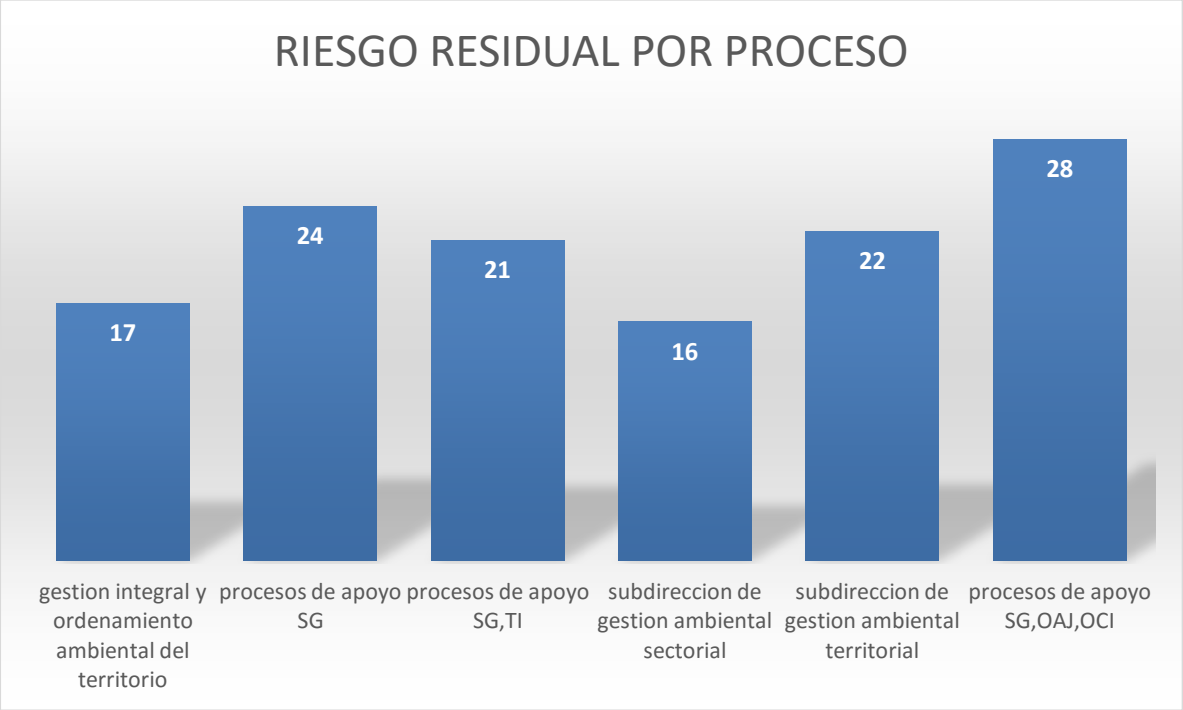


Figura 17. Riesgo residual por proceso

Esta figura muestra el promedio de riesgo residual encontrado en cada uno de los procesos. De acuerdo a este gráfico podemos determinar que todos los procesos se encuentran en un nivel alto, ninguno llegando al nivel de extremo.

Las principales amenazas que propician el Impacto I6- Información no veraz son:

E.1 Errores de los usuarios, esta amenaza se repite 79 veces y para esta amenaza encontramos una (1) vulnerabilidad principal que es:

V24- Falta de entrenamiento, capacitación y/o sensibilización en un funcionario

E.2 Errores del administrador, esta amenaza se repite 24 veces, para esta amenaza encontramos dos (2) vulnerabilidades principales las cuales son:

V24- Falta de entrenamiento, capacitación y/o sensibilización en un funcionario.

V1- Desconocimiento de las políticas de seguridad de la información y/o sus normas, procedimientos, guías de implementación y estándares.

Las principales amenazas que propician el Impacto I2- Pérdida de integridad de la información son:

E.15 Modificación deliberada de la información, esta es la primera amenaza que se repite ochenta (80) veces y para esta amenaza encontramos dos (2) vulnerabilidades principales que son:

V1- Desconocimiento de las políticas de seguridad de la información y/o sus normas, procedimientos, guías de implementación y estándares.

V3- Ausencia de una política de control de acceso.)

A.7 Uso no previsto, esta es la segunda amenaza que más se repite para el Impacto I2, en total lo hace dos (2) veces, con la siguiente vulnerabilidad:

V8- Ausencia de un sistema de identificación de vulnerabilidades.

A.15 Modificación deliberada de la información, esta es la tercera amenaza que presenta el I2, que se repite una (1) vez con las siguientes vulnerabilidades:

V3- Ausencia de una política de control de acceso.

V6- Asignación de privilegios de administrador a usuarios que no lo requieren.

V9- Información confidencial almacenada o enviada sin ser cifrada.

V10- Información crítica sin controles para verificar la integridad en tránsito o almacenamiento.

V25- No eliminar los accesos al término del contrato.

V26- Control de acceso insuficiente.

V27- No realización de back-up.

Las principales amenazas que propician el Impacto I8- Pérdida de credibilidad, competitividad o imagen de la entidad son:

E.18 Destrucción de información, esta es la principal amenaza que presenta I8, se repite sesenta y dos (62) veces con las siguientes vulnerabilidades:

V3- Ausencia de una política de control de acceso.

V6- Asignación de privilegios de administrador a usuarios que no lo requieren.

V10- crítica sin controles para verificar la integridad en tránsito o almacenamiento.

V25- No eliminar los accesos al término del contrato.

V26- Control de acceso insuficiente.

V27- No realización de back-up.

V36- Obsolescencia tecnológica.

V38- Pantalla de trabajo desatendida.

De este análisis de riesgos surgen los siguientes planes de tratamiento:

Tabla 17: Actualización de manuales de usuario

Nombre del Plan de Tratamiento	**Actualización de manuales de usuario**				
Actividades	**Persona Responsable**	**Fecha de Inicio - Fecha de fin**	**Entrenamiento y Programas de Sensibilización**	**Evaluación de los resultados**	**Estado**
Revisión de los manuales de usuario	Dr. Rubén Darío Moreno Calidad y MECI y Dra. Irma C. Cardona Sec. General y Recursos Humanos.	* 16-03-2015 * 15-06-2015	Uso de herramientas interactivas que faciliten el aprendizaje; como presentaciones en Power Point y los videos	Encuestas de satisfacción Cantidad de usuarios que revisan la documentación	PENDIENTE POR APROBAR Y EJECUTAR
Actualización de los manuales de funciones y/o operaciones	Líderes de los procesos.	* 23-02-2015 *13-04-2015	Uso de herramientas interactivas que faciliten el aprendizaje; como presentaciones en Power Point y los videos	Encuestas de satisfacción Cantidad de funcionarios que revisan la documentación	PENDIENTE POR APROBAR Y EJECUTAR

Socialización y reinducción de los manuales de funciones y/o operaciones	Dr. Irma C. Cardona Sec, General. Recursos Humanos.	*30-04-2015 *30-06-2015	Capacitaciones enfocadas en cada activo de información para los nuevos funcionarios	Encuestas de satisfacción Cantidad de funcionarios que revisan la documentación	PENDIENTE POR APROBAR Y EJECUTAR

Tabla 18: Asignación de roles y permisos

Nombre del Plan de Tratamiento	**Asignación de roles y permisos**				
Actividades	**Persona Responsable**	**Fecha de Inicio - Fecha de fin**	**Entrenamiento y Programas de Sensibilización**	**Evaluación de los resultados**	**Estado**
Creación de un documento que contenga la lista de roles y sus correspondientes permisos	Comité de Planeación y Gestión. Líderes de los procesos.	* 13-04-2015 * 15-07-2015	N/A	Documento con el mapa de roles con sus respectivos permisos	PENDIENTE POR APROBAR Y EJECUTAR
Comparación de los permisos de los roles actuales con los	Líderes de los Procesos.	*15-07-2015 *31-07-2015	Sensibilización de los niveles de acceso	Documento en forma de lista de chequeo	PENDIENTE POR

definidos			de cada uno de los roles a los activos de información	validando los permisos de cada uno de los roles	APROBAR Y EJECUTAR
Aprobación de los nuevos permisos	Líderes de los Procesos.	*15-07-2015 *31-07-2015	Sensibilización de los niveles de acceso de cada uno de los roles a los activos de información	Documento en forma de lista de chequeo validando los permisos de cada uno de los roles	PENDIENTE POR APROBAR Y EJECUTAR
Implementación de los nuevos permisos para acceso lógico; como software y pcs	Dra. Irma C. Cardona Sec General y Oficina de Tecnología e Información.	*03-08-2015 *24-08-2014	Capacitación en una herramienta de administración de usuarios y permisos; como Active Directory, LDAP	Registro del 100% de los funcionarios a la herramienta de administración de usuarios y permisos	PENDIENTE POR APROBAR Y EJECUTAR
Sensibilización para la Implementación de los nuevos permisos para acceso físico; como oficinas, documentos, etc; a través de herramientas electrónicas	Dra. Irma C. Cardona Sec General y Oficina de Tecnología e Información.	*24-03-2015 *14-04-2015	Sensibilización para la implementación de tarjetas de identificación electrónicas, huellas dactilares	Documento con el visto bueno de la propuesta	PENDIENTE POR APROBAR Y EJECUTAR

Tabla 19: Implementación de archivos de LOG

Nombre del Plan de Tratamiento	**Implementación de archivos de LOG**				
Actividades	**Persona Responsable**	**Fecha de Inicio - Fecha de fin**	**Entrenamiento y Programas de Sensibilización**	**Evaluación de los resultados**	**Estado**
Adquisición de una herramienta para la lectura de archivos de log	Dra. Irma C. Cardona, Sec General y Oficina de Tecnología e Información.	*2016 *2016	N/A	Controlar Logs.	Planeándose
Capacitación en la herramienta	Dra. Irma C. Cardona, Sec General y Oficina de Tecnología e Información.	*2016 *2016	N/A	Manejo de Logs.	Planeándose
Implementación de la herramienta	Dra. Irma C. Cardona, Sec General y Oficina de Tecnología e Información.	*20-04-2015 *29-05-2015	Capacitación en el uso de la herramienta de monitoreo de logs	Monitoreo de la totalidad de los activos de información identificados en el	PENDIENTE POR APROBAR Y EJECUTAR

				análisis de brecha	

Tabla 20: Actualización de los documentos de los procedimientos de administración

Nombre del Plan de Tratamiento	**Actualización de los documentos de los procedimientos de administración**				
Actividades	**Persona Responsable**	**Fecha de Inicio - Fecha de fin**	**Entrenamiento y Programas de Sensibilización**	**Evaluación de los resultados**	**Estado**
Mejoramiento de los documentos	Dr. Rubén Darío Moreno Calidad y MECI y Dr. Gabriel Penilla Oficina Asesora Jurídica.	*18-05-2015 *31-07-2015	Capacitación sobre el correcto funcionamiento del sistema de gestión de la corporación.	Evaluación del funcionamiento del sistema de gestión.	PENDIENTE POR APROBAR Y EJECUTAR
Revisión de los documentos	Dr. Rubén Darío Moreno Calidad y MECI y Dr. Gabriel Penilla Oficina Asesora Jurídica.	*18-05-2015 *31-07-2015	Uso de herramientas interactivas que faciliten el aprendizaje; como presentaciones en Power Point y los videos	Encuestas de satisfacción Cantidad de funcionarios que revisan la documentación	PENDIENTE POR APROBAR Y EJECUTAR

Socialización de los cambios en los documentos	Dr. Rubén Darío Moreno Calidad y MECI	*03-08-2015 *18-08-2015	Capacitaciones enfocadas en cada activo de información para los nuevos funcionarios	Encuestas de satisfacción Cantidad de funcionarios que revisan la documentación	PENDIENTE POR APROBAR Y EJECUTAR

Tabla 21: Implementación de buenas prácticas para copias de respaldo

Nombre del Plan de Tratamiento	**Implementación de buenas prácticas para copias de respaldo**				
Actividades	**Persona Responsable**	**Fecha de Inicio - Fecha de fin**	**Entrenamiento y Programas de Sensibilización**	**Evaluación de los resultados**	**Estado**
Adecuación de un sitio externo a la entidad para almacenar las copias de respaldo	Dra. Irma C. Cardona Sec General y oficina de Tecnología e Información.	*02-01-2015 *31-03-2015	Sensibilización de la necesidad de tener fuera de las instalaciones de la entidad la copia de respaldo de los activos de información	Documento con el visto bueno de la propuesta	ADJUDICADO Y EN EJECUCIÓN.

Implementación de la buena práctica de frecuencia para sacar copias de respaldo	Dra. Irma C. Cardona Sec General y oficina de Tecnología e Información.	*02-03-2015 *20-03-2015	Capacitación en una herramienta para automatizar la generación de copias de respaldo	Generar copias de respaldo al menos 3 veces por semana	PENDIENTE POR APROBAR Y EJECUTAR
Implementación la buena práctica de pruebas de copias de respaldo	Dra. Irma C. Cardona Sec General y oficina de Tecnología e Información.	*06-04-2015 *23-04-2015	Sensibilización para hacer pruebas de las copias de respaldo para asegurar que están siendo generadas correctamente	Probar las copias de respaldo al menos 2 veces por mes	PENDIENTE POR APROBAR Y EJECUTAR

Tabla 22: Seguridad de la información en Aplicaciones

Nombre del Plan de Tratamiento	**Seguridad de la información en Aplicaciones**				
Actividades	**Persona Responsable**	**Fecha de Inicio - Fecha de fin**	**Entrenamiento y Programas de Sensibilización**	**Evaluación de los resultados**	**Estado**
Validación de las aplicaciones	Dra. Irma C. Cardona Sec	*10-08-2015 *20-10-2015	Capacitación en herramientas para la	Validación del 100% de las aplicaciones	PENDIENTE POR

	General y oficina de Tecnología e Información.		validación de aplicaciones; pueden ser automatizadas o con listas de chequeo		APROBAR Y EJECUTAR

Tabla 23: Concienciación

Nombre del Plan de Tratamiento	**Concienciación**				
Actividades	**Persona Responsable**	**Fecha de Inicio - Fecha de fin**	**Entrenamiento y Programas de Sensibilización**	**Evaluación de los resultados**	**Estado**
Charlas de concientización acerca de la importancia de la seguridad de la información	Dra. Irma C. Cardona Sec General y oficina de Tecnología e Información Y Recursos Humanos.	*23-06-2015 *30-09-2015	Uso de herramientas de comunicación visuales; como diapositivas y videos	Encuestas de satisfacción	PENDIENTE POR APROBAR Y EJECUTAR

Tabla 24: Monitoreo de tráfico de red

Nombre del Plan de	**Monitoreo de tráfico de red**

Tratamiento					
Actividades	**Persona Responsable**	**Fecha de Inicio - Fecha de fin**	**Entrenamiento y Programas de Sensibilización**	**Evaluación de los resultados**	**Estado**
Identificación de las herramientas para monitorear tráfico	Dra. Irma C. Cardona Sec General y oficina de Tecnología e Información.	*01-08-2014 *01-08-2015	Sensibilización acerca del contenido perjudicial que puede ser descargado de sitios de internet o transportados en dispositivos extraíbles.	Monitorear y controlar el 100% de los equipos y servidores en la red	EN EJECUCIÓN
Mantener actualizada la Licencia de software y el Hardware de la herramienta.	Dra. Irma C. Cardona Sec General y oficina de Tecnología e Información.	*01-08-2014 *01-08-2015	Conocer los riesgos de no actualizar el hardware y el software.	Prevención y seguridad de la información.	PENDIENTE DE EJECUCIÓN.

Tabla 25: Almacenamiento de documentos clasificados

Nombre del Plan de	**Almacenamiento de documentos clasificados**

Tratamiento					
Actividades	**Persona Responsable**	**Fecha de Inicio - Fecha de fin**	**Entrenamiento y Programas de Sensibilización**	**Evaluación de los resultados**	**Estado**
Adecuación de un espacio para almacenamiento	Dra. Irma C. Cardona Sec General y Gestión Documental.	*04-02-2014 -04-02-2015 *04-02-2016	Sensibilización de la importancia de clasificar la información y restringir el acceso a ella	Documento con el visto bueno de la propuesta	EN EJECUCIÓN
Sensibilización de la importancia de clasificar la información y restringir el acceso a ella	Dra. Irma C. Cardona Sec General y Gestión Documental.	*04-02-2014 -04-02-2015 *04-02-2016	Sensibilización de la importancia información	Documento con el visto bueno de la propuesta	EN EJECUCION
Implementar la seguridad física	Dra. Irma C. Cardona Sec General y Gestión Documental.	-04-06-2015 -04-08-2015	Conocer los beneficios de prevenir los incidentes de seguridad	Prevención y seguridad de la información.	PENDIENTE DE EJECUTAR

3.2.5. Declaración de Aplicabilidad

Uno de los puntos requeridos por ISO 27001:2013 y el Manual 3.1 de Gobierno en Línea es el documento de declaración de aplicabilidad. En este documento se hace mención de todos los controles que hacen parte de la norma, así como sus objetivos. Aquí debe especificarse si el control aplica o no en la entidad y su respectiva justificación.

La declaración de aplicabilidad de la CARDER consta de ciento trece (113) controles que aplican y uno (1) que no aplica.

Tabla 26: Declaración de Aplicabilidad

ISO27001:2013

Sección	Control	Aplica / No 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	Es un requerimiento de GEL, y un producto de todo el proceso de certificación en ISO 27001
A.5.1.2	Revisión de las políticas para la seguridad de la información	Aplica	Es necesario tener una actualización permanente del uso de las políticas y actualizadas de acuerdo a los requerimientos del gobierno y de la norma
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	Puesto que toda la organización debe estar alineada entorno a la seguridad de la información, deben existen responsables para cada uno de los activos de información
A.6.1.2	Separación de deberes	Aplica	Debe haber personas responsables del buen funcionamiento de los activos de información
A.6.1.3	Contacto con las autoridades	Aplica	La organización debe estar preparada en caso de que ocurra algún accidente y tener los números de emergencia disponible para comunicarse con las autoridades

A.6.1.4	Contacto con grupos de interés especial	Aplica	Si se está protegiendo todos los activos de información y se está utilizando tecnología para ellos, se debe mantener actualizado con las ultimas noticias que surjan en torno a la seguridad de la información
A.6.1.5	Seguridad de la información en la gestión de proyectos	Aplica	la seguridad de la información debe estar presente en todos los proyectos y en la gestión de los mismos.
A.6.2	Dispositivos móviles y teletrabajo		
A.6.2.1	Política para dispositivos móviles	Aplica	Existe información que puede ser extraída usando cámaras de celulares
A.6.2.2	Teletrabajo	Aplica	Los empleados de TI realizan sesiones remotas de soporte
A.7	**Seguridad de los Recursos Humanos**		
A.7.1	Antes de asumir el empleo		
A.7.1.1	Selección	Aplica	Hay que tener certeza que las personas que se estén contratando sean las que realmente entregan los documentos
A.7.1.2	Términos y condiciones del empleo	Aplica	La organización debe establecer la información de la cual es responsables los empleados, contratistas o usuarios
A.7.2	Durante el empleo		
A.7.2.1	Responsabilidades de la dirección	Aplica	La finalidad de las políticas y controles es que todos los empleados velen por la seguridad de la información de la organización
A.7.2.2	Concienciación sobre la seguridad de la información, la educación y la formación	Aplica	Para que los controles y políticas sean aplicado acorde con lo que la dirección tiene en mente, deben existir planes que enseñen y concienticen sobre la necesidad de proteger la información de la organización
A.7.2.3	Proceso disciplinario	Aplica	Deben existir procesos disciplinarios, pues la organización debe velar por la seguridad de la información, y esta no debe ser vulnerada.
A.7.3	Terminación y cambio de empleo		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Aplica	es necesario definir estas responsabilidades para conservar la seguridad de la información y el buen nombre de la corporación.
A.8	**Gestión de Activos**		
A.8.1	Responsabilidad de los activos		
A.8.1.1	Inventario de Activo	Aplica	Siempre se debe tener claro con que activos cuenta la organización además de mantenerlos organizados y actualizados.

A.8.1.2	Propietario de los activos	Aplica	Es necesario que los activos estén bajo la responsabilidad de una persona que se encargue del cuidado del activo.
A.8.1.3	Uso aceptable de los activos	Aplica	La organización debe velar porque los activos no sufran ningún desgaste por mala práctica, ni utilizarlos para realizar operaciones que no estas destinadas para eso
A.8.1.4	Devolución de los activos	Aplica	Los empleados cuentan con algún tipo de activo para desempeñar su labor dentro de la organización, y en el realizar algún tipo de procesamiento. Por esta razón el activo debe ser devuelto junto con la información que contiene
A.8.2	Clasificación de la información		
A.8.2.1	Clasificación de la información	Aplica	La organización debe conocer los niveles de sensibilidad de la información que posee para darle el tratamiento adecuado
A.8.2.2	Etiquetado de la información	Aplica	Se debe etiquetar la información que ha sido clasificada para que los usuarios sepan cuál es su nivel de sensibilidad
A.8.2.3	Manejo de activos	Aplica	Se debe etiquetar la información que ha sido clasificada para que los usuarios sepan cuál es su nivel de sensibilidad
A.8.3	Manejo de medios		
A.8.3.1	Gestión de medios removibles	Aplica	Los empleados pueden cargar con virus o códigos maliciosos
A.8.3.2	Disposición de los medios	Aplica	Existen DVD y Cintas que se eliminan
A.8.3.3	Transferencia de medios físicos	Aplica	La información se encuentra clasificada y se debe tratar de acuerdo a su sensibilidad
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	Los empleados y terceros tienen acceso a los servicios de procesamiento y a los sistemas de información
A.9.1.2	Acceso a redes y servicios en red	Aplica	Los empleados solo deben poder acceder a los servicios a los que estén autorizados a usar en la red
A.9.2	Gestión de acceso de usuarios		
A.9.2.1	Registro y cancelación del registro de usuarios	Aplica	Se deben dar de alta los usuarios tanto en los sistemas de información como en las redes
A.9.2.2	Suministro de acceso de usuarios	Aplica	se debe controlar los controles para restringir y limitar el acceso a la información más importante de la corporación.

A.9.2.3	Gestión de derechos de acceso privilegiado	Aplica	No todos los empleados tienen acceso a la misma información y esto debe ser controlado
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Aplica	Cada usuario debe tener conocimiento y control sobre su propia contraseña de acceso
A.9.2.5	Revisión de los derechos de acceso de usuarios	Aplica	Deben verificarse constantemente los derechos de acceso de los usuarios para mantenerlos actualizados
A.9.2.6	Retiro o ajuste de los de derechos de acceso	Aplica	Los empleados tienen acceso a los servicios de procesamiento de información, y por esta razón cuando sale de la organización deben ser retirados para evitar que la seguridad de la información vulnerada
A.9.3	Responsabilidades de los usuarios		
A.9.3.1	Uso de información de autenticación secreta	Aplica	Los empleados deben asegurar que usan contraseñas seguras
A.9.4	Control de acceso al sistema y aplicaciones		
A.9.4.1	Restricciones de acceso a la información	Aplica	Existe una política de control de acceso
A.9.4.2	Procedimiento de ingreso seguro	Aplica	Existe un procedimiento de inicio de sesión con directorio activo
A.9.4.3	Sistema de gestión de contraseñas	Aplica	La gestión de contraseñas se hace con directorio activo, pero hay aplicaciones que no vence la contraseña y es de uso común
A.9.4.4	Uso de programas utilitarios privilegiados	Aplica	Aplica por las restricciones de dispositivo y de autenticación que se realizarán
A.9.4.5	Control de acceso a códigos fuente de programas	Aplica	Se realizan desarrollos de software internos y por terceros
A.10	**Criptografía**		
A.10.1	Controles criptográficos		
A.10.1.1	Política de uso de controles criptográficos	Aplica	Se debe encriptar la información que se almacena
A.10.1.2	Gestión de llaves	Aplica	Se requieren llaves para encriptar la información almacenada
A.11	**Seguridad física y del entorno**		
A.11.1	Áreas seguras		
A.11.1.1	Perímetro de seguridad física	Aplica	En las instalaciones de la organización existen servicios de procesamiento de información que deben ser protegidos contra acceso no autorizado
A.11.1.2	Controles de acceso físicos	Aplica	En las instalaciones de la organización existen servicios de procesamiento de información que deben ser protegidos de acceso a personas no autorizadas

A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Aplica	Las oficinas deben estar aseguradas y restringir el acceso al público a sus áreas claves
A.11.1.4	Protección contra las amenazas externas y ambientales	Aplica	Las amenazas naturales no son ajenas por lo cual se deben diseñar protecciones para mantener los medios de soporte alejados al igual que los materiales combustibles
A.11.1.5	Trabajo en áreas seguras	Aplica	Al trabajar personas deben estar en un ambiente que sea seguro para que puedan desempeñar su labor sin peligro
A.11.1.6	Áreas de despacho y carga	Aplica	Debe existir un control, pues en la organización el área de carga de la entrada es compartidas
A.11.2	Equipos		
A.11.2.1	Ubicación y protección de equipos	Aplica	La organización cuenta con equipos de procesamiento de información que deben ser ubicados en zonas estratégicas que eviten el acceso no autorizado, y reducir el riesgo de daños por desastres
A.11.2.2	Servicios de suministro	Aplica	Existen equipos de procesamiento de información que se encuentran conectados a un suministro de corriente alterna
A.11.2.3	Seguridad del cableado	Aplica	En la organización existe una red eléctrica y una red de datos
A.11.2.4	Mantenimiento de los equipos	Aplica	Los equipos de los empleados y de procesamiento de información requiere mantenimiento continuo
A.11.2.5	Retiro de activos	Aplica	Los empleados realizan trabajos de campo con dispositivos de la entidad
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Aplica	Los empleados reutilizan los equipos de personas que han estado previamente en la entidad
A.11.2.7	Disposición segura o reutilización de equipos	Aplica	Debido al trabajo de campo que realizan algunos empleados
A.11.2.8	Equipo de usuario desatendido	Aplica	No se puede permitir que personas no autorizadas tengan acceso a un equipo desatendido
A.11.2.9	Política de escritorio limpio y pantalla limpia	Aplica	Hay que controlar los dispositivos removibles para evitar la fuga de información
A.12	**Seguridad de las operaciones**		
A.12.1	Procedimientos operacionales y responsabilidades		
A.12.1.1	Procedimientos de operación documentados	Aplica	Al existir activos de procesamiento de información, existen procedimientos para manejarlos y se deben documentar en caso de que haya cambio de personal
A.12.1.2	Gestión de cambios	Aplica	Los servicios y activos de procesamiento de información se deben actualizar y mantener

A.12.1.3	Gestión de la capacidad	Aplica	La organización tiene recursos de procesamiento y almacenamiento de información
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Aplica	La organización cuenta con desarrolladores que hacen mantenimiento al software que se encuentra en producción
A.12.2	Protección contra códigos maliciosos		
A.12.2.1	Controles contra códigos maliciosos	Aplica	Los empleados pueden cargar con código malicioso en dispositivos extraíbles o instaladores infectados
A.12.3	Copias de respaldo		
A.12.3.1	Respaldo de la información	Aplica	La organización almacena información, por lo tanto, debe respaldarla
A.12.4	Registro y seguimiento		
A.12.4.1	Registro de eventos	Aplica	Dentro de la organización existen activos de procesamiento de información que son manipulados por los empleados
A.12.4.2	Protección de la información de registro	Aplica	Dentro de la organización existen activos de procesamiento de información que son manipulados por los empleados
A.12.4.3	Registros del administrador y del operador	Aplica	Dentro de la organización existen activos de procesamiento de información que son manipulados por los empleados
A.12.4.4	Sincronización del reloj	Aplica	Deben estar sincronizados al encontrarse dentro de la organización
A.12.5	Control de software operacional		
A.12.5.1	Instalación de software en sistemas operativos	Aplica	Existen inventario de activos de software que puede ser instalado
A.12.6	Gestión de la vulnerabilidad técnica		
A.12.6.1	Gestión de las vulnerabilidades técnicas	Aplica	Existe un contacto con grupos de interés especializados que ayuda a detectar vulnerabilidades en los activos de procesamiento de información
A.12.6.2	Restricciones sobre la instalación de software	Aplica	es necesario prevenir la descarga de archivos maliciosos que puedan infectar los equipos.
A.12.7	Consideraciones sobre auditorías de sistemas de información		
A.12.7.1	Controles de auditoría de sistemas de información	Aplica	Son obligatorios para poder cumplir con el objetivo de Asegurar la información
A.13	**Seguridad en las comunicaciones**		
A.13.1	Gestión de la seguridad de las redes		

A.13.1.1	Controles de redes	Aplica	Existen redes de datos en la organización, tanto cableadas como inalámbricas
A.13.1.2	Seguridad de los servicios de red	Aplica	Existen redes de datos en la organización, tanto cableadas como inalámbricas
A.13.1.3	Separación en las redes	Aplica	Se deben separar los servicios de procesamientos de información de otros servicios de datos
A.13.2	Transferencia de información		
A.13.2.1	Políticas y procedimientos de transferencia de información	Aplica	Se intercambia información con entes gubernamentales
A.13.2.2	Acuerdos sobre transferencia de información	Aplica	Se intercambia información con entes gubernamentales
A.13.2.3	Mensajería electrónica	Aplica	También se realiza este intercambio a través de medios electrónicos
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Aplica	La organización tiene información sensible a la cual tienen acceso empleados y terceros, por este motivo deben existir acuerdos de confidencialidad sobre esa información sobre la cual tienen acceso
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	Se realizan desarrollos de software internos y por terceros
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	No aplica	La organización no realiza ninguna actividad con comercio electrónico
A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones	Aplica	La organización no realiza ninguna actividad con comercio electrónico
A.14.2	Seguridad en los procesos de desarrollo y de soporte		
A.14.2.1	Política de desarrollo seguro	Aplica	a pesar del poco desarrollo que se hace actualmente es necesario tener reglas definidas para evitar errores al momento del desarrollo.
A.14.2.2	Procedimientos de control de cambios en sistemas	Aplica	Se realizan desarrollos de software internos y por terceros
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma	Aplica	Existen procedimientos para realizar mantenimiento a los activos de procesamiento de información

	de operación		
A.14.2.4	Restricciones en los cambios a los paquetes de software	Aplica	Se realizan desarrollos de software internos y por terceros
A.14.2.5	Principios de construcción de los sistemas seguros	Aplica	debe existir la documentación para mantener el control y los cambios realizados a lo largo del tiempo
A.14.2.6	Ambiente de desarrollo seguro	Aplica	es importante para cumplir con la seguridad y crecer en el desarrollo de software seguro.
A.14.2.7	Desarrollo contratado externamente	Aplica	La organización contrata la construcción de software por terceros
A.14.2.8	Pruebas de seguridad de sistemas	Aplica	no se hacen pruebas ya que el desarrollo no tiene una organización adecuada.
A.14.2.9	Pruebas de aceptación de sistemas	Aplica	En la organización se contrata servicios de desarrollo de software a terceros
A.14.3	Datos de prueba		
A.14.3.1	Protección de los datos de prueba	Aplica	Se realizan desarrollos de software internos y por terceros y se requiere que los datos de prueba sean eliminados
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	La organización tiene contacto con partes externas que tienen contacto con los servicios de procesamiento de la información
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Aplica	La organización contrata los servicios relacionados con procesamiento de información con terceras partes, por eso se hacer necesario incluir consideraciones de seguridad en los acuerdos
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Aplica	fortalecer la seguridad de la información desde los acuerdos.
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	Los terceros deben estar expuestos a auditorias por los servicios que prestan a la organización
A.15.2.2	Gestión de cambios en los servicios de los proveedores	Aplica	Los terceros deben tener un plan en caso de tener que hacer algún cambio sobre los servicios que prestan y que la organización no se vea afectada
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	Se debe realizar una gestión de las políticas y controles de seguridad de la información
A.16.1.2	Reporte de eventos de seguridad de la información	Aplica	Se busca desarrollar un SGSI por lo tanto es inherente
A.16.1.3	Reporte de debilidades de seguridad de la información	Aplica	Se busca desarrollar un SGSI por lo tanto es inherente
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Aplica	la seguridad de la información debe ser una tarea de todas las personas vinculadas a la corporación.
	Respuesta a incidentes de seguridad de la información	Aplica	la seguridad de la información debe ser una tarea de todas las personas vinculadas a la corporación.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Aplica	Se debe realizar una gestión de las políticas y controles de seguridad de la información
A.16.1.7	Recopilación de evidencia	Aplica	Se debe realizar una gestión de las políticas y controles de seguridad de la información
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	La información es parte fundamental del negocio, debe protegerse
A.17.1.2	Implantación de la continuidad de la seguridad de la información	Aplica	Existen activos de procesamiento de información que son vitales para el funcionamiento del negocio
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Aplica	los planes deben evaluarse para verificar que los riesgos se encuentran controlados
A.17.2	Redundancias		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Aplica	es necesario con el fin de mejorar los niveles de seguridad e integridad de la información.
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	La organización al tener el su poder información de tipo pública, al contratar terceras partes, debe tener identificados y documentados todos los requerimientos estatutarios, reguladores y contractuales
A.18.1.2	Derechos de propiedad intelectual (DPI)	Aplica	Los activos de procesamiento de información y equipos de los empleados requieren software para funcionar, y la mayoría debe ser licenciado para su uso
A.18.1.3	Protección de registros	Aplica	Son obligatorios para poder cumplir con el objetivo de Asegurar la información
A.18.1.4	Privacidad y protección de información de datos personales	Aplica	Son obligatorios para poder cumplir con el objetivo de Asegurar la información
A.18.1.5	Reglamentación de controles criptográficos	Aplica	Son obligatorios para poder cumplir con el objetivo de Asegurar la información
A.18.2	Revisiones de seguridad de la información		
A.18.2.1	Revisión independiente de la seguridad de la información	Aplica	Hay que mantener los controles, políticas, procesos, etc relacionados con la seguridad de la información actualizados acorde a cómo cambia la organización y la información que se procesa
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Aplica	Son obligatorios para poder cumplir con el objetivo de Asegurar la información
A.18.2.3	Revisión del cumplimiento técnico	Aplica	Son obligatorios para poder cumplir con el objetivo de Asegurar la información

3.2.6. POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN.

CARDER está comprometida en salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información, físicos o electrónicos, para asegurar cumplimiento de requisitos técnicos, normativos, regulatorios y operativos a los cuales está sujeta, con base en un proceso de gestión de riesgos periódico y mejorando de manera continua la idoneidad, suficiencia y eficacia del Sistema de Gestión de Seguridad de la Información.

La CARDER ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la Corporación en cuanto a la protección de sus activos de Información:

1. Existirá un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información de la CARDER.

2. Los activos de información de la CARDER, serán identificados y clasificados para establecer los mecanismos de protección necesarios.

3. La CARDER definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.

4. Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

5. Se realizarán auditorías y controles periódicos sobre el modelo de gestión de Seguridad de la Información de La CARDER.

6. Es responsabilidad de todos los funcionarios y contratistas de La CARDER reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

7. Las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.

8. La CARDER contará con un Plan de Continuidad del Negocio que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.

3.2.7. POLITICAS DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION.

- **ACUERDOS DE CONFIDENCIALIDAD.**

Todos los funcionarios de La CARDER y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la Institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de La Corporación a personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

- **RIESGOS RELACIONADOS CON TERCEROS.**

La CARDER, identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

Los controles que se establezcan como necesarios a partir del análisis de riesgos, deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

- **USO ADECUADO DE LOS ACTIVOS.**

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del

área o dependencia específica y a los permisos y niveles de acceso de los funcionarios y contratistas determinadas por los Jefes de Área o Proceso.

Para la consulta de documentos cargados en el software de Gestión Documental SAIA se establecerán privilegios de acceso a los funcionarios y/o contratistas de acuerdo con el desarrollo de sus funciones y competencias. Dichos privilegios serán establecidos por el Jefe o Director del Área, quien comunicará al Grupo encargado de la administración del software el listado con los funcionarios y sus privilegios.

Todos los funcionarios y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un "acuerdo de confidencialidad de la información", donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; y que cualquier violación a lo establecido en este parágrafo será considerada como un "incidente de seguridad".

- **CONTROL DE ACCESO FÍSICO.**

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales

(temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

- **ACCESO A INTERNET.**

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio de La CARDER, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, web, proxies, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN Messenger, Yahoo, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de La CARDER.
- El intercambio no autorizado de información de propiedad de La CARDER, de sus clientes y/o de sus funcionarios, con terceros.
- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes)

utilizando sitios públicos en Internet debe ser autorizada por el Jefe respectivo y la Dirección de Tecnología, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

La CARDER, debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

Los funcionarios y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre de La CARDER, posiciones personales en encuestas de opinión, foros u otros medios similares.

El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de La CARDER.

- **CORREO ELECTRÓNICO.**

Los funcionarios y terceros autorizados a quienes La CARDER les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas por La CARDER, así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad.

Los mensajes y la información contenida en los buzones de correo son propiedad de La CARDER y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

El tamaño de los buzones de correo es determinado por la Dirección de Tecnología de acuerdo con las necesidades de cada usuario y previa autorización del Jefe de la dependencia correspondiente.

El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados por la Dirección de Tecnología.

No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- Utilizar la dirección de correo electrónico de La CARDER como punto de contacto en comunidades interactivas de contacto social, tales como Facebook, hi5 y/o MySpace, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.
- El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la dirección respectiva y la Dirección de Tecnología.

- El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que La CARDER proporciona.
- El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación de la Oficina Asesora de Comunicaciones y la autorización de la Dirección de Tecnología. Además, para terceros se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe, por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre de la dependencia respectiva y/o Servicio habilitado para tal fin y no a través de cuentas de correo electrónico asignadas a un usuario particular.
- Toda información de La CARDER generada con los diferentes programas computacionales (Ej. Office, Project, Access, Wordpad, etc.), que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por la Dirección de Tecnología. La información puede ser
- Enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por La CARDER y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

- **RECURSOS TECNOLÓGICOS.**

El uso adecuado de los recursos tecnológicos asignados por La CARDER a sus funcionarios y/o terceros se reglamenta bajo los siguientes lineamientos:

La instalación de cualquier tipo de software o hardware en los equipos de cómputo de La CARDER es responsabilidad de la Dirección de Tecnología, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por La CARDER a través de esta Dirección.

Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios pueden ser realizados únicamente por la Dirección de Tecnología.

La Dirección de Tecnología debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

Únicamente los funcionarios y terceros autorizados por la Dirección de Tecnología, previa inscripción en el servidor de seguridad perimetral puede conectarse a las redes inalámbricas de La CARDER.

Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de La CARDER; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por la Dirección de Tecnología.

La sincronización de dispositivos móviles, tales como PDAs, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Organización, debe estar autorizado de forma explícita por la dependencia respectiva, en conjunto con la Dirección de Tecnología.

- **PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS.**

Los equipos que hacen parte de la infraestructura tecnológica de tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los funcionarios y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica de La CARDER no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos, esto se debe comunicar al momento de realizar cualquier tipo de contratación con la Corporación.

La CARDER mediante mecanismos adecuados monitoreará las condiciones ambientales de las zonas donde se encuentren los equipos (Centros de Cómputo).

- **SEGREGACIÓN DE FUNCIONES.**

Toda tarea en la cual los funcionarios tengan acceso a la infraestructura tecnológica y a los sistemas de información, debe contar con una definición clara de los roles y responsabilidades,

así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la organización.

En concordancia:

Todos los sistemas de disponibilidad crítica o media de la Institución, deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el área asignada para tal efecto, que en ningún momento deberá ser el área de desarrollo ni la de producción.

El nivel de súper usuario de los sistemas debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

Deben estar claramente segregadas las funciones de soporte técnico, planificadores y operadores.

- **PROTECCIÓN CONTRA SOFTWARE MALICIOSO.**

La CARDER, establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad de la Dirección de Tecnología autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

Así mismo, La CARDER define los siguientes lineamientos:

No está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por La CARDER.
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.
- El uso de código móvil. Éste sólo podrá ser utilizado si opera de acuerdo con las políticas y normas de seguridad definidas y debidamente autorizado por la Dirección de Tecnología.

- **TELETRABAJO.**

Cualquier funcionario de La CARDER, autorizado por la Dirección Tecnología, que requiera tener acceso a la información de la Institución desde redes externas, podrá acceder remotamente mediante un proceso de autenticación; uso de conexiones seguras. Lo anterior asegurando el cumplimiento de requisitos de seguridad de los equipos desde los que se accede.

- **USO DE DISPOSITIVOS MÓVILES.**

El uso de los equipos portátiles fuera de las instalaciones de La CARDER únicamente se permitirá a usuarios autorizados por la Dirección de Tecnología, previa solicitud de la dependencia respectiva, y éstos se protegerán mediante el uso de los siguientes controles tecnológicos: • Antivirus. • Cifrado de datos. • Restricción en la ejecución de aplicaciones. • Restricción de conexión de dispositivos USB. La sincronización de dispositivos móviles con

cualquier sistema de información de La CARDER, sólo estará permitido para personal autorizado por la Dirección de Tecnología y la dependencia respectiva.

- **ESCRITORIO LIMPIO.**

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios de La CARDER deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida manera inmediata.

Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

- **COPIAS DE RESPALDO.**

La CARDER debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la Dirección de Tecnología y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la Institución, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y

disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

La Dirección de Tecnología establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

- **INTERCAMBIO DE INFORMACIÓN.**

La CARDER firmará acuerdos de confidencialidad con los funcionarios, clientes y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la Institución. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

Todo funcionario de La CARDER es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios

para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos.

- **DESARROLLO SEGURO DE SOFTWARE.**

Para apoyar los procesos operativos y estratégicos La CARDER debe hacer uso intensivo de las Tecnologías de la Información y las Comunicaciones. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal propio.

La Dirección de Tecnología debe elegir, elaborar, mantener y difundir el "Método de Desarrollo de Sistemas Software que incluya lineamientos, procesos, buenas prácticas, plantillas y demás artefactos que sirvan para regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad.

Todo proyecto de desarrollo de software interno debe contar con un documento de Identificación y Valoración de Riesgos del proyecto. La CARDER no debe emprender procesos de desarrollo – o mantenimiento – de sistemas software que tengan asociados riesgos altos no mitigados.

Los sistemas software adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad en el proceso de desarrollo.

- **PROTECCION DE DATOS PERSONALES.**

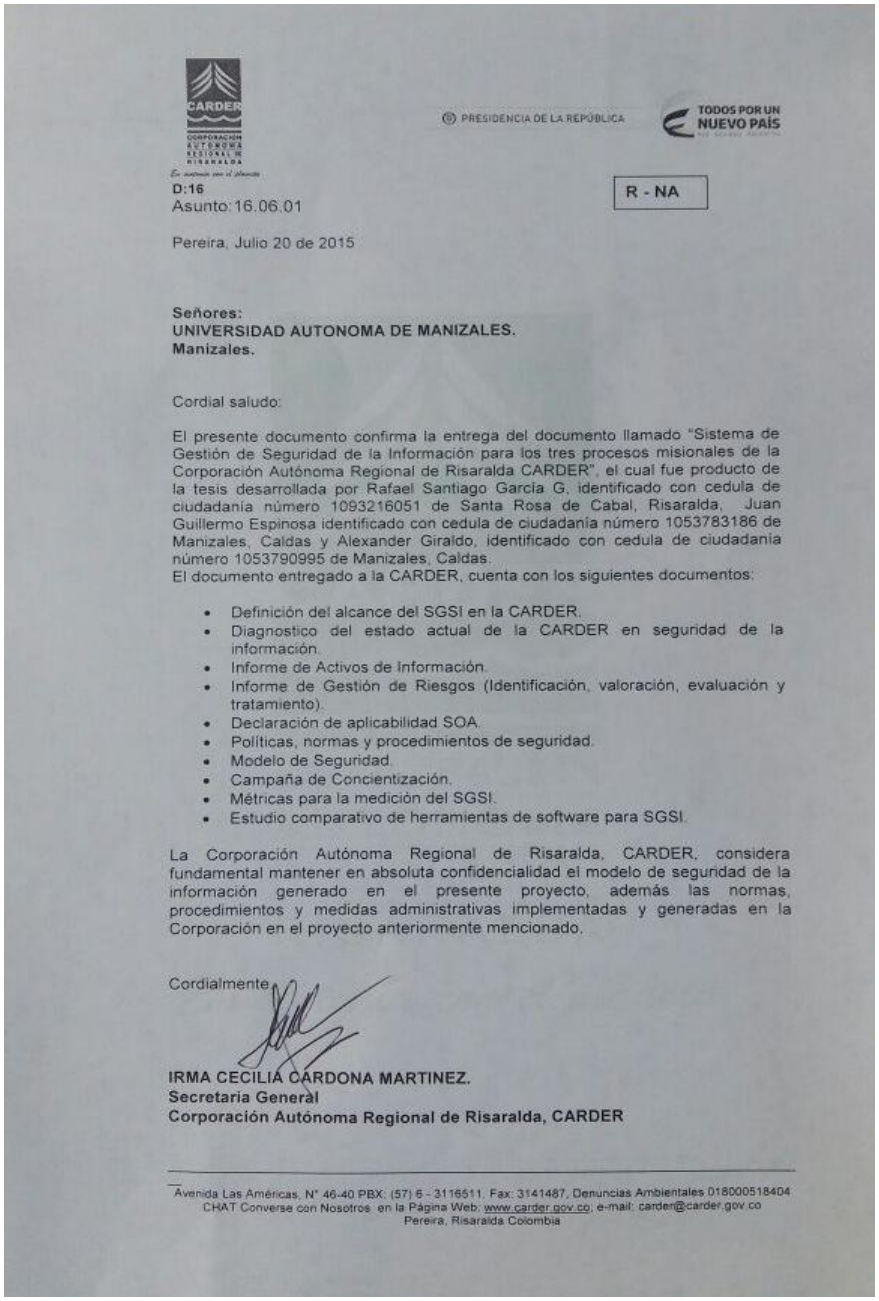
La CARDER, garantiza que los datos, registros e información de carácter privado de los usuarios, serán custodiados, administrados y manejados de acuerdo a lo ordenado en la

constitución política en sus artículos 15 y 20 y con observancia especial de lo introducido por la Ley 1581 de 2012.

En tal sentido, la Corporación como encargada y responsable del tratamiento de los datos dispondrá de las herramientas necesarias para que el o los titulares de los datos, tratándose de personas naturales o jurídicas, manifiesten de una forma libre y voluntaria la autorización para el tratamiento de sus datos personales.

3.3. Hacer

El modelo de seguridad de la información definido ha sido recibido, aceptado y puesto en marcha por la CARDER como lo corrobora la siguiente carta de aceptación.



CARDER
CORPORACIÓN AUTÓNOMA REGIONAL DE RISARALDA

PRESIDENCIA DE LA REPÚBLICA
TODOS POR UN NUEVO PAÍS

D:16
Asunto:16.06.01

R - NA

Pereira, Julio 20 de 2015

Señores:
UNIVERSIDAD AUTONOMA DE MANIZALES.
Manizales.

Cordial saludo:

El presente documento confirma la entrega del documento llamado "Sistema de Gestión de Seguridad de la Información para los tres procesos misionales de la Corporación Autónoma Regional de Risaralda CARDER", el cual fue producto de la tesis desarrollada por Rafael Santiago Garcia G, identificado con cedula de ciudadanía número 1093216051 de Santa Rosa de Cabal, Risaralda, Juan Guillermo Espinosa identificado con cedula de ciudadanía número 1053783186 de Manizales, Caldas y Alexander Giraldo, identificado con cedula de ciudadanía número 1053790995 de Manizales, Caldas.
El documento entregado a la CARDER, cuenta con los siguientes documentos:

- Definición del alcance del SGSI en la CARDER.
- Diagnostico del estado actual de la CARDER en seguridad de la información.
- Informe de Activos de Información.
- Informe de Gestión de Riesgos (Identificación, valoración, evaluación y tratamiento).
- Declaración de aplicabilidad SOA.
- Políticas, normas y procedimientos de seguridad.
- Modelo de Seguridad.
- Campaña de Concientización.
- Métricas para la medición del SGSI.
- Estudio comparativo de herramientas de software para SGSI.

La Corporación Autónoma Regional de Risaralda, CARDER, considera fundamental mantener en absoluta confidencialidad el modelo de seguridad de la información generado en el presente proyecto, además las normas, procedimientos y medidas administrativas implementadas y generadas en la Corporación en el proyecto anteriormente mencionado.

Cordialmente,

IRMA CECILIA CARDONA MARTINEZ.
Secretaria Generàl
Corporación Autónoma Regional de Risaralda, CARDER

Avenida Las Américas, N° 46-40 PBX: (57) 6 - 3116511, Fax: 3141487, Denuncias Ambientales 018000518404
CHAT Converse con Nosotros en la Página Web: www.carder.gov.co; e-mail: carder@carder.gov.co
Pereira, Risaralda Colombia

Figura 18: Carta de aceptación de la CARDER

3.3.1. Métricas de Seguridad

Las métricas, como en cualquier otro ámbito, nos ayudan a saber cuál es el estado actual del SGSI y saber cómo ha sido su evolución y así tomar decisiones que ayuden a mejorar continuamente el Sistema de Gestión. Las métricas planteadas para la evaluación del SGSI se relacionan a continuación:

Objetivo de seguridad: Mejorar continuamente la eficacia, eficiencia y efectividad en lo correspondiente al SGSI (Dar respuesta eficiente a las NC identificadas en el SGSI)

Indicador: efectividad de las acciones correctivas.

Descripción: Valorar la efectividad de las acciones correctivas implementadas

Objetivo: Verificar que las acciones correctivas eliminan la causa raíz que los originan de manera efectiva

Métricas:

Número de acciones correctivas implementadas que eliminaron causa raíz de problemas

Número total de acciones correctivas implementadas

Fórmula: (Numero de acciones correctivas implementadas que eliminaron causa raíz de problemas/número total de acciones correctivas implementadas) *100

Frecuencia de medición: Semestral.

Presentación: Histograma de comportamiento.

Gestionar eficiente y oportunamente los incidentes de seguridad de la información (Minimizar el impacto de incidentes de seguridad de la información y resolverlos en tiempo)

Indicador: Eficacia Resolución de Incidentes de Seguridad

Descripción: Oportunidad en la atención de incidentes de seguridad de la información

Objetivo: Medir el cumplimiento de los ANS (SLA) de atención de incidentes.

Métricas:

Cantidad de incidentes de seguridad resueltos en el período

Cantidad de incidentes de seguridad registrados en el período

Fórmula:

(Cantidad de incidentes de seguridad resueltos en el período / Cantidad de incidentes de seguridad registrados en el período) *100

Frecuencia de medición: Trimestral

Presentación: Histograma de comportamiento

Objetivo de Seguridad: Crear conciencia en seguridad de la información (Dar formación y concienciación en seguridad de la información)

Indicador: % efectividad de las formaciones de seguridad de la información

Descripción: % de personal que cumplió el entrenamiento en seguridad de la información

Objetivo: Asegurar que el personal está apropiadamente entrenado para cumplir sus responsabilidades de seguridad de la información

Métricas:

Cantidad de personal que ha cumplido satisfactoriamente el entrenamiento en seguridad de la información en el último año

Cantidad de funcionarios y contratistas de la entidad programados

Fórmula:

(Cantidad de personal que ha cumplido satisfactoriamente el entrenamiento en seguridad de la información en el último año/ Cantidad de funcionarios y contratistas de la entidad) *100

Frecuencia de medición: Anual

Presentación: Histograma de comportamiento

Indicador: Cumplimiento de charlas de concienciación

Descripción: % de cumplimiento de charlas de concienciación en seguridad de la información.

Objetivo: Asegurar que el personal está apropiadamente entrenado para cumplir sus responsabilidades de seguridad de la información

Métricas:

Número de charlas de concienciación en seguridad de la información realizadas

Número de charlas de concienciación en seguridad de la información programadas

Fórmula:

(Número de charlas de concienciación en seguridad de la información realizadas / Numero de charlas de concienciación en seguridad de la información programadas) * 100

Frecuencia de medición: Semestral

Presentación: Histograma de comportamiento

Objetivo de Seguridad: Proteger los activos de información de la empresa con énfasis especial en los activos de información de los servicios incluidos en el alcance del SGSI

Indicador: Cumplimiento implementación planes de tratamiento de riesgos

Descripción: % de planes de tratamiento de riesgos que avanzan de acuerdo a las actividades definidas

Objetivo: Asegurar que los planes de tratamiento de riesgos se ejecutan de acuerdo a lo planeado para mitigar las amenazas críticas

Métricas:

cantidad de planes de tratamiento de riesgo que avanzan bajo cronograma

cantidad de total de planes de tratamiento de riesgos

Fórmula:

(Cantidad de planes de tratamiento de riesgo que avanzan bajo cronograma / cantidad total de planes de tratamiento de riesgos) *100

Frecuencia de medición: Mensual

Presentación: Histograma de comportamiento

Indicador: Evaluación de riesgos que superan el Nivel de riesgo Aceptable (NRA)

Descripción: % de riesgos que superan el NRA tratados en el semestre

Objetivo: Evaluar periódicamente los riesgos de seguridad de la información que pueden afectar a los activos de información

Métricas:

Cantidad de riesgos calificados por encima del NRA que han sido tratados

Cantidad total de riesgos calificados por encima del NRA

Fórmula:

(Cantidad de riesgos calificados por encima del NRA que han sido tratados / Cantidad total de riesgos calificados por encima del NRA) *100

Frecuencia de medición: Semestral

Presentación: Histograma de comportamiento

3.3.2. Estudio de mercado

A continuación, hacemos un resumen de algunas alternativas de herramientas que existen en el mercado para la administración del SGSI.

Este estudió buscó ayudar a la CARDER a seleccionar un software especializado que le permitiera administrar adecuadamente el SGSI, por lo que se tuvo en cuenta las funcionalidades más importantes que debía cubrir, el tipo de tecnología y los precios y/o contactos de cada una de las herramientas. Estas herramientas permiten a la CARDER y futuros auditores tener un SGSI actualizado y monitoreado, que permita de manera simple el manejo de documentos, riegos, controles, activos, y en general cualquier aspecto relacionado con el SGSI.

Tabla 27: Estudio de Mercado

	GlobalSUITE	Archer	IsoTool	EAR/Pilar	GxSGSI
Idioma	Español / inglés	Ingles	Español	Español	Español
Empresa	Audisec	EMC/archer Technology	ASTIVIA Tecnologías Avanzadas S.L.L.	Mañas/CCN	SIGEA
Normas o Módulos que cubre	ISO27001, ISO20000, ISO31000, ISO22301, BSC, ISO14001, ISO18000,	ISO20000, ISO27001, ISO22301	ISO27001	AGR (Análisis y Gestión de Riesgos), ISO/IEC 13335:2004, ISO/IEC 17799:2005,	ISO27001

	ISO9001			ISO/IEC 27001:2005	
Modo de Distribución	Saas / in House	Instalación	web/SaaS	in House	in House
Perfil Usuario	**x**	**x**	**x**		**x**
Información Empresa (Usuarios, Equipo, Proyecto, Catálogos)	**x**	**x**			**x**
Usuarios	**x**	**x**	**x**		**x**
Roles y Responsabilidades	**x**	**x**	**x**		
Alcance del SG	**x**				
Objetivos del SG	**x**				
Gestión Formación y Capacitación.	**x**				
Gestión Auditoría Interna	**x**	**x**			
Gestión de No Conformidades	**x**				
Gestión Acciones Correctivas y Preventivas	**x**				
Gestión Capacidad	**x**				
Gestión de Cambios y Entregas	**x**				
Gestión de Incidentes y G. Problemas	**x**	**x**			**X**
Gestión de Suministradores	**x**				

Actas de Reunión	**x**				
Gestor de Proyecto	**x**				
Roles y Perfiles	**x**	**x**			
Módulo de Alertas y Notificaciones	**x**				
Coordinación de Múltiples Proyectos	**x**				
Asistente para la visualización de los estados de proyectos	**x**				
Gestor documental	**x**	**x**			**X**
Gestión de Versiones de Documentos	**x**				
Parametrización de estados de Documentos	**x**				
Control de cambio, estados y responsables	**x**				
Extranet de Clientes	**x**				
Peticiones	**x**				
Reclamaciones	**x**				
Satisfacción	**x**				
Relaciones con el Negocio	**x**				
Análisis Diferencial	**x**	**x**		**x**	
Declaración de Aplicabilidad	**x**	**x**		**x**	
Catálogo y Gestión del	**x**	**x**			**X**

Servicio					
Gestión de SLAs	**x**				
Plan de Adecuación y Seguimiento del Sistema	**x**				
Procesos de Negocio	**x**	**x**			**X**
Áreas y Dimensiones Configurables	**x**				
Niveles y Valoraciones Configurables	**x**				
Gestión de Indicadores	**x**		**x**		
Gestión de Métricas	**x**		**x**		
Configuración Dimensiones (inventario y análisis)	**x**				
Configurar Categorías	**x**				
Configurar Fórmulas de cálculo	**x**				
Configurar Niveles Gestión de Riesgos	**x**				
Configurar Niveles de Dimensiones	**x**				
Configurar Costos.	**x**				
Inventario Activos	**x**	**x**	**x**	**x**	**X**
Árbol de Dependencias de activos	**x**			**x**	**X**
Calcular Riesgos automáticame	**x**	**x**			

nte					
Calculo de Coste/ Gestión Coste Beneficio	**x**				
Nivel de riesgo Aceptable	**x**	**x**	**x**	**x**	
Identificación del riesgo (amenaza, vulnerabilidades)	**x**	**x**		**x**	**X**
Identificación automática del riesgo	**x**	**x**	**x**		
Análisis de Riesgos	**x**	**x**	**x**	**x**	**X**
Análisis Configurable	**x**	**x**			
Catálogo de Amenazas	**x**			**x**	
Gestión de Riesgos Múltiples	**x**				
Mapa de Riesgos	**x**	**x**		**x**	
Lista de Riesgos	**x**				
Simulación de Riesgos	**x**	**x**			
Proyección de Riesgos	**x**				
Plan de Tratamiento de Riesgos	**x**	**x**	**x**	**x**	**X**
Seguimiento del Plan de Tratamiento	**x**	**x**		**x**	**X**
Catálogo de Controles	**x**				
Evaluación efectividad de controles	**x**				
Históricos	**x**	**x**		**x**	**X**

AGR (riesgos residual y reevaluación)					
Recuperación de desastres				**x**	
Análisis de impacto al negocio				**x**	
Precios	Contacto comercial@globalsuite.es	Contacto +57 1 658 0900	Contacto +57 1 3470048 +57 3203657308	1500 € + 500 € soporte de base de datos SQL.	220,39 € usuario/trimestre 77,33 € usuario/mes 773,30 € usuario/año

4. Conclusiones.

- El desarrollo del análisis de brecha sirvió como medio para que la CARDER tomara conciencia de la crítica situación respecto a la seguridad de la información que llevaban, y ayudó a que todas las partes que hacen parte de cada proceso se involucrarán en la implementación del SGSI.
- La CARDER inició un proceso de actualización de la base de datos de activos partiendo de la identificación de activos realizada, utilizando la misma herramienta mostrada durante el desarrollo del SGSI.
- El análisis e identificación de riesgos ha permito conocer a profundidad los puntos más vulnerables de la entidad y de esta manera permitió hallar la mejor forma de mitigarlos.
- La materialización de los planes de tratamiento y la política de seguridad de la información para la CARDER, encaminan a la corporación a llevar el estado del riesgo a un punto aceptable.
- El estudio de mercado muestra algunas de las herramientas que existen y que pueden ayudar a la CARDER a administrar mejor su SGSI.
- La implementación del SGSI es beneficioso para la Corporación en cuanto a: seguridad efectiva en los sistemas de información; mejoras continuas en procesos de auditorías internas dentro de la entidad; incremento de la confianza y mejora de su imagen.

5. Recomendaciones.

- Es necesario que la Corporación se comprometa con la seguridad de la información y de esta forma mantener el comité de Seguridad de la Información activo y cumpliendo con las obligaciones del mismo.
- Hacer evaluaciones periódicas al SGSI que permita mejorarlo continuamente.
- Adoptar procesos para la actualización de todos los activos de la CARDER y mantenerlos siempre al día.
- Realizar un cronograma de actividades para cada semestre, programando las evaluaciones y actualizaciones necesarias al SGSI, esto incluyendo activos, riesgos, vulnerabilidades y toda la información generada por la corporación.
- Realizar jornadas de concientización de Seguridad de la información, esto con el fin de que el personal de la corporación cuente con el conocimiento y las herramientas necesarias para prevenir los riesgos y además para que los funcionarios o contratistas nuevos estén enterados al ingreso de la Corporación recibiendo una inducción sobre el SGSI.
- La Corporación debe estudiar la viabilidad de implementar un Software que le permita la administración de Sistemas de Gestión, ya que cuenta con un Sistema Integrado maduro y que cada vez va incrementando sus responsabilidades dentro de la entidad.
- La Corporación prestar mayor atención en la seguridad física ya que se evidencia que uno de los mayores riesgos es la falta de control al ingresar a las instalaciones y oficinas donde se almacena y produce la información de la entidad.

Bibliografía.

BSI Education. (2008). *Information Security Management Systems.* Recuperado el 11 de 09 de 2014, de BSI Education: http://www.bsieducation.org/Education/HE/security-management/management-systems.shtml#history

Department of Trade and Industry. (01 de 06 de 1991). *Information Technology Security Evaluation Criteria (ITSEC).* Recuperado el 10 de 09 de 2014, de Federal Office of Information Security: https://www.bsi.bund.de/cae/servlet/contentblob/471346/publicationFile/30220/itsec-en_pdf.pdf

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 9.

Hiles, A. (2004). *Business Continuity Best Practices.* Rothsein Associates. Inc. .

ISO. (2005). ¿Qué es seguridad de la información? . En ISO, *ISO/IEC 27001: Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información* (pág. 8). Suiza.

ISO. (2005). Alcance . En ISO/IEC, *ISO/IEC 27001: Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información* (pág. 13). Suiza.

ISO. (03 de 06 de 2010). *ISO/IEC 17799:2005.* Recuperado el 11 de 09 de 2014, de IS: http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39612

ISO. (2010). *ISO/IEC 27003: Information technology — Security techniques — Information security management system implementation guidance.* Suiza.

ISO. (2012). What is an ISMS? En I. IEC, *ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary* (pág. 12). Suiza.

Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método.* Madrid.

Peltier, T. (2001). *Information Security Risk Analysis.* Auerhach, London.

The ISO 27000 Directory. (1 de 1 de 2007). *A Short History of the ISO 27000 Standards*. Recuperado el 10 de 09 de 2014, de ISO 27000 Directory: http://www.27000.org/thepast.htm

ANEXOS

Anexo 1: Impacto (Riesgos)

I1. Brechas en la confidencialidad de la información
I2. Pérdida de integridad de la información
I3. Interrupción de servicios informáticos que afecten la operación misional
I4. Pérdida en la efectividad de los procesos (resultado)
I5. Pérdida en la eficiencia de los procesos (uso de los recursos)
I6. Información no veraz
I7. Sanciones de tipo legal
I8. Pérdida de credibilidad, competitividad o imagen de la entidad

Anexo 2: Vulnerabilidades

V1	Desconocimiento de las políticas de seguridad de la información y/o sus normas, procedimientos, guías de implementación y estándares
V2	No mantener un inventario de activos de información actualizado con su correspondiente valoración
V3	Ausencia de una política de control de acceso
V4	Equipos de cómputo o soluciones de software sin el contrato de soporte con el Fabricante o Empresa autorizada.
V5	Acuerdos de niveles de servicio insuficientes para los equipos de cómputo o soluciones de software
V6	Asignación de privilegios de administrador a usuarios que no lo requieren
V7	Software no licenciado instalado en equipos de la Organización
V8	Ausencia de un sistema de identificación de vulnerabilidades
V9	Información confidencial almacenada o enviada sin ser cifrada
V10	Información crítica sin controles para verificar la integridad en tránsito o almacenamiento
V11	Ausencia de segmentación en la red
V12	Ausencia de logs de auditoría
V13	Desincronización de los relojes de los equipos de cómputo
V14	Ausencia de control de acceso en los puertos del switch
V15	Ausencia de control de acceso a los Access Point
V16	Ausencia de requerimientos de seguridad para la adquisición o desarrollo de aplicaciones
V17	Ausencia de sistemas de detección de intrusiones de Host HIPS
V18	Ausencia de sistemas de detección de intrusiones de Red
V19	Ausencia de firmas de ataque propias de la entidad en los sistemas de detección y prevención de intrusiones

V20	Ausencia de procedimientos de revisión de logs
V21	Ausencia de FireWall de Red
V22	Ausencia de sistemas de FireWall de Red
V23	Reglas de protección insuficientes en los sistemas de FireWall Local y de Red
V24	Falta de entrenamiento, capacitación y/o sensibilización en un funcionario.
V25	No eliminar los accesos al término del contrato.
V26	Control de acceso insuficiente
V27	No realización de backup.
V28	Ausencia de segregación de funciones.
V29	Controles Ineficientes para el proceso de selección.
V30	Fuentes de agua cercanas a equipos de cómputo.
V31	Humedad en las edificaciones.
V32	Perdida de custodia de la Información.
V33	Ausencia o desactualización de sistema antimalware.
V34	Ausencia de mantenimiento a UPS.
V35	Ausencia de mantenimiento a los equipos de cómputo.
V36	Obsolescencia tecnológica.
V37	Ausencia de redundancia en sistemas críticos.
V38	Pantalla de trabajo desatendida.
V39	Materia de la edificación inflamable

Anexo 3: Controles

C01 - Acceso restringido a centros de cableado
C02 - Acuerdos con proveedores de tecnología
C03 - Acuerdos de confidencialidad
C04 - Ambientes independientes de desarrollo, pruebas y producción
C05 - ANS con responsabilidades claramente definidas e indicadores de gestión para evaluar cumplimiento
C06 - Aseguramiento de plataforma (hardening)
C07 - Asignación de roles y privilegios acordes con labores desempeñadas (menor privilegio)
C08 - Asignación de roles y responsabilidades para la coordinación de las actividades de seguridad de la información
C09 - Auditorías internas/externas periódicas
C10 - Bloqueo de sesión por inactividad
C11 - Buenas prácticas de control de cambios
C12 - Buenas prácticas de copias de respaldo (Frecuencia, Tipo de Backups, Rotación, pruebas, custodia, niveles de autorización, etc.)
C13 - Buenas prácticas de manejo de contraseñas de acceso (cambio periódico, contraseñas fuertes, etc.)
C14 - Centro de datos alterno

C15 - Cifrado de datos
C16 - Circuito Cerrado de TV conectado con el sistema de alarma
C17 - Componentes tecnológicos redundantes
C18 - Concientización y capacitación en temas de seguridad de la información.
C19 - Contratos de soporte y mantenimiento preventivo y/o correctivo
C20 - Control de acceso físico (puertas cerradas, zonas restringidas, anunciar y acompañar visitantes, huella dactilar, etc.)
C21 - Control de uso de dispositivos móviles
C22 - Controles ambientales Centro de Cómputo
C23 - Controles para evitar fuga de información (DLP, filtro de contenido HTTP y SMTP, bloqueo de USB)
C24 - Copias de respaldo almacenadas en un sitio externo
C25 - Deshabilitación de servicios de red que no se encuentran en uso
C26 - Documentación de los procedimientos de Administración y Operación
C27 - Documentos almacenados en sitio seguro y restringido según el nivel de clasificación.
C28 - Entrada y salida de equipos de equipos autorizadas y registradas en porterías.
C29 - Escritorio limpio
C30 -Etiquetado y manejo de información acorde a niveles de clasificación
C31 - Extintores contra incendio, periódicamente inspeccionados y mantenidos.
C32 - Firewall interno
C33 - Firewall perimetral
C34 - Funcionario de respaldo
C35 - Gabinetes cerrados y seguros
C36 - Guaya y/o candado para PC´s
C37 - Identificación permanente del personal
C38 - IDS / IPS
C39 - Inventario de activos actualizado y mantenido
C40 - Manual de funciones y/o operaciones documentado
C41 - Mediciones de desempeño (capacity planning)
C42 - Monitoreo y revisión de logs / pistas de auditoría
C43 - Permisos de super-usuario solo para administradores
C44 - Plan de Capacitación y entrenamiento
C45 - Plan de recuperación de desastres (DRP) y/o de continuidad de negocios (BCP)
C46 - Planes de renovación y actualización tecnológica
C47 - Planta eléctrica
C48 - Poliza de seguros
C49 - Procedimiento de autorización y acompañamiento de ingreso de visitantes o personal de soporte.
C50 - Procedimientos para el reporte y manejo de incidentes
C51 - Proceso formal de solicitud, autorización y asignación de acceso a componentes tecnológicos
C52 - Pruebas de vulnerabilidad periódicas
C53 - Registro de control de acceso a CC

C54 - Registro y análisis de fallas reportadas por usuarios o programas de monitoreo.
C55 - Rotación de personal
C56 -Salidas de emergencia para evacuar al personal en caso de desastre
C57 - Segregación de funciones
C58 - Sensores de temperatura que activen una alarma en caso de alta temperatura
C59 - Separación de VLANS´S
C60 - Sistemas de extinción de incendios
C61 - Software antivirus actualizado
C62 - UPS regulada
C63 - Validaciones a nivel de aplicaciones
C64 - Verificación periódica de roles y perfiles
C65 - Aseguramiento calidad de los datos
C66 - Manual de ética de la Organización
C67 - Brigadas (antiincendio, evacuación, primeros auxilios)
C68 - Fuerza pública
C69 - Aire acondicionado
C70 - Sensores de humo
C71 - Mantener y actualización de software
C72 - Manual de Usuario
C73 . Sensores de vibración y terremoto
C74 - Control paso de tubería de agua

Anexo 4:

CARDER Valoración de activos_V3.xlsx

Anexo 5:

Carder - Gap Analysis ISO27001 V.6.xlsx

Anexo 6:

Encuesta Analisis GAP.docx

Anexo 7:

CARDER - Gestión de Riesgos V8.xlsx

Anexo 8:

Sensibilización Seguridad de la Información_CARDER_V1.pptx