DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA LA DIRECCION DE SISTEMAS DE LA GOBERNACIÓN DE BOYACÁ

LIDIA CONSTANZA CONTRERAS ESGUERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
TUNJA
2017

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA LA DIRECCION DE SISTEMAS DE LA GOBERNACIÓN DE BOYACÁ

LIDIA CONSTANZA CONTRERAS ESGUERRA

PROYECTO DE GRADO PARA OPTAR EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTOR
SALMÓN GONZÁLEZ GARCÍA
INGENIERO DE SISTEMAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
TUNJA
2017

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Tunja, 17 de Abril de 2017

DEDICATORIA

Dedico mi Proyecto de grado primero a Dios por haberme dado inteligencia y sabiduría para poder desarrollar este trabajo y culminar con éxito la Especialización en Seguridad Informática, a mi esposo por su gran apoyo y colaboración incondicional y a mi madre por estar siempre presente en cada momento brindándome su apoyo para poder cumplir y lograr un reto más en mi vida. Los amo y Dios los bendiga siempre.

AGRADECIMIENTOS

Agradezco al Ingeniero Salomón González García por compartir sus conocimientos, brindarme su apoyo y colaboración incondicional, por tenerme paciencia guiándome en cada paso para el desarrollo de este proyecto y al Ingeniero Martin Camilo Cancelado Ruiz, por sus sugerencias en la etapa final de mi proyecto. Dios los bendiga y los proteja siempre.

Agradezco a la Universidad Nacional Abierta y a Distancia UNAD, por la modalidad de estudiar a Distancia en donde busca que cada estudiante indague y aprenda autónomamente logrando de esta manera profundizar mis conocimientos y capacidades para el desempeño en mi vida profesional.

CONTENIDO

Pág.

INTRODUCCION 20

1. TITULO 21

2. DESCRIPCIÓN DEL PROBLEMA 22

2.1. FORMULACION DEL PROBLEMA 22

3. OBJETIVO 23

3.1 OBJETIVO GENERAL 23

3.2. OBJETIVOS ESPECIFICOS 23

4. JUSTIFICACION 24

5. MARCO REFERENCIAL 25

5.1. ANTECEDENTES 25

5.2. MARCO CONTEXTUAL 26

5.3. MARCO TEORICO 27

5.3.1. SGSI Sistema de Gestión de la Seguridad de la Información 28

5.3.2. Importancia de un SGSI 29

5.3.3. Que incluye un SGSI 30

5.3.4. Como se implementa un SGSI 33
5.3.4.1. Plan: Establecer el SGSI 34
5.3.4.2. Do: Implementar y Utilizar el SGSI 35
5.3.4.3. Check: Monitorizar y revisar el SGSI 36
5.3.4.4. Act: Mantener y mejorar el SGSI 37
5.3.5. Diseño de un SGSI. ISO 27001 37
5.3.6. Clasificación de Amenazas Informáticas 39
5.3.6.1. De Interrupción 39
5.3.6.2. De Interceptación 39
5.3.6.3. De Modificación 39
5.3.6.4. De Fabricación 39
5.3.6.5. Accidentales 39
5.3.6.6. Intencionadas 39
5.3.6.7. Riesgos 39
5.3.7. Elementos del Análisis de Riesgos 39
5.3.7.1 Activos 39
5.3.7.2 Amenazas 39
5.3.7.3 Degradación 40
5.3.7.4 Vulnerabilidades 40
5.3.7.5. Impactos 40
5.3.7.6 Riesgo 40
5.3.8. Riesgos Informáticos 40
5.4. TIPO DE RIESGOS 40

5.4.1. Riesgo de Integridad 40
5.4.2. Riesgos de Acceso 41
5.4.3. Riesgo de Utilidad 42
5.4.4. Riesgo de Infraestructura 42
5.4.5. Riesgo de Seguridad General 42
5.5. CONTROLES Y CLASIFICACION 43
5.5.1. Inventario de Activos 43
5.5.2. Activos de Información 43
5.5.3. Activos de Software 43
5.5.4. Activos Físicos 43
5.5.5. Servicios 43
5.5.6. Activos Intangibles 43
5.6. PROPIEDADES DE LOS ACTIVOS 43
5.6.1. Utilización Adecuada de los Activos 43

5.7. MARCO CONCEPTUAL 44
5.7.1. Conceptos Básicos 44
5.7.2. Sobre la Norma ISO/IEC 27000 47
5.7.2.1. ISO/IEC 27000 47
5.7.2.2. ISO/IEC 27001 47
5.7.2.3 ISO/IEC 27002 48
5.7.2.4 ISO/IEC 27003 48
5.7.2.5. ISO/IEC 27004 48

5.7.2.6 ISO/IEC 27005 48
5.7.2.7 ISO/IEC 27006 48
5.7.2.8 ISO/IEC 27007 49
5.7.2.9 ISO/IEC 27008 49
5.8. MARCO LEGAL 49
5.8.1. Ley 1581 de 2012 Protección de Datos Personales 49
5.8.2 Ley 527 de 1999 De Comercio Electrónico 50
5.8.3. Ley 1343 Propiedad Intelectual 51
5.8.4. Ley 23 De 1982 Derechos de Autor 51
6. DISEÑO METODOLOGICO 52
6.1. DISEÑO 52
6.2. TIPO DE INVESTIGACION 52
6.2.1. Descriptiva 53
6.2.2. Analítica 53
6.3. METODO DE INVESTIGACION 53
6.4. UNIVERSO Y MUESTRA 53
6.4.1. Población 53
6.4.2. Muestra 53
6.5. RECOLECCION DE LA INFORMACION 54
6.5.1. Información Primaria 54
6.5.2. Información Secundaria 54
6.5.3 Instrumentos de Recolección de Información 54
6.5.3.1 Técnica de Observación 54

6.5.3.2. Técnica de Encuesta 54

6.5.3.3. Técnica de Realización de Pruebas..... 54

6.5.4. Muestra..... 55

6.5.4.1. Muestra Empleados 55

6.5.4.2. Características de la Encuesta para los Empleados de la Dirección de Sistemas G.B..... 55

6.5.5. Descripción de Instrumentos 55

6.6. PROCESAMIENTO DE LA INFORMACION..... 55

6.6.1. Metodología para el Análisis y Diseño 55

6.6.2. Análisis de la Encuesta Realizada a los Empleados de la Dirección de Sistemas G.B..... 57

6.6.3. Descripción y Análisis de la Prueba realizada a la Red de la Dirección de Sistemas G.B Zenmap. 58

6.6.3.1. Análisis de Trafico de Red con Zenmap de la Red de la Gobernación de Boyacá. 58

7. SGSI PARA LA DIRECCION DE SISTEMAS DE LA GOBERNACION DE BOYACA 61

7.1. Establecer SGSI 61

7.1.1. Alcance..... 61

7.1.2. Política del Sistema de Gestión 61

7.1.3. Metodología de Evaluación de Riesgo..... 61

7.1.4. Análisis de Riesgo de la Dirección de Sistemas de la Gobernación de Boyacá 63

7.1.5. Inventario de Activos..... 63

7.2. CARACTERIZACION DE LOS ACTIVOS..... 64

7.2.1. Identificación de los Activos..... 64

7.2.1.1. Activos Esenciales 64
7.2.1.2. Datos Información 66
7.2.1.3. Claves Criptográficas 67
7.2.1.4. Inventario de Servicios 67
7.2.1.5. Software - Aplicaciones Informáticas 68
7.2.1.6. Hardware - Equipos Informáticos 69
7.2.1.7. Redes Comunicación 70
7.2.1.8. Soportes de Información – Almacenamiento Electrónico 71
7.2.1.9. Soportes de Información – Almacenamiento no Electrónico 71
7.2.1.10. Equipamiento Auxiliar 72
7.2.1.11. Instalaciones 72
7.2.1.12. Personal 73
7.2.2. Valoración Cualitativa de los Activos 73
7.2.2.1. Valoración Cuantitativa de Activos Esenciales 75
7.2.2.2. Valoración Cuantitativa de Datos/Información 80
7.2.2.3. Valoración Cuantitativa de Claves Criptográficas 82
7.2.2.4. Valoración Cuantitativa de Servicios 82
7.2.2.5. Valoración Cuantitativa de Software – Aplicaciones Informáticas 83
7.2.2.6. Valoración Cuantitativa de Equipos Informáticos 85
7.2.2.7. Valoración Cuantitativa de Redes de Comunicaciones 88
7.2.2.8. Valoración Cuantitativa de Soportes de Información – Almacenamiento Electrónico 89
7.2.2.9. Valoración Cuantitativa Soportes de Información – Almacenamiento no Electrónico 90

7.2.2.10. Valoración Cuantitativa de Equipos Auxiliar 91

7.2.2.11. Valoración Cuantitativa de Instalaciones 92

7.2.2.12. Valoración Cuantitativa de Personal 93

7.2.3. Identificación de las Amenazas 94

7.2.4. Valoración de las Amenazas 95

7.2.4.1. Frecuencia o Probabilidad de Ocurrencia 95

7.2.4.2. Degradación 96

7.2.4.3. Identificación y Valoración de las Amenazas Generales de los Activos de la Dirección de Sistemas de la Gobernación de Boyacá. 97

7.2.5. Matriz de Riesgos Probabilidad Impacto 112

7.2.5.1 Magerit Matriz de Riesgos 114

7.2.5.2. Análisis Matriz de Riesgos 115

7.2.5.3. Informe de Calificación del Riesgo 166

7.2.6. Salvaguardas 171

7.2.6.1. Salvaguardas a Implementar 173

8. EXISTENCIA DE LOS CONTROLES DE ACUERDO A LA NORMA ISO 27001 177

8.1. Aplicabilidad de los Controles 178

9. DISEÑO DEL SISTEMA DE GESTION 253

9.1. Alcance e Importancia 253

9.2. Propósito 253

10. Políticas de Seguridad de la información para la Dirección de Sistemas de la Gobernación de Boyacá. 253

10.1. Funciones y Responsabilidades 255

10.2. Organización de la Seguridad de la Información 256

10.3. Políticas de Operación 257

10.3.1. Política 1: Control de Acceso a la Información y a las Aplicaciones ... 257

10.4. Política 2: Escritorio Limpio y Pantalla Limpia 259

10.5. Política 3: Gestión de Activos. 260

10.6. Política 4: Seguridad de los Recursos Humanos 261

10.7. Política 5: Seguridad Física y Entorno 262

10.8. Política 6: Copias de Seguridad de Archivo de Datos y Retención de Copias de Seguridad. 264

10.9. Política 7: Uso Aceptable para Correo Electrónico y otros Servicios de Internet 266

10.10. Política 8: Administración de Cambios 268

10.11. Política 9: Seguridad en Telecomunicaciones y Servicios Asociados.. 269

10.12. Política 10: Adquisición, Desarrollo y Mantenimiento de Sistemas de Información 270

10.13. Política 11: Controles Criptográficos 271

10.14. Política 12: Seguridad para Usuarios Terceros 272

10.15. Política 13: Propiedad Intelectual y Administración de Licencias de Software 273

10.16. Política 14: Control de Acceso Físico 274

10.17. Política 15. Gestión de Incidentes en la Seguridad de la Información 275

10.18. Política 16: Administración de la Seguridad 277

10.19. Política 17. Registros de Auditoria 278

10.19.1 Derechos de Vigilancia 279

10.20. Política 18: Gestión de la Continuidad de la Entidad 280

11. CONCLUSIONES 281

12. RESULTADOS Y DISCUSION 285

13. DIVULGACION 289

14. BIBLIOGRAFIA 290

ANEXOS 293

LISTA DE FIGURAS

Pág.

Figura 1. SGSI. 29
Figura 2. Utilidad de SGSI 30
Figura 3. Niveles de SGSI 31
Figura 4. Implementar un SGSI 33
Figura 5. Gestión de Riesgos 35
Figura 6. Ciclo PDCA (PHVA) SGSI 56
Figura 7. Escaneo Completo de la Red 59
Figura 8. Peticiones 59
Figura 9. Protocolo de Nivel de Transporte escaneo UDP 60
Figura 10. Exploración de todos los puertos TCP (Abiertos y Cerrados) 60
Figura 11. Puertos TCP 61

LISTA DE TABLAS

Pág.

Tabla 1. Población conformada por el personal de la Dirección de Sistemas de la Gobernación de Boyacá. 53

Tabla 2. Pasos Metodología Magerit 63

Tabla 3. Activos Esenciales 64

Tabla 4. Datos/Información 66

Tabla 5. Claves Criptográficas 67

Tabla 6. Inventarios de Servicios 67

Tabla 7. Software – Aplicaciones Informáticas 68

Tabla 8. Equipos Informáticos (Hardware) 69

Tabla 9. Reses de Comunicación 70

Tabla 10. Soportes de Información -Electrónico 71

Tabla 11. Soportes de Información – Almacenamiento no Electrónico 71

Tabla 12. Equipamiento Auxiliar 72

Tabla 13. Instalaciones 72

Tabla 14. Personal. 73

Tabla 15. Criterios de Valoración 74

Tabla 16. Valoración Cuantitativa de Activos Esenciales 75

Tabla 17. Valoración Cuantitativa de Datos/Información 80

Tabla 18. Valoración Cuantitativa de Claves Criptográficas 82

Tabla 19. Valoración Cuantitativa de Servicios 82

Tabla 20. Valoración Cuantitativa de Software – Aplicaciones Informáticas..... 83

Tabla 21. Valoración Cuantitativa de Equipos Informáticos..... 85

Tabla 22. Valoración Cuantitativa de Redes de Comunicaciones 88

Tabla 23 Valoración Cuantitativa de Soportes de Información Almacenamiento Electrónico 89

Tabla 24. Valoración Cuantitativa de Soportes de Información Almacenamiento no E. 90

Tabla 25. Valoración Cuantitativa de Equipos Auxiliar 91

Tabla 26. Valoración Cuantitativa de Instalaciones 92

Tabla 27. Valoración Cuantitativa de Personal 93

Tabla 28. Dimensiones Valoradas 94

Tabla 29. Valoración de las Amenazas 95

Tabla 30. Probabilidad de Ocurrencia 95

Tabla 31. Degradación del Valor 96

Tabla 32. Identificación de las Amenazas Generales de los Activos de la Dirección de Sistemas de la Gobernación de Boyacá. 97

Tabla 33. Datos de Información 99

Tabla 34. Claves Criptográficas 100

Tabla 35. Inventario de Servicios 101

Tabla 36. Servicios Internos 102

Tabla 37. Equipamiento SW Aplicaciones Informáticas 102

Tabla 38. Equipamiento Informáticos (Hardware) 104

Tabla 39. Redes de Comunicación 106

Tabla 40. Soportes de Información 107

Tabla 41. Elementos Auxiliares 108
Tabla 42. Instalaciones 109
Tabla 43. Personal 110
Tabla 44. Magerit Impacto 112
Tabla 45. Magerit Probabilidad 112
Tabla 46. Magerit Nivel de Riesgo 113
Tabla 47. Matriz de Riesgo Probabilidad e Impacto 114
Tabla 48. Análisis Matriz de Riesgos 115
Tabla 49. Tratamiento Tipos de Salvaguardas según Magerit 171
Tabla 50. Peso de las Salvaguardas 171
Tabla 51. Nivel de Criticidad 172
Tabla 52. Salvaguardas Inventarios de Servicios 173
Tabla 53. Salvaguardas Equipamiento SW 174
Tabla 54. Declaración de Aplicabilidad con parámetros 177
Tabla 55. Estado de los Controles 177
Tabla 56. Aplicabilidad de los Controles 178
Tabla 57. Resumen Analítico Especializado (RAE) 297

LISTA DE ANEXOS

Pág.

ANEXO A Encuesta para los funcionarios de la Dirección de Sistemas de la Gobernación de Boyacá 294

ANEXO B Resumen Analítico Especializado (RAE) 297

INTRODUCCION

Hoy en día la información se ha convertido como un activo más en cualquier Entidad y/o Organización, por esta razón se ve la necesidad de proteger la información de los diferentes riesgos en los que puede estar expuesta.

La aparición en los últimos años de las redes informáticas y fundamentalmente del Internet, ha sido el factor primordial que dado relevancia a la Seguridad Informática, ya que consiste en verificar los recursos de los sistemas de información sean utilizados de una manera correcta y que el acceso a la información almacenada como la modificación, solo sea posible a las personas autorizadas.

Con el Diseño del Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27001, se puede denotar que ayuda a la Dirección de Sistemas de la Gobernación de Boyacá a proteger la información, puesto que es un activo más de la Entidad, este proceso se puede hacer mediante controles y políticas de seguridad que deben ser aplicadas en la misma.

Sin embargo, nunca se puede lograr que un sistema sea totalmente seguro, ya que continuamente surgen nuevas amenazas, pero existen medidas de seguridad que permite evitar daños y problemas que pueden ocasionar los intrusos. Por tal motivo se han creado numerosas leyes, estándares y normas, cuyo propósito es la prevención de ataques para poder mitigar riesgos.

La Dirección de Sistemas de la Gobernación de Boyacá, a través del diseño SGSI pretende minimizar los riesgos a los que se encuentra expuesta la información de la Entidad, proceso que se hará paso a paso.

Para poder desarrollar este proyecto, se hace un análisis de los riesgos, se hace un análisis de los activos, valoración cualitativa de los activos, se identifican las amenazas y se hace la definición de las salvaguardas, con el fin de realizar una evaluación de los riesgos para determinar que activos de la Dirección de Sistemas se encuentran en Riesgo y de esta forma minimizar los mismos.

Para llevar a cabo el desarrollo de este proyecto nos apoyamos en la Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones públicas, Magerit, es un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

1. TITULO

DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION BASADO EN LA NORMA ISO/IEC 27001 PARA LA DIRECCION DE SISTEMAS DE LA GOBERNACION DE BOYACA.

2. DESCRIPCIÓN DEL PROBLEMA

Las entidades públicas en su labor diaria generan datos, reportes, actas y material de diferente índole, información de vital importancia para su funcionamiento, que puede ser almacenada en diferentes medios ya sean físicos o electrónicos, y que está a disposición del personal que requiere hacer uso de esta información, para realizar reportes, pagos contratos, proyectos entre otros.

El acceso sin autorización a la información en la mayoría de los casos se ha vuelto más fácil debido al gran cantidad de métodos para extraer la información, haciendo cada vez más complejo la labor de salvaguardar la misma.

La Dirección de Sistemas de la Gobernación de Boyacá, actualmente maneja un volumen considerable de información en sus bases de datos de impuestos, contratos, proyectos, pagos entre otros. La probabilidad de que la información sea alterada, interceptada y/o modificada ha aumentado exponencialmente, por tal motivo se ve en la necesidad de proteger su información, mediante el Diseño de un Sistema de Gestión de Seguridad de la información basado en la norma ISO/IEC 27001, que proteja a la entidad de los posibles riesgos de seguridad de la información en la que puede estar expuesta poniendo en riesgo la fuga de información, perdida de confidencialidad, integridad de aplicaciones y disponibilidad de la información.

El desconocimiento de las posibles amenazas de seguridad puede desencadenar un incidente en la Dirección de Sistemas de la Gobernación de Boyacá, al no aplicarse las recomendaciones y controles de establecidos por el desconocimiento del uso de las aplicaciones y el uso de información como activo principal de la entidad.

2.1. FORMULACION DEL PROBLEMA

¿Cómo el Diseño de un Sistema de Gestión SGSI mejorara la seguridad en la Dirección de Sistemas de la Gobernación de Boyacá?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar el Sistema de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 en la Dirección de Sistemas de la Gobernación de Boyacá.

3.2. OBJETIVOS ESPECIFICOS

- Identificar los activos informáticos mediante la aplicación de instrumentos de recolección de información para establecer los dominios del estándar ISO 27001

- Determinar las vulnerabilidades, amenazas y riesgos de seguridad existentes usando la metodología MAGERIT

- Verificar la existencia de controles de acuerdo a las normas ISO 27001 que permita la definición de políticas y procedimientos de seguridad.

- Diseñar el Sistema de Gestión de Seguridad de la Información SGSI para la Dirección de Sistemas de la Gobernación de Boyacá.

4. JUSTIFICACIÓN

Debido a los riesgos a los que pueden estar expuestos los activos de la información y el impacto que puede causar la perdida de la misma, es de gran importancia el uso de herramientas que ayuden a reducir y mitigar los riesgos.

Es por eso que se propone el Diseño de un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO/IEC 27001, que permitirá a la entidad tener los procedimientos y lineamientos necesarios para identificar y evaluar los riesgos, amenazas y vulnerabilidades de la información, para implantar los controles necesarios que permitan salvaguardar la información, adoptando medidas de seguridad de acuerdo a las normas establecidas, para afrontar cualquier eventualidad, en beneficio de los usuarios para que el desarrollo de sus actividades no se vea afectado por pérdidas de información,

Igualmente, con el desarrollo de este trabajo se busca facilitar el trabajo de los funcionarios de la Dirección de Sistemas de la Gobernación de Boyacá, permitiendo de esta forma un mayor control de la información y aumentar la efectividad de sus resultados y disminuyendo los altos niveles de riesgos de perdida de información.

5. MARCO REFERECIAL

5.1 ANTECEDENTES

El Diseño de un Sistema de Gestión de Seguridad de la Información de Leasing Bolívar, basado en la norma internacional ISO 27001. Este Manual se encuentra plasmado las especificaciones para la creación de un sistema de gestión de la seguridad de la información (SGSI), explica como recoger, analizar y definir los lineamientos que rigen al Sistema de Gestión de Seguridad de la información de Leasing Bolívar.[1]

Otro de los proyectos es el Diseño del Sistema de Gestión de Seguridad de la Información para el Grupo Empresarial la Ofrenda, basado en la norma ISO 27001, En el proyecto se explica la base de conocimiento del sistema de seguridad de la información, alimentado por encuestas y entrevistas, con el fin de determinar los posibles riesgos y amenazas de la información de la empresa.[2]

El proyecto denominado "Guía Metodológica para el Diseño del Sistema De Gestión De La Seguridad de La Información en El Icbf" basado en la norma ISO ISO/IEC 27000:2005, presentado por el Icbf en la sede nacional Bogotá. En el proyecto se explica cómo aplicar la norma en una empresa, proyecto que se planteó para determinar los dominios seleccionados para la evaluación de riesgos.

También se encuentra el proyecto de Diseños de un SGSI fue en la comunidad Nuestra señora de Gracia de la ciudad de Bogotá, El proyecto fue denominado "Diseño de un sistema de gestión de seguridad de la información (SGSI), alineado tecnológicamente con la norma ISO 27001". El alcance del proyecto, se plantea para determinar los dominios de los activos y seguridad de recursos humanos.

Debido a la efectividad del proceso de gestión que se logra obtener con el Sistema de Gestión de Seguridad de la Información, diversas organizaciones tanto del sector público como del privado, a nivel mundial como nacional, optan por el diseño de este sistema con el fin de tener una herramienta efectiva en la gestión del riesgo de activos de información dentro de la organización.

---

[1] Manual del Sistema de Gestión de Seguridad de la Información. Leasing Bolívar. Disponible en Internet: http://pegasus.javeriana.edu.co/~CIS0830IS12/documents/Anexo%20K%20MG-05%20Manual%20del%20Sistema%20de%20Gestion%20de%20Seguridad%20de%20la%20Informacion.pdf

[2] Diseño del Sistema de Gestión de Seguridad de la Información para el Grupo Empresarial La Ofrenda

Un caso puntual en el cual una organización ha reconocido la importancia de establecer un proyecto de seguridad de la información en el cual se ha contemplado el desarrollo de un Diseño Sistema de Gestión de Seguridad de la Información (SGSI) incluyendo dentro de este, el desarrollo de los controles asociados al dominio Gestión de Activos de Información. El Gobierno de la república de Colombia el cual a través de su ministerio de comunicaciones en el 2008 aprobó un documento oficial en el cual se detalla el modelo de Seguridad de la información-sistema SANSI4-SGSI Modelo de seguridad de la información para la estrategia de gobierno en línea[3], en dicho documento el gobierno de la república de Colombia ha establecido el modelo de seguridad de la información para la estrategia de gobierno en línea el cual ha establecido el SGSI partiendo de los lineamientos consolidados en la Norma ISO/27001 e ISO/27002, haciendo caso a las recomendaciones para incluidas en dichas normas respecto al establecimiento y estructuración del SGSI e implementando los controles sugeridos para la gestión del riesgo de los activos de información. El documento oficializado por el ministerio de comunicaciones presenta la consolidación del proyecto de seguridad de la información que se ha establecido por parte del gobierno nacional de la República de Colombia y en el cual se detalla la estructuración del sistema de gestión de seguridad de la información SGSI que han adelantado.

La Dirección de Sistemas de la Gobernación de Boyacá actualmente no cuenta con un diseño de sistema de gestión de seguridad de la información, es por eso que se hace necesario su diseño, para garantizar la continuidad del negocio y la preservación de sus activos.

Es importante conocer conceptos que están relacionados directamente con el tema, tener un soporte teórico que permita clarificar definiciones con la finalidad de dar respuesta a los requerimientos del proyecto; cada uno de los procesos en el desarrollo del proyecto significa la búsqueda de resultados y está acompañada de una buena investigación necesaria para alcanzar los objetivos propuestos.

5.2. MARCO CONTEXTUAL

La Gobernación de Boyacá el actual Departamento de Boyacá se conoció en la época colonial con el nombre de Provincia de Tunja y fue organizada como Corregimiento, el cual era administrado por Corregidores y Justicias Mayores; sus límites iban desde las tierras de los Muzos pasando por Turmequé, Tunja, Tundama, Sogamoso, Vélez, Socorro, San Gil, Soatá, El Cocuy, Río de Oro, Pamplona, Pedroza, San Cristóbal, Mérida y Barinas, hasta el Lago de Maracaibo

[3]Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0. Bogotá, D.C. Diciembre de 2001. Disponible en Internet: http://css.mintic.gov.co/ap/gel4/images/Modelo_Seguridad_Informacion_2_01.pdf

y Barquisimeto en Venezuela. Por la misma época colonial se separaron Mérida, San Cristóbal, Pedroza y Barinas en Venezuela, luego Socorro, San Gil, Vélez y por último Pamplona.

El Departamento de Boyacá fue creado en el Congreso de Cúcuta, en 1821, en homenaje a la batalla del Puente de Boyacá con la cual culminó la independencia de Colombia.

La Gobernación de Boyacá actualmente con dos Despachos: Despacho del Gobernador y Despacho Gestora Social, 11 Secretarias como son: Cultura y Turismo, Desarrollo Humano, Educación, Fomento Agropecuario, Hacienda, Infraestructura Pública, Minas y Energía, Participación y Democracia, Productividad, TIC y Gestión de Conocimiento, Salud, y Secretaria General esta última se involucra para el desarrollo de este proyecto donde se encuentra la Dirección de Sistemas. Por otra parte, se encuentra el Departamento Administrativo de Planeación y la Oficina de Relaciones Nacionales e Internacionales – Casa de Boyacá.[4]

En lo que compete sobre la revisión de todos los proyectos que se hagan y se implementen en la Dirección de Sistemas, es realizada por el jefe de Sistemas que se encuentre en el momento, el encargado debe contar con una excelente hoja de vida para poder ejercer este cargo, puesto que es de alta responsabilidad ya que debe proteger y salvaguardar toda la información que maneje la Gobernación de Boyacá.

Por otra parte, la mayoría del personal de la Gobernación de Boyacá son contratistas, estos se encuentran laborando en toda la Gobernación de Boyacá en las diferentes Secretarias dependiendo su perfil y conocimiento.

5.3 MARCO TEÓRICO

El sistema de gestión de seguridad de la información es para las organizaciones una herramienta que surge con el fin de concientizar a cada uno de los miembros en una organización sobre la importancia y la sensibilidad de la información para correcto funcionamiento de la organización.

[4] Página WEB: Gobernación de Boyacá. Disponible en:

www.boyaca.gov.co/dependencias

El manual de Seguridad para una organización debe ser soportado por políticas y procedimientos que permitan proteger un recurso. Para la realización del presente proyecto se tendrán en cuenta las siguientes teorías y normas internacionales las cuales proporcionan la información necesaria para el cumplimiento de los objetivos de investigación

5.3.1. *SGSI - Sistema de Gestión de la Seguridad de la Información*

El propósito de un SGSI en una organización es la de garantizar que los riesgos de la seguridad de la información sean del conocimiento de la organización, para poder ser asumidos, gestionados y minimizados, de forma sistemática, estructurada, eficiente.

La seguridad de la información, consiste en la preservación de la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas implicados en su tratamiento, dentro de una entidad y/o organización.

Los tres aspectos fundamentales a tener en cuenta para la seguridad de la información son los siguientes:

Confidencialidad: Información que maneja toda entidad y/o organización privada donde no puede ser divulgada y suministrada a personas ajenas a la empresa "Personal no Autorizado"

.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. [5]

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. [6]

En un caso práctico se debe seleccionar la más relevante en donde se pueda adoptar un proceso sistemático, documentado y reconocido por la entidad como es el ciclo de vida SGSI.

[5] Sistema de Gestión de la Seguridad de la Información.

[6] Sistema de Gestión de la Seguridad de la Información.

Figura 1. SGSI

Fuente: www.iso27000.es

Los Sistemas de Gestión de la Seguridad de la Información permiten a las organizaciones implementar políticas y procedimientos con el fin de reducir los riesgos de exposición de la información. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente. [7]

5.3.2. *Importancia de un SGSI*

Un SGSI permite a las organizaciones implementar políticas para reducir los riesgos en los que puede estar expuesta la información. En una organización la confidencialidad, integridad y disponibilidad de información puede llegar a ser esencial para mantener los niveles de competitividad, rentabilidad, para una organización. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean mínimos

[7] (Sistema de Gestión de la Seguridad de la Informaci[on , s.f.)

Figura 2. Utilidad de SGSI

Fuente: www.iso27000.es

Para realizar una gestión efectiva seguridad en una organización se debe contemplar un procedimiento adecuado y planificado que permita la implementación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) permite establecer políticas y procedimientos para el desarrollo de los objetivos de cualquier entidad y/o organización, con la finalidad de lograr un nivel de exposición siempre menor al nivel de riesgo que la propia entidad ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.[8]

5.3.3. *Qué incluye un SGSI*

Un SGSI se muestra gráficamente como una pirámide de cuatro niveles de la siguiente forma:

[8] Sistema de Gestión de la Seguridad de la Información Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

Figura 3. Niveles SGSI

Fuente: www.iso27000.es

Documentos de Nivel 1

Manual de seguridad: Documento que dirige todo el sistema, es decir determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

Documentos de Nivel 2

Procedimientos: Se caracteriza por ser un nivel operativo, donde se debe realizar de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

Documentos de Nivel 3

Instrucciones, checklists y formularios: Es un documento que describe tareas y actividades específicas relacionadas con la seguridad de la información.

Documentos de Nivel 4

Registros: Documento que proporciona evidencia de manera objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como outputque demuestra que se ha cumplido lo indicado en los mismos. [9]

[9] Sistema de Gestión de la Seguridad de la Información: Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

Alcance del SGSI*:* La entidad queda sometida al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas.

Política y objetivos de seguridad**:** Documento que establece un compromiso y orientación de la dirección hacia la entidad en la gestión de la seguridad de la información.

Procedimientos y mecanismos de control que soportan al SGSI**:** Procedimiento que ayuda a sistematizar a la entidad y/o organización en el funcionamiento del SGSI.

Enfoque de evaluación de riesgos: Metodología a emplear donde se puede evaluar amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado.

Informe de evaluación de riesgos**:** Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

Plan de tratamiento de riesgos**:** Documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc. [10]

Procedimientos documentados**:** Todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados. [11]

Registros: Es un documento que relaciona las evidencias de la conformidad con los requisitos para el buen funcionamiento eficiente del SGSI.

Declaración de aplicabilidad: Este documento contiene los objetivos de control que se necesitan para un SGSI, dependiendo de los procesos de evaluación y tratamiento de riesgos.

---

[10] Sistema de Gestión de la Seguridad de la Información Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

[11] Sistema de Gestión de la Seguridad de la Información Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

Control de la documentación

Para el Control de la documentación se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión para:

- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito. [12]

5.3.4. Cómo se implementa un SGSI

Se implementa un Sistema de Gestión de la Seguridad de la Información con base a ISO 27001, donde se utiliza el ciclo continuo PDCA, método de ayuda para los sistemas de gestión de la calidad.

Figura 4. Implementar un SGSI

Fuente: www.iso27000.es

[12] Sistema de Gestión de la Seguridad de la Información Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

Plan (planificar): Establecer el SGSI, Do (hacer): Implementar y utilizar el SGSI, Check (verificar): Monitorizar y revisar el SGSI y Act (actuar): Mantener y mejorar el SGSI.

5.3.4.1. *Plan: Establecer el SGSI*

- Definir el alcance del SGSI para las entidades y/o organizaciones su localización, activos y tecnologías.

- Definir una política de seguridad que: Incluya el marco general y los objetivos de seguridad de la información de la organización, donde se establezca los criterios con los que se va a evaluar el riesgo aprobados por la dirección.

- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos de la entidad, donde se determine la aceptación del riesgo y especificar los niveles de riesgo aceptable.

- Identificar los riesgos: Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios; identificar las amenazas en relación a los activos; identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas; identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

- Analizar y evaluar los riesgos: Análisis del impacto y/o ocurrencia que puede presentar la Dirección de Sistemas en un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información.

- Identificar y evaluar las distintas opciones de tratamiento de los riesgos para: Aplicar controles adecuados; aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos.[13]

[13] Sistema de Gestión de la Seguridad de la Información Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

Figura 5. Gestión de Riesgos

Fuente: www.iso27000.es

- Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.

- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.

- Definir una declaración de aplicabilidad que incluya: En este caso tener claro los objetivos de control y controles seleccionados y los motivos para su elección; los objetivos de control y controles que actualmente ya están implantados; los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.[14]

5.3.4.2. *Do: Implementar y utilizar el SGSI*

- Cada entidad y/o organización debe tener presente un plan de tratamiento de riesgos donde se pueda identificar qué acciones, recursos, responsabilidades y prioridades en los riesgos de seguridad de la información se pueda presentar.

- Establecer periódicamente capacitación a todos los funcionarios de la Dirección de Sistemas de la Gobernación de Boyacá, para la concienciación en relación a la seguridad de la información de la entidad.

[14] Sistema de Gestión de la Seguridad de la Información. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información en la Dirección de Sistemas de la Gobernación de Boyacá.

5.3.4.3. *Check: Monitorizar y revisar el SGSI*

Todas las entidades y/o organizaciones deben cumplir con lo siguiente:

- Ejecutar procedimientos de monitorización y revisión para: Detectar a tiempo los errores en los resultados generados por el procesamiento de la información; esto se hace mediante incidentes o fallas que puede tener la Dirección de Sistemas de la Gobernación de Boyacá.

- Se debe revisar periódicamente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI.

- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.[15]

- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.

- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.

- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

- Registrar acciones y eventos que puedan haber impactado sobre la efectividad el rendimiento del SGSI.[16]

---

[15] Sistema de Gestión de la Seguridad de la Seguridad. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

[16] Sistema de Gestión de la Seguridad de la Información. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

5.3.4.4. *Act: Mantener y mejorar el SGSI*

La Dirección de Sistemas de la Gobernación de Boyacá debe tener presente: Establecer mejoras al momento de implementar un SGSI en la Entidad.

- Se debe hacer actividades preventivas y correctivas en relación a la cláusula 8 de ISO 27001 teniendo presente las experiencias propias de la Entidad.
- Dar a conocer las mejoras del SGSI en la Dirección de Sistemas y la forma de proceder.
- Revisar que mejoras realizadas alcancen los objetivos previstos.
- Implementar controles o monitoreo que permita detectar los controles que aún no están implantados en la Entidad.

5.3.5 *Diseño de un SGSI ISO 27001*

El diseño del SGSI, abarca todos los aspectos de planeación a seguir para la implantación del SGSI en la entidad y/o organización, bajo la normativa en estudio, para ello, se utilizará como norma guía la ISO 27001, la cual sirve como ayuda a los retos a los que nos somete el propio entorno.

La norma ISO 27001 es una de las mejores prácticas a nivel mundial para gestionar la seguridad de la información, y es contemplada como su solución por múltiples organizaciones de distinto tamaño.

Para proceso de diseño de un sistema de gestión es necesario definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación.

Plan (planificar): establecer el SGSI.

Do (hacer): implementar y utilizar el SGSI.

Check (verificar): monitorizar y revisar el SGSI.

Act (actuar): mantener y mejorar el SGSI**.**

ISO 27001 / 27002: Esta norma internacional emitida por la Organización Internacional de Normalización (ISO) la ISO 27001 y su Código de Práctica ISO 27002, contemplan la continuidad de negocio como un elemento clave dentro de la gestión de la seguridad de la información y describen cómo gestionar la seguridad de la información en una empresa.
La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. Puede ser diseñada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Adicionalmente brinda soporte y conceptos generales que se y está diseñada con

el objetivo de facilitar un sistema de gestión de la seguridad de la información[17]

MAGERIT: Es una metodología de análisis y gestión de riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica.[18] Esta norma ayuda a las entidades a analizar los riesgos que soportan los Sistemas de información, y para recomendar las medidas apropiadas que deberían adoptarse en la mejora de su control.

AMENAZAS: Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los componentes de un sistema, en el caso de la Seguridad Informática, los Elementos de Información. La Seguridad Informática tiene como propósitos el garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones. **SEGURIDAD INFORMÁTICA**[19]

La Seguridad Informática en los sistemas de información se define como cualquier auditoria en donde se hace revisiones y evaluaciones de los controles, sistemas, procedimientos de informática.

Dentro de las soluciones tecnológicas que actualmente se encuentran disponibles para reforzar la seguridad de una red, encontramos el firewall, este sistema da cumplimiento de las políticas de control de acceso a la red mediante reglas que se le establezcan lo que ayuda a proteger la información activos esenciales para las entidades y/o organizaciones.

Este tipo de detección pretende cuantificar el comportamiento normal de un usuario, para una correcta distinción se debe tener presente tres distintas posibilidades que existen en un ataque.

- ***Penetración externa.*** Usuario que no tiene permiso autorizado y hace el intente mediante un equipo de cómputo (otra red).

  .

- ***Penetraciones internas.*** Usuario interno que intenta tener acceso a la información, pero no se encuentra con el perfil autorizado.

- ***Abuso de Recursos*****:** Se define como el abuso que un usuario lleva a cabo sobre unos datos o recursos de un sistema al que está autorizado su acceso.

---

[17] Norma ISO 27001, Disponible en: http://advisera.com/27001academy/es/que-es-iso-27001/

[18] (Ortiz, Anàlisis de Riesgos - Magerit, s.f.)

[19] Laudon & Laudon. Administración de los sistemas de información; Prentice Hall, 1997, Pág. 329.

Para una adecuada gestión de la información es necesario implantar un sistema de seguridad de la información, con base en normas preestablecidas que permitan a la organización asegurar la disponibilidad y seguridad de la información que maneja, contemplada en las normas ISO.

5.3.6. *Clasificación de Amenazas Informáticas*

5.3.6.1. *De interrupción:* No se encuentra habilitado el acceso a la información.

5.3.6.2. *De interceptación:* Tener acceso a la información confidencial de la Dirección de Sistemas de la Gobernación de Boyacá.

5.3.6.3 *De modificación:* Ingreso a los programas y datos de un sistema de información con el fin de modificarlos.

5.3.6.4. *De fabricación*: Información incoherente, es decir no es correcta.

5.3.6.5. *Accidentales:* Fallos en los equipos, en las redes, en los sistemas operativos o en el software, errores humanos

5.3.6.6. *Intencionadas*: Por lo general son manos intrusas, es decir software malicioso.

5.3.6.7. *Riesgos:* En el Análisis de riesgos se identifican y valoran los elementos componentes del riesgo, obteniendo una estimación de los umbrales de riesgo deseables. Es la consideración sistemática del daño probable que puede causar un fallo en la seguridad de la información, con las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.[20]

5.3.7. *Elementos del Análisis de Riesgos*

En la realización de un Análisis y Gestión de Riesgos según MAGERIT, el Analista de Riesgos es el profesional especialista que maneja seis elementos básicos:

5.3.7.1. *Activos:* Es todo aquello que una entidad y/o organización puede considerar importante, es decir su infraestructura y datos.

5.3.7.2. *Amenazas:* Identificar cual es la causa que afecta cualquier activo de las entidades y/o organizaciones.

[20] (Seguridad Informatica, 2015)

5.3.7.3. *Degradación*: Como es de perjudicial y Frecuencia: Cada cuanto se materializa la amenaza.[21]

5.3.7.4. *Vulnerabilidades:* Es una posibilidad de ocurrencia de la materialización de una amenaza en un activo de la entidad y/o organización.

5.3.7.5. *Impactos*: Es un daño que sufre cada activo de la entidad y/o organización que se genera sencillamente por cualquier amenaza.

5.3.7.6. *Riesgo*: Es la medida de la posibilidad que existe en que se materialice una amenaza. Conociendo el riesgo ya podemos calcular la frecuencia Salvaguardas (Funciones, Servicios y Mecanismos): Una salvaguarda es un mecanismo de protección frente a las amenazas, reducen la frecuencia de las amenazas y limitan el daño causado por estas.[22]

5.3.8. *Riesgos Informáticos*

Cada una de las entidades sabe de las amenazas que hoy en día se encuentran y los daños que puede ocasionar a los bienes o servicios informáticos, como equipos informáticos, periféricos, instalaciones, programas de cómputo, etc.

Es por eso que cualquier entidad y/o organización cuente con una herramienta, que garantice la correcta evaluación de los riesgos, donde permita identificar el proceso y actividad en el cual participa la Dirección de Sistemas de la Gobernación de Boyacá y lograr evaluar el desempeño del entorno informático.

5.4. TIPO DE RIESGOS

5.4.1. Riesgo de Integridad: Estos riesgos aplican en cada aspecto de un sistema de soporte de procesamiento de negocio y están presentes en múltiples lugares, y en múltiples momentos en todas las partes de las aplicaciones; no obstante, estos riesgos se manifiestan en los siguientes componentes de un sistema:

- **Interface del usuario*:*** Los riesgos en esta área generalmente se relacionan con las restricciones, sobre las individualidades de una organización y su autorización de ejecutar funciones negocio/sistema; teniendo en cuenta sus

[21] Metodología de Análisis de Riesgo: Disponible en: https://upload.wikimedia.org/wikipedia/commons/8/87/Riesgoinformatico.pdf

[22] Seguridad Informática Magerit. Disponible en: http://seguridadmagerit.blogspot.com.co/2015/07/elementos-del-analisis-de-riesgos.html

necesidades de trabajo y una razonable segregación de obligaciones.[23] Esto significa que la Dirección de Sistemas de la Gobernación de Boyacá tiene restricciones en la información y en los equipos de cómputo.

- **Procesamiento:** Hace relación a los controles defectivos y preventivos que aseguran que el procesamiento de la información ha sido completado.

- **Procesamiento de errores:** Los riesgos en esta área generalmente se relacionan con los métodos que aseguren que cualquier entrada/proceso de información de errores (Excepciones) sean capturados adecuadamente, corregidos y reprocesados con exactitud completamente.[24]

- **Administración de cambios:** Estos riesgos están asociados con la administración inadecuadas de procesos de cambios de organizaciones que incluyen: Compromisos y entrenamiento de los usuarios a los cambios de los procesos, y la forma de comunicarlos e implementarlos.[25]

- **Información:** La mala administración de los riesgos y los controles inadecuados hacen parte de este riesgo, los cuales incluyen la integridad de la información y la administración efectiva de los sistemas de bases de datos.

- **Riesgos de relación:** Hacen parte del uso adecuado y oportuno de la información que es creada mediante una aplicación.

5.4.2. Riesgos de Acceso: Hace parte a los datos de información, donde incluyen: riesgos de segregación, riesgos asociados con la integridad de la información de sistemas de bases de datos y riesgos asociados a la confidencialidad de la información.

- **Administración de la información:** Hace relación a los usuarios que tienen acceso a la información que encuentra en su entorno.

---

[23] Riesgos Informáticos. Disponible en: https://www.guardianes.com.co/CRITERIOS%20DE%20SEGURIDAD%20BASC/RIESGO_INFORMATICO_BASC.pdf

[24] Riesgos Informáticos. Disponible en: https://www.guardianes.com.co/CRITERIOS%20DE%20SEGURIDAD%20BASC/RIESGO_INFORMATICO_BASC.pdf

[25] Riesgos Informáticos. Disponible en: https://www.guardianes.com.co/CRITERIOS%20DE%20SEGURIDAD%20BASC/RIESGO_INFORMATICO_BASC.pdf

• **Entorno de procesamiento:** Estos riesgos en esta área están manejados por el acceso inapropiado al entorno de programas e información.

• **Redes*:*** Hace relación al acceso inapropiado en el procedimiento y su entorno de red.

• **Nivel físico*:*** Protección física de dispositivos y un apropiado acceso a ellos. [26]

5.4.3. Riesgo de Utilidad*:* Hace relación a los niveles de riesgo en los cuales se encuentran: Riesgos que se pueden enfrentar por el direccionamiento de sistemas antes de cualquier problema que se pueda presentar, otro riesgo recuperación/restauración empleado para mitigar la ruptura de los sistemas. Y finalmente se encuentra el nivel de Backus y planes de contingencia estos ayudan a controlar los desastres en el procesamiento de la información.

5.4.4. Riesgos de Infraestructura*:* Hace referencia sobre la estructura de información de cualquier entidad (hardware, software, redes, personas y procesos), que permita mantener necesidades futuras y presentes de los negocios de la entidad con un costo eficiente.

5.4.5. Riesgos de Seguridad General*:* Los estándar IEC 950 proporcionan los requisitos de diseño para lograr una seguridad general y que disminuyen el riesgo:

- Riesgos de choque de eléctrico: Niveles altos de voltaje.
- Riesgos de incendio: Inflamabilidad de materiales.
- Riesgos de niveles inadecuados de energía eléctrica.
- Riesgos de radiaciones: Ondas de ruido, de láser y ultrasónicas.
- Riesgos mecánicos: Inestabilidad de las piezas eléctricas.[27]

[26] Riesgos Informáticos. Disponible en: https://www.guardianes.com.co/CRITERIOS%20DE%20SEGURIDAD%20BASC/RIESGO_INFORMATICO_BASC.pdf

[27] (INFORMATICOS, s.f.)

5.5. *CONTROLES Y CLASIFICACIÓN*

5.5.1. Inventario de Activos: La norma ISO27001 nos habla sobre los activos de información que deben ser identificados de una forma clara y se tiene que realizar y mantener un inventario en el que aparezcan todos los activos de información importantes.

Entre los activos más comunes se encuentran.

5.5.2. Activos de Información*:* Encontramos bases de datos, documentación del sistema, manuales de usuarios, material de formación, procedimientos, planes de continuidad, configuración de soporte, etc.

5.5.3. Activos de Software*:* Software de aplicación, software del sistema, herramientas y programas de desarrollo, etc.

5.5.4. Activos Físicos: Equipo de cálculo, equipo de comunicación, etc.

5.5.5. Servicios: Servicios de cálculo y comunicaciones, generales, etc.

5.5.6. Activos Intangibles: Reputación, imagen de la organización, etc.

5.6. PROPIEDADES DE LOS ACTIVOS

Todos los activos deben contar con un responsable asegurar la información y los activos que se encuentran asociados a las instalaciones de la organización, son los encargados de revisar de forma periódica las restricciones en el acceso y las clasificaciones.

Las responsabilidades deben ser asignadas a:

- Proceso de negocios
- Conjunto bien definido de actividades
- Mitigación
- Conjunto definido de datos

5.6.1. Utilización Adecuada de los Activos

Se debe identificar una regla general, que sea aceptable, para que los activos asociados a las instalaciones del procesamiento de la información sean identificados, documentados e implantados.

Todos los trabajadores, internos o externos, y las terceras personas implicadas tienen que seguir ciertas reglas para utilizar de forma aceptable la información y los activos que se encuentran asociados a las instalaciones del procesamiento de información, en las que se incluyen:

- Las reglas mediante correo electrónico y la utilización de internet.
- Guías de uso de aparatos móviles, especialmente fuera de las instalaciones de la organización.[28]

El Diseño de un Sistema de SGSI, nos ayuda a proteger los activos de cualquier entidad y/o organización aparte de los riesgos informáticos, otro evento como puede ser un caso extraordinario un incendio, catástrofe natural etc.

El Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer que estas políticas y procedimientos en relación a los objetivos propios de la entidad y/o organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

5.7. MARCO CONCEPTUAL

5.7.1. Conceptos Básicos:

A continuación, se presentan algunas definiciones importantes relacionadas al SGSI que se busca diseñar.

Confidencialidad: Información disponible exclusivamente a personas autorizadas de la Dirección de Sistemas de la Gobernación de Boyacá.

Integridad: Mantenimiento de la exactitud y validez de la información, protegiéndola de modificaciones o alteraciones no autorizadas. [29]

Disponibilidad: Acceso y utilización de los servicios infraestructura o datos sólo y en el momento de ser solicitado por una persona autorizada.

Amenazas: Fuentes generadoras de eventos en las que se originan las pérdidas por riesgos de seguridad de la información.[30]

[28] (Excellence, s.f.)

[29] Sistema de Gestión de la Seguridad de la Información. Disponible en: http://www.iso27000

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones del negocio.[31]

Información*:* Datos relacionados que tienen significado para la organización. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada. [32]

Seguridad de la información: Preservación de la integridad, la confidencialidad, y la disponibilidad de la información, otras propiedades como autenticidad y responsabilidad. [33]

S.G.S.I: Sistema de Gestión de Seguridad de la Información, basado en el análisis de riesgos, que permite controlar la seguridad de la información y su infraestructura.

Políticas de Seguridad: Reglas para proporcionar la dirección gerencial y el soporte para la seguridad de la información. Es la base del SGSI para cualquier entidad y/o organización.

Organización de la seguridad de la información: Es administrar la seguridad dentro de la organización, así como mantener la seguridad de la infraestructura de procesamiento de la información y de los activos que son accedidos por terceros.

Gestión de activos: Protección de activos de información, controlando el acceso solo a las personas que tienen permiso de acceder a los mismos.

Riesgo: Amenazas asociadas a la seguridad de la información en los activos de una entidad y/o organización.

---

[30] Seguridad de la Información. Universidad Nacional de Lujan, Departamento de Seguridad Informática. Disponible en: http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf

[31] El Portal del ISO 27001 en español. Disponible en: http://www.iso27000.es/glosario.html

[32] Seguridad y Privacidad de la Información. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

[33] Introducción a la Seguridad Informática. Disponible en: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=1

Vulnerabilidad: Debilidad de un activo de información frente a una amenaza.[34]

Datos: Todos los objetos de información. Se considera información interna y externa, estructurada o no, gráficas, sonidos, etc.[35]

Aplicaciones: Sistemas de información, que integran procedimientos manuales y sistematizados.

Tecnología: Incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.

Instalaciones: Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.

Seguridad física y ambiental: Trata principalmente de prevenir el acceso no autorizado a las instalaciones para prevenir daños o pérdidas de activos o hurto de información.

Gestión de comunicaciones y operaciones: Garantizar la operación correcta de los equipos, así como la seguridad cuando la información se transfiere a través de las redes, previniendo la pérdida, modificación o el uso erróneo de la información.

Control de accesos: Es controlar el acceso a la información, el acceso no autorizado a los sistemas de información y computadoras.

Sistemas de información, adquisición, desarrollo y mantenimiento*:* Garantizar la seguridad de los sistemas operativos, proyectos de TI y el soporte se den de manera segura y mantener la seguridad de las aplicaciones.

Gestión de incidentes de seguridad de la información: Metodología de administración de incidentes, que es básicamente definir de forma clara los procedimientos.

Gestión de continuidad del negocio: Contrarrestar interrupciones de las actividades y proteger los procesos críticos como consecuencias de fallas o desastres.

Evento de seguridad de la información. Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la

34 Riesgos, Amenazas y Vulnerabilidades de los Sistemas de Información. Disponible en: http://repository.ucatolica.edu.co/bitstream/10983/1305/1/RIESGOS%20AMENAZAS%20Y%20VULNERABILIDADES%20DE%20LOS%20SISTEMAS%20DE%20INFORMACION%20GEOGRAFICA%20GPS.pdf

35 Auditora de Sistemas. Disponible: https://es.slideshare.net/cairiza/principios.

información, una falla de controles, o una situación previamente desconocida.

Análisis de riesgos. Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

Evaluación de riesgos**.** Todo proceso de análisis y valoración del riesgo.

Valoración del riesgo**.** Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.

Oficial de Seguridad**:** Persona encargada de administrar, implementar, actualizar y monitorear el SGSI.

Recurso Humano: Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información, o de procesos de TI.

Gestión del riesgo**.** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

5.7.2*. Sobre la Norma ISO/IEC 27000*

5.7.2.1 .*ISO/IEC 27000*: Publicada el 1 de mayo de 2009, revisada con una segunda edición de 01 de diciembre de 2012 y una tercera edición de 14 de enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua).[36]

5.7.2.2. *ISO/IEC 27001**:* Publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones.[37]

[36] El Portal de ISO 27001 en español. Disponible en: http://www.iso27000.es/iso27000.html
[37] ISO 27001: Disponible en: http://www.iso27000.es/iso27000.html

5.7.2.3. ISO/IEC 27002: Publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. [38]

5.7.2.4. *ISO/IEC 27003:* Publicada el 01 de febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.[39]

5.7.2.5. *ISO/IEC 27004*: Publicada el 15 de diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.[40]

5.7.2.6. *ISO/IEC 27005:* Publicada e en segunda edición el 1 de junio de 2011 (primera edición del 15 de junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su primera publicación revisó y retiró las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000.[41]

5.7.2.7. *ISO/IEC 27006:* Publicada en segunda edición el 1 de diciembre de 2011 (primera edición del 1 de marzo de 2007) y revisada el 30 de septiembre de 2015. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001:2005 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.[42]

---

[38] Destacados ISO 27000. Disponible en: http://www.iso27000.es/iso27000.html

[39] El Portal de ISO 27001 en español. Disponible en: http://www.iso27000.es/iso27000.html

[40] ISO 27001: Disponible en: http://www.iso27000.es/iso27000.html

[41] Destacados ISO 27000. Disponible en: http://www.iso27000.es/iso27000.html

[42] El Portal de ISO 27001 en español. Disponible en: http://www.iso27000.es/iso27000.html

5.7.2.8. *ISO/IEC 27007:* Publicada el 14 de noviembre de 2011. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011. En España, esta norma no está traducida. El original en inglés puede adquirirse en iso.org. Actualmente en proceso de revisión para su actualización.[43]

5.7.2.9. *ISO/IEC 27008:* Publicada el 15 de octubre de 2011. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI. En España, esta norma no está traducida. El original en inglés puede adquirirse en iso.org. Actualmente en proceso de revisión para su actualización.[44]

5.8. *MARCO LEGAL*

El creciente uso de las nuevas tecnologías de la información ha propiciado la creación de un marco legal y jurídico que protege a todas las partes interesadas en el uso de estas tecnologías y el intercambio y tratamiento de la información a través de ellas.

En cuanto a los delitos informáticos, cada día surgen nuevas formas de delitos que pueden afectar la seguridad de la información en las entidades.

Por ello, cumplir con la legislación vigente en Colombia es uno de los requisitos que se deben tener en cuenta para implantar un Sistema de Gestión de Seguridad de la Información. Protegiendo a la entidad de las amenazas externas.

Veamos cuál es la legislación colombiana relacionada con seguridad de la información.

5.8.1. ***Ley 1581 de 2012 protección de datos personales***

Esta ley tiene por objeto 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 a que se refiere el artículo 15 de la

[43] ISO 27001: Disponible en: http://www.iso27000.es/iso27000.html

Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Los principios y disposiciones contenidas en esta ley se aplican a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza ya sea pública o privada.[45]

5.8.2. ***Ley 527 de 1999 de comercio electrónico***

Ley que aplica a todo tipo de información en forma de mensaje de datos, para los efectos de la presente ley se entenderá por:

Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, el Intercambio Electrónico de Datos y el correo electrónico.

Comercio electrónico. Abarca todo lo relacionado con lo comercial a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Comprende las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial, operaciones financieras, bursátiles, seguros de construcción, consultoría, ingeniería; servicios públicos, transporte de mercancías y pasajeros.

Firma digital. Se entiende como el valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático, vinculado a la clave del creador, garantiza la transferencia de archivos electrónicos.

Entidad de Certificación. Entidad autorizada para emitir certificados electrónicos en relación con las firmas digitales de las personas.

Intercambio Electrónico de Datos. La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto.

[45]Ley 1581 de 2012 Decreto 1377 de 2013. Colombia Digital, Agosto 29, 2013, Disponible en: http://www.colombiadigital.net/actualidad/articulos-informativos/item/5543-abc-para-proteger-los-datos-personales-ley-1581-de-2012-decreto-1377-de-2013.html

Sistema de Información. Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma de mensajes de datos. [46]

5.8.3. *Ley 1343 Propiedad Intelectual*

Ley que protege sobre toda creación del talento o del ingenio humano, dentro del ámbito científico, literario, artístico, industrial o comercial. La protección de la propiedad intelectual es de tipo jurídica, sin embargo, las leyes que existen no se realiza sobre esta denominación conceptual, sino sobre dos campos muy bien diferenciados: el Derecho de Autor y la Propiedad Industrial.

5.8.4. *Ley 23 de 1982 Derechos de Autor*

La ley colombiana otorga al Derecho de Autor sobre todas las formas en que se puede expresar las ideas, no requiere ningún registro y perdura durante toda la vida del autor, más 80 años después de su muerte, después de lo cual pasa a ser de dominio público. El registro de la obra ante la Dirección Nacional del Derecho de Autor tiene como finalidad brindar mayor seguridad a los titulares del derecho.
En el caso del Software, la legislación colombiana lo asimila a la escritura de una obra literaria, permitiendo que el código fuente de un programa esté cubierto por la ley de Derechos de Autor.[47]

[46] Ley 527 de 1999, agosto 18, El Congreso de Colombia, Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

[47] Ley 23 de 1982, enero 01, El Congreso de Colombia, Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431

6. DISEÑO METODOLÓGICO

6.1 *DISEÑO*

El presente estudio se encamina dentro del tipo de investigación cuantitativa, ya que lo que se pretende es desarrollar mediante un proceso investigativo un diseño de un Sistema de Gestión de Seguridad de la Información para la Dirección de Sistemas de la Gobernación de Boyacá. El diseño de un Sistema de Gestión de Seguridad de la Información permitirá a la entidad, disminuir el riesgo de pérdida de información, mediante el análisis y medición de las vulnerabilidades, amenazas y riesgos de los activos, y las posibles pérdidas de confidencialidad, disponibilidad e integridad a la que puede estar expuesta la entidad.

Para obtener la información relevante que permita la realización de este proyecto se recurrirá a la técnica de investigación descriptiva, puesto que se conoce una situación problema, a partir de la cual se espera analizar y evaluar a través de variables los diferentes requerimientos para el análisis y diseño de un SGSI bajo la norma ISO/IEC 27001.

Para la realización de este proyecto se analizará paso a paso cuales son las necesidades en la Dirección de Sistemas de la Gobernación de Boyacá, los temas son sobre seguridad física, seguridad interna, seguridad externa, seguridad lógica, seguridad perimetral, elementos de control para la seguridad de hardware software, alcances, análisis de riesgos, amenazas, posibles ataques, plan de contingencia y políticas de seguridad.

Este proceso se llevará a cabo mediante observación directa y encuestas a empleados.

Las encuestas ejecutadas a los empleados del área de sistemas de la Gobernación de Boyacá, pretende medir las buenas prácticas de ellos para el manejo de la información, el conocimiento de los riesgos y sobre todo la importancia de la seguridad de la información.

Cabe denotar que la observación directa como la aplicación de la encuesta ambas están encaminadas a medir el grado de conocimiento sobre la gran importancia que implica el manejo de la seguridad de la información.

6.2. *TIPO DE INVESTIGACION*

El Diseño del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para la Dirección de Sistemas de la Gobernación de Boyacá, se enmarca dentro del tipo de investigación descriptiva y analítica, puesto

que comprende la recolección, descripción, registro, análisis e interpretación de la información.

6.2.1. ***Descriptiva:*** Utilizada para cuando se desea describir, básicamente se encarga de una etapa preparatoria de trabajo. en donde facilita el proceso de ordenar los resultados de las observaciones de las conductas y las características.

6.2.2. ***Analítica*****:** Es un proceso más complejo con la investigación descriptiva, pero es la encargada de establecer la comparación de diferentes variables encontradas en el proceso de búsqueda de la información, que lo que se busca es que la persona encargada de analizar defina con pruebas sin el proceso es afirmativo o negativo.

6.3. *METODO DE INVESTIGACION*

El método de investigación establecido para este estudio es de tipo descriptivo, puesto que se conoce puesto que se conoce una situación problema, a partir de la cual se espera analizar y evaluar a través de variables los diferentes requerimientos para el análisis y diseño de un SGSI bajo la norma ISO/IEC 27001.

6.4. *UNIVERSO Y MUESTRA*

6.4.1. Población**:** Para la encuesta de los empleados, la población estudio está conformada por el personal de planta que labora de la Dirección de Sistemas de la Gobernación de Boyacá.

Tabla 1. Población conformada por el personal de la Dirección de Sistemas de la Gobernación de Boyacá.

Población Estudio (Ingeniero de Sistemas)	**Número de Empleados**
Personal de Planta	4 Empleados
Contratistas	11 Empleados
Total	15 Empleados

Fuente: El Autor

6.4.2. ***Muestra:*** Teniendo en cuenta que el personal que labora en la Dirección de Sistemas de la Gobernación de Boyacá es igual a número de personas relativamente pequeño, se tomó como muestra el total de 15 Empleados.

6.5. *RECOLECCION DE LA INFORMACION*

Como se ha dicho anteriormente la información que se pretende recopilar se obtendrá de la Dirección de Sistemas de la Gobernación de Boyacá, situación actual y el tema que nos compete el análisis de riesgos de Seguridad en la Dirección de Sistemas.

6.5.1. ***Información Primaria:*** Se hace mediante Encuestas y Pruebas. Las encuestas de hacen a los empleados de la Dirección de Sistemas de la Gobernación de Boyacá, se determina la problemática interna del área referente al manejo de la información, procedimientos de seguridad actuales con el fin de mitigar los riesgos, además se ejecutan las pruebas como reconocimiento, escaneo de la red que permitan detectar los riesgos a lo que se encuentra expuesta.

6.5.2. ***Información Secundaria:*** Para poder identificar los procesos externos se tendrá presente la información de tipo bibliográfico, conceptos aprendidos en el transcurso del desarrollo de la especialización, los cuales han servido de ayuda para el desarrollo de este proyecto, así como páginas de internet que contienen información del tema a estudiar.

6.5.3. ***Instrumentos de Recolección de Información:*** Principalmente se utilizó la técnica de observación directa, la técnica de la encuesta y la ejecución de pruebas.

6.5.3.1. ***Técnica de Observación:*** Observación, integrantes de Observadores: Ha sido de forma individual, según el área donde se realiza. Se observó y se analizó las siguientes actividades: Inicio del sistema, ubicación de los servidores, ingreso de información al sistema, elaboración de los backups, actualización de información, manejo del correo electrónicos (Corporativo).

6.5.3.2. ***Técnica de Encuesta:*** Esta encuesta básicamente consiste en una serie de preguntas de tipo cerrada, preguntas categorizadas con respuestas en abanico. Se manejó variables como: Tiempo, frecuencia, calidad, problemas, reportes y una de las más relevantes el nivel de satisfacción.

6.5.3.3. ***Técnica de Realización de Pruebas:*** Básicamente nos apoyamos en herramientas de escaneo o de análisis de trafico de red, cuando la red este en operando para poder revisar y verificar su funcionamiento.

6.5.4. *Muestra*

6.5.4.1. ***Muestra Empleados:*** Técnica de la Encuesta: Para la organización o estructura del documento se tuvo presente lo siguiente: Eventos presentados relacionados con confidencialidad, integridad y disponibilidad de la información, manejo de contraseñas, políticas de seguridad, fallos, robos, virus entre otros.

6.5.4.2. ***Características de la encuesta para los empleados de la Dirección de Sistemas de la Gobernación de Boyacá:***

El instrumento básicamente consta de: 11 ítems, su forma de presentar es en forma física donde deben contestar de manera escrita en un tiempo determinado de 15 a 20 minutos.

6.5.5. *Descripción del Instrumento:*

Presentación: El instrumento está diseñado principalmente con el criterio de: La ejecución de los objetivos (Cumplimiento).

Normas de Administración**:** El instrumento fue realizado de carácter individual a los empleados de la Dirección de Sistemas de la Gobernación de Boyacá. El diseño de ítems consta de preguntas cerradas, preguntas categorizadas con respuesta en abanico, opción múltiple las cuales el empleado puede seleccionar la respuesta con la mayor que se identifique.

Áreas que explora**:** Mediante la elaboración del instrumento se permite investigar si existen falencias y dificultades en los procesos de manejo y seguridad de la información.

6.6. *PROCESAMIENTO DE LA INFORMACION*

6.6.1. ***Metodología para el análisis y diseño:*** Para el diseño de SGSI, es recomendable seguir una secuencia (procesos), con el fin de poder organizar las actividades para el desarrollo del proyecto, siempre teniendo presente el conjunto de métodos y técnicas que permitan llevar a cabo un SGSI de calidad.

Para el desarrollo del proyecto “Diseño de un sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001, para la Dirección de Sistemas de la Gobernación de Boyacá”, se tomó como guía el método denominado Ciclo PHVA.

Para la implantación de un sistema de Gestión de la seguridad de la información, se requiere del desarrollo de actividades que marquen un orden lógico para llevar organizado todo el proceso. El modelo PDCA (Plan, do, check, act), en su equivalencia en español es Planificar, hacer, verificar y actuar (PHVA), es una estrategia de mejora continua de calidad en cuatro pasos. Este modelo es muy utilizado para implantación de sistemas de gestión, como los sistemas de gestión de la calidad que muchas empresas de hoy lo implantan para la calidad administrativa y de servicios con el objetivo de perfeccionarlos y continuar en un proceso de mejora continua.

Figura 6. Ciclo PDCA (PHVA) SGSI

Fuente: El Autor

Fuente: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

Para el caso de la implantación de Sistemas de Gestión de la Seguridad informática, el ciclo PDCA es una estrategia efectiva para la organización y documentación que se requiere en este proceso

El ciclo PDCA como modelo para implantación de SGSI, permanece en una constante revaluación, por cuanto funciona, bajo la filosofía del mejoramiento continuo; en seguridad sería la revaluación de las medidas de prevención, corrección y evaluación, manteniendo un constante ciclo que por sus características no podría terminar. A continuación, se detalla cada uno de los pasos del modelo Deming como metodología apropiada los SGSI.

Planear

En esta etapa se enmarca todo el proceso de análisis de la situación en que actualmente se encuentra la empresa respecto a los mecanismos de seguridad implementados y la normativa ISO/IEC 17799:2005, la cual se pretende implantar para evaluación y certificación. Así mismo en la etapa de planeación se organizan fases relevantes como son:

- Establecer el compromiso con los directivos de la empresa para el inicio, proceso y ejecución.
- Fase de análisis de información de la organización, En esta fase se comprueba cuáles son los sistemas informáticos de hardware y los sistemas de información que actualmente utiliza la empresa para el cumplimiento de su misión u objeto social.
- Fase de evaluación del riesgo; En esta fase se evalúa los riesgos, se tratan y se seleccionan los controles a implementar.

Hacer

En esta etapa se implementan todos los controles necesarios de acuerdo a una previa selección en la etapa de planeación, teniendo en cuenta el tipo de empresa. También se formula y se implementa un plan de riesgo.

Verificar

Consiste en efectuar el control de todos los procedimientos implementados en el SGSI. En este sentido, se realizan exámenes periódicos para asegurar la eficacia del SGSI implementado, se revisan los niveles de riesgos aceptables y residuales y se realicen periódicamente auditorías internas para el SGSI.

Actuar

Desarrollar mejoras a los hallazgos identificadas al SGSI y validarlas, realizar las acciones correctivas y preventivas, mantener comunicación con el personal de la organización relevante. [48]

6.6.2. *Análisis de la encuesta realizada a los empleados de la Dirección de Sistemas de la Gobernación de Boyacá.*

Luego de recolectar la información para su correspondiente procesamiento, es decir analizar las encuestas a los empleados de la Dirección de Sistemas a través de 11 preguntas que están encaminadas a evaluar aspectos como: Incidentes presentados, manejo de contraseñas, medidas de políticas de seguridad actualmente por la Gobernación de Boyacá, se pueden exponer las siguientes conclusiones:

[48] Ciclo PDCA (Edward Deming), Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

- ✓ Se puede evidenciar que el manejo que tienen sobre el cambio de contraseñas no es el más adecuado y no se cambian las contraseñas con frecuencia.

- ✓ La mayoría de los funcionarios han manifestados su inconformismo con al utilizar su herramienta de trabajo con es el computador, ya sea por: Lentitud, bloqueos, mensajes de error, inconvenientes por acceso a la red. Por otra parte, ellos manifiestan en no conocer las políticas que deben tener presentes para la protección de la información.

Por las razones anteriormente enunciadas se hace necesario el Diseño de un Sistema de Gestión de Seguridad de la Información, donde permita clasificar la información, conocer que activos son los más relevantes para la Dirección de Sistemas de la Gobernación de Boyacá, por otra parte realizar un análisis de los riesgos, definir salvaguardas, definir responsabilidades en el manejo de la información y adoptar políticas y controles de seguridad para la protección de la misma de la Dirección de Sistemas. (Anexo A)

6.6.3. *Descripción y análisis de la prueba realizada a la red de la Dirección de Sistemas de la Gobernación de Boyacá, con Zenmap*.

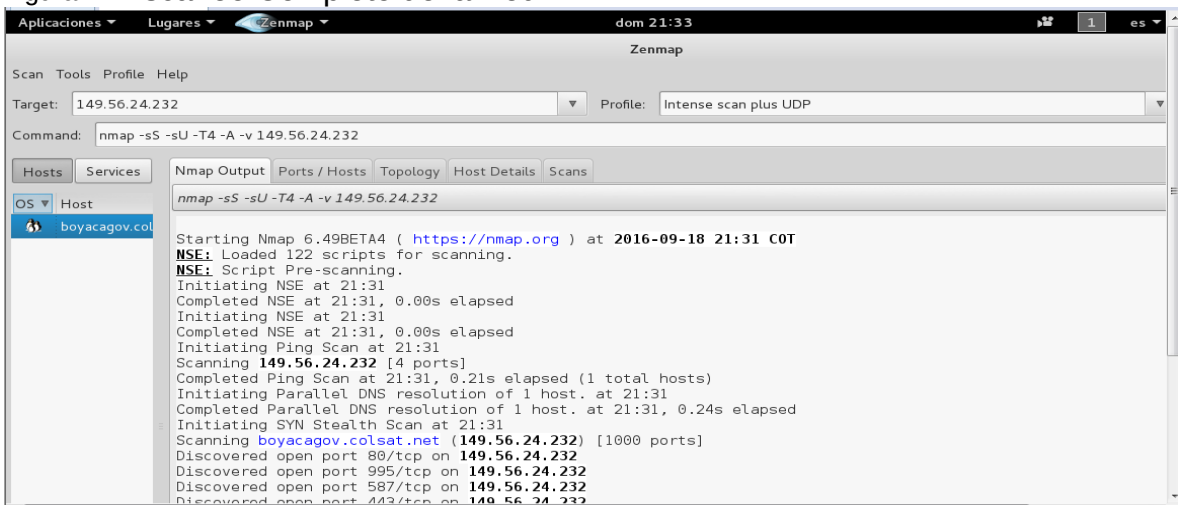
Para el análisis de la red se ejecutó instalación de una Máquina Virtual VWware en donde se instaló el Sistema Operativo Kali_Linuz, se utilizó la herramienta Zenmap para el análisis del tráfico de la red, donde se puede observar las actividades de cada uno de los host que integran la red, la dirección ip de los host, los protocolos de transmisión como UDP, TCP, HTTPs, ARP, el tiempo. Las evidencias del análisis de la red se encuentran así:

6.6.3.1. *Análisis de Trafico de Red con Zenmap de la Red de la Gobernación de Boyacá*

La herramienta Zenmap es muy útil para los funcionarios que realizan auditorias de red por su facilidad de presentar los datos y realizar diferentes tipos de escaneos, donde nos permite saber que sucede en la red.

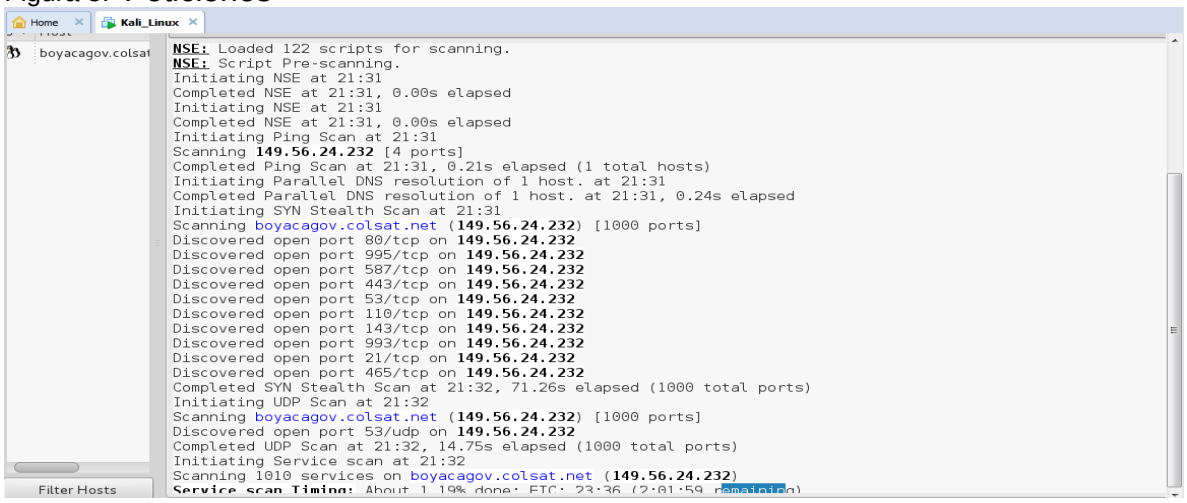
Zenmap captura todo lo que sucede en la red (todas las peticiones)

Figura 7. Escaneo Completo de la Red



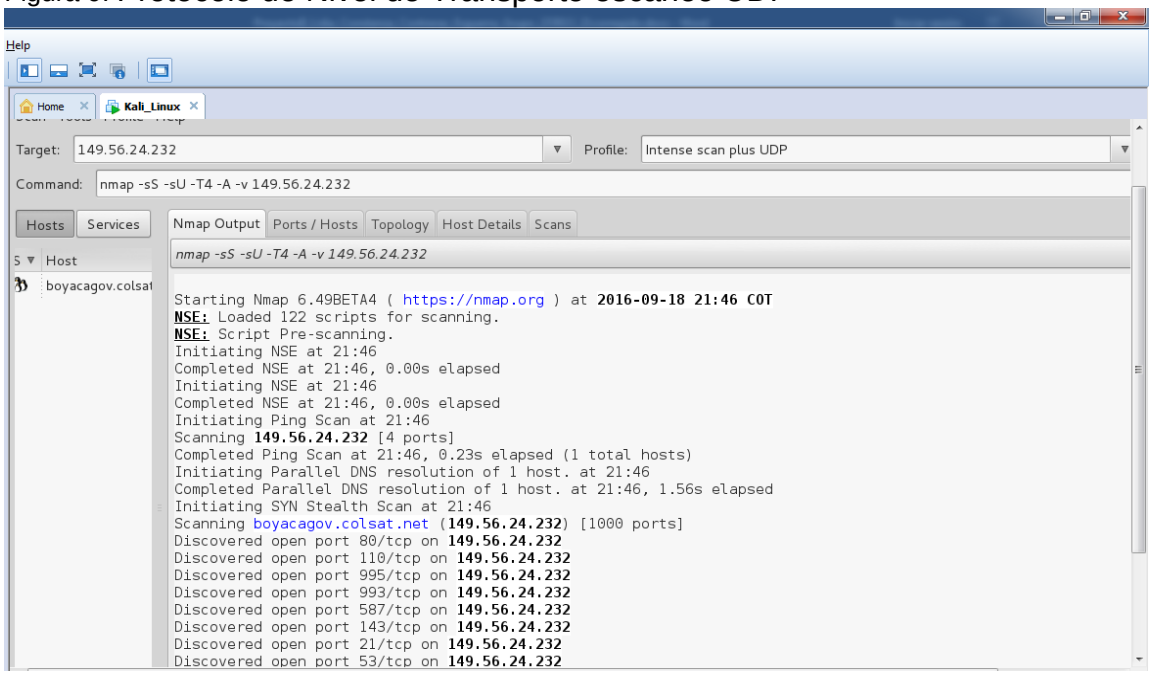
Fuente: El autor

Figura 8. Peticiones



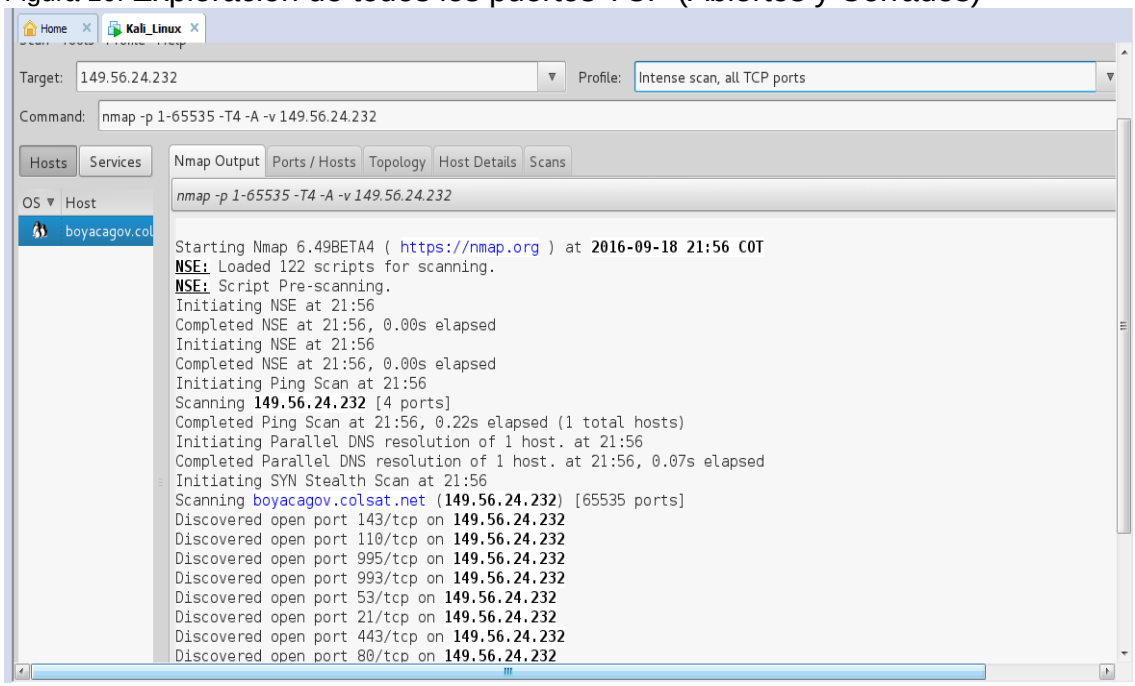
Fuente: El autor

Figura 9. Protocolo de Nivel de Transporte escaneo UDP



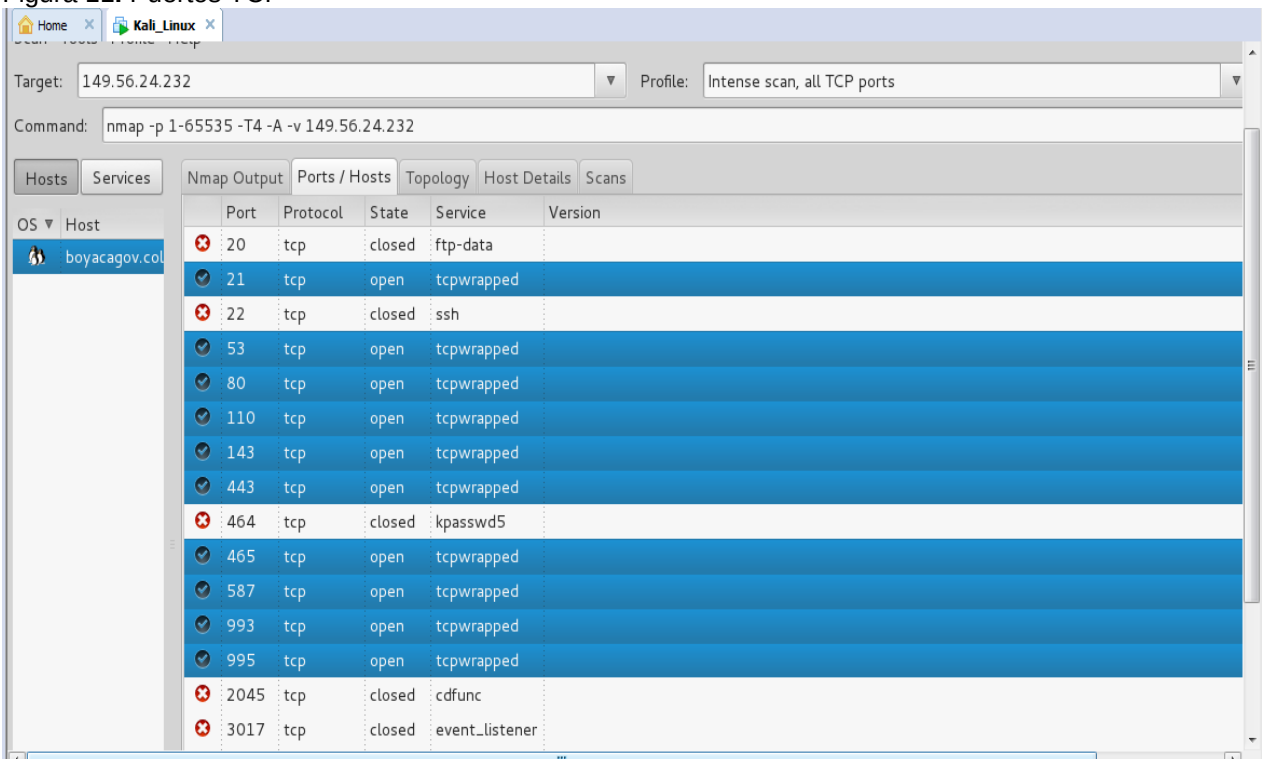
Fuente: El autor

Figura 10. Exploración de todos los puertos TCP (Abiertos y Cerrados)



Fuente: El autor

Figura 11. Puertos TCP



Fuente: El autor

Al ejecutar un escaneo completo se puede observar si la red presenta tráfico no deseado, lo que puede provocar lentitud en la misma.

7. *SGSI PARA LA DIRECCION DE SISTEMAS DE LA GOBERNACION DE BOYACA*

De acuerdo al Ciclo PDCA (PHVA) de SGSI, donde se realizan una serie de pasos y procesos, a continuación, se desarrollan cada una de las etapas así:

7.1. *ESTABLECER EL SGSI*

7.1.1. ***Alcance:*** Mejorar la calidad de los servicios que presta el Departamento de Sistemas de la Gobernación de Boyacá, en la protección de su infraestructura en los procesos de: Recursos Informativos y Tecnológicos con el fin de establecer políticas para gestionar de forma correcta y satisfactoria la seguridad de la información donde todo el personal encargado del área de sistemas tenga conocimientos sobre cómo aplicar y cumplir todos los procesos del SGSI.

7.1.2. ***Política del Sistema de Gestión*****:** La Dirección de Sistemas de la Gobernación de Boyacá pretende que toda la información manejada por la entidad correspondiente a Peticiones quejas y reclamos, Impuestos de Vehículos, Estampillas y Pasaportes se encuentren debidamente protegidas con el fin de preservar y salvaguardar la confidencialidad, disponibilidad e integridad de la información.

7.1.3. ***Metodología de Evaluación de Riesgo:*** Para el desarrollo de este Proyecto se seleccionó la Metodología Magerit para el análisis y gestión de los riesgos por las siguientes razones:

- ✓ Magerit facilita el análisis y revisar el impacto en que se encuentra la Dirección de Sistemas de la Gobernación de Boyacá.
- ✓ Los pasos para el desarrollo se encuentran definidos.
- ✓ La información que se analizo es clara, amplia lo que permite de forma adecuada llevar a cabo el desarrollo del área Dirección de Sistemas.
- ✓ Se puede identificar los riesgos con sus diferentes componentes.
- ✓ Nos ayuda a mitigar los riesgos mediante medidas de seguridad.
- ✓ Magerit ayuda a los directivos a tomar decisiones para mejorar el sistema de seguridad de la entidad y de esta forma minimizar los riesgos.
- ✓ Además, investiga los riesgos que soportan los Sistemas de Información, y sirve para recomendar las medidas apropiadas que debe adoptar la Dirección de Sistemas. para controlarlos.

Nos apoyamos en la Metodología Magerit en donde encontramos los pasos como son los siguientes:

Tabla 2. Pasos Metodología Magerit

Secuencia	Procesos
Paso 1	Inventario de Activos
Paso 2	Valoración de los Activos
Paso 3	Amenazas (Identificación y Valoración)
Paso 4	Salvaguardias
Resultados del Análisis de Riesgos	

Fuente: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-enlinea/321_paso_1_inventario_de_activos.html

7.1.4. *Análisis de Riesgos de la Dirección de Sistemas de la Gobernación de Boyacá*

Se realiza el análisis de los incidentes que podrían ocasionar riesgos para la tecnología de información y partiendo de esto se busca un tratamiento reducir hasta el estado mínimo posible.

7.1.5. *Inventario de Activos:* Hoy en día todas las entidades y/o organizaciones buscan la seguridad de la información, de esta forma saben que la continuidad del negocio es exitosa. Para proteger la información de riesgos y amenazas la Dirección de Sistemas de la Gobernación de Boyacá, realiza un inventario de los activos teniendo en cuenta la Metodología Magerit que se clasifica así:

Estos son los activos tangibles e intangibles que posee la Dirección de Sistemas de la Gobernación de Boyacá, para su buen desempeño laboral son: [S] Servicios, [D] Datos/Información, [SW] Aplicaciones (Software), [HW] Equipos Informáticos (Hardware), [COM] Redes de comunicaciones, [SI] Soportes de información, [AUX] Equipamiento auxiliar, [L] Instalaciones y [P] Personal.

7.2. *CARACTERIZACION DE LOS ACTIVOS*

En la fase se debe considerar tres actividades a realizar

- Identificación de los Activos
- Dependencias entre los Activos
- Valoración de los Activos

Estos son los activos tangibles e intangibles que posee la Dirección de Sistemas de la Gobernación de Boyacá, para su buen desempeño laboral son: [S] Servicios, [D] Datos/Información, [SW] Aplicaciones (Software), [HW] Equipos Informáticos (Hardware), [COM] Redes de comunicaciones, [SI] Soportes de información, [AUX] Equipamiento auxiliar, [L] Instalaciones y [P] Personal.

7.2.1. *Identificación de los Activos*

Los activos son bienes tangibles e intangibles necesarios que posee la Entidad para su buen desempeño laboral.

7.2.1.1 *Activos Esenciales*: Información que se maneja y los servicios que presta

Tabla 3. Activos esenciales

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[vr]		[Sistema Información]	Sistema de Información Isolución Sistema de Información Mesa de Ayuda. Sistema de Información Manuales de procedimientos, Sistema de Información Manuales de usuario Sistema de Información (Presupuesto) Sistema de Información (PQRD)

Tabla 3. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
	Datos vitales (registros de la organización)		Sistema de Información (Jurídicos) Sistema de Información (Gestión de Juntas) Sistema de Información (Gestión Documental)
		[Sistema Información Bases de Datos]	Sistema de Información Solución Sistema de Información Mesa de Ayuda. Sistema de Información Manuales de procedimientos, Sistema de Información Manuales de usuario Sistema de Información (Presupuesto) Sistema de Información (PQRD) Sistema de Información (Rentas) Sistema de Información (Recursos Humanos) Sistema de Información (Jurídicos) Sistema de Información (Gestión de Juntas) Sistema de Información (Gestión Documental)

Tabla 3. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[per]	Datos de carácter personal	[Sistema Contabilidad]	Contabilidad de la Gobernación de Boyacá
		[Documentación Proyectos]	Documentación de Proyectos Tramitados
[service]	Servicio	[Servicio Interno]	Correo electrónico, Internet y Telefonía

Fuente: El Autor

7.2.1.2 *[D] Datos/Información*: Los datos son el corazón que permite a la entidad prestar sus servicios

Tabla 4. Datos/Información

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[files]	Ficheros de datos	[Archivo Proyectos]	Archivo de proyectos entregados y radicados
		[Archivo Usuarios]	Archivo de usuarios externos
		[Archivo Contable]	Archivo Secretaria de Hacienda
[backup]	Copias de respaldo	[Archivo Copias de Respaldo]	Archivo de copias de seguridad de la Información
[conf]	Datos de configuración	[Datos Configuración de Servidores]	Datos de configuración de servidores y equipos
[int]	Datos de gestión interna	[Datos Gestión de Proyectos solicitudes]	Datos de Gestión de Proyectos radicados
[password]	Credenciales	[Contraseñas Empleados]	Contraseñas de acceso de empleados

Fuente: El Autor

7.2.1.3 ***[K] Claves Criptográficas:*** Protección de la Información (secreto o autenticar)

Tabla 5. Claves Criptográficas

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[encrypt]	Claves de cifra	[Claves C. Autenticidad Bancos]	Claves de cifra de aplicaciones bancarias para el pago de Nómina

Fuente: El Autor

7.2.1.4 ***[S] Inventario de Servicios*****:** Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.

Tabla 6. Inventario de Servicios

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[ext]	A usuarios externos (bajo una relación contractual)	[Servicio Externo]	Servicios prestados a usuarios externos (Contratistas de Proyectos)
[int]	Interno (usuarios y medios de la propia organización)	[Servicio Interno]	Servicios prestados a empleados internos
[www]	World wide web	[Servicio Internet]	Servicio de internet al que pueden acceder los empleados.

Fuente: El Autor

Tabla 6. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[email]	Correo electrónico	[Servicio Correo]	Manejo de correos electrónicos (Corporativos)
[file]	Almacenamiento de ficheros	[S_A_Bases de datos]	Servicio de almacenamiento de información en los servidores de bases de datos.
[ipm]	Gestión de privilegios	[Gestión Privilegios]	Manejo de privilegios de acuerdo al rol de cada empleado dentro de la entidad y el lugar de donde esté ingresando, considerando el desempeño como teletrabajo (Accesos Remotos)

Fuente: El Autor

7.2.1.5 *[SW] Software – Aplicaciones Informáticas*: (Programas, Aplicativos, Desarrollos, etc.)

Tabla 7. [SW] Software – Aplicaciones Informáticas

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[app]	Servidor de aplicaciones	[Server Aplicación]	Servidores de Aplicaciones
[email server]	Servidor de correo electrónico	[Server Correo]	Servidor de Correo Electrónico
[file]	servidor de ficheros	[Server Ficheros]	Servidor de Ficheros

Tabla 7. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[dbms]	Sistema de gestión de bases de datos	[SG BaseDatos]	**Nombre activo de la Entidad**
[Oficce]	Ofimática	[Oficce]	Office: 2003, 2007, 2010 y 2013
[av]	Antivirus	[Antivirus]	360 Total Security original con actualizaciones automáticas.
[os]	Sistema operativo	[OS Win xp y win 7]	Sistema operativo Windows XP y Windows 7, profesional.

Fuente: El Autor

7.2.1.6 ***[HW] Equipos Informáticos (hardware):*** Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización

Tabla 8. [HW] Equipos Informáticos (hardware)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[host]	Grandes equipos (host)	[Servicio Aplicaciones]	Servidor Aplicaciones
		[Servicio Data Base]	Servidor de Base de Datos
[mid]	Equipos medios	[PC Clientes Delgados]	Equipos de mesa
		[PC Equipos de Escritorio]	
[pc]	Informática personal	[PC portátiles]	Equipos Portátiles
[vhost]	Equipos virtuales (máquinas virtuales)	[Máquinas Virtuales Equipos virtual]	2 Máquinas Virtuales de Respaldo

Tabla 8. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[backup]	Equipamiento de respaldo	**Código Activo de la Entidad**	**Nombre activo de la Entidad**
[print]	Medios de impresión	[Equipamiento Impresoras]	Impresoras (32)
[scan]	Escáner	[Servicio Scan]	Escáner (5)
[ipphone]	Teléfono IP	[Teléfono IP]	Teléfono Ip (20
[router]	Enrutadores	[Router enrutadores]	Enrutadores
[other]	Wifi	[Wifi Red wifi]	Red Wifi

Fuente: El Autor

7.2.1.7 ***[COM] Redes de Comunicación:*** Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

Tabla 9. [COM] Redes de Comunicación:

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[radio]	red inalámbrica	[Radio]	Red Inalámbrica
[wifi]	Wifi	[Wifi]	Red Inalámbrica
[LAN]	Red local	[Red Local]	Red local
[Internet]	Internet	[Internet]	Internet

Fuente: El Autor

7.2.1.8 ***[Media] Soportes de Información – Electrónico:*** Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

Tabla 10. [Media] Soportes de Información – Electrónico

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[disk]	Discos	[Almacenamiento CD]	Almacenamientos en Disco Duro
[cd]	Cd ROM (CD_ROM)	[Almacenamiento CD]	Almacenamiento en CD
[USB]	Memorias USB	[Almacenamiento Memorias]	Almacenamiento en Memorias
[dvd]	DVD	[A_DVD]	Almacenamiento en DVD
[tape]	Cinta magnética	[Cinta Magnética]	Almacenamiento en Cinta Magnética

Fuente: El Autor

7.2.1.9 ***Soportes de Información – Almacenamiento no Electrónico***

Tabla 11. Soportes de Información – Almacenamiento no Electrónico

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[printed]	Material impreso	[Car]	Cajas con sus carpetas debidamente archivadas por Secretarias (Proyectos, procesos, correspondencia etc.)
		[Informes]	Reportes de informes de todas las Secretarias
		[Varios]	Carpetas varias

Fuente: El Autor

7.2.1.10 ***[AUX] Equipamiento Auxiliar:*** otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

Tabla 12. [AUX] Equipamiento Auxiliar

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
Ppower]	Fuentes de Alimentación	[Power Fuente]	Equipos de Escritorio
[ups] Aai	Sistemas de Alimentación ininterrumpida	[Ups Sistema A]	APC - UPS computadores
[Ac]	Equipos de Climatización	[Equipos Cli]	Aire Acondicionado en la sala de Servidores
[Wire]	Cable Eléctrico	[Cable Eléctrico]	Cable Eléctrico
[Fiber]	Fibra Óptica	[Fibra óptica]	Transmisión de comunicación
[Suplly]	Suministros Esenciales	[Suministro Esenciales]	Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc.
[Furniture]	Mobiliario	[Mobiliario]	Mobiliario: Estantes, armarios, escritorios, archivadores, sillas, etc.

Fuente: El Autor

7.2.1.11 ***[L] Instalaciones*****:** Lugares donde se hospedan los sistemas de información y comunicaciones.

Tabla 13. [L] Instalaciones

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[building]	Edificio	[Edificio Entidad]	Edificio de la Entidad (Plaza de Bolívar -Centro)
[backup]	Instalaciones de respaldo	[Sitio Alterno]	Sitio Alterno (Edifico Fondo Pensional)

Fuente: El Autor

7.2.1.12 ***[P] Personal:*** Personas relacionadas con los sistemas de información

Tabla 14. [P] Personal

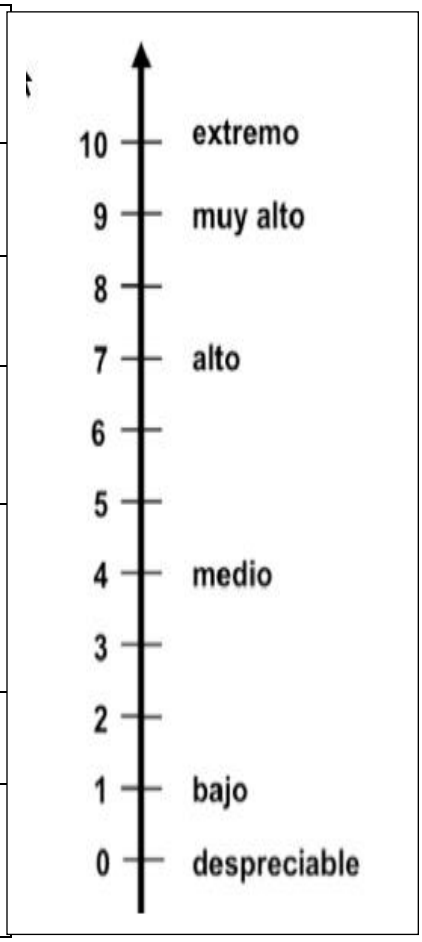
Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[ue]	Usuarios externos	[Externo personal]	Contratistas Externos en las diferentes Secretarias
[ui]	Usuarios internos	[Externo internos]	Ingenieros de la planta de la Dirección de Sistemas
[adm]	Administradores de sistemas	[Admón. sistemas]	Ingeniero encargado de Administración del Sistemas
[com]	Administradores de comunicaciones	[Administración Comunicaciones]	Ingeniero encargado de Administración del Comunicaciones
[dba]	Administradores de BBDD	[Administrador sistemas]	Ingeniero encargado de Administrar las bases de datos.
[sec]	Administradores de seguridad	[Administrador sistemas]	Ingeniero encargado de Administrar el firewall
[dev]	Desarrolladores / programadores	[Administrador sistemas]	Ingenieros y técnicos encargados de desarrollar diferentes proyectos.

Fuente: El Autor

7.2.2. ***Valoración Cuantitativa de los Activos*****:** Como sabemos todos los activos de las Entidades y/o Organizaciones son relevantes para las empresas. Esto significa que si alguno de ellos es atacado genera un tipo de impacto. A continuación, se ejecutará una valorización cuantitativa de cada uno de los activos teniendo presente las dimensiones valoradas: Confidencialidad, Integridad, Autenticidad, Disponibilidad y Trazabilidad de acuerdo a la siguiente tabla:

Tabla 15. Criterios de Valoración

VALOR		CRITERIO
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos



Fuente: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.V__64cmN2g4

7.2.2.1. *Valoración Cuantitativa de Activos Esenciales*

Tabla 16. Valoración Cuantitativa de Activos Esenciales

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	Valor
[vr]	Datos vitales (registros de la organización)	[S Información]	Sistema de Información Isolución	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4
			Sistema de Información Mesa de Ayuda.	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4
			Sistema de Información Manuales de procedimientos.	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7

Tabla 16. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	DIMENSIONES VALORADAS	VALOR
				Trazabilidad	4
			Sistema de Información Manuales de usuario	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4
			Sistema de Información (Presupuesto)	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4
			Sistema de Información (PQRD)	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4
			Sistema de Información (Rentas)	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4

Tabla 16. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	DIMENSIONES VALORADAS	VALOR
			Sistema de Información (Recursos Humanos)	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4
			Sistema de Información (Jurídicos)	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4
			Sistema de Información (Gestión de Juntas)	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4
			Sistema de Información (Gestión Documental)	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4

Tabla 16. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	DIMENSIONES VALORADAS	VALOR
		[S Información Bases de Datos]	Sistema de Información Isolución Sistema de Información Mesa de Ayuda. Sistema de Información Manuales de procedimientos, Sistema de Información Manuales de usuario Sistema de Información (Presupuesto) Sistema de Información (PQRD) Sistema de Información (Rentas)	Confiabilidad	6
			Sistema de Información (Recursos Humanos) Sistema de Información (Jurídicos) Sistema de Información (Gestión de Juntas)	Integridad	6
				Autenticidad	6
				Disponibilidad	7

Tabla 16. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	DIMENSIONES VALORADAS	VALOR
			Sistema de Información (Gestión Documental)	Trazabilidad	4
[per]	Datos de carácter personal	[S_Contabilidad]	Contabilidad de la Gobernación de Boyacá	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4
	Datos clasificados	[D_Históricos]	Datos Históricos de información en las Bases de Datos	Confiabilidad	
				Integridad	7
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	4
[classified]		[D_Proyectos]	Documentación de Proyectos Tramitados	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	4
[service]	Servicio	[S_Interno]	Correo electrónico, Internet y Telefonía	Confiabilidad	7

Tabla 16. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	DIMENSIONES VALORADAS	VALOR
				Integridad	7
				Autenticidad	7
				Disponibilidad	6
				Trazabilidad	2

Fuente: El autor

7.2.2.2 *Valoración Cuantitativa de Datos/Información*

Tabla 17. Valoración Cuantitativa de Datos/Información

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[files]	Ficheros de datos	[Archivo Proyectos]	Archivo de proyectos entregados y radicados	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4
		[Archivo Usuarios]	Archivo de usuarios externos	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4
		[Archivo Contable]	Archivo Secretaria de Hacienda	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4

Tabla 17. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	DIMENSIONES VALORADAS	VALOR
[backup]	Copias de respaldo	[Archivo Copias de Respaldo]	Archivo de copias de seguridad de la Información	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4
[conf]	Datos de configuración	[Datos Configuración de Servidores]	Datos de configuración de servidores y equipos	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4
[int]	Datos de gestión interna	Datos Gestión de Proyectos solicitudes]	Datos de Gestión de Proyectos radicados	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	7
				Trazabilidad	4
[password]	Credenciales	[Contraseñas Empleados]	Contraseñas de acceso de empleados	Confiabilidad	6
				Integridad	6
				Autenticidad	6

Fuente: El autor

7.2.2.3 *Valoración Cuantitativa de Claves Criptográficas*

Tabla 18. Valoración Cuantitativa de Claves Criptográficas

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[encrypt]	Claves de cifra	[Claves Autenticidad Bancos]	Claves de cifra de aplicaciones bancarias para el pago de Nomina	Disponibilidad	4
				Integridad	5
				Confiabilidad	4
				Autenticidad	5
				Trazabilidad	4

Fuente: El autor

7.2.2.4 *Valoración Cuantitativa de Servicios*

Tabla 19. Valoración Cuantitativa de Servicios

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones	VALOR
[ext]	A usuarios externos (bajo una relación contractual)	[Servicio Externo]	Servicios prestados a usuarios externos (Contratistas de Proyectos)	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	8
				Trazabilidad	3
[int]	Interno (usuarios y medios de la propia organización)	[Servicio Interno]	Servicios prestados a empleados internos	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	8
				Trazabilidad	3

Tabla 19. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[www]	World wide web	[Servicio Internet]		Autenticidad	6
				Disponibilidad	8
				Trazabilidad	3
[email]	Correo electrónico	[Servicio Correo]	Manejo de correos electrónicos (Corporativos)	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	8
				Trazabilidad	3
[ipm]	Gestión de privilegios	[Gestión Privilegios]	Manejo de privilegios de acuerdo al rol de cada empleado dentro de la entidad y el lugar de donde esté ingresando, considerando el desempeño como teletrabajo (Accesos Remotos	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	8
				Trazabilidad	3

Fuente: El autor

7.2.2.5. *Valoración Cuantitativa de Software – Aplicaciones Informáticas*

Tabla 20. Valoración Cuantitativa de Software – Aplicaciones Informáticas

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[app]	Servidor de aplicaciones	[Server Aplicación]	Servidores de Aplicaciones	Disponibilidad	9
				Integridad	9
				Confiabilidad	9
				Autenticidad	9
				Trazabilidad	7

Tabla 20. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[email_server]	Servidor de correo electrónico	[Server Correo]	Servidor de Correo Electrónico	Disponibilidad	9
				Integridad	9
				Confiabilidad	9
				Autenticidad	9
				Trazabilidad	7
[file]	servidor de ficheros	[Server Ficheros]	Servidor de Ficheros	Disponibilidad	9
				Integridad	9
				Confiabilidad	9
				Autenticidad	9
				Trazabilidad	7
[dbms]	Sistema de gestión de bases de datos	[SG BaseDatos]	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa.	Disponibilidad	9
				Integridad	9
				Confiabilidad	9
				Autenticidad	9
				Trazabilidad	7
[Oficce]	Ofimática	[Oficce]	Office: 2003, 2007, 2010 y 2013	Disponibilidad	9
				Integridad	9
				Confiabilidad	9
				Autenticidad	9
				Trazabilidad	7
[av]	Antivirus	[Antivirus]	360 Total Security original con actualizaciones automáticas.	Disponibilidad	9
				Integridad	9
				Confiabilidad	9
				Autenticidad	9
				Trazabilidad	7
[os]	Sistema operativo	[OS_Win xp y win 7]	Sistema operativo Windows XP y Windows 7 profesional.	Disponibilidad	9
				Integridad	9
				Confiabilidad	9
				Autenticidad	9
				Trazabilidad	7

Fuente: El autor

7.2.2.6. *Valoración Cuantitativa de Equipos Informáticos*

Tabla 21. Valoración Cuantitativa de Equipos Informáticos

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[host]	Grandes equipos (host)	[Servidor Aplicaciones]	Servidor Aplicaciones	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	3
				Trazabilidad	2
		[Servidor Data Base]	Servidor de Base de Datos	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	3
				Trazabilidad	2
[mid]	Equipos medios	[PC Clientes Delgados]	Equipos de mesa	Confiabilidad	6
				Integridad	6
		[PC Equipos de Escritorio]		Autenticidad	6
				Disponibilidad	3
				Trazabilidad	2
	Informática personal		Equipos Portátiles	Confiabilidad	6

Tabla 21. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[pc]		[PC portátiles]		Integridad	6
				Autenticidad	6
				Disponibilidad	3
				Trazabilidad	2
[vhost]	Equipos virtuales (máquinas virtuales)	[Máquinas Virtuales Equipos virtual]	2 Máquinas Virtuales de Respaldo	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	3
				Trazabilidad	2
[backup]	Equipamiento de respaldo	[Equipamiento respaldo]	Sitio Alterno (Servidor de Aplicaciones y Base de Datos)	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	3
				Trazabilidad	2
[print]	Medios de impresión	[Impresoras]	Impresoras (32)	Confiabilidad	3
				Integridad	3
				Autenticidad	3
				Disponibilidad	3
				Trazabilidad	3
	Escáner		Escáner (5)	Confiabilidad	3

Tabla 21. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[scan]		[Servicio Scan]		Integridad	3
				Autenticidad	3
				Disponibilidad	3
				Trazabilidad	3
[ipphone]	Teléfono IP	[Teléfono IP]	Teléfono Ip (20	Confiabilidad	3
				Integridad	3
				Autenticidad	3
				Disponibilidad	3
				Trazabilidad	3
[router]	Enrutadores	[Router enrutadores]	Enrutadores	Confiabilidad	2
				Integridad	2
				Autenticidad	2
				Disponibilidad	2
				Trazabilidad	2
[other]	Wifi	[W_Redwifi]	Red Wifi	Confiabilidad	2
				Integridad	1
				Autenticidad	1
				Disponibilidad	1
				Trazabilidad	1

Fuente: El autor

7.2.2.7. *Valoración Cuantitativa de Redes de Comunicaciones*

Tabla 22. Valoración Cuantitativa de Redes de Comunicaciones

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[radio]	red inalámbrica	[Radio]	Red Inalámbrica	Disponibilidad	3
				Integridad	3
				Confiabilidad	3
				Autenticidad	3
				Trazabilidad	3
[wifi]	Wifi	[Wifi]	Red Inalámbrica	Disponibilidad	3
				Integridad	3
				Confiabilidad	3
				Autenticidad	3
				Trazabilidad	3
LAN]	Red local	[Local]	Red local	Disponibilidad	3
				Integridad	3
				Confiabilidad	3
				Autenticidad	3
				Trazabilidad	3
[Internet]	Internet	[Internet]	Internet	Disponibilidad	7
				Integridad	7
				Confiabilidad	7
				Autenticidad	7
				Trazabilidad	7

Fuente: El autor

7.2.2.8 *Valoración Cuantitativa de Soportes de Información Almacenamiento Electrónico*

Tabla 23. Valoración Cuantitativa de Soportes de Información Almacenamiento Electrónico

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[disk]	Discos	[A_CD]	Almacenamientos en Disco Duro	Disponibilidad	3
				Integridad	3
				Confiabilidad	3
				Autenticidad	3
				Trazabilidad	3
[cd]	(CD_ROM)	[Almacenamiento CD]	Almacenamiento en CD	Disponibilidad	3
				Integridad	3
				Confiabilidad	3
				Autenticidad	3
				Trazabilidad	3
[USB]	Memorias USB	[Almacenamiento Memorias]	Almacenamiento en Memorias	Disponibilidad	3
				Integridad	3
				Confiabilidad	3
				Autenticidad	3
				Trazabilidad	3
[dvd]	DVD	[Almacenamiento DVD]	Almacenamiento en DVD	Disponibilidad	3
				Integridad	3
				Confiabilidad	3
				Autenticidad	3
				Trazabilidad	3
[tape]	Cinta magnética	[Cinta Mag]	Almacenamiento en Cinta Magnética	Disponibilidad	3
				Integridad	3
				Confiabilidad	3
				Autenticidad	3
				Trazabilidad	3

Fuente: El autor

7.2.2.9 Valoración Cuantitativa de Soportes de Información Almacenamiento no Electrónico

Tabla 24. Valoración Cuantitativa de Soportes de Información Almacenamiento no Electrónico

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[printed]	Material impreso	[Car]	Cajas con sus carpetas debidamente archivadas por Secretarias (Proyectos, procesos, correspondencia etc.)	Disponibilidad	4
				Integridad	4
				Confiabilidad	4
				Autenticidad	4
				Trazabilidad	3
		[Informes]	Reportes de informes de todas las Secretarias	Disponibilidad	4
				Integridad	4
				Confiabilidad	4
				Autenticidad	4
				Trazabilidad	3
		[Varios]	Carpetas varias	Disponibilidad	4
				Integridad	4
				Confiabilidad	4
				Autenticidad	4
				Trazabilidad	3

Fuente: El autor

7.2.2.10. *Valoración Cuantitativa de Equipos Auxiliar*

Tabla 25. Valoración Cuantitativa de Equipos Auxiliar

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[power]	uentes de Alimentación	[Fuente]	Equipos de Escritorio	Disponibilidad	6
				Integridad	1
				Confiabilidad	1
				Autenticidad	1
				Trazabilidad	1
[ups] sai	Sistemas de Alimentación ininterrumpida	[Sistema UPS]	APC - UPS computadores	Disponibilidad	5
				Integridad	1
				Confiabilidad	1
				Autenticidad	1
				Trazabilidad	1
[ac]	Equipos de Climatización	[Equipos Cli]	Aire Acondicionado en la sala de Servidores	Disponibilidad	3
				Integridad	1
				Confiabilidad	1
				Autenticidad	1
				Trazabilidad	1
[wire]	Cable Eléctrico	[Cable Eléctrico]	Cable Eléctrico	Disponibilidad	6
				Integridad	1
				Confiabilidad	1
				Autenticidad	1
				Trazabilidad	1
[fiber]	Fibra Óptica	[Fibra óptica]	Transmisión de comunicación	Disponibilidad	7
				Integridad	7
				Confiabilidad	7
				Autenticidad	7
				Trazabilidad	2

Fuente: El autor

Tabla 25. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[Furniture]	Mobiliario	[Mobiliario]	Mobiliario: Estantes, armarios, escritorios, archivadores, sillas, etc.	Disponibilidad	4
				Integridad	1
				Confiabilidad	1
				Autenticidad	1
				Trazabilidad	1

Fuente: El autor

7.2.2.11 *Valoración Cuantitativa de Instalaciones*

Tabla 26. Valoración Cuantitativa de Instalaciones

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[building]	Edificio	[Edificio Entidad]	Edificio de la Entidad (Plaza de Bolívar - Centro)	Disponibilidad	10
				Integridad	10
				Confiabilidad	10
				Autenticidad	10
				Trazabilidad	10
[backup]	Instalaciones de respaldo	[Sitio Alterno]	Sitio Alterno (Edifico Fondo Pensional)	Disponibilidad	10
				Integridad	10
				Confiabilidad	10
				Autenticidad	10
				Trazabilidad	10

Fuente: El autor

7.2.2.12 *Valoración Cuantitativa de Personal*

Tabla 27. Valoración Cuantitativa de Personal

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[ue]	Usuarios externos	[Externo personal]	Contratistas Externos en las diferentes Secretarias	Disponibilidad	6
				Integridad	1
				Confiabilidad	4
				Autenticidad	2
				Trazabilidad	2
[ui]	Usuarios internos	[internos]	Ingenieros de la planta de la Dirección de Sistemas	Disponibilidad	6
				Integridad	1
				Confiabilidad	4
				Autenticidad	2
				Trazabilidad	2
[adm]	Administradores de sistemas	[Administrador sistemas]	Ingeniero encargado de Administración del Sistemas	Disponibilidad	6
				Integridad	1
				Confiabilidad	4
				Autenticidad	2
				Trazabilidad	2
[com]	Administradores de comunicaciones	[Administrador Comunicaciones]	Ingeniero encargado de Administración del Comunicaciones	Disponibilidad	6
				Integridad	1
				Confiabilidad	4
				Autenticidad	2
				Trazabilidad	2
[dba]	Administradores de BBDD	[Administración sistemas]	Ingeniero encargado de Administrar las bases de datos.	Disponibilidad	6
				Integridad	1
				Confiabilidad	4
				Autenticidad	2
				Trazabilidad	2

Tabla 27. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad	Dimensiones Valoradas	VALOR
[sec]	Administradores de seguridad	[Administración sistemas]	Ingeniero encargado de Administrar el firewall	Disponibilidad	6
				Integridad	1
				Confiabilidad	4
				Autenticidad	2
				Trazabilidad	2
[dev]	Desarrolladores / programadores	[Administrador sistemas]	Ingenieros y técnicos encargados de desarrollar diferentes proyectos.	Disponibilidad	6
				Integridad	1
				Confiabilidad	4
				Autenticidad	2
				Trazabilidad	2

Fuente: El autor

7.2.3. *Identificación de las Amenazas:* Luego de haber realizado la valoración de los activos se procede a realizar la valoración de las amenazas a las que están expuestos dichos activos de la Dirección de Sistemas de la Gobernación de Boyacá, a continuación, se observa la valoración por activo, las amenazas que se pueden presentar.

Tabla 28. Dimensiones Valoradas

Dimensiones de Seguridad a valorar	Identificación
Autenticidad	**A**
Confiabilidad	**C**
Integridad	**I**
Disponibilidad	**D**
Trazabilidad	**T**

Fuente: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3232_valoracin_de_amenazas.html

Tabla 29. Valoración de las Amenazas.

IDENTIFICACION DE LAS AMENAZAS	
[N]	**Desastres naturales**
[I]	**De Origen industrial**
[E]	**Errores y fallos no intencionados**
[A]	**Ataque intencionado**

Fuente: Identificación de las Amenazas Herramienta Pilar

7.2.4. *Valoración de Amenazas*.

Los objetivos planteados en esta tarea son:

- ✓ Evaluar la probabilidad de ocurrencia de cada amenaza concerniente a cada activo.
- ✓ Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.

Para valorar las amenazas de cada activo se han tomado en cuenta la degradación de valor y la probabilidad de ocurrencia.

7.2.4.1. *Frecuencia o Probabilidad de Ocurrencia*

Se refiere a los eventos que se producen en un tiempo determinado. Los valores típicos para determinar la frecuencia se muestran a continuación.

Tabla 30. Probabilidad de Ocurrencia

CS	**CASI SEGURO**
MA	**MUY ALTO**
P	**POSIBLE**
PP	**POCO PROBABLE**
MB	**MUY BAJA**
MR	**MUY RARA**
0	

Fuente: Tomado de PILAR

7.2.4.2. *Degradación:*

Cuan perjudicado resultaría el [valor del] activo
Es que tan perjudicado quedaría el activo al materializarse las amenazas.

Tabla 31. Degradación del Valor

T	**TOTAL**
MA	**MUY ALTO**
A	**ALTO**
M	**MEDIO**
B	**BAJO**
0	

Fuente: Tomado de PILAR

A continuación, evidenciamos la valoración de las amenazas con relación a la probabilidad de ocurrencia y la degradación que sufrirán los activos en cada una de lasa las dimensiones de seguridad.

Valor propio de los activos, a continuación, se identifican las amenazas del inventario de los activos realizados en la Dirección de Sistemas de la Gobernación de Boyacá, en algunos casos se toma los activos más críticos o la categoría.

7.2.4.3. *Identificación y Valoración de las Amenazas Generales de los Activos de la Dirección de Sistemas de la Gobernación de Boyacá*

Tabla 32. Identificación y Valoración de las Amenazas Generales de los Activos de la Dirección de Sistemas de la Gobernación de Boyacá

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[B] Activos esenciales							
[Infor] Información	[E.14.] Fuga de información						
[vr] Datos vitales 1] Sistema de Información Isolución		MR	MA	MA	A	A	A
vr Datos vitales2] Sistema de Información Mesa de Ayuda		MR	MA	MA	A	A	A
vr Datos de informacion3] Sistema de Información Manuales de procedimientos		MR	MA	MA	A	A	A
vr Datos de informacion4] Sistema de Información Manuales de usuario		MR	MA	MA	A	A	A
vr Datos de Informacion5] Sistema de Información (Presupuesto)		MR	MA	MA	A	A	A
vr Datos de información] Sistema de Información (PQRD)		MR	MA	MA	A	A	A
vr Datos de informacion7] Sistema de Información (Rentas)		MR	MA	MA	A	A	A

Tabla 32. (Continuación)

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[B] Activos esenciales							
vr Datos de informacion8] Sistema de Información (Recursos Humanos)	[E.15.] Alteración de la información	MR	MA	MA	A	A	A
vr Datos de informacion9] Sistema de Información (Jurídicos)		MR	MA	MA	A	A	A
vr Datos de informacion10] Sistema de Información (Gestión de Juntas)		MR	MA	MA	A	A	A
vr Datos de informacion11] Sistema de Información (Gestión Documental)		MR	MA	MA	A	A	A
[per] Datos de carácter personal							
S Contabilidad] Contabilidad de la Gobernación de Boyacá	[E.1.] Errores de los usuarios	MR	MA	MA	M	MA	MA
	[E.2.] Errores del administrador del sistema / de la seguridad	MR	MA	MA	M	MA	MA
	[E.14.] Fugas de información	MR	MA	MA	M	MA	MA
classified] datos clásicos							
[D Históricos]] Datos Históricos de información en las Bases de Datos	[E.1.] Errores de los usuarios	MR	MA	MA	M	MA	MA
	[E.2.] Errores del administrador del sistema / de la seguridad	MR	MA	MA	M	MA	MA
	[E.14.] Fugas de información	MR	MA	MA	M	MA	MA

Fuente: El autor

Tabla 32. (Continuación)

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[B] Activos esenciales							
D Proyectos] Documentación de Proyectos Tramitados	[E.1.] Errores de los usuarios	MR	MA	MA	M	MA	MA
	[E.2.] Errores del administrador del sistema / de la seguridad	MR	MA	MA	M	MA	MA
	[E.14.] Fugas de información	MR	MA	MA	M	MA	MA

Tabla 33. Datos de Información

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[D] Datos de Información							
files Ficheros de datos1] Archivo de proyectos entregados y radicados	[E.1.] Errores de los usuarios	PP	MA	MA	MA	MA	T
	[E.2.] Errores del administrador del sistema / de la seguridad	MR	MA	MA	MA	MA	T
files Ficheros de datos2] [A Usuarios] Archivo de usuarios externos	[E.14.] Fuga de información	MR	A	A	A	A	T
files Ficheros de información] Archivo Secretaria de Hacienda	[E.15.] Alteración de la información	MR	B	B	B	B	T
	[A.5.] Suplantación de la identidad	MR	B	B	B	B	T
backup Copias de respaldo] [A Copias de Respaldo] Archivo de copias de seguridad de la Información	[A.6.] Abuso de privilegios de acceso	PP	B	B	B	B	T

Fuente: El autor

Tabla 33. (Continuación)

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[D] Datos de Información							
conf Datos de configuración] [D Configuración de Servidores] Datos de configuración de servidores y equipos	[A.11.] Acceso no autorizado	MR	B	B	B	B	T
	[A.15.] Modificación de la información	PP	B	B	B	B	T
password Credenciales] [C Empleados] Contraseñas de acceso de empleados	[A.19.] Revelación de información	MR	0	0	0	0	T

Tabla 34. Claves Criptográficas

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[Keys] Claves Criptográficas							
integrity] Claves de cifra de aplicaciones bancarias para el pago de Nomina	[E.1.] Errores de los usuarios	PP	M	M	M	M	MA
	[E.14.] Fuga de información	PP	M	M	M	M	MA
	[A.5.] Suplantación de la identidad	PP	B	B	B	B	MA
	[A.6.] Abuso de privilegios de acceso	PP	A	A	A	A	MA
	[A.11.] Acceso no autorizado	MR	A	A	A	A	MA
	[A.15.] Modificación de la información	PP	0	0	0	0	MA
	[A.18.] Destrucción de la información	MR	T	T	T	T	MA
	[A.19.] Revelación de información	MR	T	T	T	T	MA

Fuente: El autor

Tabla 35. Inventario de Servicios

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[[S]] Inventario de Servicios							
[ext A usuarios externos (bajo una relación contractual)] [S Externo] Servicios prestados a usuarios externos (Contratistas de Proyectos)	[E.1] Errores de los usuarios	P	M	M	M	M	B
	[E.2.] Errores del administrador del sistema / de la seguridad	MR	M	M	M	M	B
int Interno (usuarios y medios de la propia organización)] S Interno Servicios prestados a empleados internos	[E.9.] Errores de [re-]encaminamiento	PP	M	A	A	A	B
	[E.14.] Fuga de información	PP	B	B	B	B	B
[www World wide web] S Internet Servicio de internet al que pueden acceder los empleados	[A.5.] Suplantación de la identidad	PP	0	B	B	B	B
	[A.6.] Abuso de privilegios de acceso	PP	B	0	0	0	B
email Correo electrónico] [S Correo] Manejo de correos electrónicos (Corporativos)	[A.7.] Uso no previsto	MR	0	0	0	0	B
	[A.11.] Acceso no autorizado	PP	0	0	0	0	B
file Almacenamiento de ficheros] [S A Bases de datos] [S A Bases de datos] Servicio de almacenamiento de información en los servidores de bases de datos.	[A.13.] Repudio (negación de actuaciones)	PP	0	0	0	0	B
	[A.15.] Modificación de la información	PP	B	B	B	B	B
pm Gestión de privilegios] [G Privilegios] Manejo de privilegios de acuerdo al rol de cada empleado dentro de la entidad	[A.18.] Destrucción de la información	PP	0	0	0	0	B
	[A.24.] Denegación de servicio	PP	B	B	B	B	B

Fuente: El autor

Tabla 36. Servicios internos

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[IS] Servicios internos							
[S Interno] Correo electrónico, Internet y Telefonía	[E.1.] Errores de los usuarios	MA	A	MA	MA	MA	T
	[E.2.] Errores del administrador del sistema / de la seguridad	MA	MA	A	MA	MA	T

Fuente: El autor

Tabla 37**.** Equipamiento [E] Equipamiento SW Aplicaciones Informáticas

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[E] Equipamiento[E] Equipamiento SW Aplicaciones Informáticas							
[SW] Aplicaciones Informáticas	[E.1.] Errores de los usuarios	MA	A	A	A	A	B
[SW.std] standard (off the shelf)	[E.8.] Difusión de software dañino	MA	A	A	A	A	B
app Servidor de aplicaciones] [Server Aplicación Servidores de Aplicaciones	[E.9.] Errores de [re-]encaminamiento	MA	A	A	A	A	B
	[E.14.] Fugas de información	MA	A	A	A	A	B
Email server Servidor de correo electrónico] Server Correo Servidor de Correo Electrónico	[E.15.] Alteración de la información	MA	A	A	A	A	B

Fuente: El autor

Tabla 37. (Continuación)

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[E] Equipamiento[E] Equipamiento SW Aplicaciones Informáticas							
file servidor de ficheros] [Server_Ficheros] Servidor de Ficheros	[E.20.] Vulnerabilidades de los programas (software)	MA	A	A	A	A	B
	[E.21.] Errores de mantenimiento /actualización del programa (software)	MA	A	A	A	A	B
	[A.5.] Suplantación de la identidad	MA	A	A	A	A	B
dbms Sistema de gestión de bases de datos] SG Base Datos Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos	[A.8.] Difusión de software dañino	MA	A	A	A	A	B
	[A.11.] Acceso no autorizado	MA	A	A	A	A	B
Office Ofimática] Office Office: 2003, 2007, 2010 y 2013	[A.15.] Modificación de la información	MA	A	A	A	A	B
[av Antivirus] [Antivirus] 360 Total Security original con actualizaciones	[A.18.] Destrucción de la información	MA	A	A	A	A	B
os Sistema Operativo] OS Win xp y win 7 Sistema operativo Windows XP y Windows 7, profesional.	[A.22.] Manipulación de programas	MA	A	A	A	A	B

Fuente: El autor

Tabla 38. HW Equipamientos Informáticos (hardware)

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
HW Equipamientos Informáticos (hardware)							
[HW] Equipos Informáticos (hardware)	[E.24.] Caída del sistema por agotamiento de recurso	PP	A	M	M	M	M
host] Grandes equipos (host)	[E.25.] Perdida de equipos	MR	M	M	M	M	A
mid Equipos medios1] PC Clientes Delgados	[A.6.] Abuso de privilegios de acceso	MR	A	M	M	M	A
	[A.7.] Uso no previsto	MR	B	B	B	B	B
mid_Equipos medios2] PC Equipos de Escritorio Equipos de mesa	[A.11.] Acceso no autorizado	MR	M	M	M	M	A
	[A.23.] Manipulación de hardware	MR	M	A	A	A	MA
pc Informática personal] PC portátiles Equipos Portátiles	[A.24.] Denegación de servicio	MR	M	M	M	M	M
vhost Equipos virtuales (máquinas virtuales)] 2 Máquinas Virtuales de Respaldo	[A.25.] Robo de equipos	MR	M	B	B	B	A
backup Equipamiento de respaldo] Sitio Alterno (Servidor de Aplicaciones y Base de Datos)	[A.26.] Ataque destructivo	MR	M	B	B	B	B
[peripheral] Periféricos	[E.24.] Caída del sistema por agotamiento de recurso	PP	A	B	B	B	M
Peripheral print Medios de impresión1] E Impresoras (32)	[A.6.] Abuso de privilegios de acceso	MR	M	B	B	B	M
	[A.7.] Uso no previsto	MR	B	B	B	B	M
	[A.11.] Acceso no autorizado	MR	A	A	A	A	M

Tabla 38. (Continuación)

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
HW Equipamientos Informáticos (hardware)							
peripheral.scan Escáner2] Scan Escáner (5)	[A.13.] Repudio (negación de actuaciones)	MR	M	B	B	B	M
	[A.24.] Denegación de servicio	MR	M	B	B	B	M
	[A.25.] Robo de equipos	MR	M	M	M	M	M
	[A.26.] Robo de equipos	MR	B	B	B	B	M
[ipphone] Teléfono IP	[E.24.] Caída del sistema por agotamiento de recurso	PP	A	B	B	B	B
Tel IP] Teléfono Ip (20	[A.6.] Abuso de privilegios de acceso	MR	M	M	M	M	B
	[A.7.] Uso no previsto	MR	A	B	B	B	B
[network] Soporte de la red	[A.11.] Acceso no autorizado	MR	B	M	M	M	B
router] R enrutadores] Enrutadores	[A.13.] Repudio (negación de actuaciones)	MR	M	B	B	B	B
	[A.24.] Denegación de servicio	MR	M	B	B	B	B
other] otros	[A.25.] Robo de equipos	MR	M	B	B	B	B
[other.W Redwifi] Red Wifi	[A.26.] Robo de equipos	MR	M	B	B	B	B

Fuente: El autor

Tabla 39. [COM] Redes de Comunicación

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[COM] Redes de Comunicación							
[radio red inalámbrica] R radio Red Inalámbrica	[E.2] Errores de administrador del sistema / de la seguridad	P	A	B	B	B	B
	[E.9] Errores de [re-]encaminamiento	PP	A	B	B	B	B
[wifi] R wifi Red Inalámbrica	[E.24] Caída del sistema por agotamiento de recurso	MR	A	B	B	B	B
	[A.5.] Suplantación de la identidad	MR	M	B	B	B	B
[LAN Red local] R Local Red local	[A.6.] Abuso de privilegios de acceso	MR	B	B	B	B	B
	[A.7.] Uso no previsto	MR	B	B	B	B	B
	[A.11.] Acceso no autorizado	PP	A	B	B	B	B
[Internet] Internet	[A.14.] Interceptación de información (escucha)	PP	A	B	B	B	B
	[A.24.] Denegación de servicio	MR	B	B	B	B	B

Fuente: El autor

Tabla 40. [Media] Soportes de Información

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[Media] Soportes de Información							
[Soportes de Información1] Electrónico	[E.25.] Pérdida de equipos	MR	B	B	B	B	B
[disk Discos] A_CD Almacenamientos en Disco Duro	[A.7.] Uso no previsto	MR	B	B	B	B	B
[(CD_ROM)] A_CD Almacenamiento en CD	[A.18.] Destrucción de la información	MR	B	B	B	B	B
[USB Memorias USB] A Memorias Almacenamiento en Memorias	[A.23.] Manipulación de hardware	MR	B	B	B	B	B
dvd DVD] A_DVD Almacenamiento en DVD	[A.24.] Denegación de servicio	MR	M	M	M	M	M
tape Cinta magnética] Cinta Mag Almacenamiento en Cinta Magnética	[A.25.] Robo de equipos	MR	B	B	B	B	B
	[A.26.] Ataque destructivo	MR	B	B	B	B	B
tape Cinta magnética] C Mag Almacenamiento en Cinta Magnética	[E.15.] Alteración de la información	PP	M	M	M	M	A
	[E.25.] Pérdida de equipos	PP	M	B	B	B	M
	[A.7.] Uso no previsto	MR	B	B	B	B	B
	[A.11.] Acceso no autorizado	MR	A	A	A	A	A
	[A.18.] Destrucción de la información	MR	A	M	M	M	M
	[A.23.] Manipulación de hardware	MR	M	M	M	M	M
	[A.25.] Robo de equipos	MR	B	B	B	B	B
	[A.26.] Ataque destructivo	MR	B	B	B	B	B

Tabla 40. (Continuación)

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[Media] Soportes de Información							
Soportes de Información 2] Almacenamiento no Electrónico							
[Media] Soportes de Información							
Printed Material impreso 2] P Informes Reportes de informes de todas las Secretarias	[E.15.] Alteración de la información	MR	M	A	A	A	A
Soportes de Información 2] Almacenamiento no Electrónico							
printed Material impreso] P Varios Carpetas varios	[E.18.] Destrucción de la información	MR	M	A	A	A	A

Fuente: El autor

Tabla 41. [AUX] Elementos Auxiliares

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[AUX] Elementos auxiliares							
Powe Fuentes de Alimentación] [P Fuente] Equipos de Escritorio	[E.25.] Robo de equipos	PP	B	B	B	B	B
Ups sai Sistemas de Alimentación ininterrumpida] [U SistemaA] APC - UPS computadores	[A.7.] Uso no previsto	PP	B	B	B	B	B
ac Equipos de Climatización] E Cli Aire Acondicionado en la sala de Servidores	[A.11.] Acceso no autorizado	PP	B	B	B	B	B
wire Cable Eléctrico] Eléctrico Cable Electrico	[A.23.] Manipulación de hardware	PP	B	B	B	B	B

Fuente: El autor

Tabla 41. (Continuación)

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[AUX] Elementos auxiliares							
fiber Fibra Óptica] F óptica Transmisión de comunicación	[A.26.] Ataque destructivo	PP	B	B	B	B	B
suplly Suministros Esenciales] S_Esenciales Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc							
Furniture Mobiliario] [M_Mobiliario] Mobiliario: Estantes, armarios, escritorios, archivadores, sillas, etc.							

Fuente: El autor

Tabla. 42. [L] Instalaciones

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[L] Instalaciones							
[building Edificio] [E Entidad] Edificio de la Entidad (Plaza de Bolívar - Centro)	[A.7.] Uso no previsto	MR	M	B	B	B	B
	[A.11.] Acceso no autorizado	PP	M	B	B	B	B
	[A.26.] Ataque destructivo	PP	B	B	B	B	B
[backup Instalaciones de respaldo] S Alterno Sitio Alterno (Edifico Fondo Pensional)	[A.7.] Uso no previsto	MR	B	B	B	B	B
	[A.11.] Acceso no autorizado	MR	B	B	B	B	B
	[A.26.] Ataque destructivo	MR	B	B	B	B	B

Fuente: El autor

Tabla 43. [P] Personal

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[P] Personal							
[ue Usuarios externos] [E personal] Contratistas Externos en las diferentes Secretarias	[E.14.] Fugas de información	PP	B	M	M	M	M
	[E.28.] Indisponibilidad del personal	PP	B	M	M	M	M
	[A.11.3.] Por personas externas	P	B	M	M	M	M
	[A.12.1.] Por personas interno	PP	B	M	M	M	M
	[A.12.2.] Por subcontratistas	P	B	M	M	M	M
	[A.12.3.] Por personas externas	P	B	M	M	M	M
	[A.28.] Indisponibilidad del personal	PP	B	M	M	M	M
	[A.29.] Extorsión	MR	B	M	M	M	M
	[A.30.] Ingeniería social (picaresca)	PP	B	M	M	M	M
[ui Usuarios internos] E internos Ingenieros de la planta de la Dirección de Sistemas	[E.14.] Fugas de información	MR	B	B	B	B	B
[adm Administradores de sistemas] [A sistemas] Ingeniero encargado de Administración del Sistemas	[E.28.] Indisponibilidad del personal	MR	B	B	B	B	B

Tabla 43. (Continuación)

IDENTIFICACION DE LOS ACTIVOS /AMENAZAS	VALORACION DE LAS AMENAZAS	PROBABILIDAD DE OCURRECIA	DEGRADACION % NIVEL				
			[D]	[I]	[C]	[A]	[T]
[P] Personal							
[com Administradores de comunicaciones] [A Comunicaciones] Ingeniero encargado de Administración del Comunicaciones	[A.11.3.] Por personas externas	MR	B	B	B	B	B
[dba Administradores de BBDD] [A sistemas] Ingeniero encargado de Administrar las bases de datos.	[A.12.1.] Por personas interno	MR	B	B	B	B	B
	[A.12.2.] Por subcontratistas	MR	B	B	B	B	B
[sec Administradores de seguridad] [A sistemas] Ingeniero encargado de Administrar el firewall	[A.12.3.] Por personas externas	MR	B	B	B	B	B
	[A.28.] Indisponibilidad del personal	MR	B	B	B	B	B
	[A.29.] Extorsión	MR	B	B	B	B	B
[dev Desarrolladores / programadores] [A sistemas] Ingenieros y técnicos encargados de desarrollar diferentes proyectos.	[A.30.] Ingeniería social (picaresca)	MR	B	B	B	B	B

Fuente: El autor

7.2.5. *Matriz de Riesgos Propabilidad Impacto*

Esta matriz nos ayudara a analizar los riesgos de la Dirección de Sistemas de la Gobernación de Boyacá, para conocer la probabilidad de que ocurran repercusiones que se puedan presentar.

Tabla. 44. Magerit Impacto

CALIFICACION NUMERICA	GRAVEDAD (IMPACTO)
5	Muy grave
4	Importante
3	Moderado
2	Leve
1	Marginal

Fuente: El autor

Tabla.45. Magerit Probabilidad

CALIFICACION NUMERICA	PROBABILIDAD
5	Muy Frecuente
4	Frecuente
3	Normal
2	Poco Frecuente
1	Frecuente

Fuente: El autor

El establecimiento de nivel de riesgos se realizará de forma cuantitativa, realizando una multiplicación entre los valores numéricos de probabilidad e impacto, se clasificarán en rangos y se les asignara un nivel de riesgo de la siguiente forma:

Tabla. 46. Magerit Nivel de Riesgo

RANGO	CALIFICACION DE RIESGO
21-25	Catastrofico
16-20	Mayor
10-15	Moderado
5-9	Menor
1-4	Insignificante

Fuente: Magerit Nivel de Riesgo

7.2.5.1. *Magerit Matriz de Riesgos*

Tabla 47. Matriz de Riesgo Probabilidad e impacto

PROBABILIDAD	21 al 25	5 Muy Frecuente					
	16 al 20	4 Frecuente					
	10 al 15	3 Normal					
	5 al 9	2 Poco Frecuente					
	1 al 4	1 Muy Poco FRECUENTE					
	Rango		1	2	3	4	5
			Marginal	Leve	Moderado	Importante	Muy grave
	IMPACTO						

Fuente: El autor

7.2.5.2. *Análisis Matriz de Riesgos*

Tabla 48. Análisis Matriz de Riesgos

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[B] Activos esenciales												
[Infor] Información												
[vr] Datos vitales 1] Sistema de Información Isolución	[E.1.] Errores de los usuarios	2	2	2	3	3	3	4	4	6	6	6
	[E.14.] Fuga de información	2	2	2	2	2	2	4	4	4	4	4
	[E.15.] Alteración de la información	1	2	1	3	1	3	2	1	3	1	3
vr Datos vitales2] Sistema de Información Mesa de Ayuda	[E.1.] Errores de los usuarios	2	2	2	3	3	3	4	4	6	6	6
	[E.14.] Fuga de información	1	2	1	1	3	3	2	1	1	3	3
	[E.15.] Alteración de la información	1	2	2	3	3	3	2	2	3	3	3
vr Datos de informacion3] Sistema de Información Manuales de procedimientos	[E.1.] Errores de los usuarios	2	2	2	1	2	1	4	4	2	4	2
	[E.14.] Fuga de información	1	2	2	3	3	3	2	2	3	3	3
	[E.15.] Alteración de la información	1	2	2	1	1	1	2	2	1	1	1
vr Datos de informacion4] Sistema de Información Manuales de usuario	[E.1.] Errores de los usuarios	2	1	1	2	2	2	2	2	2	2	2
	[E.14.] Fuga de información	1	2	2	3	3	3	2	2	3	3	3
	[E.15.] Alteración de la información	1	2	2	2	3	3	2	2	2	3	3

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[B] Activos esenciales												
[Infor] Información												
vr Datos de Informacion5] Sistema de Información (Presupuesto)	[E.1.] Errores de los usuarios	2	2	2	3	2	2	4	4	6	2	4
	[E.14.] Fuga de información	1	2	2	3	3	3	2	2	3	3	3
	[E.15.] Alteración de la información	1	2	2	3	3	2	2	2	3	3	2
vr Datos de información] Sistema de Información (PQRD)	[E.1.] Errores de los usuarios	2	2	2	3	3	3	4	4	6	6	6
	[E.14.] Fuga de información	1	2	2	2	3	3	2	2	2	3	3
	[E.15.] Alteración de la información	1	2	2	3	3	3	2	2	3	3	3
vr Datos de informacion7] Sistema de Información (Rentas)	[E.1.] Errores de los usuarios	2	2	2	3	3	2	4	4	6	6	4
	[E.14.] Fuga de información	1	2	2	3	3	3	2	2	3	3	3
	[E d.15.] Alteración e la información	1	2	2	3	3	3	2	2	3	3	3
vr Datos de informacion8] Sistema de Información (Recursos Humanos)	[E.1.] Errores de los usuarios	2	2	2	3	2	3	4	4	6	4	6
	[E.14.] Fuga de información	1	2	2	3	3	3	2	2	3	3	3
	[E.15.] Alteración de la información	1	2	2	2	3	3	2	2	2	3	3

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[Infor] Información												
Sistema de Información (Jurídicos)	[E.15.] Alteración de la información	1	1	2	3	3	3	1	2	3	3	3
vr Datos de informacion10] Sistema de Información (Gestión de Juntas)	[E.1.] Errores de los usuarios	2	2	2	2	3	3	4	4	4	6	6
	[E.14.] Fuga de información	1	2	2	3	2	3	2	2	3	2	3
	[E.15.] Alteración de la información	1	2	2	3	2	3	2	2	3	2	3
vr Datos de informacion11] Sistema de Información (Gestión Documental)	[E.1.] Errores de los usuarios	2	2	2	3	3	3	4	4	6	6	6
	[E.14.] Fuga de información	1	2	2	2	3	3	2	2	2	3	3
	[E.15.] Alteración de la información	1	2	2	3	3	3	2	2	3	3	3
[per] Datos de carácter personal												
S_Contabilidad] Contabilidad de la Gobernación de Boyacá	[E.1.] Errores de los usuarios	2	2	2	3	3	2	4	4	6	6	4
	[E.2.] Errores del administrador del sistema / de la seguridad	1	2	2	3	2	3	2	2	3	2	3
	[E.14.] Fugas de información	1	2	2	3	3	3	2	2	3	3	3

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
classified] datos clásicos												
[D_Históricos]] Datos Históricos de información en las Bases de Datos	[E.1.] Errores de los usuarios	2	1	2	3	2	3	2	4	6	4	6
	[E.2.] Errores del administrador del sistema / de la seguridad	1	2	2	3	3	3	2	2	3	3	3
	[E.14.] Fugas de información	1	2	2	2	3	3	2	2	2	3	3
Proyectos] Documentación de Proyectos Tramitados	[E.1.] Errores de los usuarios	2	2	2	3	2	3	4	4	6	4	6
	[E.2.] Errores del administrador del sistema / de la seguridad	1	2	2	3	3	2	2	2	3	3	2
	[E.14.] Fugas de información	1	2	2	3	3	3	2	2	3	3	3
[D] Datos de Información												
files Ficheros de datos1] Archivo de proyectos entregados y radicados	[E.1.] Errores de los usuarios	2	3	3	3	3	2	6	6	6	6	4
	[E.2.] Errores del administrador del sistema / de la seguridad	1	3	2	3	3	2	3	2	3	3	2
	[E.14.] Fuga de información	1	3	3	2	3	2	3	3	2	3	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
	[E.15.] Alteración de la información	1	3	3	3	3	2	3	3	3	3	2
	[A.5.] suplantación de la identidad	1	3	2	3	2	2	3	2	3	2	2
[D] Datos de Información												
	[A.6.] Abuso de privilegios de acceso	1	3	2	3	2	2	3	2	3	2	2
	[A.11.] Acceso no autorizado	1	2	3	3	3	2	2	3	3	3	2
	[A.15.] Modificación de la información	1	3	3	2	3	2	3	3	2	3	2
	[A.18.] Destrucción de la información	1	3	2	3	3	2	3	2	3	3	2
	[A.19.] Revelación de información	1	2	3	3	2	3	2	3	3	2	3
files Ficheros de datos2] [A Usuarios] Archivo de usuarios externos	[E.1.] Errores de los usuarios	2	3	2	3	3	2	6	4	6	6	4
	[E.2.] Errores del administrador del sistema / de la seguridad	1	3	3	2	3	2	3	3	2	3	2
	[E.14.] Fuga de información	1	2	3	3	3	2	2	3	3	3	2
	[E.15.] Alteración de la información	1	3	3	3	2	2	3	3	3	2	2
	[A.5.] suplantación de la identidad	1	3	2	3	2	2	3	2	3	2	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[D] Datos de Información												
	[A.6.] Abuso de privilegios de acceso	1	3	2	3	2	2	3	2	3	2	2
	[A.11.] Acceso no autorizado	1	3	2	3	3	2	3	2	3	3	2
	[A.15.] Modificación de la información	1	3	3	3	3	2	3	3	3	3	2
	[A.18.] Destrucción de la información	1	3	3	2	3	2	3	3	2	3	2
	[A.19.] Revelación de información	1	3	3	2	3	3	3	3	2	3	3
files Ficheros de información] Archivo Secretaria de Hacienda	[E.1.] Errores de los usuarios	2	3	3	3	3	2	6	6	6	6	4
	[E.2.] Errores del administrador del sistema / de la seguridad	1	3	3	2	3	2	3	3	2	3	2
	[E.14.] Fuga de información	1	3	2	3	3	2	3	2	3	3	2
	[E.15.] Alteración de la información	1	3	2	3	3	2	3	2	3	3	2
	[A.5.] suplantación de la identidad	1	3	2	3	2	2	3	2	3	2	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	3	2	2	3	2	3	2	2
	[A.11.] Acceso no autorizado	1	2	3	3	3	2	2	3	3	3	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[D] Datos de Información												
	[A.15.] Modificación de la información	1	3	3	2	3	2	3	3	2	3	2
	[A.18.] Destrucción de la información	1	3	2	3	3	2	3	2	3	3	2
	[A.19.] Revelación de información	1	3	3	2	3	3	3	3	2	3	3
ackup Copias de respaldo] [Acopias de Respaldo] Archivo de copias de seguridad de la Información	[E.1.] Errores de los usuarios	2	3	3	3	3	2	6	6	6	6	4
	[E.2.] Errores del administrador del sistema / de la seguridad	1	3	2	3	3	2	3	2	3	3	2
	[E.14.] Fuga de información	1	2	3	3	3	2	2	3	3	3	2
	[E.15.] Alteración de la información	1	3	3	3	3	2	3	3	3	3	**2**
	[A.5.] suplantación de la identidad	1	3	2	3	2	2	3	2	3	2	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	3	2	2	3	2	3	2	2
	[A.11.] Acceso no autorizado	1	3	3	2	3	2	3	3	2	3	2
	[A.15.] Modificación de la información	1	3	3	2	3	2	3	3	2	3	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[D] Datos de Información												
	[A.18.] Destrucción de la información	1	2	3	3	3	2	2	3	3	3	2
	[A.19.] Revelación de información	1	2	3	3	3	3	2	3	3	3	3
	[E.1.] Errores de los usuarios	2	3	3	3	3	2	6	6	6	6	4
	[E.2.] Errores del administrador del sistema / de la seguridad	1	3	2	3	3	2	3	2	3	3	2
	[E.14.] Fuga de información	1	2	3	3	3	2	2	3	3	3	2
	[E.15.] Alteración de la información	1	2	3	3	2	2	2	3	3	2	2
	[A.5.] suplantación de la identidad	1	3	2	3	2	2	3	2	3	2	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	3	2	2	3	2	3	2	2
	[A.11.] Acceso no autorizado	1	3	2	3	3	2	3	2	3	3	2
	[A.15.] Modificación de la información	1	3	3	2	3	2	3	3	2	3	2
	[A.18.] Destrucción de la información	1	2	3	3	2	2	2	3	3	2	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[D] Datos de Información												
	[A.19.] Revelación de información	1	3	3	2	3	3	3	3	2	3	3
	[E.1.] Errores de los usuarios	2	3	3	2	3	2	6	6	4	6	4
	[E.2.] Errores del administrador del sistema / de la seguridad	1	3	2	3	3	2	3	2	3	3	2
	[E.14.] Fuga de información	1	2	3	3	3	2	2	3	3	3	2
	[E.15.] Alteración de la información	1	3	3	3	3	2	3	3	3	3	2
	[A.5.] suplantación de la identidad	1	3	2	3	2	2	3	2	3	2	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	3	2	2	3	2	3	2	2
	[A.11.] Acceso no autorizado	1	2	3	3	3	2	2	3	3	3	2
	[A.15.] Modificación de la información	1	3	2	3	3	2	3	2	3	3	2
	[A.18.] Destrucción de la información	1	3	3	3	3	2	3	3	3	3	2
	[A.19.] Revelación de información	1	3	2	3	3	3	3	2	3	3	3

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[D] Datos de Información												
password Credenciales] [Empleados] Contraseñas de acceso de empleados	[E.1.] Errores de los usuarios	2	2	3	3	3	2	4	6	6	6	4
	[E.2.] Errores del administrador del sistema / de la seguridad	1	3	3	2	3	2	3	3	2	3	2
	[E.14.] Fuga de información	1	3	3	2	3	2	3	3	2	3	2
	[E.15.] Alteración de la información	1	2	3	3	3	2	2	3	3	3	2
Keys] Claves Criptográficos												
	[A.5.] suplantación de la identidad	1	3	2	3	2	2	3	2	3	2	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	3	2	2	3	2	3	2	2
	[A.11.] Acceso no autorizado	1	3	3	3	2	2	3	3	3	2	2
	[A.15.] Modificación de la información	1	2	3	3	2	2	2	3	3	2	2
	[A.18.] Destrucción de la información	1	3	3	3	3	2	3	3	3	3	2
	[A.19.] Revelación de información	1	2	3	3	3	3	2	3	3	3	3
integrity] Claves de cifra de aplicaciones bancarias para el pago de Nomina	[E.1.] Errores de los usuarios	2	4	3	3	3	3	8	6	6	6	6
	[E.14.] Fuga de información	1	3	3	3	3	2	3	3	3	3	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
Keys] Claves Criptográficos												
	[A.5.] suplantación de la identidad	1	3	2	3	2	2	3	2	3	2	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	3	2	2	3	2	3	2	2
	[A.11.] Acceso no autorizado	1	3	2	3	3	2	3	2	3	3	2
	[A.15.] Modificación de la información	1	2	3	3	3	2	2	3	3	3	2
	[A.18.] Destrucción de la información	1	3	3	2	3	2	3	3	2	3	2
[[S]] Inventario de Servicios												
[ext A usuarios externos (bajo una relación contractual)] [S_Externo] Servicios prestados a usuarios externos (Contratistas de Proyectos)	[A.19.] Revelación de información	2	3	2	3	3	3	6	4	6	6	6
	[E.1.] Errores de los usuarios	2	2	3	3	2	2	4	6	6	4	4
	[E.2.] Errores del administrador del sistema / de la seguridad	1	4	3	3	3	3	4	3	3	3	3
	[E.9.] Errores de [re-]encaminamiento	1	2	3	3	2	2	2	3	3	2	2
	[E.14.] Fuga de información	1	3	2	3	3	2	3	2	3	3	2
	[A.5.] suplantación de la identidad	1	3	2	3	2	2	3	2	3	2	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	3	2	2	3	2	3	2	2
	[A.7.] Uso no previsto	1	2	3	3	3	2	2	3	3	3	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[[S]] Inventario de Servicios												
	[A.11.] Acceso no autorizado	1	3	3	3	3	2	3	3	3	3	2
	[A.13.] Repudio (negación de actuaciones)	1	3	3	3	3	2	3	3	3	3	2
	[A.15.] Modificación de la información	1	3	2	3	3	2	3	2	3	3	2
	[A.18.] Destrucción de la información	1	2	3	3	3	3	2	3	3	3	3
	[A.24.] Denegación de servicio	1	2	1	2	2	1	2	1	2	2	1
int Interno (usuarios y medios de la propia organización)] Interno Servicios prestados a empleados internos	[E.1.] Errores de los usuarios	2	2	3	3	2	2	4	6	6	4	4
	[E.2.] Errores del administrador del sistema / de la seguridad	1	4	3	3	3	3	4	3	3	3	3
	[E.9.] Errores de [re-]encaminamiento	1	2	3	3	2	2	2	3	3	2	2
	[E.14.] Fuga de información	1	3	3	3	3	2	3	3	3	3	2
	[A.5.] suplantación de la identidad	1	3	2	3	2	2	3	2	3	2	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	3	2	2	3	2	3	2	2
	[A.7.] Uso no previsto	1	3	3	2	3	2	3	3	2	3	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[[S]] Inventario de Servicios												
	[A.11.] Acceso no autorizado	1	2	3	3	3	2	2	3	3	3	2
	[A.13.] Repudio (negación de actuaciones)	1	3	3	3	3	2	3	3	3	3	2
	[A.15.] Modificación de la información	1	3	2	3	3	2	3	2	3	3	2
	[A.18.] Destrucción de la información	1	2	3	3	3	3	2	3	3	3	3
	[A.24.] Denegación de servicio	1	2	2	2	2	2	2	2	2	2	2
[www World wide web] Internet Servicio de internet al que pueden acceder los empleados	[E.1.] Errores de los usuarios	2	2	3	3	2	2	4	6	6	4	4
	[E.2.] Errores del administrador del sistema / de la seguridad	1	4	3	3	3	3	4	3	3	3	3
	[E.9.] Errores de [re-]encaminamiento	1	2	3	3	2	2	2	3	3	2	2
	[E.14.] Fuga de información	1	3	3	3	3	2	3	3	3	3	2
	[A.5.] suplantación de la identidad	1	3	2	3	2	2	3	2	3	2	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	3	2	2	3	2	3	2	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[[S]] Inventario de Servicios												
	[A.7.] Uso no previsto	1	3	3	3	2	2	3	3	3	2	2
	[A.11.] Acceso no autorizado	1	3	3	3	3	2	3	3	3	3	2
	[A.13.] Repudio (negación de actuaciones)	1	3	3	3	3	2	3	3	3	3	2
	[A.15.] Modificación de la información	1	3	2	3	3	2	3	2	3	3	2
	[A.18.] Destrucción de la información	1	2	3	3	3	3	2	3	3	3	3
	[A.24.] Denegación de servicio	1	2	2	2	2	2	2	2	2	2	2
email Correo electrónico] [S_Correo] Manejo de correos electrónicos (Corporativos)	[E.1.] Errores de los usuarios	2	2	3	3	2	2	4	6	6	4	4
	[E.2.] Errores del administrador del sistema / de la seguridad	1	4	3	3	3	3	4	3	3	3	3
	[E.9.] Errores de [re-]encaminamiento	1	2	3	3	2	2	2	3	3	2	2
	[E.14.] Fuga de información	1	3	3	3	3	2	3	3	3	3	2
	[A.5.] suplantación de la identidad	1	3	2	3	3	2	3	2	3	3	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	3	2	2	3	2	3	2	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[[S]] Inventario de Servicios												
	[A.7.] Uso no previsto	1	3	3	3	3	2	3	3	3	3	2
	[A.11.] Acceso no autorizado	1	3	3	3	3	2	3	3	3	3	2
	[A.13.] Repudio (negación de actuaciones)	1	3	3	3	3	2	3	3	3	3	2
	[A.15.] Modificación de la información	1	2	3	3	3	2	2	3	3	3	2
	[A.18.] Destrucción de la información	1	3	3	3	3	3	3	3	3	3	3
	[A.24.] Denegación de servicio	1	2	2	2	2	2	2	2	2	2	2
file Almacenamiento de ficheros] [S_A_Bases de datos] [S_A_Bases de datos] Servicio de almacenamiento de información en los servidores de bases de datos.	[E.1.] Errores de los usuarios	2	2	3	3	2	2	4	6	6	4	4
	[E.2.] Errores del administrador del sistema / de la seguridad	1	4	3	3	3	3	4	3	3	3	3
	[E.9.] Errores de [re-]encaminamiento	1	2	3	3	2	2	2	3	3	2	2
	[E.14.] Fuga de información	1	3	3	3	3	2	3	3	3	3	2
	[A.5.] suplantación de la identidad	1	3	2	3	2	2	3	2	3	2	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[[S]] Inventario de Servicios												
	[A.6.] Abuso de privilegios de acceso	1	3	2	3	2	2	3	2	3	2	2
	[A.7.] Uso no previsto	1	2	3	3	3	2	2	3	3	3	2
	[A.11.] Acceso no autorizado	1	3	3	3	3	2	3	3	3	3	2
	[A.13.] Repudio (negación de actuaciones)	1	3	3	2	3	2	3	3	2	3	2
	[A.15.] Modificación de la información	1	3	3	3	3	2	3	3	3	3	2
	[A.18.] Destrucción de la información	1	3	3	2	3	3	3	3	2	3	3
	[A.24.] Denegación de servicio	1	3	2	2	2	2	3	2	2	2	2
ipm Gestión de privilegios] [privilegios]	[E.1.] Errores de los usuarios	2	2	3	3	2	2	4	6	6	4	4
Manejo de privilegios de acuerdo al rol de cada empleado dentro de la entidad	[E.2.] Errores del administrador del sistema / de la seguridad	1	4	3	3	3	3	4	3	3	3	3
	[E.9.] Errores de [re-]encaminamiento	1	2	3	3	2	2	2	3	3	2	2
	[E.14.] Fuga de información	1	3	3	3	3	2	3	3	3	3	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[[S]] Inventario de Servicios												
	[A.5.] suplantación de la identidad	1	3	2	3	2	2	3	2	3	2	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	3	2	2	3	2	3	2	2
	[A.7.] Uso no previsto	1	3	3	3	3	2	3	3	3	3	2
	[A.11.] Acceso no autorizado	1	3	3	3	3	2	3	3	3	3	2
	[A.13.] Repudio (negación de actuaciones)	1	2	3	3	3	2	2	3	3	3	2
	[A.15.] Modificación de la información	1	3	2	3	3	2	3	2	3	3	2
	[A.18.] Destrucción de la información	1	3	3	3	3	3	3	3	3	3	3
	[A.24.] Denegación de servicio	1	1	2	2	1	2	1	2	2	1	2
[Interno] Correo electrónico, Internet y Telefonía	[E.1.] Errores de los usuarios	5	5	4	5	4	3	25	20	25	20	15
	[E.2.] Errores del administrador del sistema / de la seguridad	5	5	4	5	4	3	25	20	25	20	15

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
[SW] Aplicaciones Informáticas												
[SW.std] estandar (off the shelf)												
app Servidor de aplicaciones] [Server_Aplicacion Servidores de Aplicaciones	[E.1.] Errores de los usuarios	4	5	5	5	5	1	20	20	20	20	4
	[E.8.] Difusión de software dañino	2	1	1	2	2	2	2	2	4	4	4
	[E.9.] Errores de [re-]encaminamiento	2	2	1	2	1	2	4	1	4	2	4
	[E.14.] Fugas de información	1	1	2	2	2	1	1	2	2	2	1
	[E.15.] Alteración de la información	1	1	2	2	2	1	1	2	2	2	1
	[E.20.] Vulnerabilidades de los programas (software)	1	2	2	2	1	1	2	2	2	1	1
	[E.21.] Errores de mantenimiento /actualización del programa (software)	2	2	1	2	2	2	4	2	4	4	4
	[A.5.] suplantación de la identidad	1	2	2	2	1	2	2	2	2	1	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
	[A.8.] Difusión de software dañino	1	2	2	1	1	2	2	2	1	1	2
	[A.11.] Acceso no autorizado	1	2	1	2	2	2	2	1	2	2	2
	[A.15.] Modificación de la información	1	1	2	2	2	1	1	2	2	2	1
	[A.18.] Destrucción de la información	2	1	2	2	1	2	2	4	4	2	4
	[A.22.] Manipulación de programas	1	2	1	2	2	1	2	1	2	2	1
email_server Servidor de correo electrónico] Server Correo Servidor de Correo Electrónico	[E.1.] Errores de los usuarios	4	5	5	5	5	1	20	20	20	20	4
	[E.8.] Difusión de software dañino	2	1	1	2	2	2	2	2	4	4	4
	[E.9.] Errores de [re-]encaminamiento	2	2	1	2	2	2	4	2	4	4	4
	[E.14.] Fugas de información	1	2	2	1	2	1	2	2	1	2	1
	[E.15.] Alteración de la información	1	1	2	2	2	1	1	2	2	2	1
	[E.20.] Vulnerabilidades de los programas (software)	1	2	2	1	2	1	2	2	1	2	1

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
	[E.21.] Errores de mantenimiento	2	1	2	2	1	2	2	4	4	2	4
	/actualización del programa (software)											
	[A.5.] suplantación de la identidad	1	2	1	2	2	2	2	1	2	2	2
	[A.11.] Acceso no autorizado	1	1	1	2	2	2	1	1	2	2	2
	[A.15.] Modificación de la información	1	2	2	1	1	2	2	2	1	1	2
	[A.18.] Destrucción de la información	1	1	2	2	2	2	1	2	2	2	2
	[A.22.] Manipulación de programas	1	2	2	1	2	1	2	2	1	2	1
file servidor de ficheros] [Server_Ficheros] Servidor de Ficheros	[E.1.] Errores de los usuarios	4	5	5	5	5	1	20	20	20	20	4
	[E.8.] Difusión de software dañino	2	2	2	1	2	2	4	4	2	4	4
	[E.9.] Errores de [re-]encaminamiento	2	1	2	2	2	1	2	4	4	4	2
	[E.14.] Fugas de información	1	2	1	2	2	1	2	1	2	2	1
	[E.15.] Alteración de la información	1	2	1	2	2	1	2	1	2	2	1

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
	[E.20.] Vulnerabilidades de los programas (software)	1	1	2	2	2	1	1	2	2	2	1
	[E.21.] Errores de mantenimiento /actualización del programa (software)	2	2	1	2	2	1	4	2	4	4	2
	[A.5.] suplantación de la identidad	1	1	2	1	2	2	1	2	1	2	2
	[A.11.] Acceso no autorizado	1	2	1	2	2	2	2	1	2	2	2
	[A.15.] Modificación de la información	1	2	1	2	1	2	2	1	2	1	2
	[A.18.] Destrucción de la información	1	1	2	2	2	1	1	2	2	2	1
	[A.22.] Manipulación de programas	1	2	2	2	1	2	2	2	2	1	2
dbms Sistema de gestión de bases de datos] SG_BaseDatos Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos	[E.1.] Errores de los usuarios	4	5	5	5	5	1	20	20	20	20	4
	[E.8.] Difusión de software dañino	2	2	2	1	2	2	4	4	2	4	4
	[E.9.] Errores de [re-]encaminamiento	2	2	1	2	1	2	4	2	4	2	4
	[E.14.] Fugas de información	1	2	2	2	1	1	2	2	2	1	1

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
	[E.15.] Alteración de la información	1	2	1	2	2	1	2	1	2	2	1
	[E.20.] Vulnerabilidades de los programas (software)	1	2	2	2	2	1	2	2	2	2	1
	[E.21.] Errores de mantenimiento /actualización del programa (software)	2	1	2	2	2	1	2	4	4	4	2
	[A.5.] suplantación de la identidad	1	2	1	2	2	2	2	1	2	2	2
	[A.11.] Acceso no autorizado	1	2	1	1	2	2	2	1	1	2	2
	[A.15.] Modificación de la información	1	2	2	1	2	2	2	2	1	2	2
	[A.18.] Destrucción de la información	1	1	2	2	2	1	1	2	2	2	1
	[A.22.] Manipulación de programas	1	1	2	2	2	2	1	2	2	2	2
Office Ofimática] Office Office: 2003, 2007, 2010 y 2013	[E.1.] Errores de los usuarios	4	5	5	5	5	1	20	20	20	20	4
	[E.8.] Difusión de software dañino	2	2	1	1	2	2	4	2	2	4	4
	[E.9.] Errores de [re-]encaminamiento	2	1	1	1	2	2	2	2	2	4	4

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
	[E.14.] Fugas de información	1	2	1	2	2	1	2	1	2	2	1
	[E.15.] Alteración de la información	1	1	2	2	2	1	1	2	2	2	1
	[E.20.] Vulnerabilidades de los programas (software)	1	1	2	2	2	1	1	2	2	2	1
	[E.21.] Errores de mantenimiento /actualización del programa (software)	2	2	1	2	2	2	4	2	4	4	4
	[A.5.] suplantación de la identidad	1	2	2	2	1	2	2	2	2	1	2
	[A.11.] Acceso no autorizado	1	2	2	1	2	2	2	2	1	2	2
	[A.15.] Modificación de la información	1	1	2	2	2	2	1	2	2	2	2
	[A.18.] Destrucción de la información	1	2	2	2	1	2	2	2	2	1	2
	[A.22.] Manipulación de programas	1	2	2	2	1	2	2	2	2	1	2
[av. Antivirus] [Antivirus] 360 Total Security original con actualizaciones	[E.1.] Errores de los usuarios	4	5	5	5	5	1	20	20	20	20	4

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
	[E.8.] Difusión de software dañino	2	2	2	1	2	2	4	4	2	4	4
	[E.9.] Errores de [re-]encaminamiento	2	1	2	2	1	2	2	4	4	2	4
	[E.14.] Fugas de información	1	2	1	2	2	1	2	1	2	2	1
	[E.15.] Alteración de la información	1	1	2	2	2	1	1	2	2	2	1
	[E.20.] Vulnerabilidades de los programas (software)	1	2	2	2	1	1	2	2	2	1	1
	[E.21.] Errores de mantenimiento /actualización del programa (software)	2	2	1	2	2	2	4	2	4	4	4
	[A.5.] suplantación de la identidad	1	2	2	2	1	1	2	2	2	1	1
	[A.11.] Acceso no autorizado	1	2	2	2	1	2	2	2	2	1	2
	[A.15.] Modificación de la información	1	2	1	2	2	2	2	1	2	2	2
	[A.18.] Destrucción de la información	1	2	1	2	2	2	2	1	2	2	2
	[A.22.] Manipulación de programas	1	2	2	1	2	2	2	2	1	2	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
os Sistema Operativo] OS_Win xp y win 7 Sistema operativo Windows XP y Windows 7, profesional.	[E.1.] Errores de los usuarios	4	5	5	5	5	1	20	20	20	20	4
	[E.8.] Difusión de software dañino	2	2	1	1	2	2	4	2	2	4	4
	[E.9.] Errores de [re-]encaminamiento	2	2	2	1	2	2	4	4	2	4	4
	[E.14.] Fugas de información	1	1	2	1	2	1	1	2	1	2	1
	[E.15.] Alteración de la información	1	2	2	1	2	1	2	2	1	2	1
	[E.20.] Vulnerabilidades de los programas (software)	1	2	2	2	2	1	2	2	2	2	1
	[E.21.] Errores de mantenimiento /actualización del programa (software)	2	1	1	2	1	1	2	2	4	2	2
	[A.5.] suplantación de la identidad	1	1	2	2	2	1	1	2	2	2	1
	[A.11.] Acceso no autorizado	1	2	1	2	2	2	2	1	2	2	2
	[A.15.] Modificación de la información	1	2	1	2	1	2	2	1	2	1	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
	[A.18.] Destrucción de la información	1	1	2	2	1	2	1	2	2	1	2
	[A.22.] Manipulación de programas	1	2	1	2	1	2	2	1	2	1	2
[HW] Equipos Informáticos (hardware)												
host] Grandes equipos (host)	[E.24.] Caída del sistema por agotamiento de recurso	2	3	2	2	2	2	6	4	4	4	4
	[E.25.] Perdida de equipos	1	3	2	2	2	2	3	2	2	2	2
	[A.6.] Abuso de privilegios de acceso	1	2	2	2	2	2	2	2	2	2	2
	[A.7.] Uso no previsto	2	3	2	2	2	2	6	4	4	4	4
	[A.11.] Acceso no autorizado	1	3	2	1	2	2	3	2	1	2	2
	[A.23.] Manipulación de hardware	1	1	2	2	2	2	1	2	2	2	2
	[A.24.] Denegación de servicio	1	3	2	1	2	2	3	2	1	2	2
	[A.25.] Robo de equipos	1	3	2	2	2	2	3	2	2	2	2
	[A.26.] Ataque destructivo	1	2	1	2	2	2	2	1	2	2	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
mid Equipos medios1] PC_Clientes Delgados	[E.24.] Caída del sistema por agotamiento de recurso	2	3	2	2	1	2	6	4	4	2	4
	[E.25.] Perdida de equipos	1	3	2	2	2	2	3	2	2	2	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	2	2	2	3	2	2	2	2
	[A.7.] Uso no previsto	2	3	2	1	2	2	6	4	2	4	4
	[A.11.] Acceso no autorizado	1	3	2	1	2	2	3	2	1	2	2
	[A.23.] Manipulación de hardware	1	3	2	2	2	2	3	2	2	2	2
	[A.24.] Denegación de servicio	1	2	1	2	2	1	2	1	2	2	1
	[A.25.] Robo de equipos	1	3	2	2	2	2	3	2	2	2	2
	[A.26.] Ataque destructivo	1	1	2	1	2	2	1	2	1	2	2
mid_Equipos medios2] PC_Equipos de Escritorio Equipos de mesa	[E.24.] Caída del sistema por agotamiento de recurso	2	3	2	2	2	2	6	4	4	4	4
	[E.25.] Perdida de equipos	1	3	2	1	2	2	3	2	1	2	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
	[A.6.] Abuso de privilegios de acceso	1	3	2	2	2	2	3	2	2	2	2
	[A.7.] Uso no previsto	2	3	2	2	1	2	6	4	4	2	4
	[A.11.] Acceso no autorizado	1	2	2	1	2	2	2	2	1	2	2
	[A.23.] Manipulación de hardware	1	3	2	1	2	2	3	2	1	2	2
	[A.24.] Denegación de servicio	1	3	2	1	2	2	3	2	1	2	2
	[A.25.] Robo de equipos	1	3	2	2	2	2	3	2	2	2	2
	[A.26.] Ataque destructivo	1	3	2	2	1	2	3	2	2	1	2
pc Informática personal] PC_portatiles Equipos Portátiles	[E.24.] Caída del sistema por agotamiento de recurso	2	3	2	2	2	2	6	4	4	4	4
	[E.25.] Perdida de equipos	1	2	1	2	2	2	2	1	2	2	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	2	2	2	3	2	2	2	2
	[A.7.] Uso no previsto	2	3	2	2	2	2	6	4	4	4	4
	[A.11.] Acceso no autorizado	1	2	2	2	1	2	2	2	2	1	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
	[A.23.] Manipulación de hardware	1	3	1	2	2	2	3	1	2	2	2
	[A.24.] Denegación de servicio	1	2	2	1	2	2	2	2	1	2	2
	[A.25.] Robo de equipos	1	3	2	2	2	2	3	2	2	2	2
	[A.26.] Ataque destructivo	1	2	2	1	2	1	2	2	1	2	1
vhost Equipos virtuales (máquinas virtuales)] 2 Máquinas Virtuales de Respaldo	[E.24.] Caída del sistema por agotamiento de recurso	2	3	2	2	2	2	6	4	4	4	4
	[E.25.] Perdida de equipos	1	3	2	2	2	1	3	2	2	2	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	2	2	2	3	2	2	2	2
	[A.7.] Uso no previsto	2	3	2	2	1	2	6	4	4	2	4
	[A.11.] Acceso no autorizado	1	3	2	2	2	1	3	2	2	2	1
	[A.23.] Manipulación de hardware	1	1	2	2	2	2	1	2	2	2	2
	[A.24.] Denegación de servicio	1	3	2	2	1	2	3	2	2	1	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
	[A.25.] Robo de equipos	1	1	2	2	1	2	1	2	2	1	2
	[A.26.] Ataque destructivo	1	3	2	2	1	2	3	2	2	1	2
backup Equipamiento de respaldo] Sitio Alterno (Servidor de Aplicaciones y Base de Datos)	[E.24.] Caída del sistema por agotamiento de recurso	2	3	2	2	2	2	6	4	4	4	4
	[E.25.] Perdida de equipos	1	3	2	2	1	2	3	2	2	1	2
	[A.6.] Abuso de privilegios de acceso	1	3	2	2	2	2	3	2	2	2	2
	[A.7.] Uso no previsto	2	3	2	1	2	2	6	4	2	4	4
	[A.11.] Acceso no autorizado	1	3	2	2	2	2	3	2	2	2	2
	[A.23.] Manipulación de hardware	1	3	2	2	1	2	3	2	2	1	2
	[A.24.] Denegación de servicio	1	3	2	1	2	2	3	2	1	2	2
	[A.25.] Robo de equipos	1	2	2	2	2	2	2	2	2	2	2
	[A.26.] Ataque destructivo	1	3	2	2	2	2	3	2	2	2	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
[peripheral] Periféricos												
peripheral. Print Medios de impresión1] E Impresoras (32)	[E.24.] Caída del sistema por agotamiento de recurso	2	2	1	3	2	1	4	2	6	2	2
	[A.6.] Abuso de privilegios de acceso	1	2	2	3	2	1	2	2	3	2	1
	[A.7.] Uso no previsto	1	2	2	3	2	1	2	2	3	2	1
	[A.11.] Acceso no autorizado	1	2	2	3	2	1	2	2	3	2	1
	[A.13.] Repudio (negación de actuaciones)	1	2	2	3	2	1	2	2	3	2	1
	[A.24.] Denegación de servicio	1	2	2	3	2	1	2	2	3	2	1
	[A.25.] Robo de equipos	1	2	1	3	2	1	2	1	3	2	1
	[A.26.] Robo de equipos	1	2	2	3	2	1	2	2	3	2	1
peripheral. scan Escáner2] S_Scan Escáner (5)	[E.24.] Caída del sistema por agotamiento de recurso	2	2	2	3	2	1	4	4	6	2	2
	[A.6.] Abuso de privilegios de acceso	1	2	2	3	2	1	2	2	3	2	1

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
	[A.7.] Uso no previsto	1	2	1	3	2	1	2	1	3	2	1
	[A.11.] Acceso no autorizado	1	2	2	3	2	1	2	2	3	2	1
	[A.13.] Repudio (negación de actuaciones)	1	2	2	3	2	1	2	2	3	2	1
	[A.24.] Denegación de servicio	1	2	2	3	2	1	2	2	3	2	1
	[A.25.] Robo de equipos	1	2	1	3	2	1	2	1	3	2	1
	[A.26.] Robo de equipos	1	2	2	3	2	1	2	2	3	2	1
[iPhone] Teléfono IP												
Tel_IP] Teléfono Ip (20	[E.24.] Caída del sistema por agotamiento de recurso	2	2	2	3	2	1	4	4	6	2	2
	[A.6.] Abuso de privilegios de acceso	1	2	2	3	2	1	2	2	3	2	1
	[A.7.] Uso no previsto	1	2	1	3	2	1	2	1	3	2	1
	[A.11.] Acceso no autorizado	1	2	2	3	2	1	2	2	3	2	1

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
	[A.13.] Repudio (negación de actuaciones)	1	2	2	3	2	1	2	2	3	2	1
	[A.24.] Denegación de servicio	1	2	1	3	2	1	2	1	3	2	1
	[A.25.] Robo de equipos	1	2	2	3	2	1	2	2	3	2	1
	[A.26.] Robo de equipos	1	2	2	3	2	1	2	2	3	2	1
[network] Soporte de la red												
router] enrutadores] Enrutadores	[E.24.] Caída del sistema por agotamiento de recurso	2	2	2	3	2	1	4	4	6	2	2
	[A.6.] Abuso de privilegios de acceso	1	2	2	3	2	1	2	2	3	2	1
	[A.7.] Uso no previsto	1	2	2	2	2	1	2	2	2	2	1
	[A.11.] Acceso no autorizado	1	2	2	3	2	1	2	2	3	2	1
	[A.13.] Repudio (negación de actuaciones)	1	2	2	3	2	1	2	2	3	2	1

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
	[A.24.] Denegación de servicio	1	2	2	3	2	1	2	2	3	2	1
	[A.25.] Robo de equipos	1	2	1	3	2	1	2	1	3	2	1
	[A.26.] Robo de equipos	1	2	2	3	2	1	2	2	3	2	1
other] otros												
[other. W_Redwifi] Red Wi-Fi	[E.24.] Caída del sistema por agotamiento de recurso	2	2	2	3	2	1	4	4	6	2	2
	[A.6.] Abuso de privilegios de acceso	1	2	1	3	2	1	2	1	3	2	1
	[A.7.] Uso no previsto	1	1	2	3	2	1	1	2	3	2	1
	[A.11.] Acceso no autorizado	1	2	2	3	2	1	2	2	3	2	1
	[A.13.] Repudio (negación de actuaciones)	1	2	2	1	2	1	2	2	1	2	1
	[A.24.] Denegación de servicio	1	1	2	3	2	1	1	2	3	2	1
	[A.25.] Robo de equipos	1	2	2	3	2	1	2	2	3	2	1

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento SW												
	[A.26.] Robo de equipos	1	2	2	3	2	1	2	2	3	2	1
[COM] Redes de Comunicación												
[radio red inalámbrica] R_radio Red Inalámbrica	[E.2] Errores de administrador del sistema / de la seguridad	3	3	2	2	2	2	9	6	6	6	6
	[E.9] Errores de [re-]encaminamiento	2	1	2	2	2	1	2	4	4	4	2
	[E.24] Caída del sistema por agotamiento de recurso	2	2	2	1	2	2	4	4	2	4	4
	[A.5.] suplantación de la identidad	1	1	1	2	2	2	1	1	2	2	2
	[A.6.] Abuso de privilegios de acceso	1	1	2	2	2	2	1	2	2	2	2
	[A.7.] Uso no previsto	1	1	2	1	2	2	1	2	1	2	2
	[A.11.] Acceso no autorizado	1	1	2	2	2	1	1	2	2	2	1
	[A.14.] Interceptación de información (escucha)	1	1	2	1	2	2	1	2	1	2	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[COM] Redes de Comunicación												
	[A.24.] Denegación de servicio	1	1	2	1	2	2	1	2	1	2	2
[wifi] R_wifi Red Inalámbrica	[E.2] Errores de administrador del sistema / de la seguridad	3	3	2	2	2	2	9	6	6	6	6
	[E.9] Errores de [re-]encaminamiento	2	2	2	2	2	2	4	4	4	4	4
	[E.24] Caída del sistema por agotamiento de recurso	2	2	2	2	1	2	4	4	4	2	4
	[A.5.] suplantación de la identidad	1	1	2	2	2	2	1	2	2	2	2
	[A.6.] Abuso de privilegios de acceso	1	1	2	2	1	2	1	2	2	1	2
	[A.7.] Uso no previsto	1	1	1	2	2	2	1	1	2	2	2
	[A.11.] Acceso no autorizado	1	1	2	2	1	2	1	2	2	1	2
	[A.14.] Interceptación de información (escucha)	1	1	2	2	2	2	1	2	2	2	2
	[A.24.] Denegación de servicio	1	1	2	1	2	2	1	2	1	2	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[COM] Redes de Comunicación												
[LAN Red local] R_Local Red local	[E.2] Errores de administrador del sistema / de la seguridad	3	3	2	2	2	2	9	6	6	6	6
	[E.9] Errores de [re-]encaminamiento	2	1	1	2	2	2	2	2	4	4	4
	[E.24] Caída del sistema por agotamiento de recurso	2	2	1	2	2	2	4	2	4	4	4
	[A.5.] suplantación de la identidad	1	1	2	2	2	2	1	2	2	2	2
	[A.6.] Abuso de privilegios de acceso	1	1	2	2	2	2	1	2	2	2	2
	[A.7.] Uso no previsto	1	1	2	1	2	2	1	2	1	2	2
	[A.11.] Acceso no autorizado	1	1	2	2	2	2	1	2	2	2	2
	[A.14.] Interceptación de información (escucha)	1	1	1	2	2	2	1	1	2	2	2
	[A.24.] Denegación de servicio	1	1	2	2	2	2	1	2	2	2	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[COM] Redes de Comunicación												
[Internet] Internet	[E.2] Errores de administrador del sistema / de la seguridad	3	3	2	2	2	2	9	6	6	6	6
	[E.9] Errores de [re-]encaminamiento	2	2	2	2	2	1	4	4	4	4	1
	[E.24] Caída del sistema por agotamiento de recurso	2	2	1	2	2	1	4	2	4	4	2
	[A.5.] Suplantación de la identidad	1	1	2	2	2	1	1	2	2	2	1
	[A.6.] Abuso de privilegios de acceso	1	1	1	2	2	2	1	1	2	2	2
	[A.7.] Uso no previsto	1	1	2	2	1	2	1	2	2	1	2
	[A.11.] Acceso no autorizado	1	1	2	2	2	1	1	2	2	2	1
	[A.14.] Interceptación de información (escucha)	1	1	2	2	2	2	1	2	2	2	2
	[A.24.] Denegación de servicio	1	1	2	2	1	2	1	2	2	1	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[Media] Soportes de Información												
[Soportes de Información1] Electrónico												
[disk Discos] A_CD Almacenamientos en Disco Duro	[E.25.] Pérdida de equipos	1	1	2	2	2	2	1	2	2	2	2
	[A.7.] Uso no previsto	1	2	2	2	2	1	2	2	2	2	1
	[A.18.] Destrucción de la información	1	1	2	1	2	2	1	2	1	2	2
	[A.23.] Manipulación de hardware	1	2	1	2	2	2	2	1	2	2	2
	[A.24.] Denegación de servicio	1	2	2	3	2	2	2	2	3	2	2
	[A.25.] Robo de equipos	1	1	2	1	2	2	1	2	1	2	2
	[A.26.] Ataque destructivo	1	2	1	2	2	1	2	1	2	2	1
[cd (CD_ROM)] A_CD Almacenamiento en CD	[E.25.] Pérdida de equipos	1	2	1	2	2	2	2	1	2	2	2
	[A.7.] Uso no previsto	1	1	2	2	2	1	1	2	2	2	1
	[A.18.] Destrucción de la información	1	2	2	1	1	2	2	2	1	1	2
	[A.23.] Manipulación de hardware	1	2	1	2	2	2	2	1	2	2	2
	[A.24.] Denegación de servicio	1	1	2	2	3	2	1	2	2	3	2
	[A.25.] Robo de equipos	1	2	1	2	2	2	2	1	2	2	1

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[Media] Soportes de Información												
	[A.26.] Ataque destructivo	1	1	2	2	2	2	1	2	2	2	2
[USB Memorias USB] A Memorias Almacenamiento en Memorias	[E.25.] Pérdida de equipos	1	2	2	2	1	2	2	2	2	1	2
	[A.7.] Uso no previsto	1	2	1	2	2	2	2	1	2	2	2
	[A.18.] Destrucción de la información	1	2	1	2	1	2	2	1	2	1	2
	[A.23.] Manipulación de hardware	1	1	2	2	1	2	1	2	2	1	2
	[A.24.] Denegación de servicio	1	2	2	2	1	2	2	2	2	1	2
	[A.25.] Robo de equipos	1	2	3	2	2	2	2	3	2	2	2
	[A.26.] Ataque destructivo	1	1	1	2	2	2	1	1	2	2	2
dvd DVD] A_DVD Almacenamiento en DVD	[E.25.] Pérdida de equipos	1	2	2	3	2	2	2	2	3	2	2
	[A.7.] Uso no previsto	1	2	2	2	2	2	2	2	2	2	2
	[A.11.] Acceso no autorizado	1	2	1	2	2	2	2	1	2	2	2
	[A.18.] Destrucción de la información	1	1	2	2	1	2	1	2	2	1	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[Media] Soportes de Información												
	[A.23.] Manipulación de hardware	1	2	1	2	2	1	2	1	2	2	1
	[A.26.] Ataque destructivo	1	1	2	2	1	2	1	2	2	2	2
tape Cinta magnética] C_Mag Almacenamiento en Cinta Magnética	[E.15.] Alteración de la información	2	1	2	1	1	1	2	4	2	2	2
	[E.25.] Pérdida de equipos	1	4	2	4	4	2	1	2	1	1	2
	[A.7.] Uso no previsto	2	1	1	1	2	1	2	2	2	4	2
	[A.11.] Acceso no autorizado	1	2	1	1	2	1	2	1	1	2	1
	[A.18.] Destrucción de la información	1	4	2	4	2	4	4	2	4	2	4
	[A.23.] Manipulación de hardware	1	1	2	1	1	1	1	2	1	1	1
	[A.25.] Robo de equipos	1	1	2	1	2	1	1	2	1	2	1
	[A.26.] Ataque destructivo	1	4	2	4	2	4	4	2	4	2	4
Soportes de Información 2] Almacenamiento no Electrónico												
printed Material impreso 1] P_Car Cajas con sus carpetas debidamente archivadas por	[E.15.] Alteración de la información	1	1	2	2	1	2	1	2	2	1	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
Soportes de Información 2] Almacenamiento no Electrónico												
Secretarias (Proyectos, procesos, correspondencia etc.	[E.18.] Destrucción de la información	2	2	1	1	2	2	4	2	2	4	4
printed Material impreso 2] P_Informes Reportes de informes de todas las Secretarias	[E.15.] Alteración de la información	1	1	2	2	2	2	1	2	2	2	2
	[E.18.] Destrucción de la información	2	2	1	2	2	2	4	2	4	4	4
printed Material impreso] P_Varios Carpetas varios	[E.15.] Alteración de la información	1	2	1	1	2	2	2	1	1	2	2
	[E.18.] Destrucción de la información	2	2	2	2	1	2	4	4	4	2	4
[AUX] Elementos auxiliares												
powe Fuentes de Alimentación] [P_Fuente] Equipos de Escritorio	[E.25.] Robo de equipos	2	1	2	2	2	2	2	4	4	4	4
	[A.7.] Uso no previsto	2	2	2	1	2	2	4	4	2	4	4
	[A.11.] Acceso no autorizado	2	2	2	2	2	2	4	4	4	4	4
	[A.23.] Manipulación de hardware	2	1	2	1	2	2	2	4	2	4	4
	[A.26.] Ataque destructivo	2	2	1	2	2	1	4	2	4	4	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[AUX] Elementos auxiliares												
ups sai Sistemas de Alimentación ininterrumpida] [U_SistemaA] APC - UPS computadores	[E.25.] Robo de equipos	2	2	1	2	2	2	4	2	4	4	4
	[A.7.] Uso no previsto	2	1	2	2	1	2	2	4	4	2	4
	[A.11.] Acceso no autorizado	2	1	2	1	2	2	2	4	4	2	4
	[A.23.] Manipulación de hardware	2	1	2	2	2	2	2	4	4	4	4
	[A.26.] Ataque destructivo	2	2	2	1	1	2	4	4	2	2	4
ac Equipos de Climatización] E_Cli Aire Acondicionado en la sala de Servidores	[E.25.] Robo de equipos	2	1	2	2	1	2	2	4	4	2	4
	[A.7.] Uso no previsto	2	2	1	2	2	2	4	2	4	4	4
	[A.11.] Acceso no autorizado	2	2	1	2	1	1	4	2	4	2	2
	[A.23.] Manipulación de hardware	2	2	1	2	2	2	4	2	4	4	4
	[A.26.] Ataque destructivo	2	2	2	1	2	2	4	4	2	4	4
wire Cable Eléctrico] Eléctrico Cable Eléctrico	[E.25.] Robo de equipos	2	1	2	1	2	2	2	4	2	4	4
	[A.7.] Uso no previsto	2	2	1	2	2	1	4	2	4	4	2
	[A.11.] Acceso no autorizado	2	2	1	1	2	2	4	2	2	4	4

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[AUX] Elementos auxiliares												
	[A.23.] Manipulación de hardware	2	1	2	2	1	2	2	4	4	2	4
	[A.26.] Ataque destructivo	2	1	2	2	2	1	2	4	4	4	2
fiber Fibra Óptica] Óptica Transmisión de comunicación	[E.25.] Robo de equipos	2	2	1	2	1	2	4	2	4	2	4
	[A.7.] Uso no previsto	2	1	2	2	1	2	2	4	4	2	4
	[A.11.] Acceso no autorizado	2	2	2	1	2	2	4	4	4	2	4
	[A.23.] Manipulación de hardware	2	2	1	2	2	2	4	2	4	4	4
	[A.26.] Ataque destructivo	2	2	2	1	2	2	4	4	2	4	4
suplly Suministros Esenciales] Esenciales Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc.	[E.25.] Robo de equipos	2	1	2	2	1	2	2	4	4	2	4
	[A.7.] Uso no previsto	2	2	2	1	1	2	4	4	4	4	4
	[A.11.] Acceso no autorizado	2	1	2	1	2	2	2	4	4	2	4
	[A.23.] Manipulación de hardware	2	2	1	2	2	1	4	2	4	4	2
	[A.26.] Ataque destructivo	2	2	2	1	1	2	4	4	2	2	4

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[AUX] Elementos auxiliares												
Furniture Mobiliario] [Mobiliario] Mobiliario: Estantes, armarios, escritorios, archivadores, sillas, etc.	[E.25.] Robo de equipos	2	2	1	2	2	2	4	2	4	4	4
	[A.7.] Uso no previsto	2	1	2	2	1	2	2	4	4	2	4
	[A.11.] Acceso no autorizado	2	2	2	2	2	1	4	4	4	4	2
	[A.23.] Manipulación de hardware	2	2	1	2	1	2	4	2	4	2	4
	[A.26.] Ataque destructivo	2	1	2	1	2	2	2	4	2	4	4
[L] Instalaciones												
[building Edificio] [Entidad] Edificio de la Entidad (Plaza de Bolívar -Centro)	[A.7.] Uso no previsto	1	3	2	3	2	2	3	2	3	2	2
	[A.11.] Acceso no autorizado	1	3	2	3	2	2	3	2	3	2	2
	[A.26.] Ataque destructivo	1	3	2	3	2	2	3	2	3	2	2
[backup Instalaciones de respaldo] S_Alterno Sitio Alterno (Edifico Fondo Pensional)	[A.7.] Uso no previsto	1	4	2	4	2	2	4	2	4	2	2
	[A.11.] Acceso no autorizado	1	4	2	4	1	2	4	2	4	1	2
	[A.26.] Ataque destructivo	1	4	2	4	2	2	4	2	4	2	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[P] Personal												
[ue Usuarios externos] [E personal] Contratistas Externos en las diferentes Secretarias	[E.14.] Fugas de información	1	4	3	3	2	3	4	3	3	2	3
	[E.28.] Indisponibilidad del personal	3	2	2	3	1	3	6	8	9	3	9
	[A.11.3.] Por personas externas	2	4	3	3	3	3	8	6	6	6	6
	[A.12.1.] Por personas interno	2	4	3	3	3	3	8	6	4	6	6
	[A.12.2.] Por subcontratistas	2	4	3	3	3	3	8	6	6	6	6
	[A.12.3.] Por personas externas	2	4	3	2	3	3	8	6	4	6	6
	[A.28.] Indisponibilidad del personal	3	4	3	3	3	3	12	9	9	9	9
	[A.29.] Extorsión	1	4	3	3	3	3	4	3	3	3	3
	[A.30.] Ingeniería social (picaresca)	1	4	3	3	2	3	4	3	3	2	3
[ui Usuarios internos] E internos Ingenieros de la planta de la Dirección de Sistemas	[E.14.] Fugas de información	1	4	3	3	3	1	4	3	3	3	1
	[E.28.] Indisponibilidad del personal	3	4	3	3	3	3	12	9	9	9	9
	[A.11.3.] Por personas externas	2	4	3	3	3	3	8	6	6	6	6

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[P] Personal												
	[A.12.1.] Por personas interno	2	4	3	2	3	3	8	6	4	6	6
	[A.12.2.] Por subcontratistas	2	4	2	3	3	3	8	4	6	6	6
	[A.12.3.] Por personas externas	2	4	3	3	3	3	8	6	6	6	6
	[A.28.] Indisponibilidad del personal	3	4	3	3	2	3	12	9	9	6	9
	[A.29.] Extorsión	1	4	3	1	3	3	4	3	1	3	3
	[A.30.] Ingeniería social (picaresca)	1	4	3	3	2	3	4	3	3	2	3
[adm Administradores de sistemas] [A_sistemas] Ingeniero encargado de Administración del Sistemas	[E.14.] Fugas de información	1	4	2	3	3	3	4	2	3	3	3
	[E.28.] Indisponibilidad del personal	3	4	3	3	3	3	12	9	9	9	9
	[A.11.3.] Por personas externas	2	4	3	3	3	3	8	6	6	6	6
	[A.12.1.] Por personas interno	2	4	3	2	3	3	8	6	4	6	6
	[A.12.2.] Por subcontratistas	2	4	3	2	3	3	8	6	4	6	6
	[A.12.3.] Por personas externas	2	4	3	3	3	2	8	6	6	6	4

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[P] Personal												
	[A.28.] Indisponibilidad del personal	3	4	3	3	3	3	12	9	9	9	9
	[A.29.] Extorsión	1	4	3	3	1	3	4	3	3	1	3
	[A.30.] Ingeniería social (picaresca)	1	4	3	2	3	3	4	3	2	3	3
[com Administradores de comunicaciones] [A Comunicaciones] Ingeniero encargado de Administración del Comunicaciones	[E.14.] Fugas de información	1	4	3	2	3	3	4	3	2	3	3
	[E.28.] Indisponibilidad del personal	3	4	3	3	3	3	12	9	9	9	9
	[A.11.3.] Por personas externas	2	4	3	3	3	2	8	6	6	6	4
	[A.12.1.] Por personas interno	2	4	2	3	3	3	8	4	6	6	6
	[A.12.2.] Por subcontratistas	2	4	3	3	3	3	8	6	6	6	6
	[A.12.3.] Por personas externas	2	4	3	3	3	3	8	6	6	6	6
	[A.28.] Indisponibilidad del personal	3	4	3	3	3	3	12	9	9	9	9
	[A.29.] Extorsión	1	4	3	3	2	3	4	3	3	2	3
	[A.30.] Ingeniería social (picaresca)	1	4	3	2	2	3	4	3	2	2	3

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[P] Personal												
[dba Administradores de BBDD] [A_sistemas] Ingeniero encargado de Administrar las bases de datos.	[E.14.] Fugas de información	1	4	3	3	3	2	4	3	3	3	2
	[E.28.] Indisponibilidad del personal	3	4	3	3	3	3	12	9	9	9	9
	[A.11.3.] Por personas externas	2	4	3	3	2	3	8	6	6	4	6
	[A.12.1.] Por personas interno	2	4	3	3	3	3	8	6	6	6	6
	[A.12.2.] Por subcontratistas	2	4	3	2	3	3	8	6	4	6	6
	[A.12.3.] Por personas externas	2	4	3	3	3	3	8	6	6	6	6
	[A.28.] Indisponibilidad del personal	3	4	3	3	3	3	12	9	9	9	9
	[A.29.] Extorsión	1	4	3	2	3	3	4	3	2	3	3
	[A.30.] Ingeniería social (picaresca)	1	4	3	2	3	2	4	3	3	3	2

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[P] Personal												
[sec Administradores de seguridad] [A_sistemas] Ingeniero encargado de Administrar el firewall	[E.14.] Fugas de información	1	4	3	3	2	3	4	3	3	2	3
	[E.28.] Indisponibilidad del personal	3	4	3	3	3	3	12	9	9	9	9
	[A.11.3.] Por personas externas	2	4	3	3	3	3	8	6	6	6	6
	[A.12.1.] Por personas interno	2	4	3	3	3	3	8	6	6	6	6
	[A.12.2.] Por subcontratistas	2	4	3	3	3	3	8	6	6	6	6
	[A.12.3.] Por personas externas	2	4	3	3	3	3	8	6	6	6	6
	[A.28.] Indisponibilidad del personal	3	4	3	3	3	3	12	9	9	9	9
	[A.29.] Extorsión	1	4	3	3	3	3	4	3	3	3	3
	[A.30.] Ingeniería social (picaresca)	1	4	3	2	3	3	4	3	2	3	3
[dev Desarrolladores / programadores] [A_sistemas] Ingenieros y técnicos encargados de desarrollar diferentes proyectos.	[E.14.] Fugas de información	1	4	3	3	3	2	4	3	3	3	2
	[E.28.] Indisponibilidad del personal	3	4	3	3	3	3	12	9	9	9	9
	[A.11.3.] Por personas externas	2	4	3	3	3	3	8	6	6	6	6

Tabla 48. (Continuación)

ACTIVO	VULNERABILIDAD	PROBABILIDAD	IMPACTO					RIESGO				
			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[P] Personal												
	[A.12.1.] Por personas interno	2	4	3	2	3	3	8	6	4	6	6
	[A.12.2.] Por subcontratistas	2	4	3	3	3	3	8	6	6	6	6
	[A.12.3.] Por personas externas	2	4	3	2	3	3	8	6	4	6	6
	[A.28.] Indisponibilidad del personal	3	4	3	3	3	3	12	9	9	9	9
	[A.29.] Extorsión	1	4	3	2	3	3	4	3	2	3	3
	[A.30.] Ingeniería social (picaresca)	1	4	3	3	3	2	4	3	3	3	2

Fuente: El Autor

7.2.5.3. Informe de Calificación del Riesgo

Con la realización del análisis de matriz de riesgos se puede observar que existen unos activos de la Dirección de Sistemas de la Gobernación de Boyacá, que presentan riesgos catalogados como críticos y su probabilidad de es alta tal es el caso de los equipos informáticos, datos e información, este riesgo puede generar perdida de la información, divulgación de la información confidencial, daño en equipos y servidor, manipulación y daños en la base de datos

Podemos decir que los activos con mayor prioridad para protección son equipos informáticos, software y aplicaciones, puesto que son vulnerables y blanco fácil de los atacantes. Por esta razón estos activos se deben proteger de errores de usuarios y errores del administrador de la seguridad.

Para la protección de los activos de la Dirección de Sistemas, se deben mejorar políticas de seguridad que permitan capacitar al usuario y al administrador en el manejo y clasificación de la información, gestión de contraseñas, control de acceso, implementación de equipos y software que permitan mejorar la seguridad, seguridad física y lógica, actualizaciones permanentes del software, elaboración permanente de backups.

Clasificación del Riesgo

Telefonía: Este recurso es importante en la medida de las comunicaciones, ya que todos los funcionarios de la Dirección de Sistemas se tienen que comunicar a nivel interno y externo, sin embargo, se pueden tomar las siguientes medidas para mitigar el riesgo:

- ✓ Tener cámaras de seguridad en las oficinas de cada dependencia con el fin de tener mayor vigilancia en las actividades realizadas por los funcionarios.

- ✓ Tener a manera de seguridad un servicio de monitoreo de llamadas, en los casos que se requiera.

Internet*:* Este activo pertenece a la capa de servicios internos y afecta notablemente la disponibilidad, integridad y confidencialidad, en este recurso se deben tomar las siguientes medidas con el fin de mitigar el riesgo actual:

- ✓ La medida que se deben de tomar es el de restricción de páginas como son redes sociales, descargar programas para que el uso de Internet solo sea para actividades de trabajo y no para distracciones de empleados.

- ✓ Instalar y mantener actualizado el software de los equipos eso incluye el firewall, actualizaciones del sistema operativo, antivirus y demás herramientas y aplicaciones encargadas de proteger y monitorear el sistema

Correo Corporativos: Este activo pertenece a la capa de servicios internos y afecta la disponibilidad, integridad y confidencialidad, si esta amenaza se llegará a materializar se vería seriamente afectada la empresa en cuanto a envió de email con información importante a otras dependencias.

Las medidas para reducir este riesgo actual son las siguientes:

- ✓ Se debe realizar una configuración adecuada de este servicio

- ✓ Utilizar una contraseña segura para impedir que personal no autorizado ingrese a la cuenta de un funcionario
- ✓ No enviar correos cadena o spam, estos violan la seguridad y se estaría en riesgo de infección por virus y ataques informáticos

- ✓ Se debe realizar un monitoreo constante de las cuentas de correo electrónico desde la Dirección de sistemas, con el fin de evitar posibles fraudes mediante encriptación de información confidencial y que podría salir al exterior de la entidad.

- ✓ No permitir el uso de la cuenta institucional fuera de la empresa ni en horarios que no sean laborales

S.O. Windows: El sistema operativo es un activo que pertenece a la capa de equipamiento y posterior subcapa de aplicaciones, este es importante para el funcionamiento de las máquinas o equipos de cómputo y permite realizar las diversas actividades diarias y posee las siguientes amenazas que tienen como resultado niveles altos de riesgo en:

Errores de los usuarios y Difusión de software dañino, que indisponen a las dimensiones de disponibilidad, integridad y confidencialidad. Este tipo de errores

se da por el mal del uso de esta aplicación, lo que pueda generar inhabilitado el sistema operativo. Puede disponer de antivirus, pero si este no se actualiza constantemente no puede detectar posibles formas de contagio existentes.

Las medidas para reducir el riesgo actual de este activo, son las siguientes:

- ✓ La adquisición de software con licencia.
- ✓ Control de acceso al sistema operativo: con el uso de claves de usuario.

Servidor de Aplicaciones: Es el encargado de proporcionar un entorno de servicio de las aplicaciones informáticas.

Los administradores deben prestar atención a los programas o servicios instalados ya que estos pueden ser brechas de seguridad para los sistemas. Se debe verificar los servicios o programas innecesariamente instalados o configurados con sus valores por defecto y posiblemente activados por defecto. Esto puede causar que servicios no deseados, tales como Telnet, DHCP, o DNS, se ejecuten en un servidor o estación de trabajo sin que el administrador se entere, lo cual en consecuencia puede causar problemas de seguridad, o más aún, un camino de entrada potencial para los softwares piratas.

Las medidas a implantar para mitigar este riesgo son:

- ✓ Instalación de parches y actualizaciones que son muy necesarios.
- ✓ Incrementar el desempeño y la seguridad mediante equipamiento con aplicaciones de cifrado que permite tener seguridad de los servidores.
- ✓ Monitoreo y control sobre la red la cual se realiza la conexión para el manejo de estos servidores, evitar los puertos abiertos o mal configurados.
- ✓ Controles en los permisos de acceso a las bases de datos ya que es parte vital de la Dirección de Sistemas de la Gobernación de Boyacá.

Servidor de Correo Electrónico: Es una aplicación informática es el encargado de enviar y recibir correos mediante las redes de transmisión de datos, se pueden enviar adjuntos de ficheros de cualquier extensión.

Las medidas para reducir el riesgo actual de este activo, son las siguientes:

- ✓ Mantener protegido el servidor con firewall.
- ✓ Revisar regularmente los correos electrónicos.
- ✓ Utilizar una solución confiable del software de la comercialización de email y el servidor del smpt.
- ✓ Estar eliminando periódicamente los mensajes que rebotan y los de suscripción.

Servidor de Ficheros: Sencillamente es un servidor de archivos que permite el almacenamiento y administración de los archivos para que otros equipos que pertenezcan a la misma red puedan acceder a estos archivos.

Las medidas para reducir el riesgo actual de este activo, son las siguientes:

- ✓ Asegurarse de que el servidor es de archivos es físicamente seguro.
- ✓ Se debe cifrar cada una de las unidades
- ✓ En la medida que sea posible el servidor de archivos mantenerse fuera de internet.
- ✓ El servidor de archivos debe mantenerse actualizado.
- ✓ Debe estar protegido con un buen antivirus.
- ✓ Detener los servicios innecesarios.

Sistema de Gestión de Base de Datos: Son los programas que permite el almacenamiento, modificación y permite extraer información de la base de datos.

Las medidas para reducir el riesgo actual de este activo, son las siguientes:

- ✓ Seguridad del servidor de base de datos físicas

- ✓ Firewall para servidores de base de datos
- ✓ Software de base de datos
- ✓ Estaciones de trabajo de usuario y cliente.
- ✓ Roles de la base de datos de usuarios como son los permisos, contraseñas, gestión e informes
- ✓ Auditoria de base de datos
- ✓ Copias de seguridad y recuperación de base de datos.
- ✓ Cifrado de base de datos y gestión de claves

Antivirus: Es un software de seguridad que se instala en un equipo de computo para protegerlo de cualquier software malicioso o infecciones malware como los que ya se conocen: Virus, gusanos, troyanos.

Las medidas para reducir el riesgo actual de este activo, son las siguientes:

- ✓ Mantener actualizado el software de antivirus todo el tiempo.
- ✓ Asegurarse de que los bloqueadores de ventanas emergentes siempre estén habilitados en el navegador de internet.
- ✓ Nunca deshabilitar el firewall, puesto que el coloca un bloqueo que permite proteger los equipos de cómputo e internet.
- ✓ Desactivar la pre visualización automática y configuración de descarga automática en un sistema de correo electrónico.

Sistema Operativo: Es un software o programa uno de los más importantes en todos los equipos de cómputo, permite que mediante este sistema funciones otros softwares para poder comunicar de usuario a máquina.

Las medidas para reducir el riesgo actual de este activo, son las siguientes:

- ✓ Utilizar programas de limpieza, eliminar programas innecesarios lo que significa que cada programa es otro punto de entrada potencial para un hacker.
- ✓ Estar actualizados instalando las versiones más recientes.

7.2.6. Salvaguardas

Una vez realizado el inventario de activos, e identificado las amenazas y vulnerabilidades, se definen las salvaguardas que son procedimiento tecnológico que reduce el riesgo, de acuerdo a los activos que se van proteger, en este caso se tiene en cuenta las salvaguardas definidas en Magerit.

Selección de salvaguardas más relevantes, el tratamiento que trata los salvaguardas como:

G para Gestión
T para Técnico
F para Seguridad Física
P Para gestión de Personal

Tabla 49: Tratamiento tipos de salvaguardas según Magerit.

Efecto	Tipo
Preventivas: Reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Fuente: Tipos de Salvaguardas. Magerit v3

Tabla 50**:** Peso de las Salvaguardas

Máximo Peso	**Critica**
Peso Alto	**Muy Importante**
Peso Normal	**Importante**
Peso Bajo	**Interesante**

Fuente: Tomado de Pilar

Tabla 51: Nivel de Criticidad

9	
8	
7	Extremedamente Critico
6	Muy Critico
5	Critico
4	Muy Alto
3	Alto
2	Medio
1	Bajo
0	Despreciable

Fuente: Tomado de Pilar

7.2.6.1. Salvaguardas a Implementar

Tabla 52. Salvaguardas Inventarios de Servicios

CODIGO	ACTIVO	AMENAZA	TRATAMIENTO	PESO DE SALVAGURADAS	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGURADAS
[Interno]	Correo Electrónico	[E.1.] Errores de los usuarios. [E.2.]Errores del administrador del sistema/ de la seguridad	[DC]	CRITICA	7	✓ 10.8.4 ✓ 11.3.1	✓ Protección de correo electrónico ✓ Protección de Servicios y Aplicaciones web
	Internet	[E.1.] Errores de los usuarios. [E.2.]Errores del administrador del sistema/ de la seguridad	[DC]	CRITICA	7	✓ 9.1.2 ✓ 11.2.3 ✓ 13.2.2	✓ Protección de las comunicaciones. ✓ Aseguramiento de la disponibilidad. ✓ Protección de la confidencialidad de los datos intercambiados.
	Telefonía	[E.1.] Errores de los usuarios. [E.2.]Errores del administrador del sistema/ de la seguridad	[DC]	CRITICA	7	✓ 9.1.2 ✓ 11.2.3	✓ Protección de las comunicaciones. ✓ Aseguramiento de la disponibilidad.

Fuente: El autor

Tabla 53. Salvaguardas Equipamiento SW

CODIGO	ACTIVO	AMENAZA	TRATAMIENTO	PESO DE SALVAGUARDAS	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGURADAS
[Server_Application]	Servidor de Aplicaciones	[E.1.] Errores de los usuarios.	[DC]	CRITICA	7	✓ 12.5.1	✓ Protección de las Aplicaciones Informáticas. ✓ Copias de Seguridad (bakcup) ✓ Cambios (Actualizaciones y mantenimiento Se aplican perfiles de seguridad.
[email_server]	Servidor de Correo	[E.1.] Errores de los usuarios.	[DC]	CRITICA	7	✓ 11.3.1 ✓ 11.5.3 ✓ 12.3.1 ✓ 12.5.1	✓ Protección de las Aplicaciones Informáticas ✓ Se aplican perfiles de seguirdad
[Server_Ficheros]	File Servidor de Ficheros	[E.1.] Errores de los usuarios.	[DC]	CRITICA	7	✓ 12.5.1	✓ Protección de las Aplicaciones Informáticas. ✓ Copias de Seguridad (bakcup) ✓ Cambios (Actualizaciones y mantenimiento

Tabla 53. (Continuación)

CODIGO	ACTIVO	AMENAZA	TRATAMIENTO	PESO DE SALVAGUARDAS	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGURADAS
[SG_Base Datos]	Dbms Sistema de gestión de bases de datos	[E.1.] Errores de los usuarios.	[DC]	CRITICA	7	✓ 12.5.1	✓ Protección de las Aplicaciones Informáticas. ✓ Copias de Seguridad (bakcup) ✓ Cambios (Actualizaciones y mantenimiento ✓ Se aplican perfiles de seguridad.
[office Ofimática]	Office	[E.1.] Errores de los usuarios.	[DC]	CRITICA	7	✓ 10.8.3	✓ Protección de las Aplicaciones Informática. ✓ Copias de Seguridad (backup)
[Antivirus]	Antivirus	[E.1.] Errores de los usuarios	[DC]	CRITICA	7	✓ 12.2.1	✓ Protección de las Aplicaciones Informáticas. ✓ Se aplican perfiles de Seguridad.

Tabla 53. (Continuación)

CODIGO	ACTIVO	AMENAZA	TRATAMIENTO	PESO DE SALVAGUARDAS	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGURADAS
OS_Win	OS Sistema Operativo	[E.1.] Errores de los usuarios	[DC]	CRITICA	7	✓ 12.2.1 ✓ 12.5.1 ✓ 12.6.1	✓ Protección de las Aplicaciones Informáticas. ✓ Copias de Seguridad (backup) ✓ Se aplican perfiles de seguridad.

Fuente: El autor

8. EXISTENCIA DE LOS CONTROLES DE ACUERDO A LA NORMA ISO 27001

Para la declaración de aplicabilidad de la Dirección de Sistemas de la Gobernación de Boyacá, se ha tenido en cuenta los siguientes documentos: Los 133 controles sugeridos en el Anexo A de la norma ISO 27001, la evaluación y tratamiento de riesgos.

Una vez identificados los riesgos la declaración de aplicabilidad permite identificar los controles necesarios documentando si cada uno de estos controles es aplicable o no o si ya está implementado o no.

Tabla. 54. Declaración de Aplicabilidad con los siguientes parámetros

Dominio	Que indica el número del control de acuerdo al anexo A de la Norma ISO/IEC 27001.
Controles según la ISO/IEC 27001	Se identifica el nombre del control
Aplicabilidad	Se identifica si es o no es aplicable a la Dirección de Sistemas de la Gobernación de Boyacá.
Justificación	Explica porque es o no es aplicable dicho control
Objetivo del Control	Características
Actividades	Para la Implementación del Control
Estado	Del Control

Fuente: www.iso27000.es

Para el control se identifica y clasifica con la siguiente tabla teniendo en cuenta la abreviatura y el color.

Tabla. 55 Estado de los Controles

ESTADO	ABREVIATURA	COLOR
Planificado (No Implementado)	**(P)**	**Rojo**
Parcialmente implementado	**(PI)**	**Amarillo**
Totalmente Implementado	**(TI)**	**Verde**
	(NA)	**Sin Color**

Fuente: Basado en Magerit

8.1. *Aplicabilidad de los Controles*

Tabla 56. Aplicabilidad de los Controles

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
5	**Políticas de seguridad**					
5.1	**Políticas de seguridad de la información.**	**Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes**				
5.1.1	Documentos de políticas de seguridad de la información	Si	La implementación de las políticas de seguridad debe estar debidamente documentada y para que sirva como guía en la implementación del SGSI	La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes. ✓ Garantizar que los procedimientos para el manejo de la información sean conocidos por los todos los funcionarios de la Dirección de Sistemas.	Actualizar los documentos de los procesos que se desarrollan para la Implementación de la seguridad	PI

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
5.1	**Políticas de seguridad de la información.**	**Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes**				
5.1.2	Revisión de políticas para seguridad de la información	Si	Es necesario revisar seguidamente	La política de seguridad de la información se debe revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz. ✓ Garantizar que las políticas de seguridad de la información se mantengan actualizadas.	Revisión de las políticas de seguridad de la information.	PI

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
6	**Aspectos organizativos de la seguridad de la información**					
6.1	**Organización interna**	**Objetivo: gestionar la seguridad de la información dentro de la organización.**				
6.1.1	Compromiso de la dirección con la seguridad de la información	SI	Cada funcionario de la Dirección de Sistemas debe conocer cuáles son sus responsabilidades frente al manejo de la información.	La dirección debe apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información. ✓ Garantizar que sólo personas dentro de cierta jerarquía dentro de la empresa tengan acceso a la información	Políticas de gestión de privilegios.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
6	**Aspectos organizativos de la seguridad de la información**					
6.1	**Organización interna**	**Objetivo: gestionar la seguridad de la información dentro de la organización.**				
6.1.2	Coordinación de la seguridad de la información	SI	Es importante que cada funcionario de la Dirección de Sistemas conozca su límite en el manejo de la información	Las actividades de la seguridad de la información deben ser coordinadas por los representantes de todas las partes de la organización con roles y funciones laborales pertinentes. ✓ Garantizar que sólo personas idóneas tengan acceso a la información.	Políticas de seguridad para el personal que maneja la información al interior de la entidad.	NA
6.1.3	Asignación de las responsabilidades relativas a la seguridad de la información	SI	Los funcionarios de la Dirección de Sistemas que tiene acceso a la información deben contribuir de manera	Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información. ✓ Garantizarque las políticas de seguridad de la información estén acordes con los requerimientos y exigencias del entorno.	Se realiza periódicamente capacitación para el personal a cargo del manejo de la información.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
6	**Aspectos organizativos de la seguridad de la información**					
6.1	**Organización interna**	**Objetivo: gestionar la seguridad de la información dentro de la organización.**				
6.1.4	Procesos de autorización de recursos para el tratamiento de la información	SI	Toda información nueva que ingrese a la Dirección de Sistemas debe ser protegida bajo los parámetros y políticas de seguridad (software nuevo, programas, bases de datos etc.)	Se debe definir e implementar un proceso de autorización de la dirección para nuevos servicios de procesamiento de información. ✓ Garantizar la protección de la información de nuevos proyectos que llega a la entidad.	Políticas de seguridad para nuevos activos de información.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
6	**Aspectos organizativos de la seguridad de la información**					
6.1	**Organización interna**	**Objetivo: gestionar la seguridad de la información dentro de la organización.**				
6.1.5	Acuerdos de confidencialidad	SI	Se deben definir acuerdos de confidencialidad para el manejo de la información que deben quedar establecidos en el contrato laboral o en los contratos de prestación de servicios.	Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información. ✓ Garantizar el adecuado manejo de la información en todos los niveles de acceso a la misma.	Se encuentran los acuerdos de confidencialidad para los empleados de la entidad.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
6	**Aspectos organizativos de la seguridad de la información**					
6.1	**Organización interna**	**Objetivo: gestionar la seguridad de la información dentro de la organización.**				
6.1.6	Contacto con las autoridades	SI	La información debe ser manejada de acuerdo a las políticas de seguridad y a través de canales De comunicación seguros para evitar incidentes.	Se deben mantener contactos apropiados con las autoridades pertinentes. ✓ Evitar fallas en los canales de comunicación para el manejo de la información.	Definir canales seguros para el manejo de la información.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
6	**Aspectos organizativos de la seguridad de la información**					
6.1	**Organización interna**	**Objetivo: gestionar la seguridad de la información dentro de la organización.**				
6.1.7	Contacto con los grupos de especial interés	SI	Para el cumplimiento de los objetivos y alcances del SGSI se deben definir políticas internas para la protección de la información que deben ser conocidas por la Dirección de Sistemas de la Gobernación de Boyacá.	Se deben mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales. ✓ Estandarizar el manejo de la información a nivel interno.	Políticas para el manejo de la información al interior de la organización.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
6	**Aspectos organizativos de la seguridad de la información**					
6.1	**Organización interna**	**Objetivo: gestionar la seguridad de la información dentro de la organización.**				
6.1.8	Revisión independiente de la seguridad de la información	SI	Se debe definir de qué manera serán adoptadas y modificadas las políticas de seguridad cuando se presenten cambios en los activos de la Dirección de Sistemas (nuevos programas, nuevos servicios etc.)	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad. ✓ Dinamizar las políticas de seguridad para que se ajusten a los nuevos activos que entran a formar parte de la Dirección de Sistemas.	Maneja Políticas pensadas en futuros activos que formaran parte de la entidad.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
6.2	**Partes Externas**	**Objetivo: Mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.**				
6.2.1	Identificación de los riesgos derivado del acceso a terceros	No	Es necesario identificar los posibles riesgos asociados a los accesos otorgados a la información entidades externas o a terceros, considerando el uso de aplicaciones electrónicos. (cuando se dé la conectividad con planeación y se haga uso de un servidor)	Identificar los riesgos asociados al acceso a la información y sistemas de información por parte de terceros. ✓ Identificar los riesgos asociados al acceso a la Información y sistemas de información por parte de terceros.	Controles de acceso a la información redundantes.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
6.2	**Partes Externas**	**Objetivo: mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.**				
6.2.2	Tratamiento de la seguridad en la relación con los clientes	SI	Es necesario que los terceros que necesiten acceder a la información conozcan bajo qué condiciones pueden tener acceso a la información.	Todos los requisitos de seguridad identificados se deben considerar antes de dar acceso a los clientes a los activos o la información de la organización. ✓ Brindar lineamientos a la hora de que un cliente requiera tener acceso a la información.	Controles de seguridad para clientes externos.	NA
6.2.3	Tratamiento de la seguridad en contratos con terceros	SI	Cualquier convenio o acuerdo realizado con otra entidad como planeación que implique la relación con los activos internos (información) de la Dirección de S. deben Garantizar el Cumplimiento	✓ Establecer controles de seguridad para el acceso activos internos de la empresa por parte de terceros.	Políticas para el manejo de acuerdos que impliquen la relación con información interna de empresa.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
7	**Gestión de Activos**					
7.1	**Responsabilidad sobre los activos**	**Objetivo: lograr y mantener la protección adecuada de los activos organizacionales.**				
7.1.1	Inventario de activos	SI	Es importante identificar los activos de acuerdo a su grado de importancia dentro de la Dirección de Sistemas, en la que se deja claro que el activo más relevante es la base de datos donde se registran los proyectos y archivo físico.	Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes. ✓ Jerarquizar la importancia de los activos al interior de la entidad.	Se debe mejorar la Clasificación de los activos y establecimiento to del nivel de importancia de los mismos.	PI

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
7	**Gestión de Activos**					
7.1.2	Propietario de activos	SI	Cada activo dentro de la Dirección de Sistemas debe tener relacionado un responsable de la seguridad.	Toda la información y los activos asociados con los servicios de procesamiento de información deben ser propiedad) de una parte designada de la organización ✓ Tener responsables de los activos que forman parte de la Dirección de Sistemas de la Gobernación de Boyacá.	Asignar responsables tanto para los activos de información a través del área de gestión de proyectos, como para activos físicos que forman parte de los sistemas de información.	NA
7.1.3	Uso aceptable de los activos	SI	Las políticas sobre manejo de la informacióndeben permitir tener claridad acerca del manejo adecuado de activos.	Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información	Políticas de Manejo de activos.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
7	**Gestión de Activos**					
7.2	**Clasificación de la información**	**Objetivo: asegurar que la información recibe el nivel de protección adecuado.**				
7.2.1	Directrices de clasificación	SI	La información debe ser clasificada de acuerdo a su grado de importancia para establecer los controles adecuados para el manejo de la misma.	La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización. ✓ Identificar el nivel de importancia de los activos de información al interior de la Dirección de Sistemas.	Establecimiento de prioridades en el manejo de la información.	NA
7. 2.2	Etiquetado y manipulado de la información	SI	Cada tipo de información debe ser identificado para que cada persona conociendo su naturaleza respete su nivel de confidencialidad, es decir debe ser etiquetada relacionando sus restricciones.	Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización. ✓ Identificar el nivel de confidencialidad y acceso a la información.	Políticas de acceso a la información.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
8	**Seguridad en los recursos Humanos**					
8.1	**Seguridad antes del empleo**	**Objetivo: Asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.**				
8.1.1	Funciones y responsabilidades	SI	Antes de contratar personal es necesario definir claramente el perfil y responsabilidades del cargo.	Se deben definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la entidad ✓ Contratar personal idóneo para ocupar un cargo determinado.	Actualizar las Políticas de contratación.	NA
8.1.2	Investigación de antecedentes.	SI	Para contratar al personal se deben evaluar las cualidades profesionales, el nivel de ética y compromiso con la empresa.	✓ Garantizar en los nuevos funcionarios tanto cualidades profesionales específicas como principios éticos.	Claridad en las políticas de contratación.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementació	Estado
8	**Seguridad en los recursos Humanos**					
8.1	**Seguridad antes del empleo**	**Objetivo: Asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.**				
8.1.3	Términos y condiciones de contratación.	SI	Es necesario que los nuevos funcionarios conozcan políticas y responsabilidades en cuanto a sus funciones y manejo de la información	✓ Establecer las reglas que debe seguir quien desee formar parte de la entidad.	Claridad	NA
8.2	**Seguridad en el desempeño de las funciones al interior de la empresa**					
8.2.1	Responsabilidades de la dirección	SI	Se debe asegurar que las políticas diseñadas para el manejo de la información sean cumplidas por la Dirección de Sistemas de la Gobernación de Boyacá.	La dirección debe exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización. ✓ Garantizar que los funcionarios usen las políticas definidas por la entidad.	Definición de políticas	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los	Estado
8	**Seguridad en los recursos Humanos**					
8.2	**Seguridad en el desempeño de las funciones al interior de la empresa**					
8.2.2	Concienciación, formación y capacitación en seguridad de la información	SI	Todas las políticas de seguridad de la información deben ser conocidas al interior de la Dirección de Sistemas.	Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad. ✓ Dar a conocer las políticas de seguridad de la	Realiza capacitación en políticas de seguridad de la información.	NA
8.2.3	Proceso disciplinario.	SI	Las posibles sanciones por incumplimiento de las políticas de seguridad o el mal manejo de la información que pongan en riesgo la seguridad de la información deben ser conocidas por todos los empleados de la Dirección de	✓ Dar a conocer las sanciones que acarrea el mal manejo de la información.	Planes de capacitación en políticas de seguridad de la información.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los	Estado
8.3	**Finalización o cambio de empleo**					
8.3.1	Responsabilidad del cese o cambio	SI	Es necesario garantizar que después de la finalización de un contrato interno, la información que maneja esta persona no se vea afectada divulgada.	✓ Evitar impacto negativo en la información tras la salida de un funcionario que tenga conocimiento sobre la misma.	Implementación de políticas de manejo de privilegios sobre la información.	NA
8.3.2	Devolución de activos	SI	Se deben tener protocolos que garanticen al funcionario hacer entrega de los activos que tiene a su cargo.	Todos los empleados, contratistas o usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo. ✓ Garantizar que los activos no se vean afectados tras la salida de un empleado de la entidad.	Tiene definidos los mecanismos para la devolución de activos.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los	Estado
8.3	**Finalización o cambio de empleo**					
8.3.3	Retirada de los derechos de acceso	SI	Se debe contar con procedimientos para revocar privilegios a personal que no requiera de los mimos.	✓ Evitar niveles de acceso a la información inadecuados, que pongan en riesgo la seguridad de la misma.	Implementación de políticas de manejo de privilegios sobre la	NA
9	**Seguridad física y del ambiente**					
9.1	Áreas Seguras	Objetivo: evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.				
9.1.1	Perímetro de seguridad física.	SI	Se debe garantizar la seguridad de las zonas que manejan información sensible (archivo físico, ubicación de servidores, equipos, almacenamiento copias de seguridad etc.).	Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento ✓ Asegurar las áreas que contengan información sensible	Maneja Políticas de control de acceso físico a áreas que contienen información sensible.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
9.1	Áreas Seguras	Objetivo: evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.				
9.1.2	Controles físicos de entrada.	SI	Sólo personal autorizado debe acceder a áreas que contengan activos sensibles. (Archivo histórico físico, almacenamiento de copias de seguridad, uso de servidor).	Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento. ✓ Restringir el acceso a áreas que contengan información sensible.	Políticas de control de acceso físico a áreas que contienen información sensible.	P
9.1.3	Seguridad de oficinas, despachos e instalaciones .	SI	Los funcionarios de la Dirección de Sistemas son los únicos que tienen acceso a información sensible.	✓ Garantizar la seguridad en oficinas y despachos.	Políticas de control de acceso físico.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
9.1	Áreas Seguras	Objetivo: evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.				
9.1.4	Protección contra las amenazas externas y de origen ambiental.	SI	Se debe garantizar que ninguna amenaza ambiental externa pueda generar daño sobre la información.	Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial. ✓ Garantizar la protección contra amenazas ambientales externas.	Se encuentra protegido contra factores atmosféricos como temperatura, humedad, etc.	NA
9.1.5	Trabajo en áreas seguras.	SI	Las áreas sobre las que se desarrollan las actividades deben cumplir estándares de seguridad lo cual es muy importante tanto para equipos como para el personal.	Se deben diseñar y aplicar la protección física y las directrices para trabajar en áreas. ✓ Garantizar el desarrollo de las actividades sobre áreas seguras.	Verificación del nivel de seguridad de las áreas de trabajo.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
9.1	Áreas Seguras	Objetivo: evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.				
9.1.6	Áreas de acceso público y de carga y descarga.	SI	Las áreas como archivo histórico y ubicación de servidores se Denominan áreas sensibles por la información que maneja, por tanto, se debe evitar que terceros puedan llegar a tener acceso a esta.	✓ Garantizar que el acceso a áreas sensibles dentro de la entidad tenga mecanismos de control.	La Dirección de Sistemas maneja el Control de acceso físico a determinadas áreas de la empresa.	NA
9.2	**Seguridad en Equipos**					
9.2.1	Emplazamiento y protección de equipos.	SI	Es necesario tener protecciones contra daños ambientales, especialmente para los servidores que se maneja al interior de la Gobernación.	Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno. ✓ Garantizar la integridad de los equipos al interior de la entidad.	Implementar controles para el control de factores ambientales como humedad, polvo, etc.	PI

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
9.2	**Seguridad en Equipos**					
9.2.2	Instalaciones de suministro.	SI	La integridad de los equipos depende de los controles para la protección antes fallas eléctricas, ya un fallo de energía puede dejar inutilizable un equipo, dañar su disco duro etc.	Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro. ✓ Garantizar que fallos eléctricos no afecten la integridad de los equipos que forman parte del sistema de información.	Cambiar UPS.	PI
9.2.3	Seguridad del cableado.	SI	Se debe garantizar que las redes de datos no vean afectada su integridad y confidencialidad de los datos que transportan.	El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información debe estar protegidos contra interceptaciones o daños. ✓ Garantizarque las redes de datos no sean alteradas físicamente y no puedan ser interceptados los datos que se transportan a través de estas.	Implementar y/o actualizar los sistemas de cableado existentes.	TI

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
9.2	**Seguridad en Equipos**					
9.2.4	Mantenimiento de los equipos.	SI	Se debe realizar mantenimiento periódico de los equipos como política interna de la empresa.	Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad. ✓ Garantizar la integridad y disponibilidad de los equipos.	Implementar planes periódicamente de mantenimiento de equipos al interior de la Gobernación	PI
9.2.5	Seguridad de los equipos fuera de las instalaciones.	SI	Todo equipo que trabaje fuera de la Gobernación, pero tenga injerencia interna debe tener reglas y restricciones de acceso.	Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización. ✓ Garantizar la seguridad al interior de la entidad al permitir acceso a equipos que trabajen fuera.	Aplicar controles de acceso a equipos externos que tengan que ver directamente con la actividad de la empresa (Acceso remoto derivado del teletrabajo)	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
9.2	**Seguridad en Equipos**					
9.2.6	Reutilización o retirada segura de equipos.	SI	Al dar de baja un equipo puede quedar almacenada información que puede comprometer la confidencialidad de la empresa.	Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura. Garantizar que ningún dato sensible o licencia sean expuestos a terceros tras un proceso de baja de equipos.	Maneja políticas para el proceso de baja de equipos.	NA
9.2.7	Retiro de activos	SI	Tanto las aplicaciones propias como de terceros, software que la empresa utiliza deben ser protegidas para evitar que puedan ser sacadas de la empresa.	Ningún equipo, información ni software se deben retirar sin autorización previa. ✓ Garantizar que ningún tipo de aplicación salga de la entidad.	Maneja políticas sobre el manejo de aplicaciones y licencias al interior de la empresa.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10	**Administración de comunicaciones y operaciones**					
10.1	Procedimientos y responsabilidades operacionales					
10.1.1	Documentación de los procedimientos de operación.	SI	Para garantizar la continuidad de procesos se debe contar con bitácoras que permitan conocer los procedimientos operacionales especialmente los que tengan q que ver con activos esenciales.	Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten. ✓ Garantizar la documentación de procesos operacionales.	Políticas para la documentación de procedimientos.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10	**Administración de comunicaciones y operaciones**					
10.1.2	Gestión de cambios.	SI	Se debe tener claridad de quienes serán los encargados de realizar el proceso de administración de la información.	Se deben controlar los cambios en los servicios y los sistemas de procesamiento. ✓ Gestionar los cambios de roles encargados de la administración de la información.	Implementación las políticas de manejo de privilegios sobre la información.	NA
10.1.3	Segregación de tareas.	SI	Sólo el personal autorizado debe tener acceso a la información.	Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización. ✓ Garantizar que un número reducido de personas tengan acceso a la información.	Implementación de políticas de Manejo de privilegios sobre la información.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10	**Administración de comunicaciones y operaciones**					
10.1.4	Separación de los recursos de desarrollo, prueba y operación.	SI	Cada área dentro de la empresa debe ser separada de acuerdo a sus funciones y competencias.	Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo. ✓ Reducir los riesgos de acceso no autorizado a la información.	Implementar controles de acceso a áreas seguras.	TI
10.2	**Supervisión de los servicios prestados por terceros**					
10.2.1	Provision de servicios	SI	Cualquier servicio subcontratado debe contar con políticas de seguridad de la información.	✓ Garantizarque los servicios prestados por terceros cumplan con requerimientos mínimos de seguridad.	Definir políticas para la integración y control de sistemas de terceros al interior de la empresa.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10.2	**Supervisión de los servicios prestados por terceros**					
10.2.2	Supervisión y revisión de los servicios prestados por terceros.	SI	Cualquier servicio prestado por terceros debe ser controlado internamente mediante procesos de autoridad.	Los servicios, reportes y registros suministrados por terceras partes se deben controlar y revisar con regularidad y las auditorias se deben llevar a cabo a intervalos regulares. ✓ Garantizar la calidad en la prestación de servicios ofrecidos por tercero.	Definir políticas para la integración y control de sistemas de terceros al interior de la Gobernación.	NA
10.2.3	Gestión del cambio en los servicios prestados por terceros.	SI	Cualquier cambio en los servicios prestados por terceros debe ser monitoreado constantemente.	✓ Garantizar que los cambios en la prestación de servicio sean acordes con las necesidades y requerimientos de la entidad.	Definir políticas para la integración y control de sistemas de terceros al interior de la Gobernación.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
A.10.3	Planificación y aceptación del sistema					
10.3.1	Gestión de capacidades.	Si	Es importante que dentro de las políticas internas sea planificado el crecimiento de la Gobernación para que los recursos sean acordes con el mismo.	Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema. ✓ Garantizarque los recursos con los que cuenta la entidad sean acordes con los requerimientos de la misma.	Planificación de recursos acordes con las necesidades y proyecciones de crecimiento de la Generation.	TI
10.3.2	Aceptación del sistema.	Si	Se debe definir la capacidad de integración de nuevos elementos al sistema, ya sea por actualización, renovación o totalmente nuevos.	Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo. ✓ Garantizar la compatibilidad de nuevos elementos	Definición de políticas para la integración de nuevos elementos al sistema de información.	P

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10.4	Protección contra software malicioso y código móvil.					
10.4.1	Controles contra el código malicioso.	Si	Se deben tener controles que garanticen que códigos maliciosos no terminen afectando el sistema.	Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los funcionarios. ✓ Garantizar la seguridad en contra de amenazas lógicas al Sistema de información.	Implementar mecanismos de seguridad para garantizar el control lógico al interior de la entidad.	TI
10.4.2	Controles contra el código descargado en el cliente.	NA	Por seguridad no se autoriza el uso de código móvil.	NA	NA	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10.5	Gestión interna de soportes y recuperación					
10.5.1	Copias de seguridad de la información.	SI	Respaldar la información garantiza que ante cualquier problema de seguridad se tendrá una fácil recuperación de la información. bases de datos, archivo de contabilidad, archivo de manejo técnico, bases de datos de clientes, ingenieros, de acuerdo con la política de recuperación	Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada. ✓ Garantizar políticas de respaldo para el manejo de la información.	Tiene implementado los Backups regulares de la información de acuerdo a las políticas de la Dirección de Sistemas.	NA
A.10.6	**Gestión de redes**					
10.6.1	Controles de red.	SI	Es necesario que la red inalámbrica que maneja la empresa sea controlada.	Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito. ✓ Garantizar la protección de las redes contra ataques informáticos.	Tiene implementado políticas de administración y uso de redes.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
A.10.6	**Gestión de redes**					
10.6.2	Seguridad de los servicios de red.	SI	Deben existir políticas que permitan la definición de acuerdos sobre el manejo de las redes.	En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente. ✓ Garantizar el uso adecuado de los recursos de red en cada nivel del servicio.	Definición de políticas de administración y uso de redes.	NA
A.10.7	**Utilización y seguridad de los soportes de información**					
10.7.1	Gestión de soportes extraíbles.	SI	No se permite el uso de medios informáticos removibles para evitar fugas y amenazas que puedan contener.	Se deben establecer procedimientos para la gestión de los medios extraíbles. ✓ Garantizar que la información no sea extraída por los funcionarios de la entidad.	Definición de políticas para que la información no sea extraída	PI

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
A.10.7	**Utilización y seguridad de los soportes de información**					
10.7.2	Retirada de soportes.	SI	Se debe contar con políticas que permitan eliminar de forma segura los soportes de información de la Dirección de Sistemas. (Destrucción segura de elementos desde papel hasta discos duros.)	Evitar que información almacenada en medios que van a ser eliminados pueda quedar expuesta a terceros. ✓ Evitar que la información almacenada que se encuentra en los equipos que serán eliminados pueda quedar expuesta a terceros.	Definir políticas para la gestión y eliminación de medios de almacenamientos.	PI
10.7.3	Procedimiento de manipulación de la información.	SI	Se debe garantizar que la información en cualquier nivel sea manipulada y almacenada de forma segura.	Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.	Definir políticas para la manipulación y almacenamiento de información.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
A.10.7	**Utilización y seguridad de los soportes de información**					
10.7.4	Seguridad de la Documentación del sistema.	SI	La documentación de los sistemas (información de proyectos y bases de datos) deben ser protegidos.	La documentación del sistema debe estar protegida contra el acceso no autorizado. ✓ Garantizar la protección del activo más importante al interior de la entidad.	Mejorar el sistema de políticas y sistemas de protección para la Documentación de los sistemas de información.	TI
10.8	**Intercambio de información y software**					
10.8.1	Políticas y procedimiento de intercambio de información.	Si	Se debe garantizar que la información se encuentre segura al ser transportada haciendo uso de diferentes servicios de comunicación.	Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación. ✓ Garantizar la seguridad de la información al ser enviada por diferentes medios de comunicación.	Diseñar políticas e Implementar controles para el intercambio seguro de información.	TI

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10.8	**Intercambio de información y software**					
10.8.2	Acuerdos de intercambio.	SI	Se debe tener claridad de la forma como se puede compartir información al interior de la empresa.	Se deben establecer acuerdos para el intercambio de la información y del software entre la organización y partes externas. ✓ Garantizar el intercambio seguro de la información.	Diseñar políticas e implementar controles para el intercambio seguro de información.	NA
10.8.3	Soportes físicos en tránsito.	SI	Se debe proteger la información durante el transporte de la misma	Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización. ✓ Garantizar la protección de la información al ser transportada.	Implementar mecanismos de protección de información como por ejemplo encriptación (se garantiza con los controles con que cuenta la Gobernación)	P

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10.8	**Intercambio de información y software**					
10.8.4	Mensajería electronica.	SI	Se debe proteger la información contenida en correos electrónicos.	La información contenida en la mensajería electrónica debe tener la protección adecuada. ✓ Garantizarque la información de mensajería electrónica se encuentre totalmente protegida.	Implementar mecanismos de protección para evitar accesos no autorizados a los servicios de mensajería.	P
10.8.5	Sistemas de información empresariales.	SI	Todos los sistemas de información tanto internos como externos deben estar conectados de forma segura.	Garantizar la conexión segura entre los sistemas de información. ✓ Garantizar la conexión segura entre los sistemas de información.	Políticas para el acceso a la información tanto a nivel interno como externo.	TI

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10.9	**Servicios de comercio electrónico**					
10.9.1	Comercio electrónico	SI	De debe garantizar que la información involucrada en comercio sea protegida, por la naturaleza de la entidad esto se puede garantizar.	La información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizada. ✓ Proteger la información usada en comercio electrónico.	Implementación De mecanismos para la protección de la información involucrada en comercio electrónico	NA
10.9.2	Transacciones en línea	SI	La información involucrada en procesos de transacciones electrónicas que maneja la Dirección de Sistemas por su actividad económica deber ser protegida para evitar problemas de seguridad.	La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje. ✓ Garantizar la seguridad de la información involucrada en transacciones en línea	Implementar mecanismos de seguridad para garantizar la seguridad de la información usada en transacciones en línea.	TI

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los	Estado
10.9	**Servicios de comercio electrónico**					
10.9.3	Información disponible al público	SI	La información que se maneja por aplicaciones de acceso público debe ser protegida.	La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada. ✓ Garantizar la integridad de la información disponible en sistemas de acceso público.	Políticas para la verificación de la integridad de sistemas de información de acceso público.	NA
10.10	**Monitorización**					
10.10.1	Registros de Auditoria	SI	Se deben tener registros de auditorías que permitan facilitar investigaciones futuras en caso de detectarse algún incidente de seguridad.	Se deben elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso. ✓ Contar con soportes de actividades para procesos de investigación asociados a los mismos.	Políticas de implementación y control de registros de actividad.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10.10	**Monitorización**					
10.10.2	Supervisión del uso del sistema	SI	Se debe realizar monitoreo de cualquier cambio en los sistemas de información, revisando sus resultados. Revisar las actividades de monitoreo	Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad. ✓ Verificar la instalación de sistemas de información.	Políticas de implementación y control de registros de actividad.	NA
10.10.3	Protección de la información de los registros	SI	Se debe tener control sobre los registros de actividad para que no puedan ser alterados (intentos forzosos o no autorizados)	Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados. ✓ Proteger los registros de actividad contra acciones de modificación de los mismos.	Políticas de implementación y control de registros de actividad.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10.10	**Monitorización**					
10.10.4	Registros de administración y operación.	SI	Es muy importante que la actividad de quienes tengan mayores privilegios sean monitoreados.	Se deben registrar las actividades tanto del operador como del administrador del sistema. ✓ Garantizar que la acción de carácter administrativo se lleve de forma adecuada.	Políticas de implementación y control de registros de actividad.	NA
10.10.5	Registro de fallos.	SI	Se debe controlar cualquier avería que se presente en el sistema de información.	Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas. ✓ Garantizar la trazabilidad de averías en el sistema.	Políticas de control y gestión de fallas en el sistema.	NA
10.10.6	Sincronización del reloj.	SI	Es muy importante que todos los sistemas estén sincronizados para que cualquier registro coincida en tiempos y se pueda hacer la trazabilidad del mismo.	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada. ✓ Garantizarque todo el sistema esté sincronizado.	Políticas de implementación y control de registros de actividad.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11	**Control de Acceso**					
11.1	**Requisitos de negocio para control de accesos**	**Objetivo: controlar el acceso a la información.**				
11.1.1	Política de control de acceso.	SI	Basado en los servicios que presta la Dirección de Sistemas de la Gobernación de Boyacá, se deben establecer políticas de control de acceso.	Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos de la entidad y de la seguridad para el acceso ✓ Controlar el acceso de acuerdo a las actividades que desarrolla la empresa.	Definir políticas para el control de acceso teniendo en cuenta áreas críticas.	NA
11.2	**Gestión de acceso de usuario**	**Objetivo: asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.**				
11.2.1	Registro de usuario.	SI	Es importante gestionar los usuarios para que sean asignados y dados de alta en el sistema sin generar problemas de seguridad.	Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información. ✓ Brindar o quitar acceso a usuarios basado en procedimientos propios de la entidad	Definir políticas para el ingreso o eliminación de usuarios del sistema.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.2	**Gestión de acceso de usuario**	**Objetivo: asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.**				
11.2.2	Gestión de privilegios	SI	Se debe garantizar que cada usuario tenga acceso al sistema de información basado en privilegios.	Se debe restringir y controlar la asignación y uso de privilegios. ✓ Controlar los privilegios de acceso	Definir políticas para la gestión de privilegios.	NA
11.2.3	Gestión de contraseñas de usuario.	NO	Debe existir un procedimiento para la asignación de contraseñas al interior de la empresa.	La asignación de contraseñas se debe controlar a través de proceso formal de Gestión. ✓ Asignar contraseñas de forma segura	Establecer políticas para la asignación de contraseñas.	P
11.2.4	Revisión de los derechos de acceso de usuario.	SI	Se debe verificar que los usuarios puedan acceder sólo a los sistemas que tienen permiso.	La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios. ✓ Verificar el acceso a sistemas de información	Establecer políticas para la verificación regular del acceso a sistemas de información.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.3	**Responsabilidades del usuario**	**Objetivo: evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.**				
11.3.1	Uso de contraseñas.	SI	Se debe definir y verificar el uso de contraseñas seguras.	Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas. ✓ Controlar el uso de contraseñas seguras.	Establecer políticas para que los usuarios realicen un adecuado manejo de los sistemas de información ofrecidos	P
11.3.2	Equipo de usuario desatendido.	SI	Es importante que los servidores tengan mecanismos de protección para los sistemas de la entidad.	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada. ✓ Garantizarla seguridad de las aplicaciones entregadas a los clientes.	Establecer políticas para que los usuarios realicen un adecuado manejo de los sistemas de información ofrecidos por la entidad	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.3	**Responsabilidades del usuario**	**Objetivo: evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.**				
11.3.3	Política de puesto de trabajo despejado y pantalla limpia.	SI	Se debe evitar que por alguna razón quede expuesta información a la vista de terceros.	Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información. ✓ Garantizarque la información no sea expuesta a la vista de	Establecer políticas para que los usuarios realicen un adecuado manejo de los sistemas de información ofrecidos por la entidad.	NA
11.4	**Control de acceso en red**	**Objetivo: evitar el acceso no autorizado a servicios en red.**				
11.4.1	Política de uso de los servicios en red.	SI	Los clientes de los servicios de la entidad sólo podrán tener acceso a los servicios autorizados.	Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados. ✓ Garantizar el acceso a servicios autorizados.	Establecer políticas de acceso a servicios ofrecidos Entidad	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.4	**Control de acceso en red**	**Objetivo: evitar el acceso no autorizado a servicios en red.**				
11.4.2	Autenticación de usuario para conexiones externas.	SI	Tanto para clientes externos de servicios alojados en la entidad como para empleados con acceso remoto deben existir políticas de acceso adecuadas.	Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos. ✓ Garantizar el acceso remoto seguro	Establecer políticas de acceso a servicios ofrecidos por la entidad	NA
11.4.3	Identificación de los equipos en las redes.	SI	Se debe garantizar conocer la procedencia de cualquier petición de servicio.	La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos y ubicaciones específicas. ✓ Garantizarque todas las conexiones establecidas sean seguras.	Establecer políticas de acceso a servicios ofrecidos por la entidad.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.4	**Control de acceso en red**	**Objetivo: evitar el acceso no autorizado a servicios en red.**				
11.4.4	Protección de los puertos de diagnóstico y configuración remotos.	SI	El entorno de diagnóstico de la entidad debe estar protegido.	El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado. ✓ Proteger el sistema de diagnóstico de los sistemas de información	Establecer políticas de acceso a servicios ofrecidos por la entidad.	NA
11.4.5	Segregación de las redes.	SI	Se debe tener claramente definido el papel de cada usuario dentro de la red, asignándolo a un grupo determinado.	En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información ✓ Garantizar la identificación de los usuarios en un grupo determinado.	Establecer políticas de acceso a servicios ofrecidos por la entidad	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.4	**Control de acceso en red**	**Objetivo: evitar el acceso no autorizado a servicios en red.**				
11.4.6	Control de la conexión a la red.	SI	El acceso a los sistemas internos de la entidad debe estar limitado para que no se puedan usar servicios que pongan en juego la seguridad.	Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación del negocio ✓ Restringir el acceso a servicios de red desde ubicaciones externas.	Establecer políticas de acceso a servicios ofrecidos por la entidad	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.4	**Control de acceso en red**	**Objetivo: evitar el acceso no autorizado a servicios en red.**				
11.4.7	Control de encaminamiento (routing) de red.	SI	Se debe controlar el enrutamiento de información.	Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones del negocio. ✓ Garantizar que la información de la empresa no use rutas que pongan en peligro su integridad.	Establecer políticas de enrutamiento de la información.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.5	**Control de acceso al sistema operativo**	**Control de acceso al sistema operativo**				
11.5.1	Procedimiento seguro de inicio de sesión.	SI	Se debe controlar el acceso a los sistemas operativos con los procedimientos adecuados.	El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro. ✓ Controlar el acceso al Sistema Operativo con procedimientos seguros.	Establecer políticas de acceso a los sistemas operativos.	NA
11.5.2	Identificación y autenticación de usuario.	SI	Deben existir mecanismos de identificación únicos para los usuarios.	Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario. ✓ Garantizarque los usuarios tengan credenciales únicas de acceso.	Establecer políticas de manejo de credenciales de usuarios.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.5	**Control de acceso al sistema operativo**	**Control de acceso al sistema operativo**				
11.5.3	Sistema de gestión de contraseñas.	SI	Se debe garantizar que los sistemas de gestión de contraseñas sean eficientes.	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas. ✓ Garantizar la eficiencia y seguridad en los sistemas de gestión de contraseñas.	Establecer políticas de manejo de credenciales de usuarios.	P
11.5.4	Uso de los recursos del sistema.	SI	Se debe controlar el uso de aplicaciones administrativas seguras que pueden ser usadas para generar algún tipo de daño al sistema.	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación. ✓ Realizar control sobre el uso de aplicaciones administrativas	Establecer políticas de uso de aplicaciones de carácter administrativo propias del sistema.	NA
11.5.5	Desconexión automática de sesión.	SI	Se debe controlar el tiempo de inactividad del equipo.	Garantizar el bloqueo de equipos tras cierto tiempo de inactividad. ✓ Garantizar el bloqueo de equipos tras cierto tiempo de inactividad.	Establecer políticas de acceso a los sistemas operativos.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.5	**Control de acceso al sistema operativo**	**Control de acceso al sistema operativo**				
11.5.6	Limitación del tiempo de conexión.	SI	Se debe controlar el tiempo de conexión al SO basado en el uso de aplicaciones.	Se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo ✓ Controlar el uso del sistema operativo.	Establecer políticas de acceso a los sistemas operativos.	NA
11.6	**Control de acceso a las Aplicaciones**	**Objetivo: evitar el acceso no autorizado a la información contenida en los sistemas de información.**				
11.6.1	Restricción del acceso a la información.	SI	Se debe restringir el acceso a los sistemas en especial al programa que maneja la base de datos, estado de proyectos.	Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.	Establecer controles para el acceso a los diferentes niveles de aplicaciones.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.6	**Control de acceso a las Aplicacione**	**Objetivo: evitar el acceso no autorizado a la información contenida en los sistemas de información.**				
11.6.2	Aislamiento de sistemas sensible.	SI	Los sistemas sensibles como copias de seguridad, archivo físico y servidores deben estar aislados	Los sistemas sensibles deben tener un entorno informático dedicado (aislados). ✓ Garantizarque los sistemas sensibles de la entidad tengan un entorno informático propio.	Establecer controles para el acceso a los diferentes niveles de aplicaciones.	NA
11.7	**Informática móvil y tele trabajo**					
11.7.1	Ordenadores portátiles y comunicaciones móviles.	SI	La conexión a través de red inalámbrica hace necesario la definición de políticas de protección de recursos móviles.	Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles. ✓ Brindar protección contra riesgos derivados del uso de recursos móviles.	Establecer políticas para el manejo de riesgos derivados de la informática móvil.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.7	**Informática móvil y tele trabajo**					
11.7.2	Teletrabajo.	SI	Ya que se considera el teletrabajo al interior de la entidad es necesario considerar políticas y procedimientos tanto para acceso como para cumplimiento de funciones.	Garantizar el desempeño seguro y eficiente de actividades de teletrabajo. ✓ Garantizar el desempeño seguro y eficiente de actividades de teletrabajo	Diseñar e implementar políticas para la gestión del teletrabajo.	NA
12	Adquisición, desarrollo y mantenimiento de sistemas de información					
12.1	**Requisitos de seguridad delos sistemas**	Objetivo: garantizar que la seguridad es parte integral de los sistemas de información.				
12.1.1	Análisis y especificación de los requisitos de seguridad	SI	Es importante que todo nuevo sistema de seguridad especifique los controles necesarios para su implementación.	Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad. ✓ Garantizar que todo nuevo sistema incluya controles de seguridad	Establecer políticas para la integración de sistemas de información.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
12.1	**Requisitos de seguridad delos sistemas**					
12.2	Seguridad de las aplicaciones del sistema	SI	Las aplicaciones del sistema deben brindar seguridad.	✓ Garantizar seguridad en las aplicaciones del sistema.	Establecer políticas de seguridad para las aplicaciones.	NA
12.2.1	Validación de los datos de entrada.	SI	Cualquier acceso debe ser validado para garantizar que se esté haciendo desde una aplicación confiable.	Se deben validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados. ✓ Garantizar la seguridad del acceso a las aplicaciones.	Establecer políticas de seguridad para las aplicaciones.	P
12.2.2	Control el procesamiento interno.	SI	Se deben verificar las aplicaciones para detectar alteraciones en la información.	Se deben incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados. ✓ Garantizar que la información no tenga ningún cambio al momento de procesarla.	Establecer políticas de seguridad para las aplicaciones.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
12.1	**Requisitos de seguridad de los sistemas**					
12.2.3	Integridad de los mensajes.	SI	Se debe asegurar la autenticidad de la información en los mensajes en las aplicaciones.	Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados. ✓ Garantizar que los mensajes en las aplicaciones no sean alterados.	Establecer políticas de seguridad para las aplicaciones.	NA
12.2.4	Validación de los datos de salida.	SI	Se debe garantizar la correcta funcionalidad de la aplicación al arrojar los datos esperados.	Se deben validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias. ✓ Garantizar la integridad de la información de salida de la aplicación.	Establecer políticas de seguridad para las aplicaciones.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
12.3	**Controles criptográficos**	**Objetivo: proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos**				
12.3.1	Política de uso de los controles criptográficos.	NO	Es necesario contar con políticas de protección de la información al ser entregada al usuario.	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. ✓ Garantizar la confidencialidad de la información.	Establecer políticas de protección de la información.	P
12.3.2	Gestión de claves.	NO	Se debe gestionar adecuadamente las claves como por ejemplo haciendo uso de un PKI (Claves Pública y Privada).	Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la entidad. ✓ Garantizar la gestión adecuada de claves al interior de la empresa.	Establecer políticas de protección de la información.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
12.4	Seguridad de los ficheros del sistema					
12.4.1	Control del software en explotación.	SI	Es necesario controlar la instalación de software de tal manera que responda a las necesidades de la entidad.	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos. ✓ Controlar la instalación de software.	Establecer políticas para la instalación de software	NA
12.4.2	Protección de los datos de prueba del sistema.	SI	Se deberían seleccionar, proteger y controlar cuidadosamente los datos utilizados para las pruebas.	Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse. ✓ Proteger la información empleada en el entorno de pruebas.	Establecer políticas para la protección de códigos fuente y archivos del	NA
12.4.3	Control de acceso al código fuente de los programas.	NO	Se debería restringir el acceso al código fuente de los programas	Se debe restringir el acceso al código fuente de los programas. ✓ Garantizar la protección del código fuente de aplicaciones desarrolladas por la empresa.	Establecer políticas para la protección de códigos fuente y archivos del sistema	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
12.5	**Seguridad en los procesos de desarrollo y soporte**	**Objetivo: mantener la seguridad del software y de la información del sistema de aplicaciones.**				
12.5.1	Procedimiento de control de cambios.	SI	Se debe tener control de versiones de aplicaciones para que los cambios sean realizados conforme a necesidades reales de la entidad.	Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios. ✓ Garantizar que los cambios respondan a procedimientos formales dentro de la entidad	Establecer políticas para garantizar la seguridad de las aplicaciones en desarrollo y funcionamiento.	p
12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	SI	Se debe revisar la funcionalidad de las aplicaciones tras realizar cambios en el Sistema Operativo para no crear conflictos	Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la entidad. ✓ Garantizar que un cambio en el SO no afecte el funcionamiento Aplicaciones	Establecer políticas para garantizar la seguridad de las aplicaciones en desarrollo y funcionamiento	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los	Estado
12.5	**Seguridad en los procesos de desarrollo y soporte**	**Objetivo: mantener la seguridad del software y de la información del sistema de aplicaciones.**				
12.5.3	Restricciones a los cambios en los paquetes de software.	SI	Se debe tener control de cualquier modificación en el software de la entidad.	Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente. ✓ Garantizar el adecuado funcionamiento de las aplicaciones.	Establecer políticas para garantizar la seguridad de las aplicaciones en desarrollo y funcionamiento	NA
12.5.4	Fugas de información.	SI	Se debe garantizar la confidencialidad de la información referente a aplicaciones como programa, base de datos, licencias etc.	Se deben evitar las oportunidades para que se produzca fuga de información. ✓ Garantizarla confidencialidad de la información.	Establecer políticas para garantizar la seguridad de las aplicaciones en desarrollo y funcionamien	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma	Aplicabilidad	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementac	Esta de
12.5	**Seguridad en los procesos de desarrollo y**	**Objetivo: mantener la seguridad del software y de la información del sistema de aplicaciones.**				
12.5.5	Externalización del desarrollo de software.	SI	Si se contrata desarrollo de software a la medida es importante realizar monitorización para evitar incidentes en el manejo.	Se debe realizar monitorización para evitar errores y/o incidentes en el manejo. ✓ Garantizar la monitorización del software que se encuentre en desarrollo.	Establecer políticas para garantizar la seguridad en el desarrollo del software	NA
12.6	**Gestión de las vulnerabilidades técnicas**	**Objetivo: reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.**				
12.6.1	Control de Vulnerabilidades técnicas	SI	Se debe estar verificando constantemente las vulnerabilidades que puedan presentar los sistemas o tecnologías usadas dentro de la Dirección de Sistemas.	Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados. ✓ Garantizar la protección contra vulnerabilidades de los sistemas empleados en la entidad	Definir políticas para la gestión de vulnerabilidades de aplicaciones o sistemas usados por la entidad	p

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los	Estado
13	**Gestión de incidentes de seguridad de la información**					
13.1	**Comunicación de eventos y debilidades en la seguridad de la información**					
13.1.1	Notificación de los eventos de seguridad de la información.	SI	Se deben disponer canales de comunicación que permitan dar a conocer eventos de seguridad que afecten la seguridad de la Dirección de Sistemas.	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible. ✓ Garantizar la pronta solución a eventos de seguridad presentes en la	Definir políticas para la gestión de incidentes de seguridad de la información.	NA
13.1.2	Notificación de puntos débiles de seguridad.	SI	Se deben definir mecanismos para que todas las personas que tengan que ver con el sistema de información puedan reportar incidentes de seguridad.	Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios. ✓ Garantizar la rápida solución de incidentes informáticos.	Definir políticas para la gestión de incidentes de seguridad de la información.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los	Estado
13.2	**Gestión de incidentes y mejoras en la seguridad de la**	**Objetivo: asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.**				
13.2.1	Responsabilidades y procedimientos.	SI	Se debe establecer quién es el responsable de manejar determinado tipo de incidente para que sea mucha más rápida la respuesta.	Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información ✓ Definir responsables para la gestión de eventos de seguridad.	Definir políticas para la gestión de incidentes de seguridad de la información.	NA
13.2.2	Aprendizaje de los incidentes de seguridad de la información.	SI	Se debe poder establecer el costo de un evento de seguridad de la información.	Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información. ✓ Determinarel costo de un evento de seguridad informática.	Definir políticas para la gestión de incidentes de seguridad de la informaci	PI

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
13.2	**Gestión de incidentes y mejoras en la seguridad de la Inf.**	**Objetivo: asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.**				
13.2.3	Recopilación de evidencias.	SI	Se deben tener mecanismos para determinar la forma como se debe actuar contra personas que se les compruebe la generación de eventos de seguridad informática.	Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente. Definir medidas en contra de quienes generen eventos de seguridad informática.	Definir políticas para la gestión de incidentes de seguridad de la información.	P

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
14	**Gestión de continuidad del negocio**					
14.1	**Aspectos de la gestión de continuidad del negocio**	**Objetivo: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.**				
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	SI	Es necesario contar con procesos de seguridad de la información que aseguren la continuidad del negocio al interior de la entidad.	Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad de la entidad. ✓ Contar con procedimientos de seguridad de la información que garanticen la continuidad de la Entidad.	Definir políticas de seguridad de la información que garanticen la continuidad de la entidad.	PI

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
14	**Gestión de continuidad del negocio**					
14.1	**Aspectos de la gestión de continuidad del negocio**	**Objetivo: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.**				
14.1.2	Continuidad del negocio y evaluación de riesgos.	SI	Es necesario tener claridad de los eventos que pueden afectar el negocio y el impacto de los mismos.	Se deben identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información. Determinado. ✓ Tener claridad del grado de afectación sobre el negocio de un evento determinado.	Definir políticas de seguridad de la información que garanticen la continuidad de la entidad.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
14	**Gestión de continuidad del negocio**					
14.1	**Aspectos de la gestión de continuidad del negocio**	**Objetivo: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.**				
14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.	SI	Es muy importante contar con planes de contingencia que permitan la recuperación del negocio ante cualquier evento que ponga en riesgo la información.	Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para la entidad. ✓ Tener planes de contingencia ante eventos informáticos.	Definir políticas de seguridad de la información que garanticen la continuidad del negocio.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
14	**Gestión de continuidad del negocio**					
14.1	**Aspectos de la gestión de continuidad del negocio**	**Objetivo: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.**				
14.1.4	Marco de referencia para la planificación de la continuidad del negocio.	SI	Tener estandarizado el esquema del plan de continuidad para garantizar su fácil aplicabilidad en la entidad.	Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento. ✓ Contar con un plan de continuidad estandarizado	Definir políticas de seguridad de la información que garanticen la continuidad del negocio.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
14	**Gestión de continuidad del negocio**					
14.1	**Aspectos de la gestión de continuidad del negocio**	**Objetivo: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.**				
14.15	Pruebas, mantenimiento y reevaluación de planes de continuidad.	SI	Se deben evaluar los planes de continuidad garantizando que evoluciones con los requerimientos del negocio.	Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia. ✓ Garantizar que los planes de continuidad evolucionen en concordancia con los requerimientos del negocio.	Definir políticas de seguridad de la información que garanticen la continuidad del negocio.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
15	**Conformidad**					
15.1	**Conformidad con los requisitos legales**	**Objetivo: evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.**				
15.1.1	Identificación de la legislación aplicable.	SI	Importante que la entidad sea consciente de sus obligaciones legales para garantizar el cumplimiento de las mismas.	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización. ✓ Distribuir los sistemas de información con los requerimientos legales.	Definir políticas que permitan el cumplimiento del requerimiento de carácter legal por parte de la entidad.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
15	**Conformidad**					
15.1	**Conformidad con los requisitos legales**	**Objetivo: evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.**				
15.12	Derechos de propiedad intelectual (DPI).	SI	Se debe garantizar el uso de cualquier material y/o software de acuerdo a las licencias definidas para los mismos.	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos sobre el uso de productos de software patentados	Definir políticas que permitan el cumplimiento de los requerimientos de carácter legal por parte de la entidad.	NA
15.13	Protección de los documentos de la organización	SI	Se debe garantizar la integridad de los registros importantes para evitar cualquier pérdida de información.	Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio. ✓ Definir mecanismos para garantizar la integridad de los registros importantes de carácter legal.	Definir políticas que permitan el cumplimiento de los requerimientos de carácter legal por parte de la entidad.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los	Estado
15	**Conformidad**					
15.1	**Conformidad con los requisitos legales**	**Objetivo: evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.**				
15.14	Protección de datos y privacidad de la información de carácter personal.	SI	Debe garantizar la protección de los datos en concordancia con requerimientos de carácter legal.	Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato. ✓ Brindar protección de los datos de	Definir políticas de protección de información alineadas con requerimientos de carácter legal.	NA
15.15	Prevención del uso indebido de recursos de tratamiento de la información.	SI	Se debe garantizar que los recursos información sean dedicados sólo para este fin.	Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados. ✓ Garantizar el uso exclusivo de los sistemas de tratamiento de la información para este propósito.	Definir políticas para el manejo de los sistemas de información.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación	Estado
15	**Conformidad**					
15.1	**Conformidad con los requisitos**	**Objetivo: evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.**				
15.16	Regulación de los controles criptográficos.	NO	Los controles deben estar cifrados para asegurar su concordancia con la legislación vigente teniendo en cuenta el tipo de información que se maneja.	Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes. ✓ Garantizarla confidencialidad de los controles de seguridad y su concordancia con la legislación	Definir políticas para el manejo de los sistemas de información.	NA
15.2	**Revisiones de la política de seguridad y de la conformidad técnica**					
15.21	Cumplimiento de las políticas y normas de seguridad.	SI	Cada director de área debe asegurarse de que los procedimientos de seguridad se realicen adecuadamente.	Los directores deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad. ✓ Garantizar la adecuada realización de los procedimientos de seguridad en cada área de la entidad.	Revisar el uso de Procedimientos de seguridad de conformidad con los lineamientos de la entidad y estándares.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controle	Estado
15.2	**Revisiones de la política de seguridad y de la conformidad técnica**					
15.22	Comprobación del cumplimiento técnico.	SI	Es importante que los procedimientos de seguridad estén en concordancia con los estándares definidos para los mismos.	Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad. ✓ Garantizarla alineación entre procedimientos de seguridad y estándares.	Revisar el uso de procedimientos de seguridad de conformidad con los lineamientos de la entidad y estándares.	NA
15.3	**Consideraciones sobre la auditoría de sistemas**	**Objetivo: maximizar la eficacia de los procesos de auditoría de los sistemas de información y minimizar su interferencia.**				
15.31	Controles de auditoria de los sistemas de información	SI	Importante tener control sobre los procedimientos de auditoría desarrollados al interior de la entidad sobre sistemas en funcionamiento.	Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.	Establecer políticas para el desarrollo de procesos de auditoria.	NA

Tabla 56. (Continuación)

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los	Estado
15.3	**Consideraciones sobre la auditoría de sistemas**					
15.32	Protección de las herramientas de auditoria de los sistemas de información	SI	Se deben tener control sobre el acceso a herramientas de auditoría ya que muchas pueden comprometer la seguridad al interior de la entidad.	Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro. ✓ Evitar el uso inadecuado de herramientas de auditoría.	Establecer políticas para el desarrollo de procesos de auditoria.	NA

Fuente: El Autor

9. DISEÑO DEL SISTEMA DE GESTION

9.1. Alcance e Importancia

El presente documento establece la Política de Seguridad de la Información únicamente de la Dirección de Sistemas de la Gobernación de Boyacá para ayudar a lograr los objetivos Institucionales de la Entidad.

El departamento de la Dirección de Sistemas administrativamente depende de la Secretaria General, en donde juega un papel importante como es el de brindar un servicio público de calidad, con soporte tecnológico en toda la Entidad, por esta razón es de gran importancia llevar a cabo cada una de las políticas en donde su objetivo principal es cumplir a cabalidad las Políticas de Seguridad de la Información establecidas en este documento:

9.2. Propósito

La Dirección de Sistemas de la Gobernación de Boyacá se comprometerá a la protección de la información de la Seguridad Informática en donde se proteja: Confidencialidad, Integridad, Disponibilidad de la Información, también su infraestructura como son cada uno de sus activos en donde se garantice la revisión y verificación de todos los requerimientos que lleva a cabo la Entidad o lo que necesite.

10. Políticas de Seguridad de la Información para la Dirección de Sistemas de la Gobernación de Boyacá.

Generalidades: Establecer las políticas de seguridad de información para el uso de Tecnologías de Información y comunicación de la Dirección de Sistemas de la Gobernación de Boyacá, donde se denote lo siguiente: Objetivos organizacionales en donde se proteja los activos de información, responsabilidades y los derechos que se deben conocer y cumplir los funcionarios internos y externos, propietarios y administradores de la infraestructura tecnológica para lograr que los recursos tecnológicos de la entidad presten su servicio de manera accesible, confiable y oportuna.

Objetivo: La política de seguridad de la Información es la declaración general que representa la posición de la administración de la Gobernación de Boyacá con respecto

a la protección de los activos de información (funcionarios, la información, los procesos, las tecnologías de información incluido el hardware y el software), a la implementación del Sistema de Gestión de Seguridad de la Información y el apoyo, generación y publicación de sus políticas, procedimientos e instructivos. Esto ayuda a propender para que la información de la entidad se provea con requerimientos de confidencialidad, integridad y disponibilidad.

La seguridad de la información es un esfuerzo de equipo. Se requiere la participación y apoyo de todos los miembros de la organización que trabajan con sistemas de información o utilizan la Infraestructura Tecnológica de la Gobernación de Boyacá, es decir, que las políticas aplican a todos los funcionarios públicos, contratistas, proveedores y demás usuarios internos y externos de la infraestructura tecnológica de la entidad.

Todos los usuarios contarán con un documento que incluye los requisitos de la política de seguridad de la información y otra documentación relacionada. Quienes deliberadamente o por negligencia infrinjan las políticas de seguridad de la información estarán sujetos a acción disciplinaria.

Esta política se aplica a toda la infraestructura tecnológica (tal como hardware, software y redes de datos) y a todos los activos de información operados por los funcionarios y otros usuarios de la Gobernación de Boyacá que hacen uso de esta infraestructura. Se incluyen también aquellos equipos de cómputo personales que no son propiedad de la entidad pero que están al servicio de la misma y afectan la red de datos interna.

Se tiene como meta concientizar a los usuarios de la necesidad del buen uso de la las Tecnologías de la Información y Comunicación de la Gobernación de Boyacá, presentando y dando a conocer las responsabilidades y las medidas que se deben adoptar para proteger la infraestructura tecnológica y evitar pérdidas y/o divulgación no autorizada.

La gestión de Tecnología de Información y Comunicación de la Gobernación de Boyacá propone esfuerzos de seguridad de la información a través de la Dirección de Sistemas con el proceso de Gestión de NTICs (Nuevas Tecnologías de la Información y la Comunicación) para la implementación de la política de seguridad de la información y de uso de la Infraestructura de Tecnología de Información y Comunicación.

Alcance*:* Esta política se debe aplicar a todos los procesos y dependencias relacionados con la Dirección de Sistemas de la Gobernación de Boyacá.

Responsables: Director de Sistemas de la Gobernación de Boyacá y posteriormente los funcionarios de planta, Secretarios, Directores o funcionarios de las dependencias y finalmente por contratistas internos y externos.

Cumplimiento: Su objetivo es hacer cumplir las políticas de seguridad anteriormente establecidas y hacer cumplir las obligaciones establecidas por las leyes, el reglamento, los contratos e imponer sanciones por incumplimiento de las mismas.

10.1. Funciones y Responsabilidades

A fin de coordinar los esfuerzos de seguridad de la información, la Gobernación de Boyacá ha dividido las responsabilidades de sus miembros en las siguientes categorías de responsabilidad:

Responsabilidades del Propietario

- Los propietarios de los activos de información son en general los Secretarios, Directores o funcionarios asignados por la Gobernación de Boyacá, quienes adquirieren y mantienen las aplicaciones operativas que apoyan la toma de decisiones y otras actividades de la organización.

- Los propietarios deben indicar la clasificación que mejor refleja el carácter sensible, el valor crítico y la disponibilidad de cada tipo de información. La clasificación, a su vez, determinará el nivel de acceso de los usuarios.

Responsabilidades del Usuario

Todo el personal que maneja activos de información e infraestructura tecnológica tiene la denominación de usuario y tiene las siguientes responsabilidades:

- Almacenamiento de información de la Entidad, de custodiar la información confiada, de usar el sistema de control de acceso lógico y ejecutar periódicamente copias de seguridad.

- Aplicación, mantenimiento y revisión las medidas de seguridad definidas por los dueños de la información.

- Aplicación las políticas de seguridad de la información, normas, procedimientos y legislación aplicable. Deben comprender perfectamente estos requisitos y cumplir con ellos

- Actualización de la información de registro de inventario de activos
- Identificación del nivel de clasificación de los activos de información.
- Aplicación de los controles apropiados para asegurar la confidencialidad, integridad y disponibilidad de la información.
- Aplicación de medidas de seguridad para garantizar su cumplimiento y reporte de situaciones de incumplimiento

Responsabilidades de los Administradores de Información y de recursos TI

El personal de la Dirección de Sistemas son administradores de sistemas y tienen responsabilidad sobre la administración de la información.

Los administradores de información son los servidores públicos que están encargados de la custodia de la información de la Entidad que generalmente se encuentra centralizada en equipos servidores.

Los Administradores de Información son responsables de usar el sistema de control de acceso, y de ejecutar plan de continuidad y contingencia de TI, lo que incluye: copias de seguridad de las bases de datos alojadas en equipos servidores.

Los Administradores están facultados para depurar datos e información electrónica según tipo y clasificación. El personal de la Dirección de Sistemas está facultado para tomar instantáneas del sistema, reconfigurar, reiniciar, apagar y restaurar cada equipo de cómputo de la Entidad con fines de eficacia en la recuperación del sistema para retornarlo a un estado funcional, y de eficiencia energética.

10.2. *Organización de la Seguridad de la Información*

Generalidades: Establecer la seguridad de la información con uno de los objetos vitales de la Dirección de Sistemas.

Objetivo*:* Organizar, controlar y administrar la información dentro de la entidad.

Alcance: Esta política se debe aplicar a todos los procesos de la Dirección de Sistemas de la Gobernación de Boyacá tanto internos como externos.

Responsables: La responsabilidad de la organización de seguridad de la información es el Director de Sistemas, seguida por los funcionarios de planta de la Dirección.

Responsable del Área de Informática y de la seguridad informática: Se encargará de dirigir las políticas de seguridad con la asesoría de profesionales especializados, e implementar medidas de seguridad como la restricción del acceso a la información que sea catalogada como confidencial.

Responsable del área de Administración: Se encarga de destinar y disponer de recursos necesario para la adquisición de elementos necesarios para el cumplimiento de dichas políticas (Hardware, software, elementos de logística, asesoría especializada)

10.3. Políticas de Operación

10.3.1. POLÍTICA 1: Control de Acceso a la Información y a las Aplicaciones.

Generalidades*:* Todos los funcionarios públicos, contratistas, proveedores y demás usuarios de la Infraestructura de Tecnología de Información y Comunicación de la Gobernación de Boyacá pueden tener acceso sólo a la información necesaria y suficiente para el desarrollo de sus actividades. El otorgamiento de acceso a la información está regulado por niveles de accesibilidad que define el Director Administrativo de Sistemas de la Gobernación de Boyacá.

Objetivo: Controlar el acceso a la Información y Aplicaciones

Alcance: Esta política se debe aplicar a todos los procesos de la Dirección de Sistemas de la Gobernación de Boyacá.

Responsables: Los usuarios externos de la Gobernación de Boyacá, que requieran ingresar a los sistemas de información de la entidad, deberán contar con el visto bueno del Director del área de interés, así como la autorización del Director de Sistemas.

Políticas:

Toda vez que algún trabajador deje de prestar sus servicios a la Entidad, debe asegurar la entrega total de la información que gestionó durante el ejercicio de sus funciones. Una vez retirados se obligan a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la Entidad, por el periodo establecido en la normatividad aprobada de retención documental por la Gobernación de Boyacá.

Todas las prerrogativas para el uso de los sistemas de información de la Gobernación de Boyacá terminan inmediatamente después de que el trabajador cesa de prestar sus servicios a la Entidad. Para el cumplimiento de esta directriz, cada uno de los Directores de las Secretarías o Dependencias está obligado a solicitar la desactivación de cuentas de acceso (especificando los sistemas en los que se tenía uso) a la Dirección de Sistemas a través de los canales dispuestos para tal fin. El director que no cumpla esta política se responsabiliza de las acciones que se generen por la omisión.

Mediante el monitoreo de registros automáticos de eventos en las diversas plataformas tecnológicas se efectuará seguimiento a los accesos realizados por los usuarios a la información y recursos de TI de la Entidad, con el objeto de minimizar riesgos tecnológicos de la información. Cuando se presenten eventos que pongan en riesgo la integridad, disponibilidad, confiabilidad, confidencialidad, eficiencia y/o efectividad de la información, se deberán documentar y realizar las acciones tendientes a su solución.

Todas las Tecnologías de Información y Comunicación (equipos de cómputo, software del sistema, software de aplicaciones, bases de datos, etc) deben contar con mecanismos de identificación, autenticación y roles de privilegios de usuario apropiados según la clase de información y el tratamiento que se autorice a la misma.

Las identificaciones de usuario deben individualizar a usuarios específicos y ser utilizada con el fin de permitir el acceso al sistema de acuerdo a las funciones, responsabilidades y actividades de dichos usuarios.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y claves personales.

El nivel de Superusuario de cada uno de los sistemas críticos deberá tener un control dual, de tal forma que exista una conciliación de las actividades realizadas en el sistema por otro administrador. No se debe crear o disponer de cuentas de Superusuario por más de dos Administradores para cada Sistema de Información, debido a que el control se perdería.

Todos los equipos servidores deberán tener controles de acceso para garantizar la integridad y disponibilidad de la información y de los Sistemas de información controlados y almacenados en dichos equipos.

Antes que un nuevo sistema de información se desarrolle o se adquiera por parte de la Gobernación de Boyacá, la Dirección de Sistemas deberá definir las especificaciones y requerimientos de seguridad necesarios para su implementación.

La seguridad en el acceso a las aplicaciones debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño de sistemas hasta la conversión a un sistema en producción.

Directriz de Contraseñas para Acceso a la Información y a las Aplicaciones

La autenticación (clave o contraseña), para el acceso a un sistema o recurso informático, debe ser definida por el usuario de las Tecnologías de Información de la Gobernación de Boyacá, y es considerada como un dato sensible, y es el usuario quien tiene la responsabilidad exclusiva de manejarla, no divulgarla, ni compartida.

Al establecer la contraseña para acceso a un sistema ésta debe ser fácil de recordar para el usuario pero difícil de adivinar por un extraño; no utilizar palabras únicas que se encuentren en un diccionario o que se refieran a datos personales o familiares; no utilizar solo números; se deben combinar caracteres alfanuméricos; y como mínimo debe tener una longitud de ocho (8) caracteres; la contraseña debe modificarse a intervalos regulares, preferiblemente cada 180 días o menos para el caso de aquellos sistemas que no exijan un cambio periódico obligado.

Las contraseñas no deberán ser almacenadas en ningún formato legible en archivos desprotegidos, almacenados en lugares o carpetas donde las personas no autorizadas puedan encontrarlas. Las contraseñas en ningún momento deberán estar escritas y a la vista, como en monitores de computadoras y escritorios.

Si un usuario tiene acceso a varios sistemas de información, estará obligado a definir una contraseña diferente para cada uno.

10.4. POLÍTICA 2: Escritorio Limpio y Pantalla Limpia

Generalidades: Con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo se ha establecido que no deben colocarse medios de almacenamiento (CDs, DVDs, cintas, memorias USB) ni documentos físicos sobre el escritorio o puesto de trabajo, estos deberán quedar bajo llave en gabinetes o en archivadores seguros. Todos los equipos de cómputo y las impresoras de la entidad se deberán apagar o poner en estado de suspensión cuando no estén en uso; además, limpiar las impresoras de documentos. Cuando el usuario se retira de su puesto de trabajo, bloquear el equipo (instrucción: ⊞ + L). Los equipos de escritorio estarán obligados a utilizar protector de pantalla

protegido con contraseña para que el bloqueo sea automático después de unos minutos de inactividad (entre tres y cinco minutos es razonable).

Objetivo: Reducir los riesgos de acceso no autorizado.

Alcance: Esta política se debe aplicar a todos los activos de la organización.

Responsables de los Equipos*:* Son los funcionarios de la Dirección de Sistemas los encargados de mantener limpios los escritorios y pantallas.

Política

Los equipos de escritorio estarán obligados a utilizar protector de pantalla protegido con contraseña para que el bloqueo sea automático después de unos minutos de inactividad (entre tres y cinco minutos es razonable).

10.5. POLÍTICA 3: Gestión de Activos

Generalidades: Una vez realizado el inventario de activos y la evaluación de riesgos se clasifican los activos de acuerdo a su sensibilidad y vulnerabilidad.

Objetivo*:* Clasificar la información de acuerdo a su grado de confidencialidad, definir niveles de protección y garantizar que los activos de la organización sean protegidos de manera adecuada.

Alcance: Esta política se debe aplicar a todos los activos de la organización. Responsables: La responsabilidad de la seguridad de la información está en manos de:

Responsables de la Información: Son los encargados de clasificar la información de acuerdo a su grado de confidencialidad, mantener actualizada y documentada la clasificación y de definir los permisos de acceso a los usuarios.

Política

Inventario de Activos*:* Se realiza un inventario de activos los cuales debe estar debidamente clasificados y ordenados según su importancia, propietario, ubicación e información almacenada, este inventario debe ser actualizado constantemente y conservarse de manera ordenada.

10.6 POLÍTICA 4: Seguridad de los Recursos Humanos

Generalidades: Es fundamental educar y concienciar al personal sobre la importancia de la aplicación de las políticas de seguridad, desde el primer instante que se ingresa a la empresa y de las sanciones que conlleva el incumplimiento de las mismas. Por lo tanto, es importante que el personal este consiente de la importancia, este capacitado y en caso de ocurrir un incidente informar en qué condiciones ocurrió para establecer mecanismos que conduzcan a que dichas fallas o incidentes no vuelvan a ocurrir y establecer los correctivos necesarios.

Objetivo: Minimizar los riesgos ocasionados por errores humanos y promover un uso adecuado de los recursos informáticos, así como capacitar y concienciar sobre la importancia de la aplicación de las políticas de seguridad e información oportuna de incidentes para ser corregidos en debida forma.

Alcance: Esta política se debe aplicar a todo el personal de la organización, interno y externo de la Gobernación de Boyacá.

Responsables:

El personal de recursos humanos que es el encargado de seleccionar el personal, informara, capacitara y establecerá acuerdos de confidencialidad y de cumplimiento de todas las políticas de seguridad con el personal que ingrese a la empresa.

Responsable de la seguridad informática: Se encargará de capacitar y concienciar al personal con asesoría de profesionales especializados, sobre el uso correcto de los recursos informáticos y el cumplimiento de las políticas de seguridad, así como del acuerdo de confidencialidad.

Política

Antes de la contratación Laboral: La entidad antes de la contratación laboral debe documentar los roles y responsabilidades que estos van a desempeñar.

En la selección del personal se debe revisar antecedentes (hoja de vida, experiencia laboral, experiencia crediticia etc.). Se debe seleccionar y clasificar que información va estar disponible para estos tanto para personal como para terceros.

Términos y condiciones laborales*:* Tanto para empleados como para terceros estos deben conocer los términos y las condiciones del contrato laboral haciendo énfasis en los aspectos relativos a la seguridad, la confidencialidad y se debe verificar que los contratos estén firmados. (El contrato debe contener, derechos, deberes, responsabilidades, estar de acuerdo a la ley y posibles sanciones por incumplimiento).

Durante la Vigencia del contrato: La dirección debe exigir que los empleados y terceras partes cumplan a cabalidad con las políticas de seguridad establecidas por la empresa. Para esto debe darles a conocer las políticas de seguridad, motivarlos y verificar que estén de acuerdo con los términos y condiciones establecidas en el contrato laboral.

Capacitación y formación: La Dirección de Sistemas capacitara e informara sobre las políticas de seguridad establecidas en la organización, así mismo capacitara e informara cuando se presenten cambios y modificaciones.

El funcionario debe someterse a*:* Cumplir con el control y la política de seguridad, formar y cumplir el compromiso de confidencialidad, cumplir los términos y condiciones del contrato, capacitarse, comunicar sobre incidentes y anomalías.

Para el personal y terceras partes que violen o incumplan las políticas de seguridad se llevara a cabo un proceso disciplinario de acuerdo a los estatutos de la Gobernación de Boyacá

Terminación o Cambio del contrato laboral: La entidad gestiona de manera adecuada la terminación del contrato o cambio de contrato y una vez terminado el contrato verifica la suspensión de los servicios, la devolución de los activos, devolución de documentos, dispositivos (equipos de escritorios, portátiles, celulares, usb etc), verifica y gestiona el cambio de contraseñas. Los responsables de realizar estos procesos son el responsable de seguridad y el Departamento de Recursos Humanos y Sistemas.

10.7 POLÍTICA 5: Seguridad Física y del Entono

Generalidades*:* Para la seguridad física se deben tener en cuenta: Protección física de acceso, protección y mantenimiento de equipos de acuerdo a su importancia, los

posibles daños e interferencias; El mantenimiento de las instalaciones se debe hacer bajo estrictas normas de seguridad.

Objetivo*:* Evitar el daño, interferencias y el acceso no autorizado a la información de la Gobernación de Boyacá.

Alcance: Esta política se debe aplicar las instalaciones de Dirección de Sistemas y todos sus equipos, cableados, entre otros.

Responsables:

Responsable de la seguridad informática*:* Este se encargará de dirigir las políticas a seguir mantenimiento.

El Responsable del Área informática: Se encargará de adoptar todas las políticas establecidas por el responsable de la seguridad y verificará el cumplimiento de las mismas.

Política

Perímetro de Seguridad Física: Servidores y almacenamiento de información confidencial) y se deben adoptar las siguientes medidas:

- ✓ Definir claramente el perímetro de seguridad
- ✓ Establecer barreras de seguridad
- ✓ Definir el personal autorizado para el acceso al área restringida.

Controles de Acceso Físico: El responsable de la seguridad junto con el responsable de la Dirección de Sistemas establecerán controles:

- ✓ Limitar el acceso al área donde se encuentra almacena la información, llevar un registro solo del personal autorizado.
- ✓ Verificar que el personal que ingrese porte un documento visible que lo catalogue como personal autorizado.
- ✓ Revisar periódicamente los registros del personal que accede.
- ✓ Actualizar constantemente la lista de personal autorizado.

Seguridad de Oficinas e instalaciones: Se debe tener en cuenta las condiciones de iluminación ventilación salubridad, equipamiento antiincendios, medidas que prevengan inundaciones robos etc.

Ubicación y protección de copias de seguridad y equipamiento: El equipamiento se ubicará en un sitio donde se minimice el riesgo, un sitio protegido tanto de amenazas naturales ambientales, físicas y humanas, adicional a esta medida se restringirá el acceso. Por lo tanto, solo podrá acceder personal autorizado con su credencial y los ingresos y tareas a realizar serán debidamente documentadas por el responsable de la seguridad; las labores de aseo serán verificadas para evitar daños y hurtos.

Suministro de Energía: Periódicamente se deben revisar el buen funcionamiento de las instalaciones eléctricas para evitar incidentes, la organización debe optar por contrarrestar fallas en el suministro de energía tales como la adquisición de una planta eléctrica, la compra de ups para los pc etc.

Seguridad en el Cableado: Proteger el cableado que transporta datos de daños e interceptación cumpliendo con las normas.

Mantenimiento de Equipos: Los responsables de la Dirección de Sistemas deben someter todos los equipos periódicamente e mantenimiento preventivo y correctivo, este mantenimiento debe ser registrado y documentado (hojas de vida) Plataforma GLPI Mesa de Ayuda, cada equipo debe tener un inventario de dispositivos para saber qué cambio se hicieron y que dispositivos se retiraron.

Seguridad en la reutilización o eliminación de equipos: Cuando un equipo es cambiado de sitio o eliminado se debe tener total precaución con los dispositivos de almacenamiento como discos duros los cuales deben ser formateados o destruidos de forma segura para evitar incidentes con la información.

10.8. POLÍTICA 6: Copias de Seguridad de Archivo de Datos y Retención de Copias de Seguridad

Generalidades: En los sistemas de archivo electrónico implementados, se debe garantizar la autenticidad, integridad, confidencialidad y la conservación a largo plazo de los documentos electrónicos de archivo que de acuerdo con las Tablas de Retención Documental o las Tablas de Valoración Documental lo ameriten, así como su disponibilidad, legibilidad (visualización) e interpretación, independientemente de las tecnologías utilizadas en la creación y almacenamiento de los documentos (Art. 18 Decreto 2609 de 2012).

Objetivo: Las copias de seguridad (Backup) de la información y documentos en ambientes electrónicos generadas en la Gobernación de Boyacá tienen el propósito de preservar y retener datos por un periodo de tiempo determinado para garantizar la autenticidad, integridad, confidencialidad y conservación.

Alcance: Se debe realizar copias de seguridad de los documentos de archivo, bases de datos y de la información más relevante de acuerdo a los tipos de información producida señalados en el Decreto 2609 de 2012, y la clasificación de la información identificada en instrumentos de recolección de información señalados en la ley 1712 de 2014, la cual será almacenada en discos o medios de propiedad de la Entidad. Cada sectorial o área dueña de la información es responsable de definir e informar a la Dirección de Sistemas cuál es la información que se encuentra y se protege en computadores de escritorio (clientes gruesos) y que no se encuentra en equipos Servidores, para proceder al seguimiento de la realización de copias de seguridad periódicas atendiendo a lo establecido en el Plan de Continuidad del negocio de la Gobernación de Boyacá.

Responsables: Los funcionarios públicos y contratistas son los encargados de los respaldos de la información que generan en los equipos que tengan asignados; deberán velar por la integridad y disponibilidad de la información que manejen, especialmente si dicha información está protegida por reserva legal o ha sido definida como clasificada o reservada.

En el Centro de Procesamiento de Datos (CPD) donde permanecen los Servidores de la Gobernación de Boyacá se deberán generar copias de seguridad (backups) periódicas de la información que ha sido almacenada a través de las aplicaciones que procesan información en las bases de datos y bodegas de datos, o a través de clientes que tienen allí carpetas de usuario remoto; los backups se realizarán de acuerdo a las políticas de continuidad y recuperación, al plan de Continuidad del Negocio y Recuperación de Desastres definido por la Dirección de Sistemas y al instructivo de Administración de Recursos de almacenamiento de información.

Se establecerá el procedimiento de copia de seguridad y de recuperación de la información debidamente documentado, se definirá la extensión, frecuencia y periodo de retención de las copias de seguridad de conformidad con los requisitos de seguridad de la información y la importancia de la información para el funcionamiento continuo de la entidad.

Las copias de seguridad deberán tener un nivel adecuado de protección tanto físico como ambiental junto con los controles respectivos y los medios o soportes deben verificarse periódicamente para asegurar que pueden responder efectivamente en caso de ser requerida la recuperación de la información.

Se establecerá periodo de retención de la información almacenada en medios o soportes de almacenamiento magnético, óptico o unidades de estado sólido, y su disposición final según las Tablas de Retención documental (TRD) de la Entidad.

Adicionalmente y por seguridad de la información, deberá establecerse procedimiento para la gestión de los soportes extraíbles, que aseguren la protección de la información.

10.9. POLÍTICA 7: Uso Aceptable para Correo Electrónico y Otros Servicios de Internet

Generalidades: Para garantizar la integridad y confidencialidad de los servicios de correo electrónico, sus redes, instalaciones y datos, los funcionarios y demás usuarios que utilizan el servicio de correo electrónico institucional, servicios de correo de servidores gratuitos y de otros servicios de Internet deben aceptar y cumplir los siguientes lineamientos:

Objetivos: El intercambio electrónico de información se realizará con base en estándares de documentos electrónicos y mensajes de datos de dominio público, regidas por organismos idóneos de carácter nacional e internacionales, y en algunos casos utilizando mecanismos criptográficos de clave pública y firma digital, especialmente en el caso de la información sensible.

Alcance: Las comunicaciones oficiales por parte de los funcionarios públicos deben ser enviadas y recibidas a través de la dirección de correo electrónico institucional proporcionada por la Dirección de Sistemas. Las cuentas personales de correo electrónico no pueden ser usadas para tal fin.

Responsables:

- Los funcionarios públicos, contratistas y demás usuarios no deben utilizar versiones escaneadas de firmas hechas a mano para aparentar que un mensaje de correo o cualquier otro tipo de comunicación electrónica fue firmado por el remitente. Se debe utilizar una firma estándar de texto que se compone de nombres y apellidos, cargo, dirección y número de teléfono.

Políticas:

- Cuando se envíe un correo electrónico a múltiples destinatarios, se deberá ocultar los destinatarios utilizando el apartado CCO (con copia oculta) para evitar la revelación de sus direcciones, especialmente cuando va dirigido a ciudadanos o personas externas. Así mismo, se deberá ingresar las direcciones de correo institucional a la lista de contactos.
- No violar las normas del proveedor del servicio de correo electrónico.

- El funcionario o tercero es responsable de todos los contenidos que se transmiten, reciben y almacenan a través del uso del cliente de servicio de correo electrónico; la Dirección de Sistemas de la Gobernación de Boyacá no se hace responsable por el contenido almacenado en los buzones o por el contenido de paso en la red.

- El sistema de correo electrónico, el servicio de comunicación instantánea, y el servicio de Internet, deben ser usados únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades establecidas.

- El servicio de correo electrónico institucional puede ser retirado a un usuario o su cuenta desactivada en cualquier momento, a discreción de la Administración, si se observa un uso indebido o un alto porcentaje de recepción de mensajes spam.

- Periódicamente el administrador de cuentas revisará las cuentas que llevan más de 60 días sin ningún acceso. En caso tal, se procederá a enviar una comunicación de dichas cuentas sin uso advirtiendo del proceso de desactivación y se darán 30 días adicionales a partir de la fecha de la comunicación para la utilización de las cuentas. Vencidos los 30 días, de no presentarse uso o de no haber recibido la solicitud de no desactivación, se procederá a la desactivación y se entenderá que el usuario ya ha sido comunicado.

- Cuando un funcionario, al que le haya sido autorizado el uso de una cuenta de correo electrónico, se retire de la entidad su cuenta de correo será desactivada.

- Las cuentas de correos que permanezcan con estado desactivado se conservarán por el término de un (1) año, después de ese lapso de tiempo se realizará el proceso de eliminación.

- La clave o contraseña de acceso que se defina por el usuario de correo electrónico

deberá cumplir con la Directriz de contraseñas para acceso a la información y a las aplicaciones definida en la política de control de acceso.

10.10. POLÍTICA 8: Administración de Cambios

Generalidades: Para la administración de cambios de las Tecnologías de Información y Comunicación se efectuará el procedimiento correspondiente definido por la Dirección de Sistemas de la Gobernación de Boyacá, de acuerdo con el tipo de cambio solicitado y la infraestructura tecnológica relacionada.

Objetivo: Todo cambio (creación y modificación de programas, pantallas y reportes) que se necesite a las aplicaciones informáticas, debe ser requerido por los usuarios de la información mediante el formato “requerimientos para investigación y desarrollo” y deberá ser aprobado formalmente por la Dirección de sistemas.

Alcance: Esta política se debe aplicar a todo el personal de la Dirección de Sistemas de la Gobernación de Boyacá.

Responsables: Los responsables de la administración de las aplicaciones tendrán la facultad de aceptar o rechazar la solicitud, bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por el usuario, o un tercero externo.

Políticas:

- Cualquier cambio que se requiera en los equipos de cómputo de la Gobernación de Boyacá (repotenciación o reparación) se debe evaluar técnicamente y ser autorizado por la Dirección de Sistemas.
- La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal de la Dirección de Sistemas; y se registrará el cambio de repuesto o reparación en la hoja de vida del equipo.

- Los equipos de cómputo: Desktop (cliente grueso), Servidores, Thin Client (cliente liviano), Workstation; las impresoras no deben moverse o reubicarse sin la aprobación previa del Director de Sistemas, jefe o coordinador del área involucrada.

- Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de manera acorde a los requisitos de seguridad existentes y autorizados por la Dirección de Sistemas.

- Cualquier tipo de cambio en la plataforma tecnológica debe ser documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

10.11. POLÍTICA 9: Seguridad en Telecomunicaciones y Servicios Asociados

Generalidades: Es indispensable que la Dirección de Sistemas disponga de direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser consideradas y tratadas como información sensible.

Objetivo: Asegurar el funcionamiento continuo de la entidad.

Alcance: Esta política se debe aplicar a todos los procesos críticos y prioritarios de Gobernación de Boyacá.

Responsables: Se encarga de dirigir normas y procedimientos para implementar Sistemas operativos, Gateway, firewall, servicios de red etc., debe verificar que todos estos dispositivos y servicios queden debidamente configurados, debe realizar pruebas de escaneo, monitoreo para evitar intromisión. Además, debe promover y realizar la gestión de contraseñas y privilegios, capacitar y concientizar a los usuarios de la utilización de las medidas de control de acceso.

Políticas:

- La red de cobertura geográfica local debe estar dividida en forma lógica por diferentes segmentos de red, cada uno separado con controles de seguridad perimetral y mecanismos de control de acceso, a través del Firewall.
- Todas las conexiones de redes externas de tiempo real que accedan a la red interna, deberán pasar a través del sistema de defensa electrónica con tecnologías: Sistema

de Prevención de Intrusos (IPS), Firewall, Filtro de contenido o de Red Privada Virtual (VPN), anti-virus y anti-spyware, y de control de aplicaciones.

- Los servidores de aplicaciones y servidores Web internos tendrán configuraciones para la protección de tráfico, en cuanto a amenazas ocultas, con tecnologías como la de cifrado SSL.
- El servicio de acceso a Internet se deberá prestar con restricciones de acuerdo a políticas de Firewall definidas para proporcionar una conectividad confiable y controlar ataques informáticos por la red. Un filtrado web ayudará a proteger contra las amenazas basadas en Web impidiendo que los usuarios accedan a sitios de phishing conocidos y fuentes de software malicioso (malware).
- El servicio de acceso a Internet puede ser retirado en cualquier momento, a discreción de la Administración, si se observa un uso indebido o un bajo rendimiento del Servidor, para dar espacio a procesos que tengan mayor prioridad o mayor relevancia.
- El servicio de acceso a la Intranet por el portal de la Gobernación en Internet se prestará con restricciones de acuerdo a políticas de Firewall definidas para proporcionar una conectividad confiable y controlar ataques informáticos por la red.
- Los funcionarios públicos se obligan a NO utilizar la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras, o cualquier equipo que genere caída de la energía.

10.12. POLÍTICA 10: Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

Generalidades: Se debe documentar y aprobar los requerimientos de seguridad a aplicar en la implementación de los sistemas de información; se debe llevar a cabo adecuadas políticas de seguridad para las bases de datos, los sistemas operativos, todo esto con el fin de evitar que personas conocedoras de los procesos puedan cometer fraudes o ilícitos y si es el caso identificarlos de manera inmediata.

Objetivo: Adoptar medidas de seguridad en la implementación de los sistemas de información.

Alcance: Esta política se debe aplicar a todos los sistemas informáticos tanto sistemas operativos como software requerido para la entidad.

Responsables:

El Responsable del Área informática se encargará de definir el procedimiento para asignar claves, de garantizar el cumplimiento de los requisitos de seguridad del software, de controlar los cambios en los sistemas etc.

Política

- ✓ **Análisis y especificaciones de los requerimientos de seguridad:** Identificar y definir los requerimientos y controles necesarios en materia seguridad desde las etapas de análisis y diseño del sistema ya que implementar medidas de seguridad desde estas etapas sale menos costoso que hacerlo después.

- ✓ **Seguridad en los sistemas de aplicaciones:** Se debe establecer controles del registro de auditoria para evitar la pérdida de los datos de los sistemas de información (validación y autenticación de los datos de entrada y de salida)

- ✓ **Validación de datos de entrada:** Se debe establecer un control de validación de los datos de entrada como: Revisión periódica de contenidos.

10.13. POLÍTICA 11: Controles Criptográficos

Política controles criptográficos: Se debe utilizar controles criptográficos para los siguientes casos: Protección de claves de acceso a sistemas, datos y servicios, transmisión de información clasificada, resguardo de información. El responsable de la seguridad se encargará de definir la política de controles criptográficos, el método y el responsable de administración de claves (Uso de algoritmo de cifrado y firma digital, servicios de no repudio)

Seguridad de los procesos de soporte

Procedimiento de control de cambios: Verificar que los cambios sean propuestos por personal autorizado, mantener un registro del nivel de autorización, identificar todos los elementos que requieren modificaciones, obtener aprobación por parte del responsable del área de informática para cumplir con los requerimientos del software.

Canales ocultos y código malicioso: Se debe adquirir software a personal confiable y conocido, examinar códigos fuentes que estén libres de virus, llevar un control de acceso al software y las modificaciones instaladas, utilizar antivirus y software de monitoreo y escaneo de campos claves, se debe establecer como se realizará y con qué método, además se definirá las responsabilidades del personal.

10.14 POLÍTICA 12: Seguridad para Usuarios Terceros

Generalidades: Una vez contratados servicios de TI por outsourcing deberán negociarse y aclararse, dentro del contrato, las políticas y procedimientos para asegurar que los objetivos de seguridad del Sistema se sigan cumpliendo: efectividad, eficiencia, adecuación, integridad, validez, autorización y privacidad.

Objetivo: Adoptar medidas de seguridad para usuarios terceros.

Alcance: Esta política la deben cumplir todos los funcionarios internos y externos de la Gobernación de Boyacá.

Responsable: La Dirección de Sistemas debe concientizar y capacitar a los funcionarios de la Gobernación de Boyacá para que estén atentos a eventos sospechosos y en caso de presentarse los reporten de inmediato.

Políticas:

- Los recursos informáticos que no sean propiedad de la Entidad y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento.
- Cuando se requiera utilizar las Tecnologías de Información y Comunicación de la Gobernación de Boyacá para el funcionamiento o el alojamiento de elementos tecnológicos que no sean propios de la entidad y que deban ubicarse en sus instalaciones serán administrados por la Dirección de Sistemas de la Gobernación de Boyacá.
- Los usuarios contratistas o terceros, tendrán acceso a los Recursos Informáticos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien sea su Jefe inmediato, Interventor o Supervisor.
- Los contratistas deberán firmar y renovar dentro de cada contrato, un acuerdo de buen uso de los Recursos Informáticos, confidencialidad y no divulgación de la información sensible y de la información de carácter personal del ciudadano; en cumplimiento de la seguridad y buen manejo de la información. Después de que el

trabajador deja de prestar sus servicios a la Entidad, está obligado a entregar toda la información respectiva del trabajo realizado se debe comprometer a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la Entidad.

- La conexión entre sistemas de información internos y otros de terceros, debe ser aprobada y certificada por la Dirección de Sistemas con el fin de no comprometer la seguridad de la información interna de la entidad.
- Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad informática vigentes en la Entidad y deben estar registrados ante la Dirección de Sistemas.
- Como requisito para interconectar las redes de la entidad con las de terceros, los sistemas de comunicación de terceros deben cumplir con las políticas de seguridad establecidas por la Gobernación de Boyacá. La Gobernación de Boyacá se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La entidad se reserva el derecho de cerrar o inactivar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos.
- El personal no deberá suministrar información de la entidad a ningún ente externo sin las autorizaciones respectivas de la Dirección de Sistemas y la dependencia interesada.
- Los proveedores y/o terceros que sean autorizados para ingresar a las redes o a los Sistemas de Información de la Gobernación de Boyacá, solamente pueden tener privilegios de acceso a los recursos informáticos durante el periodo de tiempo necesario determinado para llevar a cabo las funciones a su cargo.

10.15. POLÍTICA 13: Propiedad Intelectual y Administración de Licencias de Software

Generalidades: Todo software que utilice la Gobernación de Boyacá será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos o reglamentos internos de contratación, además del visto bueno técnico por parte de la Dirección de Sistemas.

Objetivo: Asegurar que el software cumpla con las licencias correctas.

Alcance: Esta política se debe aplicar correctamente a la Dirección de Sistemas

Responsables: Dirección de Sistemas (Todos los Funcionarios)

Políticas:

- La Dirección de Sistemas debe manejar un inventario en donde se lleve actualizado cada una de las licencias de software, logrando asi un control y uso adecuado de las mismas, de esta manera se evita posibles sanciones de instalación de software no licenciado.
- Los productos de software con licencia de evaluación o de prueba instalados en los computadores de la Gobernación de Boyacá deberán desinstalarse una vez caduque la licencia.
- La instalación de software debe ser autorizada y realizada por funcionarios de la Dirección de sistemas. Los funcionarios públicos, contratistas y demás usuarios no deben instalar ningún tipo de software; el software pirata, ilegal o material digital que viole las normas de seguridad y de derechos de autor será desinstalado o eliminado.

10.16. POLÍTICA 14: Control de Acceso Físico

Generalidades: La política de control debe ser documentada, revisada y actualizada constantemente con el fin de evitar el acceso a los sistemas de información, bases de datos y documentos por personal no autorizado que pongan en peligro la información de la empresa.

Objetivo: Controlar el acceso a la información

Alcance: Esta política se aplica a todas los procesos o formas de acceso a los sistemas de información, bases de datos o servicios de información de la empresa.

Responsables:

Los funcionarios de la Dirección de Sistemas: Se encarga de dirigir normas y procedimientos para implementar Sistemas operativos, Gateway, firewall, servicios de red etc., debe verificar que todos estos dispositivos y servicios queden debidamente configurados, debe realizar pruebas de escaneo, monitoreo para evitar intromisión. Además, debe promover y realizar la gestión de contraseñas y privilegios, capacitar y concientizar a los usuarios de la utilización de las medidas de control de acceso.

El centro de datos, cableado y demás áreas que la Dirección de Sistemas considere críticas deben ser de acceso restringido y cualquier persona que ingrese a ellos deberá estar debidamente autorizada por el Director de Sistemas y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares.

Políticas:

- Los particulares, tales como familiares y conocidos de los funcionarios, no están autorizados a acceder a los recursos informáticos instalados por la Entidad.
- Todos los equipos servidores y equipos de comunicaciones deberán estar ubicados en sitios con seguridad adecuada para protegerlos de usos no autorizados y posibles alteraciones.

- Todos los computadores portátiles, módems y equipos de comunicación sean de la entidad, de terceros o de otros usuarios de la Gobernación de Boyacá deberán ser registrados a su ingreso y salida del edificio en un libro o sistema de registro; para el caso de equipos de la Entidad no podrán abandonar las instalaciones a menos que estén acompañados por la autorización respectiva y la validación de la Dirección de Sistemas.
- En los Centros de Procesamiento de Datos (salas de servidores), los centros de cableado y demás áreas que la Dirección de Sistemas considere críticas para la administración de las Tecnologías de Información y Comunicación, deberán existir elementos de control de incendio, inundación y alarmas.
- Los computadores portátiles deberán estar protegidos por cables de seguridad, u otros dispositivos de protección contra el robo cuando estén situados en un entorno no controlado, en horas no laborables deberán almacenarse en lugares cerrados con llave.

10.17 POLÍTICA 15: Gestión de Incidentes en la Seguridad de la Información

Generalidades: Todos los funcionarios de la Gobernación de Boyacá deben tener muy clara la obligación de reportar formalmente fallas, eventos y debilidades de manera inmediata al responsable de la seguridad.

Objetivo: Garantizar que todos los eventos maliciosos, como fallas y debilidades de la seguridad de la información sean comunicados de manera inmediata

Alcance: Esta política la deben cumplir todos los funcionarios de la Gobernación de Boyacá.

Responsables:

Dirección de Sistemas: El responsable de la seguridad debe establecer un protocolo el cual deben conocer todos empleados para conozcan cual es el proceso a seguir en caso de presentarse una falla. Es decir, cómo y a quien reportarlo para que se tomen los correctivos necesarios. Se debe concientizar y capacitar a los empleados para que estén atentos a eventos sospechosos y en caso de presentarse los reporten de inmediato.

Políticas:

- Los usuarios deberán comunicar incidencias de manera oportuna a través de los diferentes canales dispuestos para tal fin a la Dirección de Sistemas para que sea atendido por un Administrador del sistema; los incidentes que no puedan resolverse de forma inmediata serán escalados apropiadamente de acuerdo a los procedimientos adecuados con el propósito de tomar acciones efectivas para minimizar el impacto.
- Para gestionar los incidentes de Seguridad de la Información deberá existir un grupo con conocimientos en el manejo de incidentes en las Áreas de Seguridad de la Información.
- Para cuando los incidentes reportados requieran judicialización se deberá coordinar con el/ los organismos que cuentan con función de policía judicial. Se deberá establecer los mecanismos de control establecidos en el manual de procedimientos del Sistema para Cadena de Custodia de la Fiscalía General de la Nación para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de Seguridad de la Información
- Se debe llevar un registro detallado de los incidentes de Seguridad de la Información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.
- La Dirección de Sistemas deberá propender por la adquisición de herramientas que faciliten el proceso de gestión de incidentes de Seguridad de la Información.
- Los siguientes son incidentes de exposición de seguridad, que deberán tener registro en documento electrónico o físico:

✓ Persistencia de infección por virus, u otro código malicioso en cualquier computador después de que el antivirus ha escaneado discos

✓ Virus, gusanos, troyanos o cualquier otro malware con un impacto significativo sobre la confidencialidad, la disponibilidad y la integridad de una aplicación crítica, de un

servicio o de la red

- ✓ Instalación de software ilegal o no licenciado en los equipos de cómputo de la Entidad
- ✓ Intentos de acceso no autorizado o intrusión en los sistemas de información, ya sea exitoso o no
- ✓ Escaneo o sondeo de la red por cualquier usuario no autorizado
- ✓ Acceso con perfil de administrador desde alguna cuenta de usuario legítima, realizado por usuario no autorizado
- ✓ Pérdida o robo de un activo de Tecnología de la Información
- ✓ Fraude, daño, o pérdida de información sensible o de uso interno
- ✓ Revelación no autorizada de información sensible, de contraseñas, o de información de uso interno
- ✓ Pérdida de computadores de la Gobernación de Boyacá o de computadores personales no institucionales que contengan información sensible o de uso interno sin encriptar.
- ✓ Vulnerabilidades encontradas en la red de información
- ✓ Violación de las políticas de seguridad de la información

Una vez verificada por la Dirección de sistemas la existencia de un incidente crítico que involucre a un funcionario, el cual incurra en incumplimientos o faltas que ameriten sanción disciplinaria sin perjuicio de la ley, se reportará a Control Interno Disciplinario para que se coordine y determine el alcance a las investigaciones según sea el caso.

10.18. POLÍTICA 16: Administración de la Seguridad

Generalidades: La Dirección de Sistemas Gobernación de Boyacá deben tener muy clara la obligación de reportar formalmente fallas, eventos y debilidades de manera inmediata al responsable de la seguridad.

Objetivo: Garantizar que todos los eventos maliciosos, como fallas y debilidades de la seguridad de la información sean comunicados de manera inmediata

Alcance: Esta política la deben cumplir los funcionarios de la Dirección de Sistemas de la Gobernación de Boyacá.

Responsables:

Dirección de Sistemas: El responsable de la seguridad debe establecer un protocolo el cual deben conocer todos funcionarios para conozcan cual es el proceso a seguir en caso de presentarse una falla. Es decir, cómo y a quien reportarlo para que se tomen los correctivos necesarios.

Políticas:

- La evaluación de riesgos de seguridad para los Recursos Informáticos en producción se debe ejecutar al menos una vez cada año. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.
- Los funcionarios públicos y contratistas de la Gobernación de Boyacá que realizan las labores de administración del recurso informático y de servicios son responsables por la implementación, permanencia y monitoreo de los controles sobre los Recursos Computacionales. La implementación debe ser consistente con las prácticas establecidas por la Dirección de sistemas.

- La Dirección de Sistemas divulgará, las políticas, estándares y procedimientos en materia de seguridad informática. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará a la dirección General los casos de incumplimiento con copia a las oficinas de control interno.

- Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar a los usuarios que lo requieran, de acuerdo con su competencia según las actividades a desarrollar y los niveles de seguridad establecidos previamente.

10.19. POLITICA 17. Registros de Auditoría

Generalidades: La Dirección de Sistemas Gobernación de Boyacá deben tener muy clara la obligación de reportar formalmente fallas, eventos y debilidades de manera inmediata al responsable de la seguridad.

Objetivo: Garantizar que todos los eventos maliciosos, como fallas y debilidades de la seguridad de la información sean comunicados de manera inmediata

Alcance: Esta política la deben cumplir los funcionarios de la Dirección de Sistemas de la Gobernación de Boyacá.

Responsables:

Dirección de Sistemas: El responsable de la seguridad debe establecer un protocolo el cual deben conocer todos funcionarios para conozcan cual es el proceso a seguir

en caso de presentarse una falla. Es decir, cómo y a quien reportarlo para que se tomen los correctivos necesarios.

Políticas:

- Todos los sistemas automáticos que operen y administren información sensible, valiosa o crítica para la Gobernación de Boyacá, como son sistemas de aplicación en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones deberán generar pistas de auditoría o logs de registro de sucesos de la operación, las cuales deben proporcionar suficiente información para apoyar el monitoreo, control y las mismas auditorias.

- Todos los archivos de logs de auditorías deben ser almacenados y custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que con razón justificada y autorizada por la sectorial correspondiente requieran los registros deberán solicitarlos ante dicha dependencia, quien a su vez deberá solicitar el soporte adecuado a la Dirección de Sistemas, encargada de su administración y custodia.
- Todos los computadores de la Entidad deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoria y en las transacciones sea correcto.
- No se permite la instalación, ni utilización de cualquier herramienta de auditoría ni de pruebas de seguridad informática, ni de Ethical Hacking sin previa autorización del Director de Sistemas.

10.19.1. Derechos de Vigilancia

- La Administración se reserva el derecho de supervisar e inspeccionar los sistemas de información de la entidad en cualquier momento.
- Estas inspecciones pueden llevarse a cabo con o sin el consentimiento y/o la presencia de los empleados involucrados.
- Los sistemas de información que pueden ser objeto de inspección incluyen el registro de actividad de los usuarios, los archivos del disco duro y correo electrónico.
- También pueden estar sujetos a inspección los documentos impresos, cajones del escritorio y áreas de almacenamiento de medios.

10.20. POLITICA 18. Gestión de la continuidad de la Entidad

Generalidades: Es indispensable que toda entidad y/o organización disponga de un proceso de gestión de continuidad del negocio en caso de llegarse a presentar una eventualidad como un desastre natural, robo, daños en los servidores etc.

Objetivo: Asegurar el funcionamiento continuo de la Gobernación de Boyacá.

Alcance: Esta política se debe aplicar a todos los procesos críticos y prioritarios de la entidad.

Responsables:

El Director de Sistemas y su grupo debe participar en la elaboración y documentación del plan de contingencia.

Política

Elaboración e implantación de los planes de continuidad de las actividades de la entidad: El comité de seguridad junto con el responsable de la seguridad debe elaborar el plan de contingencia que debe contemplar los siguientes aspectos: Responsables de los procedimientos de emergencia, definir acciones y correctivos, implementar procedimientos de emergencia, documentar estos procedimientos e instruir al personal; actualizar constantemente el plan de contingencia.

Marco para la planificación de la continuidad de las actividades de la entidad: Se debe especificar claramente los requisitos y condiciones para su puesta en marcha, los responsables y los requerimientos etc. Adicionalmente debe prever las condiciones de implementación, definir los procedimientos de emergencia, y las acciones a realizarse, describir los procedimientos de recuperación, definir un cronograma de mantenimiento y documentar las responsabilidades y funciones de las personas. (elaborar un documento muy completo del plan de contingencia.)

11. CONCLUSIONES

Es de gran importancia aplicar la Metodología Magerit para el análisis de riesgos es el primer paso para garantizar la seguridad de los activos de la Dirección de Sistemas de la Gobernación de Boyacá.

Con el Diseño de SGSI se logra una planeación anticipada de diferentes eventos, para que todo esté bajo control, lo que significa que utilizando esta estrategia la Dirección de Sistemas de la Gobernación de Boyacá minimice cualquier falla que se presente tanto es su infraestructura o de información.

Cabe denotar que al utilizar esta metodología SGSI permite identificar varias características como son: Conocer, gestionar y minimizar todos los posibles riesgos que puedan atentar con la seguridad de la información Además con el SGSI permite analizar y ordenar la estructura los sistemas de información, facilitara la definición de procedimientos de trabajo para mantener su seguridad y disponer de controles que permita medir la eficacia de las medidas tomadas con el fin de proteger a la Dirección de Sistemas de amenazas y riesgos que puedan poner en peligro la continuidad de la Entidad.

Con la Norma Internacional ISO 27001 estándar de calidad en los sistemas de seguridad en las Entidades, mejorara el Sistema de Gestión de Seguridad de la Información de la Dirección de Sistemas, con la finalidad de evaluar todos los requisitos para la aplicación de controles de seguridad adaptados a cada una de las necesidades que requiera la misma, todo esto con el fin de garantizar y proteger la confidencialidad, integridad y disponibilidad de la información que maneja la Gobernación de Boyacá.

Para la ejecución Proyecto del Diseño de un Sistema de Gestión de Seguridad de la información basado en La Norma ISO/IEC 27001 para La Dirección de Sistemas de la Gobernación de Boyacá, se tuvo en cuenta en primer lugar la observación directa, posteriormente se aplicó una encuesta a los funcionarios de la Dirección de Sistemas y la aplicación de la prueba de análisis de red, con el fin de recolectar información, para poder identificar y definir el punto de partida del desarrollo del SGSI.

El conocer el inventario de activos de la Dirección de Sistemas es fundamental para saber en qué grado están expuestos ante el riesgo. Los activos tangibles e intangibles de la ya mencionada anteriormente se encuentra: Servicios, Datos de Información, Aplicaciones Software, Equipos Informáticos Hardware, Redes de Comunicación, Soportes de Información, Equipamiento Auxiliar, Instalaciones y Personal.

Realizando el análisis y la revisión exhaustiva de estos activos se encontró que la Dirección de Sistemas presenta los siguientes activos en riesgos: Inventarios de Servicios y Equipamiento SW.

Posteriormente se determina las vulnerabilidades, amenazas y riesgos de seguridad existentes en la Dirección de Sistemas por lo que se hace una valoración de cada uno de los activos teniendo presente las dimensiones valoradas como son: Confidencialidad, Integridad, Autenticidad, Disponibilidad y Trazabilidad

Se identifica y valora las amenazas generales de los activos de la Dirección de Sistemas de la Gobernación de Boyacá, en donde se tiene presente la probabilidad de ocurrencia es decir se refiere a los eventos que se puede producir en un tiempo determinado y la degradación del % nivel que activo es tan perjudicado al poderse materializar esa amenaza.

Por lo que con la aplicación del SGSI se pudo determinar el análisis de riesgos donde se ve reflejado algunos inconvenientes que presenta la Dirección de Sistemas de la Gobernación de Boyacá, lo que permite analizar y encontrar elementos críticos del área, por otra parte, permite valorar los riesgos, identificar las amenazas, el impacto para cada dimensión de seguridad (frecuencia – impacto), valorar los riesgos y determinar las salvaguardas del Departamento de Sistemas.

Para el desarrollo del proyecto se utilizó la Metodología de Magerit, herramienta que ayuda a identificar el análisis de riesgos de cualquier entidad y/o organización y de esta forma mitigar los riesgos, para este caso se ejecutara en la Dirección de Sistemas, Magerit permite documentar paso a paso el Inventario de activos, la valoración cuantitativa de activos, Identificación de amenazas, Identificación de salvaguardas para los activos, Valoración y evaluación del riesgo y el Informe de calificación del riesgo donde se evidencia claramente los activos que se encuentran en riesgo y que deben ser tratados de inmediato para la protección de seguridad de la Entidad.

Con el presente proyecto de grado se pretendió realizar un Diseño de Seguridad de la Información para la Dirección de Sistemas de la Gobernación de Boyacá, en donde se decidió como marco de referencia la norma ISO 27001. Se logró obtener una serie de diagnósticos que permite ver el estado de madures en que se encuentra la Dirección de Sistemas frente a la gestión de la seguridad de la información.

Se conocerán los diagnósticos que se encontró en la Dirección de Sistemas de la Gobernación de Boyacá: El análisis de Riesgos determino que los activos que presentan vulnerabilidad de carácter critico son:

- Inventarios de Servicios: Correo Electrónico, Internet y Telefonía.
- Equipamiento SW: Servidor de Aplicaciones, Servidor de Correo, Servidor de Ficheros, Servidor de Base de Datos, Office, Antivirus y OS Sistema Operativo.

Los activos anteriormente mencionados son los que presentan mayor nivel de riesgo en la Dirección de Sistemas de la Gobernación de Boyacá, esto es debido a la falta de implementación de salvaguardas de seguridad como se recomienda en las buenas prácticas para lo concerniente Gestión de la Seguridad de la Información.

La Dirección de Sistemas es consciente de las falencias que presenta los activos en cuanto a sus vulnerabilidades como se presenta en: error de usuarios y error de administrador del sistema/ de la seguridad por lo que a partir de este proyecto realizo unas medidas de salvaguardas que les ayudara a mitigar estas amenazas y proteger su información de forma más adecuada.

Por otra parte, ya determinado el análisis de riesgos de la Dirección de Sistemas de la Gobernación de Boyacá, donde permite conocer a fondo los riesgos a los que se ve expuesta se procede a definir las políticas de seguridad, con la aplicabilidad de los controles de la Norma ISO/IEC 27001.

El proceso realizado para el análisis de riesgos, definición de políticas de seguridad, aplicabilidad de los controles conforma el diseño SGSI, para la Dirección de Sistemas de la Gobernación, donde el objetivo principal es garantizar la confidencialidad, disponibilidad, e integridad de la información.

El conocer las políticas de seguridad por parte de los funcionarios de la Dirección de Sistemas, es de gran utilidad puesto que identifican la problemática que puede existir en cualquier proceso que maneja la entidad, ya que con las labores cotidianas pueden identificar algún riesgo que se presente y esto ayuda a mejorar y robustecer el sistema de seguridad de la Gobernación de Boyacá.

Es importante la documentación de los procesos, puesto que es una excelente herramienta para el mantenimiento y/o mejora de cualquier sistema que tenga la entidad.

Cabe denotar que la Dirección de Sistemas tiene implementado el Fortinet, lo que permite publicar todas las aplicaciones y brinda seguridad a la Entidad; algunos de estos beneficios son: Controla las aplicaciones, antivirus, firewall, filtro web, spam, vpn, control wifi, y una de las características de este equipo fortinet es que se adapta a cualquier arquitectura de red ya que posee los servicios de enrutamiento, creación de redes múltiples, este equipo permite parametrizar las políticas de seguridad de diferentes maneras como son: A nivel de usuarios, ips, dispositivos y redes, por eso la Dirección de Sistemas de la Gobernación de Boyacá tiene un fortinet ya que a nivel de seguridad es bastante completo, también maneja auditorias en tiempo real lo que permite la detección de cualquier hacker que quiera ingresar a la red de la Dirección de Sistemas.

De forma clara y detallada se puede concluir que el Diseño del SGSI en la Dirección de Sistemas de la Gobernación de Boyacá, puede ayudar al mejoramiento de actualización de diferentes procesos que esta lleva, a corto y mediano plazo, logrando fortalecer la continuidad de la Entidad, y mitigar riesgos a los que puede estar expuesta alguna información.

12. RESULTADOS Y DISCUSIÓN

Los resultados que se obtuvieron en este proyecto provienen del desarrollo de cuatro fases para dar cumplimiento a los objetivos específicos establecidos con el propósito de poder alcanzar el objetivo general de proyecto.

Las fases planteadas para llevar a cabo el proyecto:

Diagnóstico: Esta actividad se desarrolló con el fin de realizar un análisis previo de la información para identificar todos los procesos internos llevados a cabo en la en la Dirección de Sistemas de la Gobernación de Boyacá, la documentación necesaria que permita establecer el alcance del objetivo general del proyecto.

Auditoria inicial: Para poder conocer cuál es la situación en temas de seguridad de la información en la entidad, para poder realizar una planificación concreta para las líneas de trabajo que se van a seguir.

Análisis y gestión de riesgos: En esta fase se realiza identificación de inventario de activos en el que se determina que posibles amenazas presenta la entidad, el impacto y las vulnerabilidades, en esta etapa se desarrolla el plan para el tratamiento de riesgos.

En el desarrollo de estas fases se utilizaron varios métodos los cuales encontramos: Recolección de información, este proceso se ejecutó mediante entrevistas verbal, encuesta y análisis de red.

Entrevista Verbal: Se logra obtener cierta información a primera vista de la infraestructura de la entidad, es decir como manejan los activos, que problemas presentan en conectividad, problemas de incidentes de los diferentes activos, cuentas institucionales de la Dirección de Sistemas.

Encuesta: Se realizó con el fin de obtener la opinión de los funcionarios de la Dirección de Sistemas sobre los procesos que manejan día a día en los cuales se encuentran: El uso de internet, incidencias o requerimientos que se presentan en el equipo de cómputo, cambio de contraseñas, conocimiento sobre los activos de la entidad y apropiación de las políticas de seguridad en general de la Gobernación de Boyacá.

Análisis de Red: Se realizó un análisis de red con la herramienta Zenmap, este software es fácil su ejecución y sirve como guía a la Dirección de Sistemas sobre el uso de escaneo de red, donde se puede identificar un escaneo completo de la red, peticiones, escaneo de UDP, uno de los aspectos más importantes de esta aplicación es que permite conocer que puertos se encuentran abiertos y cerrados para conocer las vulnerabilidades que se pueden presentar en la red.

Este escaneo se hizo a la ip 149.56.24.232 de la Gobernación de Boyacá, donde se identificó que existen algunos puertos que se encuentran abiertos, y se hace la recomendación de revisar este riesgo puesto que puede presentar fallas en la red de la entidad.

Fase de diagnóstico:

Se identificaron los activos y recursos a proteger y las posibles vulnerabilidades de cada proceso y las amenazas asociadas.

Se evaluó la viabilidad y efectividad de las políticas de seguridad establecidas para el acceso de la información.

Se calculó el costo del impacto de materialización de las amenazas identificadas en la entidad .

Se valoró la capacidad de recuperación de información frente a incidentes y la probabilidad de continuidad de los procesos de la entidad.

Esta fase de diagnóstico permitió determinar la situación actual en relación con la gestión de seguridad de la información, en términos generales se identificó lo siguiente.

- Falta de concientización y conocimiento por parte de los funcionarios en temas seguridad de la información.

- No hay una política de seguridad de la información asociada a la entidad en términos de definición de controles y evaluación de riesgos.

- No se cuenta con un sistema de información adecuado para la Gestión de Seguridad y valoración adecuada de los riesgos de seguridad.

- La política de seguridad no se encuentra alineada con los objetivos de la entidad.

La fase de diagnóstico fue fundamental ya que permito obtener los lineamientos para el trabajo a desarrollar.

Auditoria inicial: Se realiza una auditoría interna, se realiza un listado de todos los controles a revisar y todos los aspectos del sistema que necesitan ser analizados. Con este listado se realiza una revisión del sistema para identificar aquellos aspectos de mejora que se han detectado, así como la prioridad o gravedad de cada uno de ellos.

Con los datos arrojados por la auditoría inicial se realizará un análisis previo, donde la información de salida serán las brechas generales de las áreas tratadas, con el fin de encontrar las vulnerabilidades prioritarias a ser tratadas.

Análisis y gestión de riesgos:

En esta fase se tuvieron en cuenta los activos de información, es decir todos aquellos recursos involucrados en la gestión de la información como datos y hardware, documentos y recurso humano. Se realiza un análisis de todos los riesgos para que la entidad pueda tomar decisiones sobre cómo actuar ante los diferentes riesgos encontrados. Se realizó una valoración para determinar cuáles son los más críticos para la entidad, valoración que se hace en términos de la posibilidad de ocurrencia de un riesgo y del impacto que pude tener en caso de materializarse.

Una vez identificados los riesgos la siguiente tarea es identificar y evaluar las acciones más apropiadas para el tratamiento de los riesgos, decisión que se toma teniendo en cuenta los activos que se encuentran involucrados y el impacto que puede tener la entidad, otro aspecto que se tiene en cuenta es el nivel de riesgo aceptable identificado.

Para el estándar ISO 27001 requiere que la entidad en relación al tratamiento de riesgos siga cuatro posibles acciones.

- Aplicar los controles apropiados para reducir los riesgos.
- Aceptar de forma objetiva los riesgos partiendo de las políticas de la entidad y el criterio de aceptación de riesgos.
- Evitar los riesgos
- Trasferir el riesgo asociado a otras partes

La entidad por cada uno de los riesgos identificados, debe evaluar las opciones anteriores e identificar la más adecuada.

Para reducir el riesgo que ha sido evaluado dentro del alcance del SGSI el estándar ISO 27001, la selección de los controles se sustenta por los resultados obtenidos en la selección de los riesgos encontrados.

A continuación, se describen las acciones principales del plan de tratamiento sugeridos para mitigar los riesgos encontrados:

- Se recomienda realizar la actualización de la política para el manejo de la información.
- Se recomienda revisar y mejorar los procesos establecidos para el manejo de la seguridad de la información.

- Es necesario actualizar las políticas de los activos de la Dirección de Sistemas, se debe implementar una metodología de gestión de riesgos para evaluarlos y ajustarlos al plan de tratamiento de riesgos.
- Se deben establecer controles ambientales para evitar el deterioro de los activos de la Dirección de Sistemas.
- Se deben cambiar las UPS y contar con un buen respaldo eléctrico.
- Es necesario que se establezca un plan para el mantenimiento de equipos al interior de la entidad.
- Es necesario definir controles que se deben tener en cuenta en el caso de que ingresen nuevos elementos al sistema de información
- Capacitar y concientizar al personal sobre la seguridad de la información para minimizar la probabilidad de materialización de una amenaza.
- Se debe definir políticas a tener en cuenta para la eliminación de medios de almacenamiento tales como discos duros, CD, DVD, memorias USB.
- Es necesario definir políticas de seguridad para el manejo de herramientas criptográficas, en caso de ser implementadas.
- Es necesario definir políticas de seguridad para la gestión de incidentes de seguridad de la información.
- Definir políticas de seguridad de la información a implementarse encaminadas a garantizar la continuidad de la entidad.

Actualizar el Plan de Continuidad de la Gobernación de Boyacá. La entidad debe actualizar el plan de continuidad, pues ante situaciones de riesgo que puedan afectan la continuidad del negocio de forma crítica. No importa el tamaño de la entidad o el costo de las medidas de seguridad implementadas, toda entidad necesita actualizar Plan de Continuidad del Negocio, ya que tarde o temprano se encontrará con una incidencia de seguridad.

Respecto a los requisitos obligatorios de la norma de SGSI la Gobernación de Boyacá alcanza un nivel alto de cumplimiento se requiere invertir para alinear la gestión con las mejores prácticas según la norma.

La Gobernación posee documentos y registros de actividades de seguridad de la información, pero no hay un procedimiento formal para esta actividad. No se encontraron registros de revisiones de la gestión de la seguridad de la información, pero se encontraron registros de auditorías tanto externas como internas en las que se encontraron conformidades e inconformidades respecto a normas de seguridad. Las acciones correctivas fueron desarrolladas y las acciones de mejora continua.

La mayor debilidad se encuentra en la seguridad organizativa, debido a la falta de procedimientos y políticas orientadas a la gestión de seguridad de la información y la falta de cultura organizacional.

13. DIVULGACIÓN

El presente proyecto denominado DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA LA DIRECCION DE SISTEMAS DE LA GOBERNACIÓN DE BOYACÁ, tendrá como único medio de divulgación el repositorio institucional de la Universidad, en donde quedará como referencia de consulta para las personas externas y estudiantes de la universidad de los diferentes programas académicos de pregrado y posgrado de la Universidad Nacional Abierta y a Distancia “UNAD”.

14. BIBLIOGRAFIA

ISO 27000 “Norma que compone el alance de actuación” {En línea } http://www.iso27000.es/download/doc_iso27000_all.pdf {10 de Septiembre de 2015}

NORMA ISO 27001 “Norma principal que contiene los requisitos del sistema de gestion de seguridad de la informacion” {En línea}.http://advisera.com/27001academy/es/que-es-iso-27001{11 de Septiembre de 2015}.

UNIVERSIDAD NACIONAL DE LUJAN “Seguridad de la Información” {En línea}.http://www.unlu.edu.ar/v1-5-v2-0-v3-noved-seguridad.html{11 de Septiembre de 2015}

RIESGO VS. SEGURIDAD DE LA INFORMACIÓN “Riesgo Seguridad de la Informacion” {En línea}.disponible en: http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf {11 de Septiembre de 2015}

ABC PARA PROTEGER LOS DATOS PERSONALES “Ley 1581 de 2012 Decreto 1377 de 2013” {En línea}.http://www.colombiadigital.net/actualidad/articulos-informativos/item/5543-abc-para-proteger-los-datos-personales-ley-1581-de-2012-decreto-1377-de-2013 {12 de Septiembre de 2015}

CICLO PDCA (PLANIFICAR, HACER, VERIFICAR Y ACTUAR “El círculo de Deming de mejora continua” {En línea}.http://www.pdcahome.com/5202/ciclo-pdca. {12 de Septiembre de 2015}

SENN, James A (1997) “Análisis y diseño de sistemas de Información, Divinni Editorial LTDA, Colombia” {En línea}.https://sisteminformacii.wikispaces.com/METODOLOG%C3%8DA+DE+JAMES+SENN?responseToken=b63c65390016c092708375d8b5113753 {12 de Septiembre de 2015}

ALEXANDER A.G. (2007) “Diseño y gestión de un Sistema de Seguridad de Información” {En línea}.disponible en: http://www.marcombo.com/Diseno-de-un-sistema-de-gestion-de-seguridad-de-informacion_isbn9789586827133.html {12 de Septiembre de 2015}

CORLETTI Alejandro “Controles de seguridad. 2006.” {En línea}.{25 de Noviembre de 2015} http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_II.pdf.

ISO 27001 “Statement of Applicability of ISO/IEC 27001 Annex A controls”{En línea}.disponible en: www.ISO27001security.com. {25 de Noviembre de 2015}

UNIVERSIDAD JAVERIANA “Manual del sistema de gestión de la seguridad de la información” {En línea}. http://pegasus.javeriana.edu.co/~CIS0830IS12/documents/Anexo%20K%20MG-05%20Manual%20del%20Sistema%20de%20Gestion%20de%20Seguridad%20de%20la%20Informacion.pdf. {25 de Noviembre de 2015}

NORMAS ISO DE SEGURIDAD DE LA INFORMACIÓN “Red temática de criptografía y seguridad de la información”{En línea}.disponible en: http://www.criptored.upm.es/guiateoria/gt_m327a.htm. {25 de Noviembre de 2015}

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN “según iso 27001 (2006)” {En línea}.disponible en: http://www.nexusasesores.com/docs/ISO27001-norma-e-implantacion-SGSI.pdf. {25 de Noviembre de 2015}

ANÁLISIS Y EVALUACIÓN DEL RIESGO DE INFORMACIÓN “Aplicación de la ISO 27001 (2011)” {En línea}. http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf. {25 de Noviembre de 2015}

GUSTAVO Pallas y CORTI María Eugenia “Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica, Grupo de Seguridad Informática, Instituto de Computación, Facultad de Ingeniería, Universidad de la República” {En línea}. disponible en: http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2-Sesion3%284%29.pdf. {25 de Noviembre de 2015}

GUACHI T, (2012), “Norma de Seguridad Informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito —San Francisco Ltda. Tesis de Grado Facultad de Ingeniería en Sistemas. Universidad de Ambato” {En línea}. disponible en: http://repo.uta.edu.ec/handle/123456789/2361 {25 de Noviembre de 2015}

GUZMÁN, A (2015),” Diseño de un sistema de gestión de la seguridad informática –SGSI para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá d.c a través de la auditoria. Proyecto de Grado, Universidad Nacional Abierta y a Distancia”. {En línea}. http://repo.uta.edu.ec/handle/123456789/2361 {25 de Noviembre de 2015}

AGUIRRE J (2013), “Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda, Diseño del sistema de gestión de seguridad de la información para el grupo empresarial, Proyecto de Grado, universidad tecnológica de Pereira” {En línea}.
https://scholar.google.es/citations?user=WLWJECAAAAAJ&hl=es {25 de Noviembre de 2015}

BUITRAGO J (2012), “Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información - SGSI, en el sector de laboratorios de análisis microbiológicos, basado en iso 27001, Proyecto de Grado, Universidad EAN” {En línea}.
http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1 {28 de Septiembre de 2016}

PALLAS G (2009), “Metodología de Implantación de un SGSI en un grupo empresarial jerárquico, Tesis de Maestría, Instituto de Computación Facultad de Ingeniería, Universidad de la República” {En línea}.
https://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf {28 de Septiembre de 2016}

ANEXOS

ANEXO A

ENCUESTA PARA LOS FUNCIONARIOS DE LA DIRECCION DE SISTEMAS DE LA GOBERNACION DE BOYACA

Como contratista de la Gobernación de Boyacá, le solicitamos responder esta sencilla encuesta con el fin de mejorar los procesos y mitigar los riesgos de la Seguridad de la Información.

La presente encuesta tiene duración de 15 minutos.

Como funcionario de la Dirección de Sistemas y en su experiencia marque con una X su respuesta en la letra correspondiente:

1. ¿Con que frecuencia utiliza Internet?

a) Una vez al día

b) Varias veces al día

c) Todo el tiempo

2. Las incidencias o requerimientos que se presentan en el equipo de cómputo que tiene a su cargo son:

Dónde: 1) Siempre 2) Alguna Vez 3) Nunca

	1	2	3
a) El equipo de cómputo se bloquea con frecuencia	___	___	___
b) El equipo de cómputo no se conecta a la red	___	___	___
c) El equipo de cómputo es lento	___	___	___

3. ¿Con que frecuencia se cambian las contraseñas del equipo de cómputo a su cargo?

a) Cada mes

b) Entre 2 y 6 meses

c) Dos veces al año

d) Nunca

4. Usted como funcionario de la Gobernación de Boyacá del área Dirección de Sistemas califique las siguientes afirmaciones:

Dónde: 1) Malo 2) Aceptable 3) Bueno 4) Excelente

	1	2	3	4
a) Actualización de software permanente	_____	_____	_____	_____
b) Respaldo de Backups	_____	_____	_____	_____
c) Conocimiento sobre las responsabilidades para el manejo de información.	_____	_____	_____	___
d) La ubicación de los servidores se encuentran aislados y seguros	_____	_____	_____	_____
e) Cambio de contraseñas periódicamente	_____	_____	_____	_____

5. ¿Usted considera que las dificultades presentadas en el equipo de cómputo influyen en la atención al cliente?

SI_____ NO_____

6. Usted considera que las medidas de seguridad utilizadas en la Dirección de Sistemas son suficientes para la protección de información y prevenir posibles incidentes?

SI_____ NO_____

7. ¿Usted tiene conocimientos sobre las políticas de seguridad de la información y de esta forma mitigar riesgos de la misma?

SI_____ NO_____

8. ¿Las dificultades que usted ha encontrado en su equipo de cómputo influyen en el tiempo utilizado y en la calidad de su trabajo?

SI_____ NO_____

9. ¿Usted tiene conocimiento sobre el plan de continuidad de la Gobernación de Boyacá?

SI_____ NO_____

10. ¿Usted ha tenido problemas en el momento de utilizar el equipo de cómputo?

SI_____ NO_____

11. Usted tiene claras las políticas de seguridad en cuanto el correo electrónico (Eliminar usuario, crear, cambio de contraseñas)

SI_____ NO_____

Observaciones:_____
_____
_____
_____
_____
_____

ANEXO B

RESUMEN ANALÍTICO ESPECIALIZADO (RAE)

Tabla 57. Resumen Analítico Especializado (RAE)

Fecha de Realización: 6/12/2016
Título: DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA LA DIRECCION DE SISTEMAS DE LA GOBERNACIÓN DE BOYACÁ
Autor: CONTRERAS, Lidia
Palabras Claves: Diseño de un Sistema de Gestión de Seguridad, Norma ISO/IEC 27001, SGSI, activos, amenazas, riesgos, controles, políticas de seguridad.
Descripción: Monografía de grado para optar el título de Especialista en Seguridad Informática. El presente documento se realiza con el fin de desarrollar un Diseño de un Sistema de Seguridad de la Información para la Dirección de Sistemas de la Gobernación de Boyacá basado en la norma ISO/IEC 27001.
Fuentes: SENN, James A. Análisis y diseño de sistemas de Información, Divinni Editorial LTDA, Colombia [En línea]. <https://sisteminformacii.wikispaces.com/METODOLOG%C3%8DA+DE+JAMES+SENN?responseToken=b63c65390016c092708375d8b5113753> [12 de Septiembre de 2015] ALEXANDER A.G. Diseño y gestión de un Sistema de Seguridad de Información [En línea]. <http://www.marcombo.com/Diseno-de-un-sistema-de-gestion-de-seguridad-de-informacion_isbn9789586827133.html > [12 de septiembre de 2015] CORLETTI Alejandro. Controles de seguridad. [En línea] <http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_II.pdf > [25 de noviembre de 2015] GUSTAVO Pallas y CORTI María Eugenia. Metodología de Implantación de un

SGSI en grupos empresariales de relación jerárquica, Grupo de Seguridad Informática, Instituto de Computación, Facultad de Ingeniería, Universidad de la República. [En línea].
<http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2-Sesion3%284%29.pdf> [25 de Noviembre de 2015]

GUACHI, T. Norma de Seguridad Informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito —San Francisco Ltda. Tesis de Grado Facultad de Ingeniería en Sistemas. Universidad de Ambato. [En línea].
<http://repo.uta.edu.ec/handle/123456789/2361> [25 de Noviembre de 2015]

GUZMÁN, A. Diseño de un sistema de gestión de la seguridad informática –SGSI para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá d.c a través de la auditoria. Proyecto de Grado, Universidad Nacional Abierta y a Distancia.[En línea].http://repo.uta.edu.ec/handle/123456789/2361 [25 de Noviembre de 2015]

AGUIRRE, J. Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda, Diseño del sistema de gestión de seguridad de la información para el grupo empresarial, Proyecto de Grado, universidad tecnológica de Pereira. [En línea].
<https://scholar.google.es/citations?user=WLWJECAAAAAJ&hl=es> [25 de Noviembre de 2015]

BUITRAGO, J. Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información - SGSI, en el sector de laboratorios de análisis microbiológicos, basado en iso 27001, Proyecto de Grado, Universidad EAN. [En línea].
<http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1> [28 de Septiembre de 2016]

PALLAS, G. Metodología de Implantación de un SGSI en un grupo empresarial jerárquico, Tesis de Maestría, Instituto de Computación Facultad de Ingeniería, Universidad de la República. [En línea].
https://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf [28 de Septiembre de 2016]

Contenido del documento:

Este documento inicia con una introducción acerca de la importancia que tiene un Diseño de SGSI basado en la norma ISO/IEC 27001, pretende minimizar riesgos a los que se encuentra expuesto la Dirección de Sistemas de la Gobernación de Boyacá, utilizando la Metodología Magerit donde permite realizar un análisis de los riesgos, análisis de los activos, valoración cuantitativa de los activos, identificación

de amenazas, definición de los salvaguardas, aplicabilidad de los controles que conforma el SGSI, con el fin de realizar una evaluación de riesgos. La evaluación de riegos determinara que activos de la Dirección de Sistemas están en riesgo, para tomar las medidas adecuadas y mitigarlos, teniendo como objetivo principal garantizar la confidencialidad, disponibilidad, e integridad de la información de la Dirección de Sistemas de la Gobernación de Boyacá.

Metodología:

El Diseño del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para la Dirección de Sistemas de la Gobernación de Boyacá, se enmarca dentro del tipo de investigación descriptiva y analítica, puesto que comprende la recolección, descripción, registro, análisis e interpretación de la información.

Conclusiones:

Con la aplicación del SGSI se puede determinar el análisis de riesgos donde se ve reflejado algunos inconvenientes que presenta la Dirección de Sistemas de la Gobernación de Boyacá, lo que permite analizar y encontrar elementos críticos del área, por otra parte, permite valorar los riesgos, identificar las amenazas, el impacto para cada dimensión de seguridad (frecuencia – impacto), valorar los riesgos y determinar las salvaguardas del Departamento.

Se determina el análisis de riesgos de la Dirección de Sistemas de la Gobernación de Boyacá, donde permite conocer a fondo los riesgos a los que se ve expuesta se procede a definir las políticas de seguridad, con la aplicabilidad de los controles de la Norma ISO/IEC 27001.

De forma clara y detallada se puede concluir que el Diseño del SGSI en la Dirección de Sistemas de la Gobernación de Boyacá, puede ayudar al proceso de actualización de diferentes procesos que esta lleva, a corto y mediano plazo, logrando fortalecer la continuidad de la Entidad, y mitigar riesgos a los que puede estar expuesta alguna información.

Recomendaciones:

Se requiere de una revisión y análisis constante de las políticas establecidas en el Sistema de Gestión Documental, con el fin de mantener las medidas o estrategias que salvaguardar la información.

Formar y capacitar el personal para que tomen conciencia de importancia de la seguridad de la información y poder asegurar que las políticas internas establecidas para el SGSI se cumplan.

Establecer mecanismos de mejora que permitan la identificación de mecanismos para la identificación de nuevos activos de información. Se recomienda que la Dirección de Sistemas de la Gobernación de Boyacá, adopte una metodología para controlar los riesgos de la Entidad, de esta forma mitiga los riesgos que pueda presentar.
Redactor: Lidia Constanza Contreras Esguerra