DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA RED DE DATOS DE LA VEEDURÍA DISTRITAL EN LA CIUDAD DE BOGOTÁ

MARIELA CABALLERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTÁ
2017

DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA RED DE DATOS DE LA VEEDURÍA DISTRITAL EN LA CIUDAD DE BOGOTÁ

MARIELA CABALLERO

Trabajo de grado presentado como requisito para optar al título de Especialista en Seguridad Informática

Director de Proyecto:
SALOMÓN GONZÁLEZ GARCÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTÁ
2017

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá, 14 de noviembre de 2017

DEDICATORIA

A mi Dios por que sin Él no soy nada, me dio la vida y me brindó la fortaleza durante este semestre, debido a inconvenientes tanto de salud como de carácter familiar y por los cuales sentía que no podría continuar con mí especialización.

Al ser más maravillo que Dios me dio, mi madrecita que desde el cielo me brinda su protección en todo momento.

Mariela Caballero

AGRADECIMIENTO

A mi familia y a mí esposo Ricardo Alfonso, por el apoyo incondicional, ayuda, comprensión y paciencia en todo momento.

A mi asesor de proyecto ingeniero Salomón González García por la paciencia, enseñanzas y el acompañamiento constante en este proyecto tan importante para mi vida profesional.

A la doctora Alexandra Rodríguez del Gallego, a la ingeniera Ángela María Restrepo Franco y a mis compañeros del Área de Sistemas, por brindarme su apoyo y colaboración para la culminación del proyecto.

CONTENIDO

pág.

1. INTRODUCCIÓN---------- 16
1.1. DESCRIPCIÓN DE PROBLEMA ---------- 16
1.2 PLANTEAMIENTO DEL PROBLEMA---------- 16
2. FORMULACIÓN DEL PROBLEMA---------- 17
3. JUSTIFICACIÓN ---------- 17
4 OBJETIVOS ---------- 18
4.1 OBJETIVO GENERAL ---------- 18
4.2 OBJETIVOS ESPECIFICOS---------- 18
5. MARCO REFERENCIAL ---------- 19
5.1 ANTECEDENTES---------- 19
5.2 MARCO CONTEXTUAL---------- 19
5.2.1 Misión ---------- 20
5.2.2 Visión ---------- 20
5.2.3 Funciones de Veeduría Distrital---------- 21
5.2.4 Funciones de Gestión de Tecnologías de Información y Comunicaciones -- 22
5.2.5 Acciones de Gestión TIC ---------- 23
5.2.6 Modificaciones a software existente ---------- 23
5.3 MARCO CONCEPTUAL ---------- 24
5.3.1 Confidencialidad----------25
5.3.2 Disponibilidad ---------- 25
5.3.3 Integridad ---------- 25
5.3.4 Amenaza ---------- 25
5.3.5 Impacto ---------- 25
5.3.6 Riesgo ---------- 25

5.3.7 Seguridad Informática ---------- 25
5.3.8 Valoración del riesgo ---------- 25
5.3.9 Vunerabilidades ---------- 25
5.4 MARCO TEÓRICO ---------- 25
5.4.1 Generalidades ---------- 25
5.4.2 Vulnerabilidad Informática ---------- 26
5.4.3 Vulnerabilidad Física ---------- 26
5.4.4 Seguridad de la Información ---------- 26
5.4.5 Gestión de Riesgos ---------- 26
5.4.6 Magerit Versión 3.0 ---------- 27
5.4.7 Norma Técnica Colombiana NTC-ISO/IEC 270 1 ---------- 27
5.4.8 Guía Técnica Colombiana GTC-ISO/IEC 27002 ---------- 27
5.4.9 Guía Técnica Colombiana GTC-ISO/IEC 27003. ---------- 27
5.5 MARCO LEGAL ---------- 28
5.5.1 Ley 1273 de 2009 ---------- 28
5.5.2 Ley Estatutaria 1266 de 2008 ---------- 29
5.5.3 Ley 1341 de 2009 ---------- 26
5.5.4 Ley 603 de 2000 ---------- 26
5.5.5 Ley 1266 de 2008 ---------- 28
5.5.6 Constitución Política de Colombia ---------- 28
5.5.7 Ley 23198 de 1929 ---------- 28
6. MARCO METODOLÓGICO ---------- 30
6.1 METODOLOGÍA DE INVESTIGACIÓN ---------- 30
6.1.1 Población y muestra. ---------- 30
6.1.2 Recolección y fuentes de Información. ---------- 30
6.1.3 Técnicas y herramientas para recolección. ---------- 30
6.1.4 Procesamiento de la Información. ---------- 30
6.1.5 Análisis de la Información ---------- 30
6.2 METODOLOGÍA DE DESARROLLO ---------- 31
6.2.1 Fase 1 Planear ---------- 31

6.2.2 Fase 2 – Hacer. ---- 31
6.2.3 Fase 3 –Verificar. ---- 31
6.2.4 Fase 4 – Actuar. ---- 31
7. RECURSOS DISPONIBLES ---- 32
8. ANÁLISIS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN -------- 33
8.1 DESCRIPCIÓN Y ANALISIS DE RIESGOS ---- 33
8.2 IDENTIFICACIÓN DE ACTIVOS Y VALOR DIMENSIONES ---- 36
8.3 VALORACIÓN DE ACTIVOS ---- 36
8.3.1 Identificacion y valoración de amenaza por tipo:Datos ---- 37
8.3.2 Identificacion y valoración de amenaza por tipo: Servicios ---- 37
8.3.3 Identificacion y valoración de amenaza por tipo: Equipos ---- 38
8.3.4 Identificacion y valoración de amenaza por tipo: Software ---- 40
8.3.5 Identificacion y valoración de amenaza por tipo: Personal ---- 41
8.4 IDENTIFICACIÓN DE AMENAZAS ---- 42
8.4.1 Identificacion de amenaza por tipo: Datos ---- 42
8.4.2 Identificacion de amenaza por tipo: Servicios ---- 43
8.4.3 Identificacion de amenaza por tipo: Software ---- 51
8.4.4 Identificacion de amenaza por tipo: Equipos ---- 81
8.5 ANALISIS DE RIESGOS ---- 88
85.1. Interpretación de los resultados ---- 122
9. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN ---- 124
10. PLAN DE TRATAMIENTO DE LA INFORMACIÓN ---- 132
12. RESULTADOS ---- 148
13. CONCLUSIONES ---- 14849
BIBLIOGRAFÍA ---- 150
ANEXOS ---- 157

LISTA DE TABLAS

pág.

Tabla 1. Recursos requeridos……32
Tabla 2. Identificación de los activos de información de la Entidad…… 33
Tabla 3. Rango de Valoración de activos……..……..…….. 37
Tabla 4.Valores de activos Tipo [D]Datos...…….……..…….37
Tabla 5. Valores de activos Tipo [S]Servicios…….…….. 37
Tabla 6. Valores de activos Tipo[HW]Equipos..……...…… 39
Tabla 7. Valores de activos Tipo [WS]Software ……..……40
Tabla 8. Valores de activos [AUX]Elementos Auxiliares.....…..……41
Tabla 9. Valores de activos Tipo [P]Personal…..…….……..…..42
Tabla 10. Niveles de degradación del valor ….…….……..……42
Tabla 11. Identificación de amenaza por tipo de activo…….……55
Tabla 12. Matriz de riesgos de activos de información…… 56
Tabla 13. Criterios de seguridad de la información……..…… 92
Tabla 14. Controles de seguriad de la información……..…… 94
Tabla 15. Identificación de amenazas por tipo de activo ……..…… 119
Tabla 16. Matriz de analisis de riesgo……..……..… 119
Tabla 17. Controles de seguridad de la información …….……..…….119
Tabla 18. Plan de tratamiento del riesgo por activos de información …….. 132

LISTA DE FIGURAS

pág.

Figura 1. Organigrama.....21
Figura 2. Ciclo Deming ó Ciclo PHVA 30

LISTA DE ANEXOS

pág.

Anexo A. Formato Resumen Análitico en Educación 126
Anexo B. Carta Veeduría Distrital aprobación propuesta 133

RESUMEN

En el presente proyecto se realiza la propuesta para el diseño de un sistema de gestión de la seguridad de gestión de la información, basado en la norma ISO/IEC 27001:2013, para la Veeduría Distrital buscando garantizar la seguridad al interior de la organización, la mitigación de amenazas y la disminución de riesgos de seguridad, se recomiendan mejoras y nuevas medidas de seguridad para la red de datos de la Veeduría Distrital en la ciudad de Bogotá.

TÍTULO DEL PROYECTO

DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA RED DE DATOS DE LA VEEDURÍA DISTRITAL EN LA CIUDAD DE BOGOTÁ.

DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y privacidad de TI, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea. Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la Norma Técnica Colombiana NTC ISO/IEC 27001, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

Este documento contiene información confidencial de la infraestructura tecnológica de la Veeduría Distrital.

1. INTRODUCCIÓN

La evolución y el gran avance de la tecnología moderna van creciendo vertiginosamente día a día, al igual la forma de continuas amenazas y ataques cibernéticos, por lo cual se crea la necesidad de adoptar medidas y controles que permitan proteger y salvaguardar los activos informáticos. Lo anterior, sumado a que cada vez la seguridad de la información forme parte de los objetivos y planes estratégicos de las organizaciones. Por lo tanto, es imprescindible que los responsables encargados de velar por la protección y seguridad de sus recursos, infraestructura e información, constantemente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir y/o detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información del negocio, bien sea de tipo pública o privada.

Es así que la seguridad de la información constituye un mecanismo que permite a través de estándares y metodologías, determinar acciones que logren identificar el grado de exposición a las amenazas que puedan afectar a la Entidad.

2. DESCRIPCIÓN DEL PROBLEMA

2.1 PLANTEAMIENTO DEL PROBLEMA

Con el objetivo de fortalecer la seguridad de la información en la Veeduría Distrital y a pesar de los esfuerzos realizados por mejorar las situaciones como, la falta de una adecuada gestión de riesgos de seguridad, apropiación, concienciación y conocimiento en temas de seguridad por parte de los funcionarios de la Entidad, debido, una posible sensación de seguridad que hace creer que nada va a suceder o en otros casos no le dan la importancia a la seguridad de la información que por consiguiente generan la poca efectividad de las acciones en materia de seguridad de la información. Esta situación, también conlleva a que los funcionarios no diferencian entre seguridad informática y seguridad de la información.

Adicionalmente la Veeduría Distrital no cuenta con un sistema de información adecuado y robusto para la gestión de riesgos de seguridad, dificultando el estado global y transversal de su seguridad, en cuanto a procesos, tecnología y recurso humano, esto implica entre otros aspectos, que no está involucrada en forma activa toda la Entidad, sin contar con políticas de seguridad, procedimientos adecuados e identificación de controles de seguridad.

En este de orden de ideas, es indispensable contar con una normatividad de gestión de seguridad informática que cumpla con los estándares internacionales como es la norma ISO/IEC 27001:2013 que contribuirá a mejorar la seguridad en cuanto al manejo de información confiable y siempre disponible

2.2 FORMULACIÓN DEL PROBLEMA

Cómo el diseño de un Sistema de Gestión de la Seguridad de la Información - SGSI para la red de datos de la Veeduría Distrital permitirá establecer políticas y procedimientos para la seguridad informática y de la información.

3. JUSTIFICACIÓN

El desarrollo del presente proyecto es importante para la Veeduría Distrital ya que brindará solución a la problemática de seguridad presentada en la red de datos de su sistema informático, dichas problemáticas han sido ocasionados por el mal manejo de la información, afectando de manera general a usuarios y ciudadanía, y dado que en toda organización el activo más importante en una organización es la información se hace necesario protegerla de los riesgos y amenazas a las que constantemente está expuesta, garantizando su seguridad en aspectos tales como disponibilidad, confiabilidad, accesibilidad e integridad de la información.

El presente proyecto está enfocado en establecer la política y planificación del sistema de gestión de seguridad informático basado ISO 27001:2013, siendo ésta la base para el diseño del sistema de gestión de la seguridad de la información el cual servirá como guía para el proceso e implementarlo.

Por lo anterior, se considera necesario contar con un sistema de gestión de seguridad de la información basado en la norma 27001:2013 que mejore las condiciones que adolece actualmente la Veeduría Distrital, además del incumplimiento y/o desconocimiento por parte de funcionarios de lo estipulado por la norma ISO/IEC al no contar con un sistema de gestión de seguridad de la información, evitando sanciones y demandas judiciales por responsabilidades civiles y penales que son de obligación y disposición de cumplimiento por parte de la Entidad.

4. OBJETIVOS

4.1 GENERAL

Establecer políticas y procedimientos mediante el diseño de un Sistema de Gestión de la Seguridad Informática y de la información SGSI para la red de datos de la Veeduría Distrital en la ciudad de Bogotá, D.C.

.

4.2 ESPECIFICOS

Identificar y determinar los activos informáticos mediante la aplicación de instrumentos de recolección de información para establecer dominios del estándar ISO/IEC 27001:2013.

Determinar las vulnerabilidades, amenazas y riesgos de seguridad existentes para hacer valoración de los mismos aplicando la metodología MAGERIT.

Verificar la existencia de controles de acuerdo a la norma ISO/IEC 27001:2013 que ayuden a definir la existencia de políticas y procedimientos de seguridad.

Establecer los controles de la norma ISO 27001:2013, planes de mejoramiento y procedimientos que permitan mitigar las causas que originan los riesgos de seguridad de la información en la Veeduría Distrital.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

Con el fin de realizar el diseño de un sistema de gestión de la seguridad de la Información para la red de datos de la Veeduría Distrital en la ciudad de Bogotá, a continuación se relacionan los proyectos, guías y artículos que se consultaron para tal fin.

El proyecto de grado Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Financiera - Universidad Politécnico Gran Colombiano, Carlos Alberto Guzmán – Bogotá, Colombia, que cuentan con la infraestructura tecnológica adecuada y tiene implementado una serie de mecanismos de seguridad, como propósito proteger la confidencialidad, integridad y disponibilidad de la información del negocio.

El proyecto sobre “Seguridad Informática” presentado por Luis Daniel Álvarez Basuldúa, en la Universidad Iberoamérica, en la ciudad de México D.F., en el proyecto nos explica cómo el objetivo es evaluar el grado de efectividad en la seguridad de las tecnologías de información y en qué medida se garantiza la información, dado que se evalúa en toda su dimensión.

La guía “Implantación de un SGSI”, elaborada por la Agencia para el Desarrollo AGESIC, versión 1.0, tiene la finalidad de ayudar al responsable de la seguridad de la información y en la definición y lineamientos a la organización para el diseño de un SGSI.

El artículo “Los activos de la Seguridad de la Información - ISO 27001”, elaborado por el ingeniero José Manuel Poveda, nos explica sobre los principales activos informáticos para diseñar un Sistema de Gestión de la Seguridad de la Información – SGSI.

5.2 MARCO CONTEXTUAL

Como reseña histórica, tenemos que el Estatuto Orgánico de Bogotá, Decreto Ley 1421 de 1993, establece en sus artículos 118 al 124, la creación de la Veeduría

Distrital, define la estructura orgánica, las funciones; con el objeto de velar por la moralidad y la eficacia administrativa, sin perjuicio de las funciones que la Constitución y las leyes asignan a otros organismos o entidades. Esta Entidad lleva 24 años liderando el control social a través de actividades como creación de grupos de veedurías ciudadanas en las diferentes localidades y grupos especializados gestión pública[1].

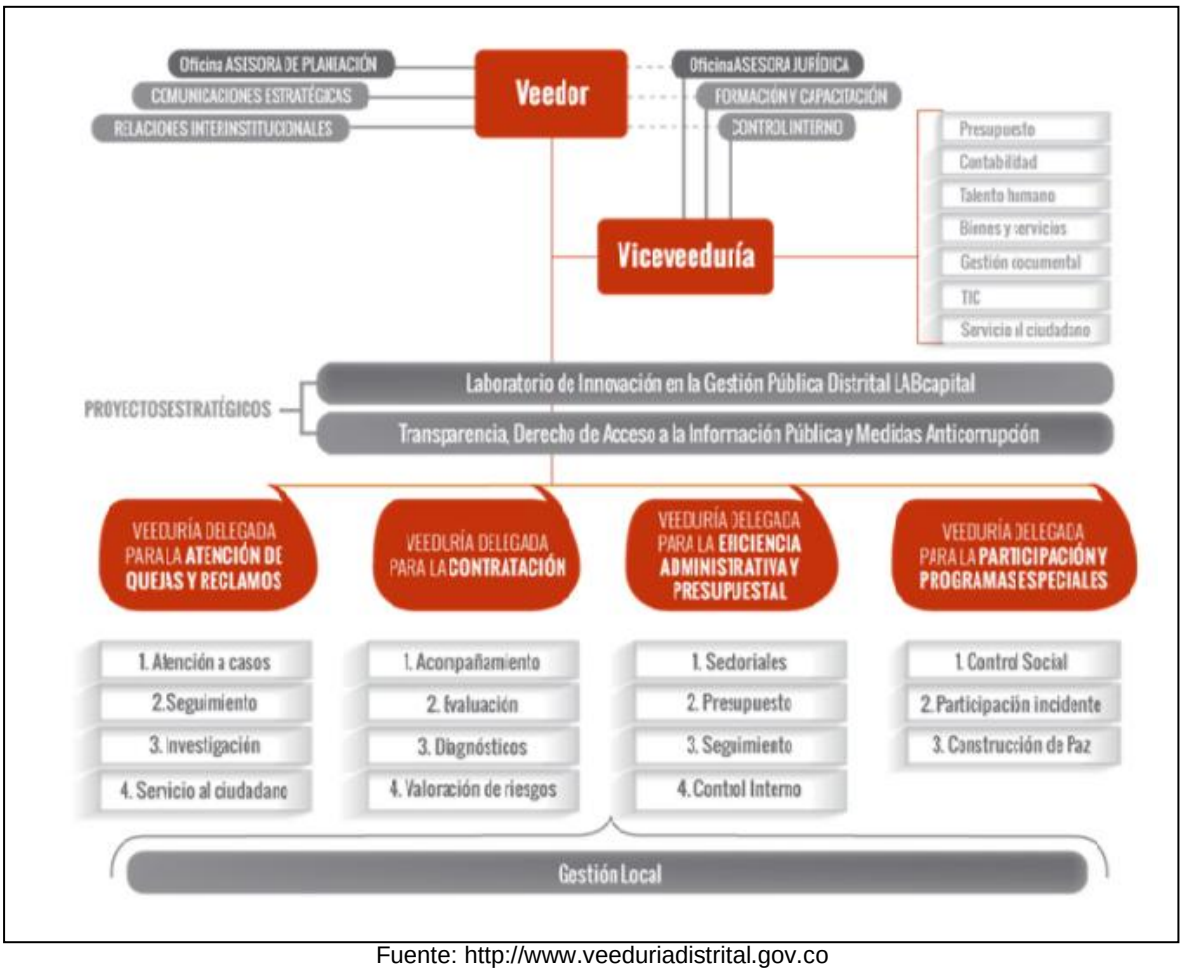
La Veeduría es un organismo de control de la Administración Distrital de carácter asesor y preventivo, con autonomía administrativa y presupuestal, que brindar herramientas diversas sobre gestión pública y control interno a las entidades del Distrito Capital en aras de mejorar sus niveles de transparencia, eficiencia y participación ciudadana[2].

5.2.1 Misión: La Veeduría es Promover la transparencia y prevenir la corrupción en la gestión pública distrital[3]

5.2.2 Visión: Es ser una Entidad respetada por su capacidad técnica para fortalecer el control preventivo, recuperar la confianza en las instituciones e incidir en todos los escenarios de la gestión pública[4].

[1] http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=1507
[2] http://veeduriadistrital.gov.co/sites/default/files/planeacion/DOCUMENTO%20PLAN%20ESTRAT%C3%89GICO%20final%2022122016%20%281%29%20%282%29%20%281%29.pdf
[3] http://www.veeduriadistrital.gov.co/
[4] http://www.contraloriabogota.gov.co/intranet/contenido/informes/Obligatorios/PRESUPUESTO/2001/Finanzas/informe-presupuesto/3central/6veeduria.htm

Figura 1. Organigrama



Fuente: http://www.veeduriadistrital.gov.co

5.2.3 Funciones de la Veeduría Distrital

a. Apoyar a los funcionarios responsables de lograr la vigencia de la moral pública en la gestión administrativa, así como a los funcionarios encargados del control interno, sin perjuicio de las funciones que la Constitución y las Leyes asignan a otros organismos o entidades;
b. Verificar que se obedezcan y ejecuten las disposiciones vigentes;
c. Controlar que los funcionarios y trabajadores distritales cumplan debidamente sus funciones, deberes y responsabilidades y como consecuencia de ello, exigir a las autoridades Distritales la adopción de las medidas;

d. Velar porque el desarrollo organizacional y de gestión administrativa esté de acuerdo con las políticas, planes, programas y proyectos identificados en el Plan de Desarrollo del Distrito Capital, de tal manera que se les dé adecuado y oportuno cumplimiento;
e. Propender por el cumplimiento de los compromisos adquiridos por la Administración con la comunidad;
f. Identificar, para que la administración las erradique, las prácticas administrativas corruptas o propicias para la ocurrencia de la corrupción;
g. Velar porque se sancione oportunamente a los servidores públicos y particulares que cometan delitos contra la administración pública, así como a los que atenten contra el interés general;
h. Promover la participación ciudadana para el seguimiento, evaluación y control del diseño y ejecución de las políticas públicas, los contratos de administración y la actuación de los servidores públicos, así como para la co-gestión del desarrollo de la ciudad[5].

5.2.4 Funciones de Gestión de Tecnologías de Información y Comunicaciones

El área de sistemas del Despacho de la Viceveeduría Distrital, realiza el soporte tecnológico de la Entidad, tiene como objetivo gestionar los recursos tecnológicos para asegurar el adecuado flujo de información necesaria en el cumplimiento de las funciones misionales de la Veeduría Distrital, además teniendo en cuenta las principales funciones como son:[6]

- Liderar y orientar la gestión de tecnologías de información y comunicaciones y responder por la administración de la plataforma tecnológica, los sistemas de información y el desarrollo e implementación de nuevos aplicativos, para garantizar a la Entidad, información oportuna y confiable y la automatización requerida para la simplificación y agilización de los procesos y procedimientos[7].

[5] www.contraloriabogota.gov.co/intranet/contenido/informes/.../6veeduria.htm
[6] Daruma Manual de funciones y competencias laborales de la planta de cargos- Código TH-MAN-01 Versión 02- Veeduría Distrital .
[7] Daruma Manual de funciones y competencias laborales de la planta de cargos- Código TH-MAN-01 Versión 02- Veeduría Distrital .

- Gestionar el soporte técnico y el soporte al usuario para el adecuado funcionamiento y uso de los sistemas de información[8].

- Desarrollar e implementar los sistemas de información útiles para la toma de decisiones, definiendo y simplificando el manejo de los mismos, propendiendo por la funcionalidad y pertinencia de la información, de acuerdo con el desarrollo tecnológico requerido.

- Elaborar informes en materia de su competencia o los que le sean solicitados por su Jefe inmediato sobre los planes, programas, proyectos o actividades de la dependencia.

- Contar con una infraestructura computacional actualizada y brindar a los usuarios las herramientas tecnológicas apropiadas para el desarrollo de sus funciones y depende orgánicamente del Despacho de Viceveeduría Distrital.

5.2.5 Acciones Gestión TIC:

- **Copias de seguridad:** Se realizan copias de seguridad semestral, mensual, semanal y diaria de las bases de datos. La copia mensual es de la información que se genera en toda la entidad y es enviada a un servidor de datos externo que se encarga de custodiar la información.
- **Desarrollo y mantenimiento de aplicaciones*:*** Se desarrollan aplicaciones de acuerdo a los requerimientos de los usuarios.
- Mantenimiento correctivo y preventivo equipos de cómputo: Revisión periódica de los equipos de cómputo con que cuenta la Entidad. Se realizan dos (2) limpiezas anuales a las estaciones de trabajo, impresoras, servidores de datos, etc, para prevenir daños futuros.
- **Soporte a usuarios:** El área de sistemas garantiza que los usuarios finales cuenten con las herramientas necesarias para el desarrollo de sus funciones.
- **Administración tecnológica y de la infraestructura de la red:** Revisión y mantenimiento de la red de datos de la entidad. Se realiza periódicamente la revisión de logs que genera el sistema.

[8] Daruma Manual de funciones y competencias laborales de la planta de cargos- Código TH-MAN-01 Versión 02- Veeduría Distrital

- **Desarrollo y mantenimiento de aplicaciones**: El área de sistemas realizó el desarrollo de software a la medida de acuerdo a las necesidades de los usuarios, adicionalmente se realizaron ajustes al software existente con el fin de cumplir con todas las solicitudes de los mismos. A continuación se relaciona el software desarrollado:

5.2.6. Modificaciones a software existente:

- **Ejercicios de control social- IWA**: Se han realizado ajustes a esta herramienta de acuerdo a las necesidades de la Entidad, con el fin de tener la información actualizada sobre la administración de los ejercicios de control social de la Delegada para la Participación y los avances de los mismos.

- **Software DARUMA**: Implementación de un sistema integrado de gestión de la calidad. Nos encontramos en la etapa de implementación y puesta en marcha[9].

- **Software SIGCO:** Software de seguimiento a la gestión contractual de la Veeduría Distrital.

5.3 MARCO CONCEPTUAL

Para realizar el diseño de un sistema de gestión de la seguridad de la información para la red de datos de la Veeduría Distrital en la ciudad de Bogotá, D.C., el presente proyecto se tendrán en cuenta aplicar en forma clara y concisa los siguientes conceptos:

Según la norma ISO/IEC 27001:2013-27002 las variables medibles que se identifican dentro del desarrollo del proyecto son:

.

[9] Informe de Gestión TIC- 2016

5.3.1 Confidencialidad. La seguridad de la información no sé deja a disposición ni de individuos, organizaciones o procesos que no estén autorizados.

5.3.2 Disponibilidad. El 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.

De igual forma 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 tiempos requeridos, posterior a la falla de los procesos críticos para el proyecto[10].

5.3.3 Integridad. Hace referencia al mantenimiento de la exactitud y complejidad de la información y los métodos de proceso.

5.3.4 Amenaza. Es la probabilidad de ocurrencia de un imprevisto que puede ser de origen natural o intencionado; las amenazas representan factores de riesgos externos que pueden explotar una vulnerabilidad existente en la Entidad.

5.3.5 Impacto: Es la consecuencia o pérdida que puede ocurrir en la materialización de una amenaza o la explotación de una vulnerabilidad; el impacto puede afectar las aspectos financieros, tecnológicos, físicas, de imagen o aspectos legales de la entidad.

5.3.6 Riesgo. Es la magnitud de pérdidas proyectadas tras la ocurrencia de explotación de una amenaza o vulnerabilidad.

5.3.7 Seguridad Informática. Consiste en los procedimientos, políticas, técnicas y herramientas de hardware y software implementadas, con el fin de proteger los sistemas informáticos y la información.

5.3.8 Valoración de riesgos. Proceso que permite la identificación, análisis y administración de los riesgos que internos y externos que posee una organización.

5.3.9 Vulnerabilidad. Es un factor de riesgo interno que representa las debilidades o el grado de exposición de los activos informáticos de la entidad, lo cual facilita la explotación de una amenaza.

[10] https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

5.4 MARCO TEÓRICO

5.4.1 Generalidades. Hoy en día las organizaciones manejan grandes volúmenes de información muy susceptible a través del correo electrónico, videoconferencias en vivo, información almacena en servidores, bases de datos de clientes, proveedores, finanzas, proyectos etc. y el avance tecnológico penetra en cualquiera de estos medios o dispositivos, generando vulnerabilidades en la información de las organizaciones. Por lo anterior se deben mantener en un entorno seguro donde los niveles de riesgos informáticos sean muy bajos y la seguridad informática se manifiesta cumpla con los principios básicos: confidencialidad, integridad y disponibilidad.

5.4.2 Vulnerabilidad Informática. Es cuando la información se vuelve susceptible a una potencial amenaza, por lo cual puede considerar una capacidad de reaccionar ante la presencia dicha situación, aplicando los controles adecuados para minimizar las posibilidades de que se materialicen.

5.4.3 Vulnerabilidad Física. Hace referencia a la vulnerabilidad que tiene el entorno físico del sistema de información debido a que en ataque cibernético ha violentado el acceso a la información para modificar o eliminar información sensible de la organización.

Tanto la información y como los activos de información constantemente se ven expuestos a gran cantidad de amenazas y riesgos a ser explotadas por las vulnerabilidades que se presentan en cualquier modalidad, almacenada o comparte información sin tener la protección y el tratamiento adecuado.

5.4.4 Seguridad de la Información. La seguridad de la información es ineludible para ser implementada en una organización y garantizar o mantener la disponibilidad, la integridad y la confidencialidad de la misma.

5.4.5 Gestión de Riesgos. Mecanismo que permite llevar a cabo el análisis, evaluación y planificación de los eventos internos o externos que pueden ocasionar un desastre y cuyos orígenes pueden ser intencionados o no. El resultado del proceso de gestión del riesgo, permite de manera sistemática realizar el procedimiento ideal con el fin de determinar el impacto que puede afectar el activo de TI; al mismo tiempo definir el plan de tratamiento de riesgos el cual permita administrar sus riesgos de manera adecuada permitiendo disminuir costos en la aceptación, transferencia, mitigación o reducción de los mismos.

5.4.6 Magerit Versión 3.0. Constituye una herramienta que administrar en forma eficiente los activos informáticos, comenzando por el levantamiento adecuado de los activos, su valoración y recomendando salvaguardas que puedan garantizar el control adecuado de los riesgos, siendo partícipes en el plan de mejora y seguimiento al mismo. Además esta metodología permite realizar en forma organizada el Proceso de Gestión de Riesgos, cuyo fin es efectuar y mantener el plan de tratamiento de riesgos.

5.4.7 Norma Técnica Colombiana NTC-ISO/IEC 27001. Esta norma Colombiana, se fundamenta en un estándar internacional que explica la forma de cómo se debe promover la seguridad de la información en una organización, ya que establece una metodología mediante el ciclo PHVA – planear, hacer, verificar y actuar con el fin de implementar y mantener el Sistema de Gestión de Seguridad de la Información.

5.4.8 Guía Técnica Colombiana GTC-ISO/IEC 27002. Esta Guía Técnica Colombiana establece de forma detallada controles de seguridad contenidos en la norma NTC-ISO/IEC 27001:2013 que deben aplicarse, con el fin de implementar de manera adecuada el Sistema de Gestión de Seguridad de la Información, finalmente está es la última actualización consta de: 14 dominios, 35 objetivos y 114 controles[11].

5.4.9 Guía Técnica Colombiana GTC-ISO/IEC 27003. Es la Guía de implementación para llevar a cabo el Sistema de Gestión de la Seguridad de la información, en la cual se establece las fases que deben desarrollarse para definir el proyecto a realizar, el diseño y la implementación del SGSI, de acuerdo y en concordancia con la norma ISO/IEC 27001

5.5 MARCO LEGAL

5.5.1 Ley 1273 de 2009. Los delitos informáticos estos se definen como "Ofensas que son cometidas contra individuos o grupos de individuos con un motivo criminal para dañar intencionalmente la reputación de la víctima o causarle daño mental o físico directa o indirectamente, utilizando redes de telecomunicación modernas como el Internet o teléfonos móviles". El término delito informático generalmente

[11] Norma Técnica Colombiana NTC - http://www.mineducacion.gov.co/1621/articles-96894_Archivo_pdf

es usado indistintamente a la palabra crimen cibernético, a la cual en inglés se le conoce como cybercrime, Organización de las Naciones Unidas (ONU) lo divide en dos categorías con sus respectivas definiciones

5.5.2 Ley Estatutaria 1266 del 31 de diciembre de 2008. “Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

5.5.3 Ley 1341 del 30 de julio de 2009. Define los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

5.5.4 Ley 603 de 2000. Hace refiere esta ley a la protección de los derechos de autor en Colombia. Es recordar que el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

5.5.5 La Ley 1266 de 2008. A través de esta ley se dictan las disposiciones generales del habeas data y se regula el manejo de la información, la cual está contenida en bases de datos personales, financiera, crediticia, comercial, de servicios y además proveniente de terceros países.

5.5.6 Constitución Política de 1991, en su artículo, que expresa: “El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley”.

5.5.7 Ley 23 de 1982, contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia.

La estrategia de Gobierno en Línea. En Colombia, busca construir un Estado más eficiente, más transparente y más participativo gracias a las TIC, lo cual significa

que a través de esta estrategia el Gobierno, logrará la excelencia en la gestión, los mejores servicios en línea al ciudadano y generará confianza en los ciudadanos.

6. MARCO METODOLÓGICO

6.1 METODOLOGÍA DE INVESTIGACIÓN

Para el desarrollo del presente proyecto de investigación el enfoque de la investigación se adelantará mediante la fase de la investigación cualitativa y cuantitativa, se pretende realizar una medición de las vulnerabilidades, amenazas y riesgos con respecto a las características de las variables de confidencialidad, integridad y disponibilidad de la información. Lo anterior tomando como base la Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 en concordancia con la Norma NTC-ISO/IEC 27003.

6.1.1 Población y muestra. Para la muestra de la investigación la población seleccionada serán todos los servidores públicos de la Veeduría Distrital y también se tomaran referencias de algunos datos suministrados por ciudadanos y grupos de interés.

6.1.2 Recolección y Fuentes de Información. Los aspectos generales que se tendrán en cuenta son de gestión, ubicación, propiedad, acceso, clasificación y de criticidad, por cada uno de los activos de información inmersos en el proceso Gestión de Tecnologías de las TIC's y Comunicaciones" pueden ser datos, información, servicios, software, hardware, redes de comunicaciones, instalaciones, personal responsable del manejo de cada activo de información, responsables de documentación, manuales material multimedia etc.

6.1.3 Técnicas o herramientas para recolección. Las técnicas o herramientas para recolección de datos son tanto cuantitativos y cualitativos: para llevar a cabo la recolección de datos se emplearán las siguientes técnicas.

Se hará uso de las siguientes técnicas para la recolección de información:

- Entrevista,
- Lista de chequeo,
- Cuestionario,
- Observación directa
- Pruebas de cumplimiento

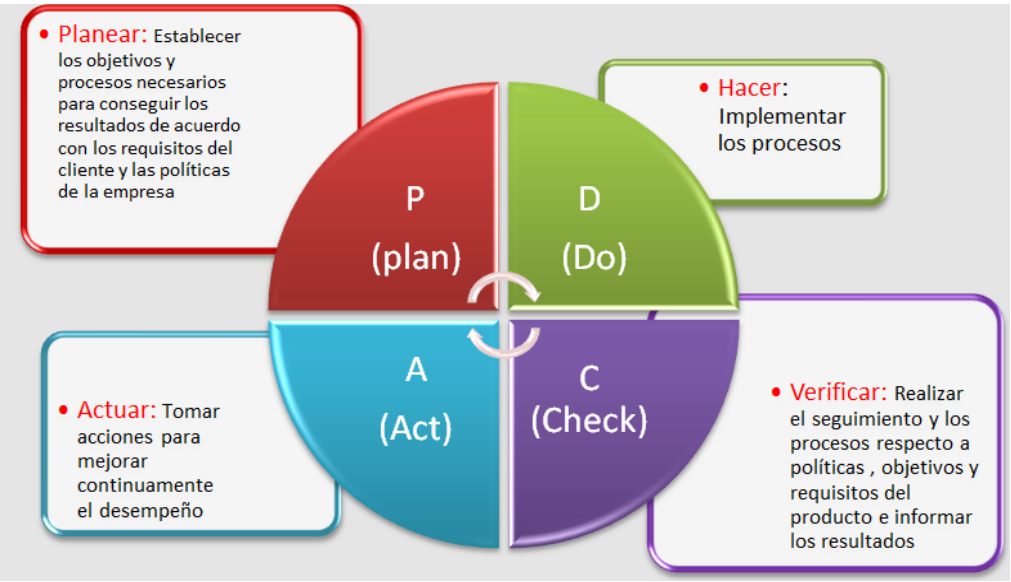
6.1.4 Procesamiento de la información. El procesamiento de la información para la implementación del Sistema de Gestión de Seguridad de la Información en la Veeduría Distrital, inicia con la recolección de la información y posteriormente será analizada y tabulada, con el fin de obtener datos estadísticos.

6.1.5 Análisis de datos. Teniendo la información recolectada, se procede a realizar el análisis, el cual se basa en las técnicas de recolección cuantitativa y cualitativa, lo que permitirá de la toma de decisión. Para efectuar este análisis se hace indispensable emplear hojas de cálculo (excel), que permite formular celdas, trabajar con gráficas y tablas dinámicas.

6.2 METODOLOGÍA DE DESARROLLO

Para el desarrollo del presente proyecto de investigación se aplicará la metodología MAGERIT Versión 3, que permitirá realizar el análisis y evaluación de riesgo de los activos de información, de acuerdo con la Norma Técnica Colombiana NTC-ISO/IEC 27001:2013:2013 y el ciclo PHVA (Planear, hacer, verificar y actuar), compuesto de las siguientes fases:

Figura 2. Ciclo Deming ó Ciclo PHVA



Fuente: http://administraciondelacalidadpaola.blogspot.com.co/2015/05/el-ciclo-de-deming.html

6.2.1 Fase 1 - Planeación. Se efectuará el análisis del estado actual del SGSI en la Entidad a través del análisis diferencial, esto permitirá definir el alcance real del proyecto.

6.2.2 Fase 2 - Hacer. En esta segunda fase se definirán objetivos, alcance y tiempo de implementación del Sistema de Gestión de Seguridad de la Información, las actividades y tiempos deben ser aprobadas por el Comité de Seguridad de la información.

6.2.3 Fase 3 - Verificar. En esta fase se permitirán realizar las revisiones necesarias con el fin que se cumplan los objetivos propuestos de manera adecuada y correcta, a través del seguimiento de cada una de las actividades establecidas.

6.2.4 Fase 4 - Actuar. Esta última fase es la de Mejora continua, se revisarán y evaluarán las acciones de mejora, preventivas y correctivas de las actividades que permitan la implantación del SGSI.

7. RECURSOS REQUERIDOS

Los costos por servicios personales y gastos generales son los siguientes:

Tabla 1. Recursos requeridos para el desarrollo del proyecto

RECURSOS	Ítem / Actividad	Cantidad	Costo Unitario ($)	Costo Total ($)
HUMANO	Investigador	1	6.500.000	6.500.000
	Técnico	1	2.150.000	2.150.000
	Asistente	1	1.200.000	1.200.000
MATERIALES	Resma de papel	5	40.000	200.000
	Fotocopias	2	8.000	16.000
	DVD-CD	100	300	30.000
	Tóner impresora	1	90.550	90.550
	Esferos	3	8.200	24.600
	Refrigerios	10	3.500	35.000
	Transporte	5	2.000	10.000
	Gasolina	40	8.000	320.000
TÉCNICOS / TECNOLÓGICOS	Equipos de Cómputo	3	2.450.000	7.350.000
	Celular	3	2.000.000	6.000.000
	Discos Duros	4	400.000	1.600.000
	Memorias USB	3	20.000	60.000
Costo Total del Proyecto				**$15.910.000**

Fuente: el autor

8. ANÁLISIS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

8.1 DESCRIPCIÓN Y ANÁLISIS DE RIESGOS

El siguiente análisis de riesgos permite identificar activos de información pueden estar expuestos a unos niveles altos de riesgo y cuáles activos de información podrían causar un gran impacto si se materializan las amenazas que podrían afectar al a Veeduría Distrital.

De acuerdo a lo anterior, la metodología a utilizar es la Magerit con la cual se debe seguir los siguientes pasos:

- Identificar los activos relevantes para la organización
- Valorar los activos
- Identificar a qué amenazas están expuestos los activos
- Valorar la influencia de la amenaza en cada uno de los activos, en cuanto a la probabilidad de ocurrencia y el porcentaje de degradación que afectaría al valor del activo.
- Determinar el impacto potencial
- Determinación del riesgo potencial

8.2 IDENTIFICACIÓN DE ACTIVOS Y VALOR DE DIMENSIONES

Para dar inicio al análisis de riesgos de los activos de TI, se procede a identificar los activos de información que a continuación se listan en la “tabla 1”, organizados según el tipo.

Tabla 2. Identificación de activos informáticos de la Entidad

N°	TIPO ACTIVO	NOMBRE DEL ACTIVO
A1	**[D] DATOS / INFORMACIÓN**	Documentación Técnica
A2	**[S] SERVICIOS**	Controlador de dominio principal (PDC)
A3		Controlador de dominio backup (BDC)
A4		Portal Institucional
A5		Portal intranet
A6		Correo electrónico Gmail-Drive

Tabla 2. (Continuación)

N°	TIPO ACTIVO	NOMBRE DEL ACTIVO
A7	[S] SERVICIOS	Almacenamiento en la nube
A8		Sistema Distrital de Quejas y Soluciones -SDQS-
A9		Sistema acceso Biométrico
A10		Redes Sociales
A11		Portal Académico (B-Learning) Control social
A12		Canal dedicado ETB
A13	[SW] SOFTWARE/ APLICACIONES INFORMÁTICAS	Software de Sistemas operativos (medios)
A14		Software de Base de Datos (medios)
A15		Sistema de Selección de Personal - Sicop
A16		Sistema de Gestión de Calidad - Daruma
A17		Aplicativo de Nómina
A18		Sistema de Gestión Documental - ORFEO
A19		Seguimiento al Plan de Desarrollo - SEGPLAN
A20		Software aplicativo para manejo de bases de datos de gestión documental - Winisis
A21		Software Historias Laborales
A22		Software Ofimático
A23		Aplicativo Opget - SDH
A24		Software Inventario Equipos
A25		Software Inventario de Almacén
A26		Software Aplicación de Archivo Inactivo.
A27		Software Aplicación de gestor de máquinas virtuales
A28		Storm User 5.0 Secretaria de Ambiente
A29		Aplicativo Reservas
A30		Antivirus McAfee
A31		Antispam SymantecCloud
A32		Aplicación de Catalogo de documentación
		Software de Índice de Transparencia
A33		Aplicativo Certificaciones y Permisos
A34		Equipos de cómputo
A35		Switch de borde 4210G
A36		Sistema de almacenamiento formato rack
A38		Equipo de Seguridad Perimetral
A39		Servidor formato blade marca Hewlett Packard. Modelo proliant BL460C G7
A40		Servidor Proliant 120 G5

Tabla 2. (Continuación)

N°	TIPO ACTIVO	NOMBRE DEL ACTIVO
A41	[HW] EQUIPOS	Impresora para código de barras
A42		Servidor controlador de dominio principal
A43		Servidor DELL PowerEdge 4300/350
A44		Servidor Compaq Proliant 2500
A45		Servidor Hewlett Packard Proliant ML110
A46		Servidor DELL AntiSpam McAfee Appliance SCM 3100
A47		Servidor Proliant ML370 G6
A48		3COM Baseline Switch 2024 de 24 Puertos
A49		Switch TrendNet TE100-S24 de 24 Puertos
A50		Switch Netgear FS108 de 8 puertos
A51		Hubs 3COM SuperStack II PS Hub 40 de 24 Puertos
A52		Router Cisco 1700 Series propiedad de la ETB
A53		Router Cisco 1800 Series propiedad de la SHD
A54		Modem Adtran Express 6503 propiedad de la ETB
A55		UPS de 10K autonomía aprox. 30min.para sostenimiento del centro de cómputo
A56		PC’s para funciones de E-Mail y Proxy Servers
A57		Servidor Backups VD-BAK2015
A58		Servidor Backups VD-SERVER
A59		Copia de Respaldo - Dataprotector
A60		Sistema de Backups - Dataprotector
A61		Servidor de correo -Gmail DL 380 G5
A62		Servidor Ambiente de pruebas y desarrollo
A63		Servidor de base de datos Nómina
A64		Servidor de Virtualización
A65		Servidor de Archivos
A66		Máquina Virtual Windows NT 4.0 (Base de Sisep)
A67		Router ETB
A69		Portátiles
A68		Sistema Operativos de servidores
A69		Impresoras multifuncionales

Tabla 2. (Continuación)

N°	TIPO ACTIVO	NOMBRE DEL ACTIVO
A70	**[AUX] ELEMENTOS AUXILIARES**	Sistema de Aire Acondicionado
A71		Armario y caja fuerte
A72		Planta eléctrica
A73		Mobiliario
A74		Telefonía IP
A75		Cuarto de servidores
A76		Sistema de control de acceso físico
A77		PBX
A78		Alarmas
A79		Gabinete de 8 blades
A80	**[P] PERSONAL**	Desarrollares
A81		Operadores
A82		Soporte técnico
A83		Usuarios internos
A84		Usuarios externos

Fuente: Gestión de tecnologías de Información y Comunicaciones

8.3 VALORACIÓN DE ACTIVOS

A continuación se realiza la valoración en cada uno de los activos de información, según las siguientes dimensiones de seguridad y los criterios de valoración:

- [D] Disponibilidad
- [I] Integridad de los datos
- [C] Confidencialidad de la información
- [A] Autenticidad de los usuarios y de la información
- [T] Trazabilidad del servicio y de los datos

Tabla 3. Rangos valoración Activos

Dimensiones		Valor	Criterio
MA	Muy Alto	9 - 10	Daño muy grave
A	Alto	6 – 8	Daño grave
M	Medio	3 – 5	Daño importante
B	Bajo	1 – 2	Daño menor
MB	Despreciable	0	Irrelevante a efectos prácticos

Fuente: el autor

Estas valoraciones fueron efectuadas en entrevistas realizadas a cada uno de los responsables de los activos de información y no requiere que sean calificados los activos en sus cinco dimensiones, ésta depende si aplica o no a dicha dimensión. De igual forma "*la valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión*".[12]

Tabla 4. Valoración Activos tipo: [D] Datos/Información

Activo	**Dimensiones**				
	D	**I**	**C**	**A**	**T**
Documentos técnicos	[8]	[6]	[6]	[9]	

Fuente : El autor

Tabla 5. Valoración Activos tipo: [S] Servicios

Activo	**Dimensiones**				
	D	**I**	**C**	**A**	**T**
Controlador de dominio principal (PDC)	[10]	[10]	[10]	[9]	
Controlador de dominio backup (BDC)	[10]	[10]	[10]	[9]	[5]
Portal Institucional	[10]	[10]	[10]	[9]	
Portal intranet	[10]	[10]	[10]	[9]	
Correo electrónico Gmail	[10]	[10]	[10]	[9]	
Almacenamiento en la nube	[10]	[10]	[10]	[9]	
Sistema Distrital de Quejas y Soluciones -SDQS-	[10]	[10]	[10]	[9]	
Sistema acceso Biométrico	[10]	[10]	[10]	[7]	
Redes Sociales	[2]	[2]	[2]	[2]	
Portal Académico (B-Learning)	[10]	[10]	[10]	[9]	
Canal dedicado ETB	[10]	[10]	[10]	[9]	

Fuente: El autor

[12] Magerit-versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 2-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ p. 15

Tabla 6. Valoración Activos tipo: [SW] Software /Aplicaciones Informativas

Activo	Dimensiones				
	D	I	C	A	T
Software de Sistemas operativos (medios)	[9]	[9]			
Software de Base de Datos (medios)	[9]	[9]			
Sistema de Selección de Personal - Sicop	[9]	[3]			
Sistema de Gestión de Calidad - Daruma	[10]	[9]	[10]		
Aplicativo de Nómina	[9]	[10]	[10]	[10]	[10]
Sistema de Gestión Documental - ORFEO	[5]	[10]	[10]	[10]	
Seguimiento al Plan de Desarrollo - SEGPLAN	[10]	[10]			
Software aplicativo para manejo de bases de datos de archivos - Winisis	[8]	[8]	[6]	[4]	
Aplicativo Contratación - SIGCO	[10]	[10]	[10]		
Software Ofimático	[7]	[7]	[6]	[7]	
Aplicativo Opget - SDH	[7]	[7]	[6]	[7]	
Inventario Equipos	[9]	[9]	[8]	[9]	
Inventario de Almacén	[7]	[8]	[7]		
Aplicación de Archivo Inactivo.	[10]	[10]	[10]	[9]	[5]
Aplicación de gestor de máquinas virtuales	[7]	[7]	[6]	[7]	
Storm User 5.0 S.D.Ambiente	[7]	[7]	[6]	[7]	
Aplicativo Reserva de salones	[7]	[7]	[6]	[7]	
Antivirus McAfee	[7]	[7]	[6]	[7]	
Antispam SymantecCloud	[7]	[7]	[6]	[7]	
Aplicación de Catalogo de documentación	[7]	[7]	[6]	[7]	
Aplicativo Certificaciones y Permisos	[6]	[6]		[9]	

Fuente: El autor

Tabla 7. Valoración Activos tipo: [HW] Equipos

Activo	Dimensiones				
	D	I	C	A	T
Equipo de Seguridad Perimetral	[6]	[6]		[9]	
Servidor formato blade marca Hewlett Packard. Modelo proliant BL460C G7	[10]	[10]			
Servidor Proliant 120 G5	[7]	[7]	[9]	[10]	
Impresora para código de barras	[7]	[7]	[9]	[10]	
Servidor controlador de dominio principal	[7]	[7]	[9]	[10]	
Servidor DELL PowerEdge 4300/350	[7]	[7]	[9]	[10]	
Servidor Compaq Proliant 2500	[7]	[7]	[9]	[10]	
Servidor Hewlett Packard Proliant ML110	[6]		[7]	[7]	
Servidor DELL AntiSpam McAfee Appliance SCM 3100	[5]	[9]	[10]	[7]	
Servidor Proliant ML370 G6	[7]	[7]	[9]	[10]	
3COM Baseline Switch 2024 de 24 Puertos	[7]				[7]
Switch TrendNet TE100-S24 de 24 Puertos	[10]	[10]	[10]		
Switch Netgear FS108 de 8 puertos	[10]	[10]	[10]	[8]	
Hubs 3COM SuperStack II PS Hub 40 de 24 Puertos	[10]	[8]	[6]		
Router Cisco 1700 Series propiedad de la ETB	[8]	[8]	[9]	[10]	
Router Cisco 1800 Series propiedad de la SHD	[8]	[8]	[9]	[10]	
Modem Adtran Express 6503 propiedad de la ETB	[8]	[8]	[9]	[10]	
UPS de 10K autonomía aprox. 30min. Sostenimiento del centro de cómputo	[8]	[8]	[9]	[10]	
PC’s para funciones de E-Mail y Proxy Servers	[9]	[9]			[9]

Tabla 7. Continuación

Activo	Dimensiones				
	D	I	C	A	T
Servidor Backups VD-BAK2015	[9]	[9]	[9]	[10]	
Servidor Backups VD-SERVER-SD2,	[7]				
Copia de Respaldo - Dataprotector	[7]				
Sistema de Backups - Dataprotector	[7]				
Servidor de Correo electrónico Google- Drive DL 380 G5	[7]		[8]		
Servidor Ambiente de pruebas y desarrollo	[9]	[9]	[9]	[10]	
Servidor de base de datos Nómina	[5]	[6]			
Servidor de Virtualización	[10]	[10]	[10]		
Servidor de Archivos	[10]	[10]			
Máquina Virtual Windows NT 4.0 (Base de Sisep)	[7]	[7]	[7]		
Router ETB	[10]	[10]	[10]	[10]	
Portátiles	[10]	[10]	[10]	[10]	
Sistema Operativos de servidores	[10]	[10]	[10]	[10]	
Impresoras multifuncionales	[10]	[10]		[10]	

Fuente: El Autor

Tabla 8. Valoración Activos tipo: [AUX] Elementos Auxiliares

Activo	Dimensiones				
	D	I	C	A	T
Sistema de Aire Acondicionado	[6]				
Armario y caja fuerte	[6]				
Planta eléctrica	[6]				
Mobiliario	[6]				

Tabla 8. Continuación

Activo	Dimensiones				
	D	I	C	A	T
Telefonía IP	[6]				
Cuarto de servidores	[6]				
Sistema de control de acceso físico	[6]				
PBX	[6]				
Alarmas	[6]				
Gabinete de 8 blades	[6]				

Fuente: El autor

Tabla 9. Valoración Activos tipo: [P] Personal

Activo	Dimensiones				
	D	I	C	A	T
Desarrollares	[7]	[7]	[9]	[10]	[7]
Operadores	[5]	[9]	[10]	[7]	[5]
Soporte técnico	[7]	[7]	[9]	[10]	[7]
Usuarios internos	[7]	[7]	[9]	[10]	[7]
Usuarios externos	[7]	[7]	[9]	[10]	[7]

Fuente: El autor

Finalmente después de realizar la identificación de los activos de información de la Veeduría Distrital, se observa que activos pueden estar expuestos a niveles altos de riesgo y en el evento que se llegará a materializar las amenazas cuales podrían causar un gran impacto.

Teniendo como base la metodología MAGERIT v3, los activos informáticos de mayor riesgo y de gran impacto deben seguir los siguientes pasos:

- Identificación de los activos relevantes para la Entidad
- Valorar los activos de información
- Identificar a qué amenazas están expuestos los activos

- Valorar la influencia de la amenaza en los activos, probabilidad de ocurrencia y el porcentaje de degradación del valor del activo.
- Determinar el riesgo e impacto potencial.

8.4 IDENTIFICACIÓN DE AMENAZAS

En cuanto a la identificación de las amenazas, también se tomará como base la clasificación establecida en la metodología "MAGERIT", organizada en cuatro categorías, de la siguiente manera:

[**A**] Ataques intencionados
[**N**] De origen natural
[**I**] De origen industrial
[**E**] Errores y fallos no intencionados

Tabla 10. Niveles degradación del valor

Valor		Criterio
MA - MA	MA	Degradación MUY ALTA del activo
A - 89%	A	Degradación ALTA considerable del activo
M - 69%	M	Degradación MEDIANA del activo
B - 49%	B	Degradación BAJA del activo
1% - 9%	MB	Degradación MUY BAJA del activo

Fuente: el autor

8.4.1 Identificación y Valoración de Amenazas Tipo: [D] Datos

A continuación se realiza la identificación de amenazas por tipo de activo:

Tabla 11. Identificación de amenazas por tipo de activos: Datos

Activo	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Documentación Técnica	[N.2] Daños por agua	MA	MA	MA			
	[N.*] Desastres naturales	MA	MA	MA			
	[I.1] Fuego	MA	MA	MA			
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	B	B			
	[E.18] Destrucción de la información	M	M	M			

Fuente: Herramienta Pilar 6.2

8.4.2 Identificación y Valoración de Amenazas Tipo: [S] Servicios

Tabla 12. Identificación y valoración de amenazas en activos tipo: Servicios

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Controlador de dominio principal (PDC)	[E.2] Errores del administrador del sistema / de la seguridad	B	B	B	B		
	[E.15] Alteración de la información	MA		MA	MA		
	[E.18] Destrucción de la información	MA	MA	MA	MA		
	[E.19] Fugas de información	MA		MA	MA		
	[E.24] caída del sistema por agotamiento recursos	M	M				
	[A.5] suplantación de la identidad del usuario	MA		M	M	MA	
	[A.6] Abuso de privilegios de acceso	B		B	B		
	[A.7] uso no previsto	MA	MA	B	B		
	[A.11] Acceso no autorizado	M		B	M		
	[A.15] Modificación de la información	M		M			
	[A.18] Destrucción de la información	M	M	M			
	[A.19] revelación de información	M			M		
	[A.24] Denegación de servicio	M	M				
Controlador de dominio Backup (BDC)	[E.2] Errores del administrador del sistema / de la seguridad	B	B	B	B		
	[E.15] Alteración de la información	MA		MA	MA		

Tabla 12. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Controlador de dominio backup (BDC)	[E.18] Destrucción de la información	MA	MA	MA	MA		
	[E.19] Fugas de información	MA	MB	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	M	M				
	[A.5] suplantación de la identidad del usuario	MA		M	M	MA	
	[A.6] Abuso de privilegios de acceso	B		B	B		
	[A.7] uso no previsto	MA	MA	B	B		
	[A.11] Acceso no autorizado	M		B	M		
	[A.15] Modificación de la información	M		M			
	[A.18] Destrucción de la información	M	M				
	[A.19] revelación de información	M			M		
	[A.24] Denegación de servicio	M	M				
	[E.2] Errores del administrador del sistema	B	B	B	B		
	[E.15] Alteración de la información	MA		MA	MA		
	[E.18] Destrucción de la información	MA	MA	MA	MA		
	[E.19] Fugas de información	A	A	A	A		
	[E.24] caída sistema por agotamiento de recursos	M	M				

Tabla 12. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Portal Institucional	[E.2] Errores del administrador del sistema	MA	MA	MA			
	[E.3] Errores de monitorización (log)	M	M	M			
	[E.4] Errores de configuración	MA	MA	MA			
	[E.15] Alteración de la información	B	B	B			
	[E.18] Destrucción de la información	MA	MA	MA			
	[E.20] vulnerabilidades de los programas (software)	B	B	B			
	[E.21] Errores de mantenimiento / actualización de programas (software)	B	B	B			
	[E.24] caída del sistema por agotamiento de recursos	MA	MA	MA			
	[E.28] Indisponibilidad del personal	B	B	B			
	[A.5] suplantación de la identidad del usuario	A	A	A	MA		
	[A.6] Abuso de privilegios de acceso	B	B	B			
	[A.8] Difusión de software dañino	MA	MA	MA	MA		
	[A.11] Acceso no autorizado	A	A	A	MA		
	[A.15] Modificación de la información	M	M	M			
	[A.18] Destrucción de la información	MA	MA	MA			
	[A.22] Manipulación de programas	M	M	M			
	[A.24] Denegación de servicio	MA	MA	MA			

Tabla 12. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Portal Intranet	[E.2] Errores del administrador del sistema/seguridad	MA	MA	MA			
	[E.3] Errores de monitorización (log)	MA	MA	MA			
	[E.4] Errores de configuración	MA	MA	MA			
	[E.15] Alteración de la información	B	B	B			
	[E.18] Destrucción de la información	MA	MA	MA			
	[E.20] vulnerabilidades de los programas (softw)	M	M	M			
	[E.21] Errores de mantenimiento / actualización de programas (software)	B	B	B			
	[E.24] caída del sistema por agotamiento de recursos	MA	MA	MA			
	[E.28] Indisponibilidad del personal	B	B	B			
	[A.5] suplantación de la identidad del usuario	A	A	A	MA		
	[A.6] Abuso de privilegios de acceso	B	B	B			
	[A.8] Difusión de software dañino	MA	MA	MA	MA		
	[A.11] Acceso no autorizado	A	A	A	MA		
	[A.15] Modificación de la información	M	M	M			
	[A.18] Destrucción de la información	MA	MA	MA			
	[A.22] Manipulación de programas	M	M	M			
	[A.24] Denegación de servicio	MA	MA	MA			

Tabla 12. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Correo electrónico Google-Drive	[A.6] Abuso de privilegios de acceso	MA		A	MA		
	[A.7] uso no previsto	MA	MA	B	B		
	[A.11] Acceso no autorizado	M		B	M		
	[A.13] Repudio (negación de actuaciones)	MA		MA			
	[A.18] Destrucción de la información	M	M				
	[A.19] revelación de información	M			M		
	[A.24] Denegación de servicio	M	M				
Sistema de Acceso Biométrico	[N.*] Desastres naturales	A	A			A	
	[I.1] Fuego	A	A			A	
	[I.2] Daños por agua	A	A			A	
	[I.5] Avería de origen físico o lógico	MA	MA			MA	
	[I.6] Corte del suministro eléctrico	M	M			M	
	[A.25] Robo de equipos	MA	MA			MA	
	[A.26] Ataque destructivo	MA	MA			MA	
Sistema Distrital de Quejas - SDQS	[N.1] Fuego	MA	MA				MA
	[N.2] Daños por agua	MA	MA				MA
	[N.*] Desastres naturales	MB	MB				MB
	[I.1] Fuego	MA	MA				MA

Tabla 12. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Sistema Distrital de Quejas - SDQS	[I.5] Avería de origen físico o lógico	MA	MA				MA
	[I.6] Corte del suministro eléctrico	MA	MA				MA
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				A
	[I.8.12] Interrupción deliberada por un agente externo	MA	MA				MA
	[E.4] Errores de configuración	A	A				A
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M				M
	[E.24] caída del sistema por agotamiento de recursos	MA	MA				MA
	[A.25] Robo de equipos	MA	MA				MA
Porta Académico(B-Learning)	[E.2] Errores del administrador del sistema / de la seguridad	MA	MA	MA			
	[E.3] Errores de monitorización (log)	MA	MA	MA			
	[E.4] Errores de configuración	MA	MA	MA			
	[E.15] Alteración de la información	B	B	B			
	[E.18] Destrucción de la información	MA	MA	MA			

Tabla 12. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Porta Académico(B-Learning)	[E.20] vulnerabilidades de los programas (software)	M	M	M			
	[E.21] Errores de mantenimiento / actualización de programas (software)	B	B	B			
	[E.24] caída del sistema por agotamiento de recursos	MA	MA	MA			
	[E.28] Indisponibilidad del personal	B	B	B			
	[A.5] suplantación de la identidad del usuario	A	A	A	MA		
	[A.6] Abuso de privilegios de acceso	B	B	B			
	[A.8] Difusión de software dañino	MA	MA	MA	MA		
	[A.11] Acceso no autorizado	A	A	A	MA		
	[A.15] Modificación de la información	M	M	M			
	[A.18] Destrucción de la información	MA	MA	MA			
	[A.22] Manipulación de programas	M	M	M			
	[A.24] Denegación de servicio	MA	MA	MA			
Almacena-miento en la Nube	[E.2] Errores del administrador del sistema	MA	MA	MA			
	[E.3] Errores de monitorización (log)	M	M	M			

Tabla 12. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Almacena-miento en la Nube	[E.4] Errores de configuración	MA	MA	MA			
	[E.15] Alteración de la información	B	B	B			
	[E.18] Destrucción de la información	MA	MA	MA			
	[E.20] vulnerabilidades de los programas (software)	B	B	B			
	[E.21] Errores de mantenimiento / actualización de programas (software)	B	B	B			
	[E.24] caída del sistema por agotamiento de recursos	MA	MA	MA			
	[E.28] Indisponibilidad del personal	B	B	B			
	[A.5] suplantación de la identidad del usuario	MA	MA	MA	MA		
	[A.6] Abuso de privilegios de acceso	B	B	B			
	[A.8] Difusión de software dañino	MA	MA	MA	MA		
	[A.11] Acceso no autorizado	MA	MA	MA	MA		
	[A.15] Modificación de la información	M	M	M			
	[A.18] Destrucción de la información	MA	MA	MA			

Tabla 12. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Canal Dedicado ETB	[N.1] Fuego	MA	MA				MA
	[N.2] Daños por agua	MA	MA				MA
	[N.*] Desastres naturales	MB	MB				MB
	[I.1] Fuego	MA	MA				MA
	[I.5] Avería de origen físico o lógico	MA	MA				MA
	[I.6] Corte del suministro eléctrico	MA	MA				MA
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				A
	[I.8.12] Interrupción deliberada por un agente externo	MA	MA				MA
	[E.4] Errores de configuración	A	A				A
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M				M
	[E.24] caída del sistema por agotamiento de recursos	MA	MA				MA
	[A.25] Robo de equipos	MA	MA				MA

Fuente: Herramienta Pilar 6.2

8.4.3 Identificación y Valoración de Amenazas Tipo: [HW] Software

Tabla 13. Identificación y valoración de amenazas en activos tipo: Software

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Software de Sistemas Operativos (medios)	[N.1] Fuego	MA	MA				

Tabla 13. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Software de Sistemas Operativos (medios)	[N.2] Daños por agua	M	M				
	[N.*] Desastres naturales	A	A				
	[I.1] Fuego	MA	MA				
	[I.2] Daños por agua	M	M				
	[I.*] Desastres industriales	A	A				
	[I.3] Contaminación medioambiental	M	M				
	[I.5] Avería de origen físico o lógico	M	M				
	[I.6] Corte del suministro eléctrico	B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	B				
	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M				
	[E.25] Pérdida de equipos	MA	MA				
	[A.6] Abuso de privilegios de acceso	B	B	B			
	[A.7] uso no previsto	MA		MA			
	[A.11] Acceso no autorizado	MA	MA				

Tabla 13. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Software de Sistemas Operativos (medios)	[A.23] Manipulación del hardware	MA	MA				
	[A.24] Denegación de servicio	MA	MA				
	[A.26] Ataque destructivo	MA	MA				
Software de Bases de Datos (medios)	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.*] Desastres industriales	MA	MA				
	[I.3] Contaminación medioambiental	M	M				
	[I.4] Contaminación electromagnética	M	M				
	[I.5] Avería de origen físico o lógico	MA	MA				
	[I.6] Corte del suministro eléctrico	MA	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	B				
Software de Nómina	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.5] Avería de origen físico o lógico	M	M				
	[I.6] Corte del suministro eléctrico	A	A				

Tabla 13. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Software de Historias Laborales	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				
	[E.2] Errores del administrador del sistema	B	B	B	B		
	[E.4] Errores de configuración	M	M	M	M		
	[E.8] Difusión de software dañino	A	A	A			
Software de Daruma	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.4*] Desastres naturales	MA	MA				
	[I.5] Avería de origen físico o lógico	M	M				
	[I.6] Corte del suministro eléctrico	A	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				
	[E.2] Errores del administrador del sistema / de la seguridad	B	B	B	B		
	[E.8] Difusión de software dañino	A	A	A			
Claves con Licenciamiento	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[E.4] Errores de configuración	M	M	M	M		
	[E.8] Difusión de software dañino	A	A	A			

Tabla 13. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Software de Índice de Transparencia	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.5] Avería de origen físico o lógico	MA	MA				
	[I.6] Corte del suministro eléctrico	MA	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA	MA				
PBX	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[E.4] Errores de configuración	MA	MA				
	[E.8] Difusión de software dañino	MA	MA				
Sistema de Gestión Documental - Orfeo	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.5] Avería de origen físico o lógico	M	M				
Seguimiento al Plan de Desarrollo - Segplan	[A.6] Abuso de privilegios de acceso	M		M	M		
	[A.7] uso no previsto	MB	B	B	B		
	[A.11] Acceso no autorizado	MB		B	A		

Tabla 13. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Seguimiento al Plan de Desarrollo - Segplan	A.23] Manipulación del hardware	M	M				
	[A.24] Denegación de servicio	A	A				
	[A.26] Ataque destructivo	MA	MA				
Sistema de Gestión de documenal Winisis	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.5] Avería de origen físico o lógico	M	M				
	[I.6] Corte del suministro eléctrico	A	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				
	[E.2] Errores del administrador del sistema	B	B	B	B		
	[E.4] Errores de configuración	M	M	M	M		
	[E.8] Difusión de software dañino	A	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	B				
Redes Sociales	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	B				
	[E.25] Pérdida de equipos	A	A				
	[A.6] Abuso de privilegios de acceso	A		A	A		

Tabla 13. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Redes Sociales	[I.6] Corte del suministro eléctrico	7B	7B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	7B	7B				
	[E.2] Errores del administrador del sistema / de la seguridad	B	B	B	B		
	[E.4] Errores de configuración	M	M	M	M		
	[E.8] Difusión de software dañino	A	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	B				
	[E.25] Pérdida de equipos	MA	MA				
Software de Inventario Almacén	[A.6] Abuso de privilegios de acceso	M		M	M		
	[A.7] uso no previsto	MB	B	B	B		
	[A.11] Acceso no autorizado	MB		B	A		
	[A.23] Manipulación del hardware	M	M				
	[A.24] Denegación de servicio	7B	7B				
	[A.26] Ataque destructivo	MA	MA				

Tabla 13. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Software de Inventario Almacén	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.5] Avería de origen físico o lógico	M	M				
	[I.6] Corte del suministro eléctrico	A	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				
	[E.2] Errores del administrador del sistema / de la seguridad	B	B	B	B		
	[E.4] Errores de configuración	M	M	M	M		
	[E.8] Difusión de software dañino	A	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	B				
Software Storm User 6.5 – S. Ambiente D.	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				

Tabla 13. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Software Storm User 6.5 – S. Ambiente D.	[I.2] Daños por agua	B	B				
	[I.5] Avería de origen físico o lógico	MA	MA				
	[I.6] Corte del suministro eléctrico	M		M	M		
	[A.25] Robo de equipos	B	B	B	B		
	[I.2] Daños por agua	MB		MB	MB		
	A.26] Ataque destructivo	M	M				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	B	B	B	B	
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A	A	A	B	B	
	[E.25] Pérdida de equipos	MA	MA	MA	MA	MA	
	[A.6] Abuso de privilegios de acceso	MA	B	MA	MA	B	
	[A.7] uso no previsto	B	B	MA	MA	B	
	[A.11] Acceso no autorizado	B	B	MA	MA	B	
	[A.23] Manipulación del hardware	MA	MA	MA	B	B	
	[A.25] Robo de equipos	MA	MA	MA	MA	MA	
	[A.26] Ataque destructivo	A	A	MA	A	M	

Tabla 13. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Software Predis - SHD	[I.7] Condiciones inadecuadas de temperatura o humedad	B	B	B	B	B	
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A	A	A	B	B	
	[E.25] Pérdida de equipos	MA	MA	MA	MA	MA	
	[A.6] Abuso de privilegios de acceso	MA	B	MA	MA	B	
	[A.7] uso no previsto	B	B	MA	MA	B	
	[A.11] Acceso no autorizado	B	B	MA	MA	B	
	[A.23] Manipulación del hardware	MA	MA	MA	B	B	
	[A.25] Robo de equipos	MA	MA	MA	MA	MA	
	[A.26] Ataque destructivo	A	A	MA	A	M	
Servidor de Backup Dataprotector	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.1] Fuego	MA	MA				
	[I.3] Contaminación medioambiental	A	A%				
	[I.6] Corte del suministro eléctrico	A	A				

8.4.4 Identificación y Valoración de Amenazas Tipo: [WH]Equipos

14. Identificación y valoración de amenazas en activos tipo [WH] Equipos

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Equipos de cómputo	[N.1] Fuego	MA	MA	MA	A	A	
	[N.*] Desastres natur.	MA	MA	MA	A	A	
	[I.2] Daños/agua	MA	MA	MA	A	A	
	[I.*] Desastres indust.	MA	MA	MA	A	A	
	[I.3] Contaminación medioambiental	M	M	M	A	A	
	[I.5] Avería de origen físico/lógico	M	M	M	A	A	
	[I.6] Corte del suministro eléctrico	B	B	A	B	B	
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	B				
Servidor de correo - Prolaint DL 380 G5	[E.2] Errores del administrador del sistema	B	B				
	[E.4] Errores de configuración	B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	B				
	[A.7] uso no previsto	B	B				
	[A.11] Acceso no autorizado	B	B				
	[A.23] Manipulación del hardware	B	B				
	[A.25] Robo equipos	MA	MA				
Servidor de ambiente de pruebas	[I.6.12] Interrupción deliberada por un agente externo	MA	MA	MA			

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Equipo de Seguridad Perimetral	[N.1] Fuego	MA	MA	MA			
	[N.2] Daños por agua	MA	MA	MA			
	[N.*] Desastres naturales	MA	MA	MA			
	[E.2] Errores del administrador del sistema / de la seguridad	A	A	MA	MA	MA	
	[E.3] Errores de monitorización (log)	A		A			A
	[E.4] Errores de configuración	A		A	A		A
	[E.21] Errores de mantenimiento / actualización de programas (software)	A		A	A		B
	[A.3] Manipulación de los registros de actividad (log)			M	MA		MA
	[A.11]Acceso no autorizado	A	A	MA	MA	MA	
	[A.12] Análisis tráfico			A	A		
	[A.23] Manipulación del hardware	MA	MA	MA	A		
	[A.24] Denegación de servicio	MA	MA	MA			
Servidor bases de datos de Nómina	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor bases de datos de Nómina	[I.6] Corte del suministro eléctrico	A	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				
	[E.2] Errores del administrador del sistema / de la seguridad	B	B	B	B		
	[E.4] Errores de configuración	M	M	M	M		
Servidor Opget - Secretaria de Hacienda	[E.8] Difusión de software dañino	A	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	B				
	[E.25] Pérdida de equipos	MA	MA		MA		
	[A.6] Abuso de privilegios de acceso			M	M		
	[A.7] uso no previsto	B	B	B	B		
	[A.11] Acceso no autorizado			B	A		
	[A.23] Manipulación del hardware	M	M		M		
	[A.24] Denegación de servicio	A	A				
	[A.24.3] Saturación de los recursos hardware	M	M				
	[A.25] Robo de equipos	MA	MA		MA		
	[A.26] Ataque destructivo	MA	MA				

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Switch Netgear FS108 de 8 puertos	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.5] Avería de origen físico o lógico	M	M				
	[I.6] Corte del suministro eléctrico	A	A				
Servidor formato Blade marca Hewlett Packard. Modelo L453 G8	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				
	[E.2] Errores del administrador del sistema / de la seguridad	B	B	B	B		
	[E.4] Errores de configuración	M	M	M	M		
	[E.8] Difusión de software dañino	A	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	B				
	[E.25] Pérdida de equipos	MA	MA		MA		
	[A.6] Abuso de privilegios acceso			M	M		

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor formato Blade marca Hewlett Packard. Modelo L453 G8	[A.7] uso no previsto	B	B	B	B		
	[A.11] Acceso no autorizado	B		B			
	[A.23] Manipulación del hardware	M	M		M		
	[A.24] Denegación de servicio	A	A%				
	[A.24.3] Saturación de los recursos hardware	M	M				
	[A.25] Robo de equipos	MA	MA		MA		
	[A.26] Ataque destructivo	MA	MA				
Hubs 3COM SuperStack II PS Hub 40 de 24 Puertos	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.5] Avería de origen físico o lógico	M	M				
	[I.6] Corte del suministro eléctrico	A	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				
	[E.2] Errores del administrador del sistema / de la seguridad	B	B	B	B		
	[E.4] Errores de configuración	M	M	M	M		
	[E.8] Difusión de software dañino	A	A	A			

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Hubs 3COM SuperStack II PS Hub 40 de 24 Puertos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	B				
	[E.25] Pérdida de equipos	MA	MA		MA		
	[A.6] Abuso de privilegios de acceso			M	M		
	[A.7] uso no previsto	B	B	B	B		
	[A.11] Acceso no autorizado			B	A		
	[A.23] Manipulación del hardware	M	M		M		
	[A.24] Denegación de servicio	A	A				
	[A.24.3] Saturación de los recursos hardware	M	M				
	[A.25] Robo de equipos	MA	MA		MA		
	[A.26] Ataque destructivo	MA	MA				
Router Cisco 1700 Series propiedad de la ETB	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.5] Avería de origen físico o lógico	M	M				
	[I.6] Corte del suministro eléctrico	A	A				

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Modem Express 6503 propiedad de la ETB	[E.2] Errores del administrador del sistema / de la seguridad	B	B	B	B		
	[E.4] Errores de configuración	M	M	M	M		
	[E.8] Difusión de software dañino	A	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	B				
	[E.25] Pérdida de equipos	MA	MA		MA		
	[A.6] Abuso de privilegios de acceso			M	M		
	[A.7] uso no previsto	B	B	B	B		
	[A.11] Acceso no autorizado			B	A		
	[A.23] Manipulación del hardware	M	M		M		
	[A.24] Denegación de servicio	A	A				
Servidor Proliant ML370 G6	[A.24.3] Saturación de los recursos hardware	M	M				
	[A.25] Robo de equipos	MA	MA		MA		
	[A.26] Ataque destructivo	MA	MA				
PC’s para funciones de E-Mail y Proxy Servers	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Impresora para código de barras	[I.1] Fuego	MA	MA				
	[I.2] Daños por agua	MA	MA				
	[I.*] Desastres industriales	MA	MA				
	[I.3] Contaminación medioambiental	MA	MA				
	[I.4] Contaminación electromagnética	M	M				
	[I.5] Avería de origen físico o lógico	M	M				
	[I.6] Corte del suministro eléctrico	MA	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA	MA				
	[E.2] Errores del administrador del sistema / de la seguridad	B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	B			7	
	[E.24] caída del sistema por agotamiento de recursos	A	A				
	[E.25] Pérdida de equipos	MA	MA				
	[A.23] Manipulación del hardware	MA	MA				
	[A25]Robo de equipos	MA	MA				
	[A.26] Ataque destructivo	MA	MA				

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Impresoras Multifuncionales	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.5] Avería de origen físico o lógico	M	M				
	[I.6] Corte del suministro eléctrico	A	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				
	[E.2] Errores del administrador del sistema / de la seguridad	B	B	B	B		
	[E.4] Errores de configuración	M	M	M	M		
	[E.8] Difusión de software dañino	A	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	B				
	[E.25] Pérdida de equipos	MA	MA		MA		
	[A.26] Ataque destructivo	MA	MA				

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor Backups VD-SERVER-SD2,	[A.6] Abuso de privilegios de acceso			M	M		
	[A.7] uso no previsto	B	B	B	B		
	[A.11] Acceso no autorizado			B	A		
	[A.23] Manipulación del hardware	M	M		M		
	[A.24] Denegación de servicio	A	A				
	[A.24.3] Saturación de los recursos hardware	M	M				
	[A.25] Robo de equipos	MA	MA		MA		
	[A.26] Ataque destructivo	MA	MA				
Máquina Virtual Windows NT 4.0 (Base de Sisep)	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.1] Fuego	MA	MA				
	[I.3] Contaminación medioambiental	A	A				
	[I.6] Corte del suministro eléctrico	A	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	B				
	[E.2] Errores del administrador del sistema	B	B				
	[E.4] Errores de configuración	B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	B				

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Portátiles Toshiba	[A.7] uso no previsto	MB	MB				
	[A.11] Acceso no autorizado	B	B				
	[A.23] Manipulación del hardware	B	B				
	[A.25] Robo de equipos	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
Switch de borde - Referencia 7568G -	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.1] Fuego	MA	MA				
	[I.3] Contaminación medioambiental	A	A				
	[I.6] Corte del suministro eléctrico	A	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	B				
	[E.2] Errores del administrador del sistema / de la seguridad	B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	B				
	[A.7] uso no previsto	MB	MB				

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Copia de Respaldo - Dataprotector	[I.9] Interrupción de otros servicios o suministros esenciales	A	A				
	[E.2] Errores del administrador del sistema / de la seguridad	B	B				
	[E.4] Errores de configuración	A	A				
	[E.18] Destrucción de la información	A		A	A		
	[E.21] Errores de mantenimiento / actualización de programas (software)	A					A
	[E.24] caída del sistema por agotamiento de recursos	M	M				
	[A.23] Manipulación del hardware	MA	MA				MA
Sistema de Backups - Dataprotector	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.6] Corte del suministro eléctrico	A	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	B				
	[I.8] Fallo de servicios de comunicaciones	M	M				

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor de correo electrónico Google-Drive	[I.9] Interrupción de otros servicios o suministros esenciales	A	A				
	[E.2] Errores del administrador del sistema / de la seguridad	B	B				
	[E.4] Errores de configuración	A	A				
	[E.18] Destrucción de la información	A		A			
	[E.21] Errores de mantenimiento / actualización de programas (software)	A					A
	[E.24] caída del sistema por agotamiento de recursos	M	M				
	[A.23] Manipulación del hardware	MA	MA				MA
	[N.1] Fuego	MA	MA				
	[N.2] Daños por agua	MA	MA				
	[N.*] Desastres naturales	MA	MA				
	[I.5] Avería de origen físico o lógico	M	M				
	[I.6] Corte del suministro eléctrico	A	A				

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor DELL AntiSpam y McAfee SCM 1235	[I.7] Condiciones inadecuadas de temperatura o humedad	M	M				
	[E.2] Errores del administrador del sistema / de la seguridad	B	B	B	B		
	[E.4] Errores de configuración	B	B	B	B		
	[E.8] Difusión de software dañino	A	A				
Servidor McAfee SCM 2313	[N.1] Fuego	MA	MA	MA			
	[N.2] Daños por agua	MA	MA	MA			
	[N.*] Desastres naturales	MA	MA	MA			
	[E.1] Errores de los usuarios	B	B				
	[E.2] Errores del administrador del sistema	A	A	A	A		
	[E.4] Errores de configuración	MA	MA	MA	MA		
	[E.19] Fugas de información	B		B	A		
Servidor de base de datos Nómina	[N.1] Fuego	MA	MA	MA	MA		
	[N.2] Daños por agua	MA	MA	MA	MA		
	[N.*] Desastres naturales	MA	MA	MA	MA		
	[E.1] Errores de los usuarios	A	B	A			

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor de base de datos Nómina	[E.2] Errores del administrador del sistema / de la seguridad	A	A	B	A		
	[E.14] Fugas de información	MA			MA		
	[E.15] Alteración de la información	MA		MA	MA		
	[E.18] Destrucción de la información	MA	MA	MA	MA		
	[A.6] Abuso de privilegios de acceso	B	B	B	B	A	
	[A.15] Modificación de la información	A		A	A		
Hubs 3COM SuperStack II PS Hub 40 de 24 Puertos	[N.1] Fuego	A	A	A			
	[N.2] Daños por agua		AM	AM			
	[I.1] Fuego	AM	AM	AM			
	[I.2] Daños por agua	AM	AM	AM			
	[E.2] Errores del administrador del sistema /	B	B	B			
	[E.4] Errores de configuración	B	B	B			
	[E.24] caída del sistema por agotamiento de recursos	M	M	M			
	[A.8] Difusión de software dañino	M	M	M	M		
	[A.23] Manipulación del hardware	AM	AM	AM			

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor base de datos SQL	[A.24] Denegación de servicio	B	B	B			
	[A.26] Ataque destructivo	MA	MA	MA			
	[N.*] Desastres naturales	MA	MA	MA			
	[E.2] Errores del administrador del sistema	B	B	M			
	[E.4] Errores de configuración	B	B	M			
	[E.15] Alteración de la información	B	B	M			
	[E.21] Errores de mantenimiento / actualización de programas (software)	B	B				A
	[A.6] Abuso de privilegios de acceso	M			M		
	[A.8] Difusión de software dañino	A	A	A			
	[A.11] Acceso no autorizado	A			A		
	[A.15] Modificación de la información	A		A	A	A	
Servidor de Archivos	[N.2] Daños por agua	MA	MA	MA			
	[N.*] Desastres naturales	MA	MA	MA			
	[I.3] Contaminación medioambiental	A	A				
	[I.6] Corte del suministro eléctrico	A	A				

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Servidor de Virtualización	[I.7] Condiciones inadecuadas de temperatura o humedad	B	B				
	[E.1] Errores de los usuarios	A		A			
	[E.2] Errores del administrador del sistema / de la seguridad	B	B				M
	[E.4] Errores de configuración	B	B				M
	[E.15] Alteración de la información	A		A			
	[E.18] Destrucción de la información	A		A			
	[E.24] caída del sistema por agotamiento de recursos	M	M				M
	[A.6] Abuso de privilegios de acceso	A		A	A	A	
Router Cisco 1800 Series propiedad de la SHD	[A.8] Difusión de software dañino	A	A	M			
	[A.11] Acceso no autorizado	A		A	A		
	[A.15] Modificación de la información	A		A	A		
	[A.18] Destrucción de la información	A		A	A		
	[N.1] Fuego	MA	MA				MA

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Router Cisco 1800 Series propiedad de la SHD	[N.2] Daños por agua	MA	MA				MA
	[N.*] Desastres naturales	MA	MA				MA
	[I.5] Avería de origen físico o lógico	MA	MA				MA
	[I.6] Corte del suministro eléctrico	MA	MA				MA
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				A
	[E.2] Errores del administrador del sistema / de la seguridad	M	M				M
	[E.4] Errores de configuración	M	M				M
Impresoras multifuncionales	[E.21] Errores de mantenimiento / actualización de programas (software)	M	M				M
	[E.24] caída del sistema por agotamiento de recursos	MA	MA				MA
	[A.6] Abuso de privilegios de acceso	A	A				A
	[A.8] Difusión de software dañino	MA	MA				MA
	[A.11] Acceso no autorizado	MA	MA				MA
	[A.24] Denegación de servicio	MA	MA				MA

Tabla 14. Continuación

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Consola Vcenter	[A.23] Manipulación del hardware	MA	MA	MA			
	[A.24] Denegación de servicio	B	B	B			
	[A.26] Ataque destructivo	MA	MA	MA			
Aplicación Archivos Gestión Documental -	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A	B	MA	
	[E.15] Alteración de la información			A	MA		
Base de datos Oracle 11g	[N.1] Fuego	MA	MA	MA	MA		
	[N.*] Desastres naturales	MA	MA	MA	MA		
	[E.1] Errores de los usuarios	B	B	A			
	[E.2] Errores del administrador del sistema / de la seguridad	A	A	B	A		
	[E.14] Fugas de información				MA		
	[E.15] Alteración de la información			MA	MA		
	[E.18] Destrucción de la información	MA	MA	MA	MA		
	[A.6] Abuso de privilegios de acceso	B	B	MA	MA		
	[A.15] Modificación de la información	MB		MA	MA		

Fuente: Herramienta Pilar 6.2

8.3.5 Identificación y Valoración de Amenazas Tipo: [P] Personal

Tabla 15. Identificación y valoración de amenazas en activos tipo: Personal

Activos	Amenazas	Probabilidad	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
Administradores de Sistemas	[E.7] Deficiencias en la organización	B	B				
	[E.28] Indisponibilidad del personal	A	A				
	[A.29] Extorsión	A	B	M	A		
	[A.30] Ingeniería Social	A	B	A	A		

Fuente: Herramienta Pilar 6.2

8.5 ANALISIS DEL RIESGO

Aplicando la metodología Magerit v.3, en esta etapa es en donde se procesa e interpreta los resultados obtenidos de las actividades anteriores, estimación de impacto y del riesgo en cada uno de los riesgos según la dimensión que se fue afectada, a continuación se presenta la valoración estimada del impacto según la metodología Magerit v.3.

Tabla 15. Valoración estimada del Impacto

Riesgo		**Probabilidad**				
		MB	**B**	**M**	**A**	**MA**
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: MAGERIT v.3 – Libro II – Catálogo de elementos

En la siguiente tabla se puede apreciar los resultados obtenidos

Tabla 16. Matriz de Análisis de riesgo de los activos informáticos

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
DATOS [D]												
Documentación Técnica	[N.2] Daños por agua	A	A				MB	M	M			
	[N.*] Desastres naturales	A	A				MB	M	M			
	[I.1] Fuego	A	A				MB	M	M			
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	M				M	M	M			
	[E.18] Destrucción de la información	M	M				B	M	M			
SERVICIOS [S]												
Controlador de dominio principal (PDC)	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			B	A	A	A		
	[E.15] Alteración de la información		MA	MA			MB		A	A		
	[E.18] Destrucción de la información	MA	MA	MA			MB	A	A	A		
	[E.19] Fugas de información	M	MA	MA			B	M	MA	MA		
	[E.24] caída del sistema por agotamiento de recursos	A					B	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA		MB		M	M	A	
	[A.6] Abuso de privilegios de acceso			A			M				A	A

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Controlador de dominio principal (PDC)	[A.7] uso no previsto		A	A			M	MA	A	A		
	[A.11] Acceso no autorizado		A	A			M		A	A		
	[A.15] Modificación de la información		A				A		MA			
	[A.18] Destrucción de la información	A	A				M	A	A			
	[A.19] revelación de información			A			M			A		
	[A.24] Denegación de servicio	A					A	MA				
Controlador de dominio backup (BDC)	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			B	A	A	A		
	[E.15] Alteración de la información		MA	MA			MB		A	A		
	[E.18] Destrucción de la información	MA	MA				MB	A	A	A		
Antispam Mcafee	[N.1] Fuego	M	A				B	M	A			
	[N.2] Daños por agua	B	A				M	B	A			
	[N.*] Desastres naturales	M	A				MB	B	A			
	[I.1] Fuego	M	A				B		A			
	[I.2] Daños por agua	B	A				M	B	A			
	[I.*] Desastres industriales	M	A				MB	B	A			
	[I.3] Contaminación medioambiental	B	A				M	B	A			
	[I.5] Avería de origen físico o lógico	B	A				M	B	A			

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Antispam Mcafee	[E.24] caída del sistema por agotamiento de recursos	A					B	A				
	[A.5] suplantación de la identidad del usuario		A	A	MA		MB		M	M	A	
	[A.6] Abuso de privilegios de acceso		A	A			M		A	A		
	[A.7] uso no previsto		A	A			M	MA	A	A		
	[A.11] Acceso no autorizado		A	A			M		A	A		
	[A.15] Modificación de la información		A				A		MA			
	[A.18] Destrucción de la información	A	A				M	A	A			
	[A.19] revelación de información			A			M			A		
	[A.24] Denegación de servicio	A					A	MA				
Correo electrónico Google-Drive	[E.1] Errores de los usuarios	A	MA	MA			A	MA	MA	MA		
	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			M	A	A	A		
	[E.15] Alteración de la información	A	A				B		A			
	[E.18] Destrucción de la información	MA	MA				A	MA	MA			
	[E.19] Fugas de información			MA			A			MA		
	[E.24] caída del sistema por agotamiento de recursos	A	A				A	MA				
	[A.5] suplantación de la identidad del usuario		A	A	A		M		A	A	A	

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Correo electrónico Google-Drive	[A.6] Abuso de privilegios de acceso	MA		MA	A		M		MA	MA		
	[A.7] uso no previsto	MA		A			M	MA	A	A		
	[A.11] Acceso no autorizado			A			M		A	A		
	[A.13] Repudio (negación de actuaciones)						M		MA			
	[A.18] Destrucción de la información	A	A				M	A				
	[A.19] revelación de información			A			M			A		
Portal Institucional	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			M	A	A			
	[E.3] Errores de monitorización (log)	M	M				M	M	M			
	[E.4] Errores de configuración	A	A	A			A	MA	MA			
	[E.15] Alteración de la información	M	M		A		MB	B	B			
	[E.18] Destrucción de la información	A	A				MB	M	M			
	[E.20] vulnerabilidades de los programas (software)	M	M	A			M	M	M			
	[E.21] Errores de mantenimiento / actualización de programas (software)	M	M				M	M	M			
	[E.24] caída del sistema por agotamiento de recursos	A					B	A	A			
	[E.28] Indisponibilidad del personal	M					M	M				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Portal Institucional	[A.5] suplantación de la identidad del usuario		A	MA			B	A	A	MA		
	[A.6] Abuso de privilegios de acceso		M	A			B	M	M			
	[A.8] Difusión de software dañino	A	A	MA			M	A	A	MA		
Portal Intranet	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			MB	M	M		MB	
	[E.3] Errores de monitorización (log)	MB	MB				B	MB	MB			
	[E.4] Errores de configuración	MA	MA	MA			B	MA	MA			
	[E.15] Alteración de la información	A	A	A	B		B		A	MB	B	
	[E.18] Destrucción de la información	MA	MA				B		MA		B	
	[E.20] vulnerabilidades de los programas (software)	MA	MA	MA			M	MA	MA			
	[E.21] Errores de mantenimiento / actualización de programas (software)	A	A	A			M	A	A			
	[E.24] caída del sistema por agotamiento de recursos	MA					B	MA	MA			
	[A.8] Difusión de software dañino	A	MA	MA	B		B	A	MA		B	
	[A.11] Acceso no autorizado	MA	MA	B	M		B		MA	B	M	
	[A.15] Modificación de la información	A	A	MB			MB		M	MB		

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Portal Intranet	[A.18] Destrucción de la información	MA	MA				B	MA	MA			
	[A.24] Denegación de servicio	MA					MB	A				
Almacenamiento en la nube	[E.2] Errores del administrador del sistema / de la seguridad	A	A				MB	M	M		MB	
	[E.3] Errores de monitorización (log)	MB	MB				B	MB	MB			
	[E.4] Errores de configuración	MA					B	MA	MA			
	[E.15] Alteración de la información		A	MB	B		B		A	MB	B	
	[E.18] Destrucción de la información	MA	MA		B		B		MA		B	
	[E.20] vulnerabilidades de los programas (software)	MA					M	MA	MA			
	[E.21] Errores de mantenimiento / actualización de programas (software)	A	A				M	A	A			
	[E.24] caída del sistema por agotamiento de recursos	MA	MA				B	MA	MA			
	[A.8] Difusión de software dañino	A	A	A	B		B	A	MA		B	
	[A.11] Acceso no autorizado		MA	B	M		B		MA	B	M	
	[A.15] Modificación de la información		MA			MB	MB		M	MB		

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Almacenamiento en la nube	[A.18] Destrucción de la información	MA	MA				B	MA	MA			
	[A.24] Denegación de servicio	MA					MB	A				
Portal Académico (B-Learning) Control social	[A.11] Acceso no autorizado	A	A	MA			M	A	A	MA		
	[A.15] Modificación de la información	M	M				B	M	M			
	[A.18] Destrucción de la información	A	A				MB	M	M			
	[A.22] Manipulación de programas	M	M	A			M	M	M			
	[A.24] Denegación de servicio	A					M	A	A			
Canal Dedicado ETB	[N.1] Fuego	MA	A				MB	A				
	[N.2] Daños por agua	MA	A				MB	A				
	[N.*] Desastres naturales	MA	A				MB	A				
	[I.1] Fuego	MA	A				MB	A				
	[I.5] Avería de origen físico o lógico	MA	A				MB	A				
	[I.6] Corte del suministro eléctrico	MA	A				B	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA	A				MB	A				
	[I.8.12] Interrupción deliberada por un agente externo	MA	A				M	MA				
	[E.4] Errores de configuración	MA	A				MB	A				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Canal Dedicado ETB	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A	A				MB	M				
	[E.24] caída del sistema por agotamiento de recursos	MA	A				MB	A				
SOFTWARE/APLICATIVOS												
Software de Aplicaciones (medios)	[N.1] Fuego	MA	MA				MB	A	A			
	[I.5] Avería de origen físico o lógico	A	A				M	A	A			
	[A.7] uso no previsto	A	A				B	A	A			
Software de Bases de datos (medios)	[N.1] Fuego	MA	MA				MB	A	A			
	[I.5] Avería de origen físico o lógico	A	A				M	A	A			
	[A.7] uso no previsto	A	A				B	A	A			
Software Sistema de Gestión de Calidad - Daruma	[N.1] Fuego	MA	B				MB	A	MB			
	[I.5] Avería de origen físico o lógico	A	MB				M	A	MB			
	[A.7] uso no previsto	A	MB				B	A	MB			
Software de Sistema de Gestión Documental - Orfeo	[N.1] Fuego	MA	MA				MB	A	A			
	[I.5] Avería de origen físico o lógico	A	A				M	A	A			
	[A.7] uso no previsto	A	A				B	A	A			
Software Manejo Bases de Datos Gestión Documental - Winisis	[N.1] Fuego	MA	B				MB	A	MB			
	[I.5] Avería de origen físico o lógico	A	MB				M	A	MB			
	[A.7] uso no previsto	A	MB				B	A	MB			

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Software Gestión Contractual Sigco	[E.1] Errores de los usuarios		MA		MA		M		MA		MA	
	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			B	A	A	A		
	[E.3] Errores de monitorización (log)	MA	MA				MB	A				
Aplicación Reserva de Salones	[E.4] Errores de configuración	MA	MA	MA			MB	A				
	[E.15] Alteración de la información		MA		MA	MA	B		MA		MA	MA
	[E.19.1] Personal interno que no necesita conocerlo			MA			MB			A		
	[E.20.dos] Denegación de Servicio	MA					M	MA				
	[E.28.4] Personal insuficiente			MA		MA	M					MA
	[A.7.1] Por personal interno			MA		MA	MB			A		
	[A.15.1] Sin beneficio para nadie			MA		MA	MB			A		
Servidor Compaq Proliant 2500	[E.2] Errores del administrador del sistema / de la seguridad	B	MA	MA	MA		B	B				
	[E.4] Errores de configuración	B	MA	MA	MA		B	B				
	[E.19.1] Personal interno que no necesita conocerlo			MA			M			MA		
Software Aplicación de gestor de máquinas virtuales	[N.1] Fuego	MA	MA				M	MA	MA			
	[N.2] Daños por agua	MA	MA				M	MA	MA			

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Software Aplicación de gestor de máquinas virtuales	[I.2] Daños por agua	MA	MA				M	MA	MA			
	[E.2] Errores del administrador del sistema / de la seguridad	A	A	MA			MB	M	M			
Software Sigco	[E.4] Errores de configuración	A	A	MA			MB	M	M			
	[E.24] caída del sistema por agotamiento de recursos	A					B	A	A			
	[A.8] Difusión de software dañino	A	A				M	A	A			
	[A.23] Manipulación del hardware	MA	MA				MB	A	A			
	[A.24] Denegación de servicio	A	A				MB	M	M			
	[A.26] Ataque destructivo	MA	MA				MB	A	A			
Software Permisos y Certificaciones	[E.2] Errores del administrador del sistema / de la seguridad	A	A	B	M		M	A	A	B	M	
	[E.15] Alteración de la información	A	A	M			B		A	M		
Equipos de Computo	[N.1] Fuego	A	A	M			MB	M	M	B		
	[N.*] Desastres naturales	A	A	M			MB	M	M	B		
	[E.1] Errores de los usuarios	M	A				M	M	A			
	[E.2] Errores del administrador del sistema / de la seguridad	A	M	M			M	A	M	M		
	[E.14] Fugas de información	MA	MA	M			M			M		

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Sistema de Almacenamiento Rack	[E.15] Alteración de la información	MA	A	M			M		A	M		
	[E.18] Destrucción de la información	A	A	M			B	A	A	M		
	[A.6] Abuso de privilegios de acceso	M	A	M			M	M	A	M		
	[A.15] Modificación de la información	A	A	M			B		A	M		
	[A.30] Ingeniería social	M	M	B			MB		B	MB		
	[N.*] Desastres naturales	A					MB	M				
Software Nómina	[I.6] Corte del suministro eléctrico	A					B	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					MB	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M					B	M				
	[E.4] Errores de configuración	M					B	M				
	[E.18] Destrucción de la información		M				B		M			
	[E.21] Errores de mantenimiento / actualización de programas (software)	A	A	A			A		A			
	[E.24] caída del sistema por agotamiento de recursos	A					MB	M				
	[A.8] Difusión de software dañino	A	A	MA			MB	M	M			

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
	[A.11] Acceso no autorizado	MA	MA	M	A		M			M	A	
Software de Seguimiento al Plan de Desarrollo - Segplan	[N.*] Desastres naturales	A					MB	M				
	[I.6] Corte del suministro eléctrico	A					B	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A					MB	M				
Software Daruma	[E.1] Errores de los usuarios	A	A	A	M		B				M	
	[E.2] Errores del administrador del sistema / de la seguridad	M	A	A			B	M				
	[E.4] Errores de configuración	M	A	A			B	M				
	[E.18] Destrucción de la información		M				B		M			
	[E.21] Errores de mantenimiento / actualización de programas (software)	A	A	A					A			
	[E.24] caída del sistema por agotamiento de recursos	A					MB	M				
	[A.8] Difusión de software dañino	A	A	A			MB	M	M			
	[A.11] Acceso no autorizado	MA	MA	M	A		M			M		
Storm User 5.0 Secretaria de Ambiente	[E.1] Errores de los usuarios	M	M	M			A	A	A	A		
	[E.2] Errores del administrador	A	M	A			B	A	M	A		
	[E.4] Errores de configuración		A				M		A			
	[E.7] Deficiencias en la organización	A	A	A			A	MA				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Storm User 5.0 Secretaria de Ambiente	[E.15] Alteración accidental de la información		A				M		A			
	[E.18] Destrucción de información	A	A				B	A				
	[E.20] Vulnerabilidades de los programas (software)	A	A	M			M	A	A	M		
	[E.21] Errores de mantenimiento / actualización de	M	M				M	M	M			
Aplicativo Reservas	programas (software)											
	[E.24] Caída del sistema por agotamiento de recursos	A	A				B	A				
	[E.28] Indisponibilidad del personal	A	A				A	MA				
Antivirus McAfee	[E.1] Errores de los usuarios	A	A				B	A	A			
	[E.2] Errores del administrador del sistema / de la seguridad	MA	MA	MA			B	M	M			
	[E.3] Errores de monitorización (log)	A	A			M	MB	M	M			B
	[E.4] Errores de configuración	A	A	x			MB	M	M			
	[E.20] vulnerabilidades de los programas (software)	A	A				MB	M	M			
	[E.21] Errores de mantenimiento / actualización de programas (software)	M	M				MB	B	B			

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Antivirus McAfee	[A.6] Abuso de privilegios de acceso	A	A	A M			MB	B	B			
	[A.8] Difusión de software dañino	A	A				MB	M	M			
	[A.11] Acceso no autorizado	M	M				MB	B	B			
	[A.22] Manipulación de programas	M	M				B	M	M			
Equipos												
Sistema Operativos de servidores	[N.1] Fuego	MA	MA				MB	A				
	[N.2] Daños por agua	MA	MA				MB	A				
	[N.*] Desastres naturales	MA	MA				MB	A				
Impresora de tarjetas Datacar SD260	[I.1] Fuego	MA	MA				MB	A				
	[I.2] Daños por agua	MA	MA				MB	A				
	[I.*] Desastres industriales	MA	MA				MB	A				
	[I.3] Contaminación medioambiental	A	A				MB	M				
	[I.4] Contaminación electromagnética	A	A				MB	M				
	[I.5] Avería de origen físico o lógico	MA	MA				M	MA				
	[I.6] Corte del suministro eléctrico	MA	MA				B	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				MB	M				
	[E.2] Errores del administrador del sistema / de la seguridad	A	A				MB	M				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Impresora de tarjetas Datacar SD260	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MA	MA				B	MA				
	[E.24] caída del sistema por agotamiento de recursos	MA	MA				MB	A				
Impresora Multifuncional	[E.25] Pérdida de equipos	MA	MA				MB	A				
	[A.23] Manipulación del hardware	MA	MA				B	MA				
	[A.25] Robo de equipos	MA	MA				MB	A				
	[A.26] Ataque destructivo	MA	MA				MB	A				
Servidor Backups VD-BAKI 2016	[N.1] Fuego	A	A				B	A				
	[N.2] Daños por agua	A	A				B	A				
	[N.*] Desastres naturales	A	A				B	A				
	[I.5] Avería de origen físico o lógico	M	M				MB	B				
	[I.6] Corte del suministro eléctrico	A	A				A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A									
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	M			MB	B	B	B		
	[E.8] Difusión de software dañino	A	A	MA			M	A	A			

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Servidor Backups VD-BAKl 2016	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	A	MA			MB	MB				
	[E.25] Pérdida de equipos	A	A				MB	M				
	[A.6] Abuso de privilegios de acceso	MA	M	M			M		M	M		
	[A.7] uso no previsto	M	M	M			MB	B	B	B		
	[A.11] Acceso no autorizado		M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M	A	A			M	M		A		
	[A.24] Denegación de servicio	A					B	A				
	[A.25] Robo de equipos	A					MB	M				
Router ETB	[A.26] Ataque destructivo	A	A				MB	M				
	[N.1] Fuego	A	A				B	A				
	[N.2] Daños por agua	A	A				B	A				
	[N.*] Desastres naturales	A	A				B	A				
	[I.5] Avería de origen físico o lógico	M	A				MB	B				
	[I.6] Corte del suministro eléctrico	A	A				A	MA				
Portátiles Toshiba	[A.11] Acceso no autorizado	MA	M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M	A	A			M	M		A		
	[A.24] Denegación de servicio	A	A				B	A				
	[A.25] Robo de equipos	A	A	MA			MB	M				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Servidor de Virtualización	[A.26] Ataque destructivo	A	A				MB	M				
	[N.1] Fuego	A	A				B	A				
	[N.2] Daños por agua	A	A				B	A				
	[N.*] Desastres naturales	A	A				B	A				
	[I.5] Avería de origen físico o lógico	M	A				MB	B				
	[I.6] Corte del suministro eléctrico	A	A				A	MA				
Servidor controlador de dominio principal	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				M	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	M			MB	B	B	B		
	[E.8] Difusión de software dañino	A	A	MA	MA		M	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	A				MB	MB				
	[E.25] Pérdida de equipos	A	A	MA			MB	M				
	[A.6] Abuso de privilegios de acceso	A	M	M			M		M	M		
	[A.7] uso no previsto	M	M	M			MB	B	B	B		
	[A.11] Acceso no autorizado	A	M	MA			MB		B	A		

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Servidor DELL PowerEdge 4300/350	[A.23] Manipulación del hardware	M	M	A			M	M		A		
	[A.25] Robo de equipos	A	A				MB	M				
	[A.26] Ataque destructivo	A	A				MB	M				
	[A.11] Acceso no autorizado	B	B	A	A		M	B	A	A	A	
	[A.23] Manipulación del hardware	B	B	A			B	B	A	A		
	[A.24.1] Saturación de los canales de comunicaciones	B	B				M	B				
	[A.25] Robo de equipos	M	M				B	M				
Servidor DELL AntiSpam McAfee Appliance SCM 3100	[N.1] Fuego	A	A				B	A				
	[N.2] Daños por agua	A	A				B	A				
	[N.*] Desastres naturales	A	A				B	A				
	[I.5] Avería de origen físico o lógico	M	M				MB	B				
	[I.6] Corte del suministro eléctrico	A	A				A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				M	A	AA			
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	M			MB	B	B	B		
	[E.8] Difusión de software dañino	A	A	A			M	A	A			

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Servidor DELL AntiSpam McAfee Appliance SCM 3100	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	B	A			MB	MB	A			
Equipos de cómputo	[E.25] Pérdida de equipos	A	A	A			MB	M				A
	[A.6] Abuso de privilegios de acceso	M	M	M			M		M	M		
	[A.7] uso no previsto	M	M	M			MB	B	B	B		
	[A.11] Acceso no autorizado	M	M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M	M	A			M	M		A		
	[A.24] Denegación de servicio	A	A	A			B	A				
	[A.25] Robo de equipos	A	A	A			MB	M				
	[A.26] Ataque destructivo	A	A	A			MB	M				
Servidor Compaq Proliant 2500	[N.1] Fuego	M	MA	MA	A		MB	B	A	A	M	
	[N.2] Daños por agua	M	MA	MA	A		MB	B	A	A	M	
	[N.*] Desastres naturales	M	MA	MA	A		MB	B	A	A	M	
	[I.1] Fuego	M	MA	MA	A		MB	B	A	A	M	
	[I.2] Daños por agua	M	MA	MA	A		MB	B	A	A	M	
	[I.*] Desastres industriales	M	MA	MA	A		MB	B	A	A	M	
	[I.3] Contaminación medioambiental	M	MA	MA	A		MB	B	A	A	M	
	[I.5] Avería de origen físico o lógico	B	A	MA	A		A	M	MA	MA	MA	
	[I.6] Corte del suministro elect.	B	MA	A	M		A	M	MA	MA	A	

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Servidor Compaq Proliant 2500	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A	A	M		M	B	A	A	M	
Servidor Backups VD-BAK2015	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	MA	A	M		MA	A	MA	MA	A	
	[E.25] Pérdida de equipos	M	MA	MA	A		B	M	MA	MA	A	
	[A.6] Abuso de privilegios de acceso	B	MA	MA	M		A	M	MA	MA	A	
	[A.7] uso no previsto	B	MA	MA	M		A	M	MA	MA	A	
	[A.11] Acceso no autorizado	B	MA	MA	M		M	B	MA	MA	M	
	[A.23] Manipulación del hardware	B	MA	A	M		M	B	MA	A	M	
	[A.25] Robo de equipos	M	MA	MA	A		M	M	MA	MA	A	
	[A.26] Ataque destructivo	M	MA	MA	M		MB	B	A	A	B	
UPS de 10K autonomía aprox. 30min.para sostenimiento del centro de cómputo	[A.24] Denegación de servicio	A	A				B	A				
	[A.24.3] Saturación de los recursos hardware	M	M				MB	B				
	[A.25] Robo de equipos	A	A	MA			MB	M		A		
	[A.26] Ataque destructivo	A	A				MB	M				
Servidor Backups VD-SERVER	[N.2] Daños por agua	A	A				MB	M				
	[N.*] Desastres naturales	A	A				MB	M				
	[I.1] Fuego	A	A				MB	M				
	[I.3] Contaminación medioambiental	A	A				B	A				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Sistema de almacenamiento formato rack	[I.6] Corte del suministro eléctrico	A	A				M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	M				B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M				MB	B				
	[E.4] Errores de configuración	M	M				B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M				B	M				
	[A.7] uso no previsto	B	B				MB	MB				
	[A.11] Acceso no autorizado	M	M				MB	B				
	[A.23] Manipulación del hardware	M	M				MB	B				
	[A.25] Robo de equipos	A	A				MB	M				
	[I.6.12] Interrupción deliberada por un agente externo	MA	MA				M	MA	MA			
Servidor de correo electrónico -Gmail Drive	[N.1] Fuego	MA	A				B	MA	A			
	[N.2] Daños por agua	MA	A				B	MA	A			
	[N.*] Desastres naturales	MA	A				B	MA	A			
	[E.2] Errores del administrador del sistema / de la seguridad	MA	A	M			M	MA	A	M		
	[E.3] Errores de monitorización (log)		A	M			M		A	M		
	[E.4] Errores de configuración	MA	A	M			M	MA	A	M		

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Equipo de Seguridad Perimetral	[E.21] Errores de mantenimiento / actualización de programas (software)	MA	A	M			M	MA	A	M		
	[A.3] Manipulación de los registros de actividad (log)		M	M			B		M	M		
	[A.11] Acceso no autorizado	MA	A	M			MB	A	M	B		
	[A.12] Análisis de tráfico		A	M			B		A	M		
	[A.23] Manipulación del hardware	MA	A	M			B	MA	A	M		
	[A.24] Denegación de servicio	MA	A				MB	A	M			
Máquina Virtual Windows NT 4.0 (Base de Sisep)	[N.1] Fuego	A	A	A			B	A				
	[N.2] Daños por agua	A	A				B	A				
	[N.*] Desastres naturales	A	A				B	A				
	[I.5] Avería de origen físico o lógico	M	M				MB	B				
	[I.6] Corte del suministro eléctrico	A	A				A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				M	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	A			MB	B	B	M		
	[E.8] Difusión de software dañino	A	A	A			M	A	A			

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Máquina Virtual Windows NT 4.0 (Base de Sisep)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M	A			MB	B				
	[E.25] Pérdida de equipos	A	A	MA			MB	M		A		
	[A.6] Abuso de privilegios de acceso		M	A			B		M	A		
	[A.7] uso no previsto	M	M	A			MB	B	B	M		
	[A.11] Acceso no autorizado		M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M	M	A			M	M		A		
	[A.24] Denegación de servicio	A					B	A				
	[A.24.3] Saturación de los recursos hardware	M	M				MB	B				
Sistema de Copias de Backup	[A.25] Robo de equipos	A	A	MA			MB	M		A		
	[A.26] Ataque destructivo	A	A	A			MB	M				
Servidor formato blade marca Hewlett Packard. Modelo proliant BL460C G7	[N.1] Fuego	A	A	A			B	A				
	[N.2] Daños por agua	A	A	A			B	A				
	[N.*] Desastres naturales	A	A				B	A				
	[I.5] Avería de origen físico o lógico	M	M				MB	B				
	[I.6] Corte del suministro eléctrico	A	A	A			A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	A				M	A				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Impresora Multifuncionales	[E.2] Errores del administrador del sistema / de la seguridad	M	M	A			MB	B	B	M		
	[E.4] Errores de configuración	M	M	A			MB	B	B	M		
	[E.8] Difusión de software dañino	MA	MA	MA			M	A	A			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M				MB	B				
	[E.25] Pérdida de equipos	A	A	MA			MB	M		A		
	[A.6] Abuso de privilegios de acceso			A			B		M	A		
	[A.7] uso no previsto	M	M	A			MB	B	B	M		
Impresora para código de barras	[A.11] Acceso no autorizado		M	MA			MB		B	A		
	[A.23] Manipulación del hardware	M	M	A			M	M		A		
	[A.24] Denegación de servicio	A	A				B	A				
	[A.24.3] Saturación de los recursos hardware	M	M				MB	B				
	[A.25] Robo de equipos	A	A	MA			MB	M		A		
	[A.26] Ataque destructivo	A	A				MB	M				
	[N.1] Fuego		MA				MB	A				
	[N.2] Daños por agua	MA	MA				MB	A				
	[N.*] Desastres naturales	MA	MA				MB	A				
	[I.1] Fuego		MA				MB	A				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Impresora para código de barras	[I.2] Daños por agua	MA	MA				MB	A				
	[I.*] Desastres industriales	MA	MA				MB	A				
	[I.3] Contaminación medioambiental	MA	MA				MB	A				
	[I.4] Contaminación electromagnética	A	A				MB	M				
	[I.5] Avería de origen físico o lógico	A	A				M	A				
	[I.6] Corte del suministro eléctrico	MA	MA				B	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA	MA				MB	A				
Servidor controlador de dominio principal	[E.2] Errores del administrador del sistema / de la seguridad	A	A	x			MB	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A	A	A			B	A				
	[E.24] caída del sistema por agotamiento de recursos	MA	MA				MB	A				
	[E.25] Pérdida de equipos	MA	MA				MB	A				
	[A.23] Manipulación del hardware	MA	MA				B	MA				
	[N.1] Fuego	MA	MA				B	MA				
	[N.2] Daños por agua	MA	MA				B	MA				
	[N.*] Desastres naturales	MA	MA				B	MA				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Servidor controlador de dominio principal	[I.5] Avería de origen físico o lógico	A	A				MB	M				
	[I.6] Corte del suministro eléctrico	MA	MA				A	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA	MA				M	MA				
	[E.2] Errores del administrador del sistema / de la seguridad	A	A	A			MB	M	M	M		
	[E.4] Errores de configuración	A	A	A			MB	M	M	M		
	[E.8] Difusión de software dañino	MA	MA				M	MA	MA			
Servidor de Correo Gmail DL380 G5	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A	A				MB	M				
	[E.25] Pérdida de equipos	MA	MA	MA			MB	A		A		
	[A.6] Abuso de privilegios de acceso		A	A			B		A	A		
	[A.7] uso no previsto	A	A	A			MB	M	M	M		
	[A.11] Acceso no autorizado		A	MA			MB		M	A		
	[A.23] Manipulación del hardware	A		A			M	A		A		
	[A.24] Denegación de servicio	MA	MA				B	MA				
	[A.24.3] Saturación de los recursos hardware	A	A				MB	M				
	[A.25] Robo de equipos	MA	MA	MA			MB	A		A		

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Switch XTL3490 G	[A.26] Ataque destructivo	MA	MA				MB	A				
	[E.2] Errores del administrador del sistema / de la seguridad	M	A	x			MB	B				
	[E.4] Errores de configuración	M	A	x			B	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	A	x			B	M				
	[A.7] uso no previsto	B	A				MB	MB				
	[A.11] Acceso no autorizado	M	A				MB	B				
	[A.23] Manipulación del hardware	M	A				MB	B				
	[A.25] Robo de equipos	A	MA	x			MB	M				
Switch TrendNet TEC 240-S36 de 24 Puertos	[N.2] Daños por agua	A	MA				MB	M				
	[N.*] Desastres naturales	A	MA				MB	M				
	[I.1] Fuego		A				MB	M				
	[I.3] Contaminación medioambiental		A				B	A				
	[I.6] Corte del suministro eléctrico	A	A				M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad		A				B	M				
	[E.2] Errores del administrador del sistema / de la seguridad	x	MA	x			MB	B				
	[E.4] Errores de configuración	x	MA				B	M				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Switch TrendNet TEC 240-S36 de 24 Puertos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	A	x			B	M				
	[A.7] uso no previsto	B	A	x			MB	MB				
	[A.11] Acceso no autorizado	M	A	x			MB	B				
	[A.23] Manipulación del hardware	M	A	x			MB	B				
	[A.25] Robo de equipos	A	MA				MB	M				
Switch Netgear FS108 de 8 puertos	[N.2] Daños por agua	A	A				MB	M				
	[N.*] Desastres naturales	A	A				MB	M				
	[I.1] Fuego		A				MB	M				
	[I.3] Contaminación medioambiental	A	A				B	A				
	[I.6] Corte del suministro eléctrico	A	MA				M	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	A				B	M				
Servidor base de datos SQL	[N.*] Desastres naturales	A	A				MB	M	M			
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	x			MB	B	B			
	[E.4] Errores de configuración	M	M	x			MB	B	B			
	[E.15] Alteración de la información	M	M	x			MB	B	B			
	[E.21] Errores de mantenimiento / actualización de MBprogramas (software)	B	A	x			M	B				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Servidor de Archivos	[A.6] Abuso de privilegios de acceso			M			MB			B		
	[A.8] Difusión de software dañino	A	A				B	A	A			
	[A.11] Acceso no autorizado		x	A			B			A		
	[A.15] Modificación de la información		A	A			B		A	A		
	[N.2] Daños por agua	MA	MA				MB	A	A			
	[N.*] Desastres naturales	MA	MA				MB	A	A			
	[I.3] Contaminación medioambiental	MA	x				B	MA				
Redes Sociales	[I.6] Corte del suministro eléctrico	MA	x				B	MA				
	[I.7] Condiciones inadecuadas de temperatura o humedad	A	x				MB	M				
	[E.1] Errores de los usuarios		MA				M		MA			
	[E.2] Errores del administrador del sistema / de la seguridad	M	x	x			MB	B				
	[E.4] Errores de configuración	M	x	x			MB	B				
	[E.15] Alteración de la información		MA		x		M		MA			
	[E.18] Destrucción de la información	x	MA				A		MA			
	[E.24] caída del sistema por agotamiento de recursos	A					M	A				
	[A.6] Abuso de privilegios de acceso		MA	MA	MA		MB		A	A	A	

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Redes Sociales	[A.8] Difusión de software dañino	A	A				MB	M	M			
	[A.11] Acceso no autorizado		MA	MA			MB		A	A		
	[A.15] Modificación de la información		MA	MA			B		MA	MA		
	[A.18] Destrucción de la información		MA	MA			B		MA	MA		
Servidor de impresión	[N.1] Fuego	MA	MA			A	MB	A				M
	[N.2] Daños por agua	MA	MA			A	MB	A				M
	[N.*] Desastres naturales	MA	MA			A	B	MA				A
	[I.5] Avería de origen físico o lógico	MA	MA			A	MB	A				M
Servidor ambiente de pruebas y desarrollo	[I.6] Corte del suministro eléctrico	MA	MA			A	MB	A				M
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA	MA			A	MB	A				M
	[I.8.11] Interrupción accidental	MA	MA			A	MB	A				M
	[E.2] Errores del administrador del sistema / de la seguridad	A	x	x		M	MB	M				B
	[E.4] Errores de configuración		MA	MA		M	MB	M				B
	[E.21] Errores de mantenimiento / actualización de programas (software)	A	A	MA		M	MB	M				B
	[E.24] caída del sistema por agotamiento de recursos	MA	AA	MA		A	B	MA				A

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Servidor ambiente de pruebas y desarrollo	[A.5] suplantación de la identidad del usuario	MA	A	MA		A	MB	A				M
	[A.6] Abuso de privilegios de acceso			MA		A	MB	A				M
	[A.8] Difusión de software dañino		MA	MA	MA	A	B	MA				A
	[A.11] Acceso no autorizado	MA	A	MA		A	MB	A				M
	[A.24] Denegación de servicio	MA	A			A	B	MA				A
Elementos Auxiliares												
Sistema de aire acondicionado	[N.*] Desastres naturales	MA	A				MB	A				
	[I.5] Avería de origen físico o lógico	MA	A				MB	A				
	[I.6] Corte del suministro eléctrico	A	A				MB	M				
Planta eléctrica	[N.*] Desastres naturales	M	A				MB	B				
	[I.1] Fuego	M	A				MB	B				
	[I.3] Contaminación medioambiental	B	B				B	B				
	[I.5] Avería de origen físico o lógico	B	A				B	B				
	[I.6] Corte del suministro eléctrico	B	A				MB	MB				
	[I.7] Condiciones inadecuadas de temperatura o humedad	B	A				MB	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B	A				B	B				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Planta eléctrica	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	MA				MB	MB				
	[A.26] Ataque destructivo	M	MA				MB	B				
UPS de 10 KVA - Sede Princial	[N.2] Daños por agua	B	MA				MB	MB				
	[N.*] Desastres naturales	M	MA				MB	B				
	[I.1] Fuego	M	MA				MB	B				
	[I.5] Avería de origen físico o lógico	B	MA				MB	MB				
	[I.6] Corte del suministro eléctrico	B	MA				B	B				
Cuarto de servidores	[I.7] Condiciones inadecuadas de temperatura o humedad	MB	MA				B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B	A				B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	A				MB	MB				
	[A.7] uso no previsto	B	A				MB	MB				
	[A.23] Manipulación del hardware	B	MA	x			MB	MB				
Telefonía IP	[N.2] Daños por agua	B	A				MB	MB				
	[N.*] Desastres naturales	M	A				MB	B				
	[I.1] Fuego	M	A				MB	B				
	[I.5] Avería de origen físico o lógico	B	MA				MB	MB				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Telefonía IP	[I.6] Corte del suministro eléctrico	B	MA				B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB	A				B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B	A				B	B				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	MA	x			MB	MB				
	[A.7] uso no previsto	B	A	x			MB	MB				
Sistema de control de acceso físico	[A.23] Manipulación del hardware	B	MA	x			MB	MB				
	[N.2] Daños por agua	B	MA				MB	MB				
	[N.*] Desastres naturales	M	MA				MB	B				
	[I.1] Fuego	M	MA				MB	B				
	[I.5] Avería de origen físico o lógico	B	MA				MB	MB				
	[I.6] Corte del suministro eléctrico	B	MA				B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB	A				B	MB				
	[I.9] Interrupción de otros servicios o suministros esenciales	B	MA				B	B				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Servidor de Virtualización	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	A				MB	MB				
	[N.2] Daños por agua	B	MA				MB	MB				
	[N.*] Desastres naturales	M	MA				MB	B				
	[I.1] Fuego	M	MA				MB	B				
	[I.5] Avería de origen físico o lógico	B	MA				MB	MB				
	[I.6] Corte del suministro eléctrico	B	MA				B	B				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB	A				B	MB				
Gabinete de 8 blades	E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	MA				B	B				
	[E.24] caída del sistema por agotamiento de recursos	B	MA				MB	MB				
Cuarto de Servidores	[N.2] Daños por agua	B	MA				MB	MB				
	[N.*] Desastres naturales	M	MA				MB	B				
	[I.1] Fuego	M	MA				MB	B				
	[I.5] Avería de origen físico o lógico	B	MA				MB	MB				
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB	A				B	MB				

Tabla 16. Continuación

Activos	Amenazas	Impacto					P	Riesgo				
		[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
Armario y Caja fuerte	[A.7] uso no previsto	B	MA				MB	MB				
	[N.2] Daños por agua	B	MA				MB	MB				
	[N.*] Desastres naturales	M	MA				MB	B				
	[I.1] Fuego	M	MA				MB	B				
	[I.5] Avería de origen físico o lógico	B	MA				MB	MB				

Fuente: MAGERIT v.3 – Libro II – Catálogo de elementos

8.5.4 INTERPRETACIÓN DE LOS RESULTADOS

Los resultados de la tabla de riesgos nos dan una clara idea los activos de información que están expuestos a un alto riesgo, por lo cual se realiza un plan de acción y de seguimiento con el fin de minimizarlos.

Dentro de este grupo de activos los que mayor riesgo tienen, son: software/aplicativos de información, bases de datos, los aplicativos de información necesarios para la gestión de la Entidad, proveedores, backup, información de gestión interna de gestión interna, el riesgo puede ocurrir puesto que tiene una probabilidad alta en cuanto a errores de los usuarios y en el manejo y respaldo de la información. Así mismo en las caídas del sistema bien sea por agotamiento de recursos y denegaciones del servicio.

En el activo de equipos de cómputo, el riesgo puede ocurrir puesto que tiene una probabilidad alta, a causa de averías de origen físico o lógico, abusos de privilegios de acceso y usos no previstos.

En los activos de tipo servicio: Difusión de software dañino, Avería de origen físico o lógico, Condiciones inadecuadas de temperatura o humedad, Suplantación de la identidad del usuario, Acceso no autorizado, el riesgo puede ocurrir ya que tiene una probabilidad alta en abusos de privilegios de acceso, software dañino, usos no previstos, denegaciones de servicio y modificaciones de la información.

De igual forma que el activo “Antispam”, el riesgo puede ocurrir puesto que tiene una probabilidad alta en errores del administrador del sistema, errores de mantenimiento, denegaciones de servicio y ataques destructivos.

9. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN(Salvaguardas)

A continuación se relacionan los controles que se deben mejorar y los adicionales a implementar para reducir la exposición a los riesgos anteriormente identificados, se reitera que los riesgos calificados como Muy Bajos y Bajos, son aceptados.

Tabla 17. Controles de seguridad de la información

Ref.	Dominio de Control	Título de Control	Objetivo de Control	Estado del control	Aplica Si / No	Situación Actual
5.1.1	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**	Políticas para la seguridad de la información	**Orientación de la Dirección para la gestión**	El control se encuentra implementado y actualizado	Si	Resolución Interna N° 0166 agosto de 2017 "Por la cual establece la política de seguridad de la información de la Veeduría Distrital**"** y Manual de política de seguridad y controles sobre el manejo de la información - Código TIC_MAN-01– Daruma.
5.1.2		Revisión de las políticas para la seguridad de información			Si	Resolución Interna N° 166 agosto 18 de 2017 "Por la cual establece la política de seguridad de la información de la Veeduría Distrital**"**
6.1.1	**ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN**	Roles y responsabilidades para la seguridad de la información	**Organización Interna**	El control se encuentra implementado	Si	Manual de política de seguridad y controles sobre el manejo de la información - CódigoTIC-MAN-01 - Daruma.
6.1.2		Segregación de funciones		El control no se encuentra implementado	No	A través de la capacitación de la política de seguridad se divulga las implicaciones sobre el manejo de accesos indebidos contemplados (Ley 1273 de 2009)
6.1.3		Contacto con las autoridades		El control no se encuentra implementado	No	La oficina Asesora de Jurídica, tiene la competencia la presentación judicial de la Entidad en dado caso, en proceso elaboración del procedimiento sobre el manejo de este control.
6.1.4		Contacto con los grupos de interés especial		El control se encuentra implementado	No	No existen evidencias de relaciones con grupos que permitan estar atentos a las alertas, vulnerabilidades y amenazas sobre seguridad de la información.

Tabla 17. Continuación

Ref.	Dominio de Control	Título de Control	Objetivo de Control	Estado del control	Aplica Si / No	Situación Actual
6.1.5		Seguridad de la información en la gestión de proyectos		El control se encuentra implementado	No	Actualmente se está trabajando con la elaboración procedimientos, documentación o metodología en la formulación de proyectos.
6.2.1		Política para dispositivos móviles	**Dispositivos Móviles y de Teletrabajo**	El control se encuentra implementado parcialmente	No	La Entidad cuenta con conexiones para dispositivos móviles a través de las políticas de Vlans y GPO en el firewall sin embargo no se evidencia los registros de dichos usuarios, conexiones, copias sobre los accesos.
6.2.2		Teletrabajo		El control se encuentra implementado	Si	Resolución Interna 032 de 2017.
7.1.1	**SEGURIDAD DE LOS RECURSOS HUMANOS**	Selección personal	**Antes de asumir el empleo**	El control se encuentra implementado	No	Formato TH-FOT-023-17
7.1.2		Términos y Condiciones del empleo		El control no se encuentra implementado parcialmente	No	La política de seguridad incluye la responsabilidad sobre el cumplimiento de la seguridad de la información para todos los servidores públicos, más sin embargo no existen directrices dentro de los contratos o nombramientos en donde se especifiquen dichas responsabilidades
7.2.1		Responsabilidades de la Alta Dirección	**Durante la ejecución del empleo**	El control se encuentra implementado	Si	Resolución Interna N° 034 de 2017, ir la cual se crea el Comité del SGSI.
7.2.2		Toma de conciencia, educación y formación en la seguridad de la información		Control implrmentado	Si	En la inducción y reinducción se realiza capacitación y se crea conciencia sobre el manejo de la seguridad de la información (Código Disciplinario Ley 734 de 2002 y clausulas contractuales).
7.2.3		Proceso Disciplinario		El control se encuentra implementado	Si	De igual forma, Gestión TIC capacita y divulga a todos los servidores públicos sobre la toma de conciencia en la seguridad de la información.
7.3.1		Terminación o cambio de responsabilidad	**Terminación y cambio de empleo**	El control esta implementado	Si	Actualmente para todo el personal se incluye tanto en los funcionarios como contratistas la responsabilidad sobre el manejo de la información, manual de funciones como obligaciones contractuales.
8.1.1	**GESTION DE ACTIVOS**	Inventario de activos	**Responsabilidad por los activos**	El control esta implementado	Si	Por Deterioro o daño ó mal uso de bienes. Formato D-034-17 - Daruma.
8.1.2		Propiedad de los Activos		El control esta implementado	Si	Formato Inv-020-17 - Daruma.

Tabla 17. Continuación

Ref.	Dominio de Control	Título de Control	Objetivo de Control	Estado del control	Aplica Si / No	Situación Actual
8.1.3		Uso aceptable de los activos		El control no está implementado	No	Está en proceso ya solo existe la generación de una certificación a nivel de paz y salvo para la finalización de relaciones contractuales.
8.1.4		Devolución de Activos		El control está implementado	Si	Resolución interna 045 de 2017.
8.2.1		Clasificación de la información	**Clasificación de la información**	El control no está implementado	No	La Oficia Asesora de Planeación esta realizado el levantamiento de la información.
8.2.2		Etiquetado de la información		El control no está implementado	Si	Está en proceso de implementación no existe.
8.2.3	**GESTION DE ACTIVOS**	Manejo de activos		El control está implementado	Si	Este control esta implementado a nivel de los activos que gestiona el proceso de Gestión Tecnológica y de la información, pendiente de aprobación por el grupo de funcionarios y contratistas del TIC.
8.3.1		Gestión de medios removibles	**Manejo de medios**	El control no está implementado	No	Está pendiente ajustes el procedimiento respectivo.
8.3.2		Disposición de los medios		El control no está implementado	No	Está pendiente el procedimiento respectivo.
8.3.3		Transferencia de medios físicos		El control no está implementado	No	Está pendiente el procedimiento respectivo.
9.1.1		Política de control de acceso	**Requisitos del negocio para el control de acceso**	El control está implementado	Si	Los permisos de accesos físicos a las áreas de procesamiento de la información, Manual de política de seguridad y controles sobre el manejo de la información - Código TIC-MAN-01– Daruma y Resolución Interna N° 027 de enero 18 de 2017.
9.1.2	**CONTROL DE ACCESO**	Acceso redes y a Servicios de red		El control está implementado	Si	A medida que ingresa el personal los supervisores o jefes solicitan los perfiles de acceso a usuarios a redes y servicios.
9.2.1		Registro y cancelación del registro de usuarios	**Gestión de acceso de usuarios**	El control no está implementado	No	No se está realizando las novedades de registro de usuario. Por lo cual se está elaborando el procedimiento y la documentación respectiva.

Tabla 17. Continuación

Ref.	Dominio de Control	Título de Control	Objetivo de Control	Estado del control	Aplica Si / No	Situación Actual
9.2.2	**CONTROL DE ACCESO**	Suministro de acceso de usuarios	**Gestión de acceso de usuarios**	El control está implementado	Si	El supervisor o jefes del Área respectiva solicitud de acceso a usuarios a redes y servicios.
9.2.3		Gestión de derechos de acceso privilegiado		El control está implementado	Si	Manual de política de seguridad y controles sobre el manejo de la información - Código TIC-MAN-01- Daruma y Resolución Interna N° 027 de enero 18 de 2017.
9.2.4		Gestión de información autenticación usuarios.		El control está implementado	Si	Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código TIC-MAN-001 – Daruma.
9.2.5		Revisión de los derechos de acceso de usuarios		El control está implementado	Si	Manual de política de seguridad y controles sobre el manejo de la información - Código TIC-MAN-01 - Daruma y Resolución Interna N° 027 de enero 18 de 2017.
9.2.6		Retiro o ajuste de los derechos de usuario		El control está implementado	Si	A través del formato de Retiro de funcionario/Contratista de Daruma, se informa a Gestión TIC sobre al desvinculación de algún servidor público y así poder realizar la reasignación de la estación de trabajo.
9.3.1		Uso de información de autenticación secreta	**Responsabilidades del usuario**	El control está Implementado	Si	Dentro de las políticas de seguridad de la información mecanismos de cifrado, proceso de parametrización para el manejo de contraseñas se encuentra en el Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código TIC-MAN-001 – Daruma.
9.4.1		Restricción de acceso a la información	**Control de acceso a sistemas y aplicaciones**	El control está implementado	Si	El Área de TIC, realiza el control de acceso y contraseñas y los perfiles de seguridad necesarios a cada cuenta, se controla a través de log del sistema.

Tabla 17. Continuación

Ref.	Dominio de Control	Título de Control	Objetivo de Control	Estado del control	Aplica Si / No	Situación Actual
9.4.2		Procedimiento de ingreso seguro		El control no está implementado	Si	Se está ajustando un programa utilitario en el proceso de TIC.
9.4.3		Sistema de gestión de contraseñas		El control está implementado	Si	Resolución Interna N° 166 agosto 18 de 2017 "Por la cual establece la política de seguridad de la información de la Veeduría Distrital- Esquema de control y Manejo de Contraseñas.
9.4.4		Uso de programas utilitarios privilegiados		El control no está implementado	Si	No existe un procedimiento establecido.
9.4.5		Control de acceso a códigos fuente de programas		El control no está implementado	Si	No existe un procedimiento en la entidad o un requerimiento por un área específica sobre este control.
10.1.1	**CRIPTOGRAFIA**	Política sobre el uso de controles criptográficos	**Controles criptográficos**	El control no está implementado	No	No existe un procedimiento en la entidad o un requerimiento por un área específica sobre este control.
10.1.2		Gestión de llaves		El control no está implementado	No	No existe evidencias de procedimientos para el manejo de generación, resguardo, custodia

Tabla 17. Continuación

Ref.	Dominio de Control	Título de Control	Objetivo de Control	Estado del control	Aplica Si / No	Situación Actual
11.1.1	**SEGURIDAD FISICA Y DEL ENTORNO**	Perímetro de seguridad física	**Áreas seguras**	El control está implementado	Si	En relación con los contratistas la Entidad Control - Formato TIC-FT-005 - Daruma
11.1.2		Controles de acceso físicos		El control está implementado	Si	Actualmente existe seguridad a nivel de acceso a las instalaciones en general y en algunas áreas específicas, sin embargo debe fortalecerse el control.
11.1.3		Seguridad de oficinas, recinto e instalaciones		El control está implementado parcialmente	Si	En cuanto al proceso de Ti existen los elementos para protección contra incendio en el centro de cómputo.
11.1.4		Protección contra amenazas externas y ambientales		El control implementado	Si	Se debe revisar y documentar las políticas existentes; este control solo se ve aplicado en el Área de Tesorería
11.1.5		Trabajo en áreas seguras		El control está implementado parcialmente	Si	Se deben crear políticas y formatos aprobados donde se evidencien las actividades realizadas de implementación de este control
11.1.6		Áreas de despacho y carga		El control no está implementado	No	Existe la política aprobada sobre la seguridad y protección de los equipos de TI, sin embargo hay que fortalecer las actividades sobre este control
11.2.1		Ubicación y protección de los equipos	**Equipos**	El control está implementado	Si	Aunque se encuentra implementado se requiere revisión y documentación actualizada.
11.2.2		Servicios de suministro		El control está implementado	No	Aunque se encuentra implementado se requiere revisión y documentación actualizada; se debe contar con la documentación de acceso a los paneles de red de telecomunicaciones, (Energía Regulada)
11.2.3		Seguridad del cableado		El control está implementado	Si	Se realizan los debidos mantenimientos a todos los equipos del proceso de TIC , se existe la política y la documentación pertinente - Formatos Codigo TIC-CR-MAN-055 y Registro de Sororte Tecnico Código TIC-FT-008 - Daruma.

Tabla 17. Continuación

Ref.	Dominio de Control	Título de Control	Objetivo de Control	Estado del control	Aplica Si / No	Situación Actual
11.2.4	**SEGURIDAD FISICA Y DEL ENTORNO**	Mantenimiento de equipos		El control está implementado	Si	Este control se encuentra documentado, formato Daruma para los funcionarios y contratistas y procedimientos y políticas existentes.
11.2.5		Retiro de activos		El control está implementado	Si	Formato Daruma -Código PR-FT- 004 -
11.2.6		Seguridad de activos y equipos fuera de las instalaciones		El control no está implementado	No	Se realiza formateo de los equipos para reúso, se hace borrado de la información de dispositivos para darlos de baja, sin embargo hay que fortalecer los procedimientos y realizar la documentación pertinente.
11.2.7		Disposición segura o reutilización de los equipos		El control está implementado parcialmente	Si	Existe el bloqueo automático de sesión, a través de política de de seguridad según el Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código TIC-MAN-001 - Daruma
11.2.8		Equipos de usuario desatendido		El control no está implementado	No	Existe la política de seguridad sobre este control documentación y papeles físicos en el escritorio el proceso de Gestión Ambiental PIGA - sensibiliza y divulga sobre estas buenas prácticas ambientales.
11.2.9		Política de escritorio limpio y pantalla limpia		El control está implementado	Si	Existe la política de seguridad Resolución Interna 166 de agosto 2017 sobre este control y también la política de Cero Papel según la Directiva Presidencial 04 de 2012 y además las buenas prácticas ambientales - Plan Institucional de Gestión Ambiental.
12.1.1	**SEGURIDAD DE LAS OPERACIONES**	Procedimientos de operación documentados	**Procedimientos operacionales y responsabilidades**	El control no está implementado parcialmente	No	No existen procedimientos y políticas donde se implemente este control.
12.1.2		Gestión de cambios		El control no está implementado	No	No existe documentación ni procedimientos sobre control en la Entidad.

Tabla 17. Continuación

Ref.	Dominio de Control	Título de Control	Objetivo de Control	Estado del control	Aplica Si / No	Situación Actual
12.1.3	**SEGURIDAD DE LAS OPERACIONES**	Gestión de capacidad		El control no está implementado	No	Aunque existe la política y los ambientes de pruebas y desarrollo están separados, no existe ninguna documentación al respecto por lo tanto es indispensable realizar los formatos y procedimientos pertinentes.
12.1.4		Separación de los ambientes de desarrollo, prueba y operación		El control está implementado parcialmente	Si	El control se encuentra implementado a través de la política de seguridad y el monitoreo permanente que se hace a políticas y equipos y el respaldo de políticas es a través del equipo de seguridad perimetral.
12.2.1		Controles contra códigos maliciosos	**Protección contra los códigos maliciosos**	El control está implementado	Si	El control se encuentra implementado aunque debe reforzarse los procedimientos y realizar pruebas de restauración eventualmente. Formato de seguimiento de realización de backups: BITACORA DE BACKUP A-TIC-FT-012
12.3.1		Respaldo de la información	**Copias de respaldo**	El control está implementado	Si	Esta implementado se debe reforzarse los procedimientos, realizar pruebas de restauración eventualmente. Formato de seguimiento de realización de backups: Bitacora Backup – TIC-003-17 - Daruma
12.4.1		Registro de eventos	**Registro y seguimiento**	El control está implementado	Si	Existe el aplicativo Sistema de Reservas de Falta políticas y no existe documentación acerca de actividades sobre este control
12.4.2		Protección de la información de registro		El control está implementado	Si	Falta políticas y no existe documentación acerca de actividades sobre este control
12.4.3		Registros del administrador y del operador		El control está implementado	Si	Esta implementado a través del Protocolo W32Time
12.4.4		Sincronización de relojes		El control no está implementado	No	No hay registros de las configuraciones y actividades que evidencien el desarrollo de este control.

Tabla 17. Continuación

Referencia	Dominio de Control	Título de Control	Objetivo de Control	Estado del control	Aplica Si / No	Situación Actual
12.5.1	**SEGURIDAD DE LAS OPERACIONES**	Instalación de software en sistemas operativos	**Control de software operacional**	El control no está implementado	No	No existe evidencia ni procedimientos para la implementación de este control.
12.6.1		Gestión de las vulnerabilidades técnicas	**Gestión de la vulnerabilidad técnica**	El control no está implementado	Si	Esta aprobada la política dentro del documento Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código TIC-MAN-001 – Daruma, permisos de usuarios del directorio activo están contemplados tanto permisos y restricciones a los usuarios.
12.6.2		Restricciones sobre la instalación de software		El control no está implementado	No	No existen actividades sobre pruebas técnicas, acceso a software y procedimientos concernientes a pruebas de auditoría
12.7.1		Controles de auditorías de sistemas de información	**Consideraciones sobre auditorias de sistemas de información**	El control está implementado	Si	El control se encuentra implementado a través del Firewall sin embargo no existe documentación sobre esta implementación.
13.1.1	**SEGURIDAD DE LAS COMUNICACIONES**	Controles de redes	**Gestión de la seguridad de las redes**	El control está implementado parcialmente	Si	El control se encuentra implementado a través del Firewall y los switch sin embargo no existe documentación sobre esta implementación.
13.1.2		Seguridad de los servicios de red		El control está implementado	Si	El control se encuentra implementado a través del Firewall y los switch sin embargo no existe documentación sobre esta implementación.
13.1.3		Separación en las redes		El contro no está implementado	No	No hay evidencia de implementación de este control
				El control está implementado	Si	El control se encuentra implementado a través del servicio de correo electrónico, las políticas están definidas dentro Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código TIC-MAN-001,- Daruma- Configuración de la plataforma de correo y socialización de sus políticas.

Tabla 17. Continuación

Referencia	Dominio de Control	Título de Control	Objetivo de Control	Estado del control	Aplica Si / No	Situación Actual
13.2.2	**SEGURIDAD DE LAS COMUNICACIONES**	Acuerdos sobre transferencia de información		El control no está implementado	No	No hay evidencia de la implementación de este control
13.2.3		Mensajería electrónica		El control está implementado	Si	Aunque se llevan a cabo actividades sobre este control debe revisarse y documentarse de manera adecuada.
13.2.4		Acuerdos de confidencialidad o de no divulgación		El control está implementado	Si	Resolución Interna N° 166 de agosto 18 de 2017 sobre las políticas de seguridad de la información y los accesos de este control se realiza a través del Firewall.
14.1.1	**ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS**	Análisis y especificación de los requisitos de seguridad de la información	**Requisitos de seguridad de los sistemas de información**	El control está implementado parcialmente	Si	El control se encuentra implementado a través del código desarrollado, sin embargo no se encuentra la documentación respectiva donde se evidencie adecuadamente este manejo.
					Si	Se debe revisar y documentar este control ya que se realizan actividades en los desarrollos pero no están documentados.
14.1.2		Seguridad de los servicios de las aplicaciones en redes publicas		El control no está implementado	Si	No existe evidencia de la implementación de este control
14.1.3		Protección de transacciones de los servicios de las aplicaciones		El control está implementado parcialmente	Si	Existen actividades sobre pruebas de versiones específicamente en el sistema de información SYSMAN, ero falta la documentación y los procedimientos internos al respecto.
14.2.1		Política de desarrollo seguro	**Seguridad en los procesos de desarrollo y soporte**	El control no está implementado	No	No se evidencia documentación sobre la aplicación de este control
14.2.2		Procedimientos de control de cambio de sistemas		El control no está implementado	No	Se realizan actividades sobre sobre este control dentro del instituto, sin embargo se debe revisar la aplicación del control y la documentación respectiva.
14.2.3		Revisión técnica de las aplicaciones		El control no está implementado	No	Se deben fortalecer las obligaciones contractuales, el monitoreo a los compromisos, ya que están parcialmente ejecutados.

Tabla 17. Continuación

Referencia	Dominio de Control	Título de Control	Objetivo de Control	Estado del control	Aplica Si / No	Situación Actual
El control no está implementado		Cambios en la plataforma de operación.		El control no está implementado	No	No se encuentra documentación que evidencie la implementación de este control, por lo tanto debe revisarse y documentarse este control ya que si debe ser aplicado en el instituto.
14.2.4	**ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS**	Restricciones en los cambios a los paquetes de software		El control no está implementado	No	Las pruebas pilotos realizadas por los desarrolladores y los usuarios funcionales se documentan, sin embargo el formato no se está encaminado. Formato
14.2.5		Principios de construcción de los sistemas seguros		El control no está implementado	No	No se evidencia documentación sobre este control, por lo tanto se debe revisar y documentar estas actividades.
14.2.6		Ambiente de desarrollo seguro		El control no está implementado parcialmente	No	No existe documentación respectiva sobre políticas de seguridad de la información con proveedores
14.2.7		Desarrollo contratado externamente		El control está implementado parcialmente	Si	Esta implementado parcialmente ya que existen unas obligaciones contractuales pactadas y de acuerdo a la naturaleza de la contratación se fijan los aspectos que debe tener el personal técnico para proveer el servicio; también se manejan políticas de seguridad desde los accesos que se le asignan a los proveedores dependiendo del servicio es importante que este control se revise y fortalezca.
14.2.8		Pruebas de seguridad de sistemas		El control no se encuentra implementado	No	No se cuenta con evidencias de la implementación de este control.
14.2.9		Prueba de aceptación de sistemas		El control está implementado parcialmente	Si	Los funcionarios de TIC a través del monitoreo, hacen seguimiento de los aspectos de seguridad y niveles de desempeño del servicio que prestan los proveedores, falta más compromiso a esta actividad.
14.3.1		Protección de los datos de prueba	Datos de prueba	El control no está implementado	Si	No se realizan actividades para el cumplimiento de este control

Tabla 17. Continuación

Referencia	Dominio de Control	Título de Control	Objetivo de Control	Estado del control	Aplica Si / No	Situación Actual
15.1.1	**RELACIONES CON LOS PORVEEDORES**	Política de seguridad de la información para las relaciones con proveedores	**Seguridad de la información en las relaciones con los proveedores**	El control no está implementado	Si	No hay procedimientos establecidos sobre el registro de incidentes y procedimientos para el manejo de evidencia forense, sin embargo se realizan actividades a través del grupo de control interno disciplinario.
15.1.2		Tratamiento de la seguridad dentro de los acuerdos con proveedores.		El control no está implementado	Si	No existe procedimientos específicos y documentados sobre el manejo de reportes de seguridad de la información; el control debe revisarse y documentarse
15.1.3		Cadena de suministro de tecnología de información y comunicación		El control no está implementado	Si	No existen políticas ni procedimientos para que los empleados y contratistas reporten debilidades observadas que afectan la seguridad de la información.
15.2.1		Seguimiento y revisión de los servicios de proveedores	**Gestión de la prestación de servicios de proveedores**	El control está implementado parcialmente	Si	Existen actividades, pero no documentación sobre la implementación de este control
15.2.2		Gestión de cambios en los servicios de los proveedores		El control no está implementado	Si	No existen procedimientos para dar respuestas a incidentes de seguridad.
16.1.1	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**	Responsabilidades y procedimientos	**Gestión de incidentes y mejoras en la seguridad dela información**	El control no está implementado	Si	Aunque se realizan actividades sobre los incidentes de seguridad de la información, no hay documentación de implementación.
					Si	No hay procedimiento establecido para identificar recolectar, adquirir y preservar la información que sirva como evidencia dentro de incidentes de seguridad.
16.1.2		Reporte de eventos de seguridad de la información		El control no está implementado	Si	No hay evidencias de implementación de continuidad de seguridad de la información, el control se debe revisar y documentar
16.1.3		Reporte de debilidades de seguridad de seguridad de la información		El control no está implementado	Si	No hay evidencias de implementación de este control.

Tabla 17. Continuación

Referencia	Dominio de Control	Título de Control	Objetivo de Control	Estado del control	Aplica Si / No	Situación Actual
16.1.4	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**	Evaluación de eventos de seguridad de la información y decisiones sobre ellos		El control no está implementado	Si	Se debe realizar la valoración de activos y costos asociados con el fin de definir el plan alterno, por tanto este control debe implementarse y documentarse.
16.1.5		Respuesta a incidentes de seguridad de la información		El control no está implementado	Si	Se encuentra definida la normatividad dentro del normograma de la entidad ero falta implementarlo en forma.
16.1.6		Aprendizaje obtenido de los incidentes de seguridad de la información.		El control está implementado	Si	Existe la política aprobada en Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código TIC-MAN-001 - Daruma y están establecidas las actividades de utilización de software legal en la Veeduría Distrital.
16.1.7		Recolección de evidencia		El control está implementado	Si	Este control se maneja a través de las mismas políticas y procedimientos de toma de copias de seguridad
17.1.1	**ASPECTOS DE SEGURIDAD DE LA CONTINUIDAD DEL NEGOCIO**	Planificación de la continuidad de la seguridad de la información	**Continuidad de la seguridad de la información**	El control está implementado	Si	Se realizan actividades dentro de la seguridad específica de los sistemas de información -, sin embargo no existe una política aprobada para el manejo de este control.
17.1.2		Implementación de la continuidad de la seguridad de la información		El control no está implementado	Si	No existe manejo de controles criptográficos en la entidad.
17.1.3		Verificación, revisión y evaluación de la continuidad de la seguridad de la información		El control está implementado	Si	La oficina de control interno realiza las actividades de control sobre el proceso de Gestión Tecnológica y de la información
17.2.1		Disponibilidad de las instalaciones de procesamiento de información.	**Redundancias**	El control no está implementado	Si	La entidad periódicamente revisa la política de seguridad aprobada, sin embargo aún no existe un compromiso y seguimiento formal por cada uno de los responsables de las áreas y dependencias.

Tabla 17. Continuación

Referencia	Dominio de Control	Título de Control	Objetivo de Control	Estado del control	Aplica Si / No	Situación Actual
18.1.1	**CUMPLIMIENTO**	Identificación de la legislación aplicable y de los requisitos contractuales	**Cumplimiento de los requisitos legales y contractuales**	El control está implementado	Si	En Daruma se encuentra el módulo de Normograma en donde se encuesta la Normativa de la Entidad
18.1.2		Derechos de propiedad intelectual		El control está implementado	Si	Existe la política aprobada en Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código TIC-MAN-001 Daruma están establecidas las actividades de utilización de software legal en la entidad.
18.1.3		Protección de registros		El control está implementado	Si	Resolución Interna N° 166 de agosto 18 de 2017 "Políticas sobre seguridad de la información en la Veeduría Distrital"
18.1.4		Privacidad y protección de la información de datos personales		El control está implementado	Si	En cuanto a este control se ha realizado actividades sobre sobre la protección de datos personales.
18.1.5		Reglamentación de controles criptográficos		El control no está implementado	Si	La Entidad no cuenta con Criptografía.
18.2.1		Revisión independiente de la seguridad de la información	**Revisiones de seguridad de la información**	El control está implementado	Si	El centro de gestión de Control Interno realiza seguimiento de control sobre el proceso de Gestión Tecnológica y de la información.
18.2.2		Cumplimiento de las políticas y normas de seguridad		El control está implementado parcialmente	Si	Se realiza la revisión de la política de seguridad aprobada por resolución, pero aún debe existir mayor divulgación.
18.2.3		Revisión del cumplimiento técnico		El control no está implementado	Si	No se realizan actividades de monitoreo periódico de los sistemas de información en cuanto a pruebas pertinentes de seguridad como son las pruebas de penetración.

Fuente: http://www. ISO2700.org

9. PLAN DE TRATAMIENTO DE RIESGOS

El Plan de tratamiento de riesgos se realiza a los activos que obtuvieron unos niveles de riesgo medios, altos y muy altos.

Tabla 18. Plan de tratamiento de riesgos por activo de información

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
Documentación Técnica	[E.19] Fugas de información	Mitigar el riesgo	Resolución Interna N° 166 de 18 de agosto 2017 "Por la cual establece la política de seguridad de la información de la Veeduría Distrital" y Manual de política de seguridad y controles sobre el manejo de la información - Código TIC_MAN-01– Daruma.	Responsabilidades y proyectos de operación. Implementación y seguimiento de registros de actividad.
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			
	[E.2] Errores del administrador del sistema / de la seguridad			
	[E.15] Alteración de la información			
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			

Tabla 18. Continuación

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
Controlador de dominio principal	[E.2] Errores del administrador del sistema / de la seguridad	Mitigar el riesgo	Copias de seguridad de la información.	1.Responsabilidades y proyectos de operación. 2.Implementación y seguimiento de registros de actividad. 3.Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. 4.Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. 5.Gestión de incidentes
	[E.15] Alteración de la información			
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			
Controlador de dominio secundario	[E.19] Fugas de información	Mitigar el riesgo	Política de control de acceso, Copias de seguridad de la información y Registro y gestión de eventos de seguridad.	1.Responsabilidades y proyectos de operación. 2.Implementación y seguimiento de registros de actividad. 3.Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. 4.Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. 5.Gestión de incidentes
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			
	[E.2] Errores del administrador del sistema / de la seguridad			
	[E.15] Alteración de la información			
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			

Tabla 18. Continuación

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
Portal Institucional	[E.19] Fugas de información	Mitigar el riesgo	Ley 1273 de 2015 Acceso a la información, Manual de política de seguridad y controles sobre el manejo de la información - CódigoTIC-MAN-01 - Daruma.	Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad.
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			
	[E.2] Errores del administrador del sistema / de la seguridad			
	[E.15] Alteración de la información			
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			
Portal intranet	[E.19] Fugas de información	Mitigar el riesgo	Existe la política de seguridad de la información y Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código TIC-MAN-001, Daruma y las contraseñas se crean de acuerdo al perfil asignado en cada aplicación.	Implementación y seguimiento de registros de actividad. Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad.
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			
	[E.2] Errores del administrador del sistema / de la seguridad			
	[E.15] Alteración de la información			

Tabla 18. Continuación

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
	[E.18] Destrucción de la información			Implementación y seguimiento de registros de actividad. Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad.
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			
Correo electrónico Gmail	[E.19] Fugas de información	Mitigar el riesgo	Conjunto de políticas para la seguridad de la información, Registro y gestión de eventos de seguridad, Responsabilidades y procedimientos ante incidentes de seguridad y Registro y gestión de eventos de seguridad.	Implementación y seguimiento de registros de actividad. Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad.
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			
	[E.2] Errores del administrador del sistema / de la seguridad			
	[E.15] Alteración de la información			
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			
Almacenamiento en la nube	[E.19] Fugas de información	Mitigar el riesgo	Se tienen actividades relacionados con el control, pero falta procedimiento.	Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Responsabilidades
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			

Tabla 18. Continuación

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
Almacenamiento en la nube	[E.2] Errores del administrador del sistema / de la seguridad	Mitigar el riesgo	Se tienen actividades relacionados con el control, pero falta procedimiento	Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Responsabilidades
	[E.15] Alteración de la información			
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			
Sistema Distrital de Quejas y Soluciones - SDQS-	[E.19] Fugas de información	Mitigar el riesgo	A través de la capacitación de la política de seguridad se divulga las implicaciones sobre el manejo de accesos indebidos contemplados (Ley 1273 de 2009)	Responsabilidades y proyectos de operación. Implementación y seguimiento de registros de actividad. Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Gestión de incidentes de Seguridad de la información.
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			
	[E.2] Errores del administrador del sistema / de la seguridad			
	[E.15] Alteración de la información			
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			

Tabla 18. Continuación

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
Sistema Biométrico	[E.19] Fugas de información	Mitigar el riesgo	Gestión de claves, Políticas de control de acceso y Resolución interna 166/17.	Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad.
	[A.15] Modificación de la información		Control de acceso al código fuente de los programas Manipulación de los activos. Protección contra las amenazas externas y ambientales.	Responsabilidades y proyectos de operación. Implementación y seguimiento de registros de actividad. Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Gestión de incidentes de Seguridad de la información.
	[A.5] suplantación de la identidad del usuario			
	[E.2] Errores del administrador del sistema / de la seguridad			
	[E.15] Alteración de la información			
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			
Portal Académico (B-Learning)	[E.19] Fugas de información	Mitigar el riesgo	Política de control de acceso, Copias de seguridad de la información, Proceso disciplinario, Registro y gestión de eventos de seguridad	Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad.
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			
	[E.2] Errores del administrador del sistema / seguridad			

Tabla 18. Continuación

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
	[E.18] Destrucción de la información	Mitigar el riesgo	Política de control de acceso, Copias de seguridad de la información, Proceso disciplinario, Registro y gestión de eventos de seguridad	Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			
Software de Sistemas operativos (medios)	[E.19] Fugas de información	Mitigar el riesgo	Registros de actividad del administrador y operador de los sistema, Gestión de derechos de acceso con privilegios especiales, Respuesta a los incidentes de seguridad y .Protección contra las amenazas externas y ambientales.	Responsabilidades y proyectos de operación. Implementación y seguimiento de registros de actividad. Adaptación plan de contingencia TICS, Gestión de incidentes de Seguridad de la Información
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			
	[E.2] Errores del administrador del sistema /			
	[E.15] Alteración de la información			
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			
Software de Base de Datos (medios)	[E.19] Fugas de información	Mitigar el riesgo	Registros de actividad del administrador y operador del sistema, Gestión de derechos de acceso con privilegios.	Responsabilidades y proyectos de operación. Implementación y seguimiento de registros de actividades o Gestión de incidentes de Seguridad infor.
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			

Tabla 18. Continuación

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
Software de para manejo de bases de datos de gestión documental - Winisis	[E.2] Errores del administrador del sistema / de la seguridad	Mitigar el riesgo	Se tienen registros de actividad del administrador y operador de los sistemas. Respuesta a los incidentes de seguridad – Daruma	Responsabilidades y proyectos de operación. Implementación y seguimiento de registros de actividad. Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Gestión de incidentes de Seguridad de la información.
	[E.15] Alteración de la información			
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			
Sistema de Selección de Personal - Secop	[E.19] Fugas de información	Mitigar el riesgo	Actualmente existe una base de datos de usuarios, sin embargo esta no se actualiza continuamente, pendiente procedimiento y sincronizar el Sistemas de información por medio del directorio activo.	Implementación y seguimiento de registros de actividad. Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad.
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			
	[E.2] Errores del administrador del sistema / de la seguridad			
	[E.15] Alteración de la información			
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
Sistema de Gestión de Calidad - Daruma	[E.19] Fugas de información	Mitigar el riesgo	La Entidad cuenta con conexiones para dispositivos móviles a través de las políticas de Vlans y GPO en el firewall.	. Responsabilidades y proyectos de operación. Implementación y seguimiento de registros de actividad. Control de acceso y responsabilidades de los usuarios a los sistemas y aplicaciones. Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Gestión de incidentes de Seguridad de la información.
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			
	[E.2] Errores del administrador del sistema / de la seguridad			
	[E.15] Alteración de la información			
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			
Aplicativo de Nómina	[E.19] Fugas de información	Mitigar el riesgo	Conjunto de políticas para la seguridad de la información, Registro y gestión de eventos de seguridad, Responsabilidades y procedimientos ante incidentes de seguridad y Registro y gestión de eventos de seguridad.	Implementación y seguimiento de registros de actividad. Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad.
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			
	[E.2] Errores del administrador del sistema / de la seguridad			

Tabla 18. Continuación

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
Aplicativo de Nómina	[E.15] Alteración de la información	Mitigar el riesgo	Registro de acceso implementación de la continuidad de la seguridad de la información-proceso disciplinario.	Implementación y seguimiento de registros de actividad. Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad. Responsabilidad
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			
Equipos de cómputo	[E.19] Fugas de información	Mitigar el riesgo	En la inducción y reinducción se realiza capacitación y se crea conciencia sobre el manejo de la seguridad de la información (Código Disciplinario Ley 734 de 2002 y clausulas contractuales).	Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos) Adaptación plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio Gestión de incidentes de Seguridad de la Información
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			
	[E.2] Errores del administrador del sistema / de la seguridad			
	[E.15] Alteración de la información			
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			

Tabla 18. Continuación

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
Servidor Oracle N-90	[E.19] Fugas de información [A.15] Modificación de la información	Mitigar el riesgo	En la inducción se realiza capacitación y se crea conciencia sobre el manejo de la seguridad de la información (Código Disciplinario Ley 734 de 2002	Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos) Adaptación plan de contingencia TICS, como marco de Gestión de incidentes de Seguridad de la Información
UPS de 10K autonomía aprox. 30min.para sostenimiento del centro de cómputo.	[A.5] suplantación de la identidad del usuario [E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información [E.18] Destrucción de la información [A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.11] Acceso no autorizado	Mitigar el riesgo	Suministro en tecnologías de la información y comunicaciones Para la seguridad de la información.	Adaptación plan de contingencia TICS, como marco de Gestión de incidentes de Seguridad de la Información
Servidor base de datos SQL	[E.19] Fugas de información [A.15] Modificación de la información [A.5] suplantación de la identidad del usuario [E.2] Errores del administrador del sistema / de la seguridad	Mitigar el riesgo	De igual forma, Gestión TIC capacita y divulga a todos los servidores públicos sobre la toma de conciencia en la seguridad de la información.	Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos) Adaptación plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio Gestión de incidentes de Seguridad de Inf

Tabla 18. Continuación

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
Sistema de almacenamiento formato rack	[E.15] Alteración de la información [E.18] Destrucción de la información [A.6] Abuso de privilegios de acceso [A.7] uso no previsto	Mitigar el riesgo	Suministro en tecnologías de la información y comunicaciones Para la seguridad de la información	Implementación y seguimiento de registros de actividad. Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad.
Sistema de Gestión Documental - Orfeo	[E.19] Fugas de información [A.15] Modificación de la información [A.5] suplantación de la identidad del usuario [E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información [E.18] Destrucción de la información [A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.11] Acceso no autorizado	Mitigar el riesgo	Existe la política creada dentro del Manual de política de seguridad y controles básicos y específicos para el manejo de la información - Código TIC-MAN-001, Daruma en cuanto a las contraseñas se crean de acuerdo a la autoridad de cada aplicación, en la gestión de contraseñas para el ingreso a la red	Implementación y seguimiento de registros de actividad. Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad.
Servidor Backups VD-SERVER-SD2, Sigco, Orfeo	[E.19] Fugas de información [A.15] Modificación de la información	Mitigar el riesgo	Se están realizando actividades y se asignan responsabilidades y pendiente procedimiento	

Tabla 18. Continuación

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
Software Sisep	[A.5] suplantación de la identidad del usuario [E.2] Errores del administrador del sistema / [E.15] Alteración de la información	Mitigar el riesgo	Gestión de acceso a usuarios .Gestión de derechos de acceso asignados a usuarios .Gestión de contraseñas de usuarios. Proceso Disciplinario	Implementación y seguimiento de registros de actividad. Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad.
Aplicativo Reservas	[E.18] Destrucción de la información [A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.11] Acceso no autorizado	Mitigar el riesgo	Gestión de acceso a usuarios .Gestión de derechos de acceso asignados a usuarios .Gestión de contraseñas de usuarios.	Implementación y seguimiento de registros de actividad. Seguimiento y cumplimiento de la política de Seguridad de la información de la Entidad.
Sistema de almacenamiento formato rack	[E.19] Fugas de información [A.15] Modificación de información [A.5] suplantación de la identidad del usuario [E.2] Errores del administrador del sistema [E.15] Alteración de la información [E.18] Destrucción de la información [A.6] Abuso de privilegios de acceso [A.7] uso no previsto [A.11] Acceso no autorizado	Mitigar el riesgo	Por Deterioro o daño ó mal uso de bienes. Formato D-034-17 - Daruma.	Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos) Responsabilidades y proyectos de operación. Implementación y seguimiento de actividades Adaptación plan de contingencia TICS, Gestión de incidentes de Seguridad de la Información

Tabla 18. Continuación

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
Máquina Virtual Windows NT 4.0 (Base de Sisep)	[E.19] Fugas de información	Mitigar el riesgo	Se está formalizando el procedimiento y responsabilidades al administrador por daño ó mal uso de bienes. Formato TIC-FMT- D-034.	Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos) Responsabilidades y proyectos de operación. Implementación y seguimiento de actividades Adaptación plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio Gestión de incidentes de Seguridad de la Información
	[A.15] Modificación de la información			
	[A.5] suplantación de la identidad del usuario			
	[E.2] Errores del administrador del sistema / de la seguridad			
	[E.15] Alteración de la información			
	[E.18] Destrucción de la información			
	[A.6] Abuso de privilegios de acceso			
	[A.7] uso no previsto			
	[A.11] Acceso no autorizado			
Switch de borde 4210G	[N.2] Daños por agua	Mitigar el riesgo	Inventario de equiposuso aceptable de los activosProceso disciplinario Implantación de la seguridad de la información Cadena de suministro en tecnologías de la información y comunicaciones amenazas externas.	Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos) Responsabilidades y proyectos de operación. Implementación y seguimiento de actividades Adaptación plan de contingencia TICS, como marco de Gestión de incidentes de Seguridad de la Información
	[N.*] Desastres naturales			
	[I.1] Fuego			
	[I.7] Condiciones inadecuadas de temperatura o humedad			
	[E.4] Errores de configuración			

Tabla 18. Continuación

Activo	Amenaza	Tratamiento	Control	Acciones de Implementación
Servidor formato blade marca Hewlett Packard. Modelo proliant BL460C G7	[I.3] Contaminación medioambiental	Mitigar el riesgo		Control de acceso físico y protección de la información (Áreas Seguras y seguridad de equipos) Adaptación plan de contingencia TICS, como marco de Gestión del Plan de Continuidad del Negocio Gestión de incidentes de Seguridad de la Información
	[I.6] Corte del suministro eléctrico			
	[N.2] Daños por agua			
	[N.*] Desastres naturales			
	[I.1] Fuego			
	[I.7] Condiciones inadecuadas de temperatura o humedad			
	[E.4] Errores de configuración			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)			

Fuente: El autor

11. PLAN DE DIVULGACIÓN

La divulgación de las medidas de seguridad derivadas de este proyecto será gestionada directamente por la Alta Dirección de la Veeduría Distrital en cuanto haya sido aprobado.

A través del portal institucional se divulgará a todos los servidores públicos, la adopción de la política de seguridad de la Veeduría Distrital con sus roles, responsabilidades y compromiso del manejo de la información. De igual forma en del aplicativo para calidad y sistemas de gestión ISO – Daruma, se encontrarán los manuales de procesos, procedimientos instructivos, formatos y demás, con el propósito de garantizar su desempeño, eficacia y cumplimiento.

Adicionalmente realizarán jornadas de capacitación y acciones para que los servidores públicos adopten, interioricen y acaten los procedimientos y prácticas de seguridad definidas y que comprendan las implicaciones.

El presente proyecto de grado para su consulta se enviará al repositorio institucional de la Universidad Abierta y a Distancia – UNAD.,

12. RESULTADOS

Ante todo se ha dado cumplimiento a los objetivos propuestos: se realizó el levantamiento de los activos de información, y con la herramienta Magerit 6.2 v3 y con la colaboración de cada uno de los responsables se efectuó la valoración en cada activo de información acuerdo a su clasificación correspondiente.

Se propuso el plan de tratamiento de riesgos, con la valoración de los activos y los resultados generados en cuanto los pilares fundamentales de la seguridad de la información como lo es la Confidencialidad, Integridad y Disponibilidad de los activos que generaron resultados con una valoración de medio alto y muy alto, y con un plan de recuperación de desastres para lo referente tercerización de los servicios.

También es importante realizar un seguimiento a los resultados obtenidos en este proyecto con la finalidad de concretar la continuidad de los servicios y el plan adecuado de recuperación de desastres.

13. CONCLUSIONES

Para la Veeduría Distrital, el diseño del Sistema de Gestión de Seguridad de la Información - SGSI permitirá mejorar la seguridad de la información y de sus activos informáticos, lo cual redundará en la mejor prestación del servicio y en cumplimiento de los objetivos institucionales.

El diseño del SGSI proporcionará herramientas a cada uno de los activos, a recursos humanos y a aquellas áreas que por sus actividades requieren de la utilización de tecnologías de la información (IT) para desarrollar la gestión de cada uno de sus procesos, utilizando controles que permitan mitigar el riesgo y proporcionando una metodología adecuada para garantizar la confidencialidad, la integridad y la disponibilidad de los activos de información.

Se demostró que existe la factibilidad técnica, económica y operativa para diseñar SGSI, que le permite a la Entidad contar con un análisis y valoración de riesgos a los activos informáticos, como a su vez un proceso de concientización y cultura de la importancia de la seguridad de la información y los impactos que esta tiene a nivel institucional.

BIBLIOGRAFÍA

ICONTEC INTERNATIONAL. EL COMPENDIO DE TESIS Y OTROS TRABAJOS DE GRADO. {En línea}. {Consultado agosto 2017}. Disponible en: http://www.ICONTEC.org/BancoConocimiento/C/compendio_de_tesis_y_otros_trabajo_de_grado/compendio_de_tesis_y_otros_trabajos_de_grado.asp?CodIdioma=ESP.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Guía de Actividades. {En línea}. {Consultado septiembre 2017}. Disponible en: http://152.186.37.83/ecbti01/mod/forum/view.php?id=15243.

ÁLVAREZ BASULDÚA, Luis Daniel, Seguridad Informática, Universidad Iberoamericana, México, D.F.

AGESIC Agencia para el Desarrollo, guía “Implantación de un SGSI “versión, I
Tecnosfera. Ataques cibernéticos contra el Gobierno podrían aumentar en 2015.

UNIVERIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Capítulo 2 - Construcción del Anteproyecto de Grado. {En línea}. {Consultado abril 2017}. Disponible en: http://152.186.37.83/ecbti01/pluginfile.php/31026/mod_resource/content/1/Metodolog%C3%ADa.pdf

ALCALDÍA MAYOR DE BOGOTÁ. Norma Técnica Distrital del Sistema Integrado de gestión para las entidades y organismos distritales NTD-SIG 001:2011. Bogotá. 2012.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 2573 de 2014. {En línea}. {Consultado octubre 2017}.Disponible:http://wp.presidencia.gov.co/sitios/normativa/decretos/2014/Decretos2014/ DECRETO%202573%20DEL%2012%20DE%20DICIEMBRE%20DE%202014.pdf

--------. Norma Colombiana Guía de implementación de un sistema de gestión de seguridad de la información. Bogotá D.C. ICONTEC, 2015. 81p. NTC-ISO/IEC 27003.

--------. Norma Colombiana Guía de implementación de un sistema de gestión de seguridad de la información. Bogotá D.C. ICONTEC, 2015. 107p. NTC-ISO/IEC 27002.

--------. Norma Colombiana para la Gestión del riesgo en la Seguridad de la Información. Bogotá D.C. ICONTEC, 2015. 67p. NTC-ISO/IEC 27005.

--------. Norma Colombiana para la presentación de tesis, trabajos de grado y otros trabajos de investigación. Sexta edición. Bogotá D.C.: ICONTEC, 2008. 36p. NTC-1486.

SECRETARÍA GENERAL ALCALDÍA MAYOR DE BOGOTÁ D.C. - COMISIÓN DISTRITAL DE SISTEMAS - CDS. . {En línea}. {Consultado octubre 2017} Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=33486.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Lección 13 Fases para la implantación del SGSI. Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/51_leccin_21_fases_para_la_implantacin_del_sgsi.html

TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Guía de implementación de un sistema de gestión de la seguridad de la información. GTC-ISO/IEC 27003.

EL TIEMPO Ataques cibernéticos contra el Gobierno podrían aumentar en 2015, Tecnosfera, . {En línea}. {Consultado octubre 2017}. Disponible en Internet:http://www.eltiempo.com/tecnosfera/novedades-tecnologia/ataques-ciberneticos-contra-el-gobierno-podrian-aumentar-en-2015/16036825.

COLOMBIA DIGITAL. ¿Cómo está Latinoamérica en temas de seguridad informática? Corporación Colombia Digital**.** {En línea}. {Consultado octubre 2017}.Disponible en Internet: http://colombiadigital.net/actualidad/noticias/item/8250-como-esta-latinoamerica-en-temas-de-seguridad-informatica.html

MINISTERIO DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. . {En línea}. {Consultado octubre 2017}Fortalecimiento de la Gestión TIC en el Estado, Sistemas de Gestión de la Seguridad de la Información

(SGSI). Vive Digital para la Gente, [en línea], Sin fecha de publicación [consultado 10 de octubre 2016]. Disponible en Internet:http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

ANEXOS

Anexo A. Formato RESUMEN ANÁLITICO EN EDUCACIÓN - RAE -

UNAD Universidad Nacional Abierta y a Distancia	FORMATO
	RESUMEN ANALÍTICO EN EDUCACIÓN - RAE
Código:	**Versión: 01**
Fecha de Aprobación:	**Página 159**

1. Información General	
2. Tipo de documento	Tesis de Grado
3. Acceso al documento	Universidad Nacional Abierta y a Distancia - UNAD
4. Título del documento	Diseño de un sistema de gestión de la seguridad de la información para la red de datos de la veeduría distrital en la ciudad de Bogotá
5. Autores	CABALLERO, Mariela
6. Director	GONZALEZ, Salomón
7. Publicación	Bogotá. Universidad Nacional Abierta y a Distancia, 2017. P. 157
8. Unidad Patrocinante	Veeduría Distrital
9. Palabras Claves	Seguridad informática, Seguridad de la información, Inventario de activos, Valoración de riesgos, MAGERIT v3.0, Amenazas, NTC- ISO/IEC 27001.

10. Descripción

Este proyecto se desarrolla para comprobar los beneficios al mejorar el nivel de seguridad del sistema informático de la Veeduría Distrital de la ciudad de Bogotá, Mediante el diseño de un SGSI que permita mitigar las amenazas y vulnerabilidades presentes y gestionar adecuadamente los riesgos en cada uno de los activos de información.

11. Fuentes

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Guía de Actividades. Disponible en: http://152.186.37.83/ecbti01/mod/forum/view.php?id=15243

ÁLVAREZ BASULDÚA, Luis Daniel, Seguridad Informática, Universidad Iberoamericana, México, D.F.

AGESIC Agencia para el Desarrollo, guía "Implantación de un SGSI "versión, I

Tecnosfera. Ataques cibernéticos contra el Gobierno podrían aumentar en 2015.

UNIVERIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Capítulo 2 - Construcción del Anteproyecto de Grado. Disponible en: http://152.186.37.83/ecbti01/pluginfile.php/31026/mod_resource/content/1/Metodolog%C3%ADa.pdf

ALCALDÍA MAYOR DE BOGOTÁ. Norma Técnica Distrital del Sistema Integrado de gestión para las entidades y organismos distritales NTD-SIG 001:2011. Bogotá. 2012.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 2573 de 2014. Disponible en: http://wp.presidencia.gov.co/sitios/normativa/decretos/2014/Decretos2014/DECRETO%202573%20DEL%2012%20DE%20DICIEMBRE%20DE%202014.pdf

Norma Colombiana Guía de implementación de un sistema de gestión de seguridad de la información. Bogotá D.C. ICONTEC, 2015. 81p. NTC-ISO/IEC 27003.

Norma Colombiana Guía de implementación de un sistema de gestión de seguridad de la información. Bogotá D.C. ICONTEC, 2015. 107p. NTC-ISO/IEC 27002.

Norma Colombiana para la Gestión del riesgo en la Seguridad de la Información. Bogotá D.C. ICONTEC, 2015. 67p. NTC-ISO/IEC 27005.

Norma Colombiana para la presentación de tesis, trabajos de grado y otros trabajos de investigación. Sexta edición. Bogotá D.C.: ICONTEC, 2008. 36p. NTC-1486.

SECRETARÍA GENERAL ALCALDÍA MAYOR DE BOGOTÁ D.C. - COMISIÓN DISTRITAL DE SISTEMAS - CDS. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=33486

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Lección 13 Fases para la implantación del SGSI. Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/51_leccin_21_fases_para_la_implantacin_del_sgsi.html

GTC-ISO/IEC 27003. Tecnología de la información. Técnicas de seguridad. Guía de implementación de un sistema de gestión de la seguridad de la información. ICONTEC. 2012.

EL TIEMPO [en línea], Ataques cibernéticos contra el Gobierno podrían aumentar en 2015, Tecnosfera, consulta 2 de julio de 2015. Disponible en Internet:http://www.eltiempo.com/tecnosfera/novedades-tecnologia/ataques-ciberneticos-contra-el-gobierno-podrian-aumentar-en-2015/16036825.

Colombia Digital. ¿Cómo está Latinoamérica en temas de seguridad informática? Corporación Colombia Digital [en línea], 14 de Abril de 2015].Disponible en Internet: http://colombiadigital.net/actualidad/noticias/item/8250-como-esta-latino america-en-temas-de-seguridad-informatica.html

MINTIC Ministerio TIC. Fortalecimiento de la Gestión TIC en el Estado, Sistemas de Gestión de la Seguridad de la Información (SGSI). Vive Digital para la Gente, [en línea], Sin fecha de publicación [consultado 10 de octubre 2016]. Disponible en Internet:http://www.mintic.gov.co/gestionti/615/w3-article-5482.htm

12. Contenido

Mediante este proyecto se pretende implementar el Sistema de Gestión de Seguridad de la Información con el fin de garantizar la seguridad de la información y la preservación de los activos informáticos de la Veeduría Distrital.
El trabajo de grado consta de**:**

Objetivo general

Establecer políticas y procedimientos mediante el diseño de un Sistema de Gestión de la Seguridad Informática y de la información SGSI para la red de datos de la Veeduría Distrital en la ciudad de Bogotá, D.C.

Objetivos específicos

-Identificar y determinar los activos informáticos mediante la aplicación de instrumentos de recolección de información para establecer dominios del estándar ISO/IEC 27001:2013.

-Determinar las vulnerabilidades, amenazas y riesgos de seguridad existentes para hacer valoración de los mismos aplicando la metodología MAGERIT.

-Verificar la existencia de controles de acuerdo a la norma ISO/IEC 27001:2013 que ayuden a definir la existencia de políticas y procedimientos de seguridad.

-Establecer los controles de la norma ISO 27001:2013, planes de mejoramiento y procedimientos que permitan mitigar las causas que originan los riesgos de seguridad de la información en la Veeduría Distrital.

Marco Referencial: Compuesto por el Marco de antecedentes, marco contextual, marco conceptual, marco teórico y marco legal relacionado con el desarrollo del proyecto.

Diseño Metodológico: Se describe la metodología de investigación y la metodología de desarrollo del proyecto como es: identificación de la población, muestra, análisis y fuente de recolección de la información, como también los instrumentos utilizados para realizar el análisis de los datos y la metodología para el desarrollo de la investigación.

Recursos Requeridos

Análisis del Sistema de información de Seguridad de la Información. Identificación y valoración de activos de acuerdo a la metodología seleccionada y descripción del análisis y valoración de los riesgos.

Recomendaciones:

Concientizar a los responsables y administradores de activos de información en la importancia de mantener actualizado el Sistema de Gestión de Seguridad de la Información en aspectos legales, técnicos y financieros, y por ello la Alta Dirección debe asegurar que todo el personal de la Entidad al que se le asignen responsabilidades definidas en el SGSI esté suficientemente capacitado SGSI.

Bibliografía e infografía

13. Metodología

Para el Diseño de un SGSI en la Veeduría Distrital se utilizó la Metodología MAGERIT v.3, que permitió realizar el análisis y valoración del riesgo; en concordancia con la Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 a través del ciclo PHVA.

Fase 1 - Planeación
Fase 2 - Hacer
Fase 3 -Verificar
Fase 4 - Actuar

14. Conclusiones

Para la Veeduría Distrital, el diseño del Sistema de Gestión de Seguridad de la Información - SGSI permitirá mejorar la seguridad de la información y de sus activos informáticos, lo cual redundará en la mejor prestación del servicio y en cumplimiento de los objetivos institucionales.

El diseño del SGSI proporcionará herramientas a cada uno de los activos, a recursos humanos y a aquellas áreas que por sus actividades requieren de la utilización de tecnologías de la información (IT) para desarrollar la gestión de cada uno de sus procesos, utilizando controles que permitan mitigar el riesgo y proporcionando una metodología adecuada para garantizar la confidencialidad, la integridad y la disponibilidad de los activos de información.

Se demostró que existe la factibilidad técnica, económica y operativa para diseñar SGSI, que le permite a la Entidad contar con un análisis y valoración de riesgos a los activos informáticos, como a su vez un proceso de concientización y cultura de la importancia de la seguridad de la información y los impactos que esta tiene a nivel institucional.

15. Plan de Divulgación

La divulgación de las medidas de seguridad derivadas de este proyecto será gestionada directamente por la Alta Dirección de la Veeduría Distrital en cuanto haya sido aprobado.

A través del portal institucional se divulgará a todos los servidores públicos, la adopción de la política de seguridad de la Veeduría Distrital con sus roles, responsabilidades y compromiso del manejo de la información. De igual forma en del aplicativo para calidad y sistemas de gestión ISO – Daruma, se encontrarán los manuales de procesos, procedimientos instructivos, formatos y demás, con el propósito de garantizar su desempeño, eficacia y cumplimiento.

Adicionalmente realizarán jornadas de capacitación y acciones para que los servidores públicos adopten, interioricen y acaten los procedimientos y prácticas de seguridad definidas y que comprendan las implicaciones.

El presente proyecto de grado para su consulta se enviará al repositorio institucional de la Universidad Abierta y a Distancia – UNAD.

Elaborado por:	Mariela Caballero
Revisado por:	González García Salomón

Fecha de elaboración del Resumen:	14	11	2017

ANEXO B.

VEEDURIA
DISTRITAL

Bogotá, D.C, 2 de septiembre de 2016

Guardar como

Señores
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD
Posgrado en Especialización en Seguridad Informática
Ciudad

Cordial saludo:

La Veeduría Distrital identificada con el Nit. 899.999.061-9 ha recibido la solicitud de Mariela Caballero, identificada con la cédula de ciudadanía 51.573.183 para desarrollar en la Entidad el proyecto de seguridad informática ***"Diseño de un Sistema de Gestión de Seguridad Informática para la Red de Datos de la Veeduría Distrital en la Ciudad de Bogotá"***, como parte de la culminación de estudios de posgrado en esa institución.

La Entidad acoge la propuesta y la aprueba autorizando su realización con toda la colaboración, disposición y espacio requerido para llevar a cabo el respectivo proyecto.

Atentamente,

ALEXANDRA RODRÍGUEZ DEL GALLEGO
Viceveedora Distrital