DISEÑO DE UN SISTEMA DE SEGURIDAD INFORMÁTICA PARA LA DIRECCIÓN TERRITORIAL DE BOGOTÁ DEL MINISTERIO DEL TRABAJO

LUIS ALFONSO DOMÍNGUEZ BARRETO
COD. 10100654

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA **UNAD**
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2016

DISEÑO DE UN SISTEMA DE SEGURIDAD INFORMÁTICA PARA LA DIRECCIÓN TERRITORIAL DE BOGOTÁ DEL MINISTERIO DEL TRABAJO UBICADA EN LA CIUDAD DE BOGOTÁD.C.

LUIS ALFONSO DOMÍNGUEZ BARRETO
COD. 10100654

Trabajo de grado para optar al título de Especialista en Seguridad informática

Director
YINA ALEXANDRA GONZALEZ SANABRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA **UNAD**
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN DEN SEGURIDAD INFORMÁTICA
BOGOTÁ
2017

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 31/03/2017

A mis padres, mis hermanos, mi esposa y mis hijos por estar conmigo y apoyarme siempre.

AGRADECIMIENTOS

A cada uno de los maestros y tutores que me han orientado a través, de todos los años de formación.

CONTENIDO

PAG.

GLOSARIO 12
RESUMEN 16
INTRODUCCIÓN 18
1. PRESENTACIÓN DEL PROYECTO 20
1.1. NOMBRE DEL PROYECTO 20
1.2. TEMA DE ESTUDIO 20
1.3. LÍNEA DE INVESTIGACIÓN 20
1.4. PLANTEAMIENTO DEL PROBLEMA 20
1.5. JUSTIFICACIÓN DEL PROYECTO 22
1.6. OBJETIVOS 23
1.6.1. GENERAL. 23
1.6.2 ESPECÍFICOS. 23
1.7. ALCANCE DEL PROYECTO 24
2. MARCO REFERENCIAL 24
2.1 MARCO CONTEXTUAL 25
Misión 28
Visión 28
2.2 ESTADO DEL ARTE 31
2.2 MARCO TEÓRICO 33
2.2.1 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 34
2.2.2 NORMA ISO27001 - CICLO PHVA 38
2.2.3 METODOLOGÍA MAGERIT 39
2.3. MARCO CONCEPTUAL 41
2.4. MARCO LEGAL 49
3. DISEÑO METODOLÓGICO 52
3.1. FUENTES DE INFORMACIÓN 52
3.2. ESTADO ACTUAL - DIAGNÓSTICO 54
3.3. TIPO DE INVESTIGACIÓN 54
3.4. METODOLOGÍA MAGERIT - ISO 27001 56

4. DESARROLLO METODOLOGICO 63
4.1 IDENTIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS CRITICOS DE LA ORGANIZACIÓN 64
4.1.1 EQUIPOS DE CÓMPUTO REDES Y COMUNICACIONES 64
4.1.2 RECURSOS HUMANOS 67
4.1.3 DATOS E INFORMACIÓN 69
4.1.4 SOFTWARE Y APLICACIONES 70
4.1.5 SERVICIOS 72
4.1.6 EXPEDIENTES EN CURSO 73
4.1.7 VALORACIÓN DE LOS ACTIVOS 73
4.2 DETERMINACIÓN DE AMENAZAS 74
4.3 ESTIMACIÓN DEL IMPACTO 78
4.4 CÁLCULO DEL RIESGO 79
4.5 SALVAGUARDAS 80
5. POLÍTICAS Y CONTROLES 81
6. PLAN DE SENSIBILIZACIÓN 88
7. PLAN DE REVISIÓN PERIODICA Y ACTUALIZACIÓN DEL SGSI 89
8. CONCLUSIONES Y RECOMENDACIONES 90
BIBLIOGRAFÍA 92
ANEXOS 94

LISTA DE TABLAS

Pág.

Tabla 1. Estado del Arte 31

Tabla 2. PHVA aplicado a los procesos del SGSI 36

Tabla 3. Inventario Equipos Centro De Cómputo 65

Tabla 4. Funcionarios Y Equipos 69

Tabla 5. Aplicaciones y BD 71

Tabla 6. Escala Valoración de Activos 73

Tabla 7. Valoración de Activos 74

Tabla 8. Escala Valoración de Amenazas 77

Tabla 9. Valoración de Amenazas 77

Tabla 10. Escala Estimación del Impacto 78

Tabla 11. Estimación del Impacto 78

Tabla 12. Cálculo del riesgo 79

LISTA DE GRÁFICAS

Pág.

Gráfica 1. Nombre de la gráfica xx

Gráfica 2. Nombre de la gráfica xx

Gráfica 3. Nombre de la gráfica xx

Gráfica 4. Nombre de la gráfica xx

LISTA DE FIGURAS

Pág.

Figura 1. Ubicación de la DTBogotá en el D.C. 25

Figura 2. DT Bogotá Entrada cra 7 Bogotá 26

Figura 3. Organigrama Mintrabajo 27

Figura 4. Mapa de Procesos Mintrabajo 28

Figura 5. Modelo PHVA aplicado a los procesos del SGSI 36

Figura 6. Vista actual del cuarto de cableado 65

Figura 7. Servidor SDTCUNDI01 70

LISTA DE ANEXOS

Pág.

Anexo A. Vista encuestas digitales de Inventario y tecnología 94

Anexo B. Circular Uso de servicios Informáticos 95

Anexo C. Boletines Campaña de sensibilización 96

GLOSARIO

AMENAZA: Situación o evento con que puede provocar daños en un sistema.

ANÁLISIS DE VULNERABILIDADES: Análisis del estado de la seguridad de un sistema o sus componentes mediante el envío de pruebas y recogida de resultados en intervalos.

AUTENTICACIÓN: Proceso de confirmar la identidad de una entidad de sistema (un usuario, un proceso, etc.).

AUTORIZACIÓN: Acción de otorgar el acceso a usuarios, objetos o procesos.

GESTIÓN DE REDES: Controlar diversos aspectos de una red para optimizar su eficiencia. Las cinco categorías de gestión de red son: seguridad, fallo, auditoría, configuración y gestión de rendimiento.

GESTIÓN DE RENDIMIENTO: En gestión de redes, medición de los diferentes elementos de la red. Los resultados de estas mediciones se utilizan para optimizar su funcionamiento.

GESTIÓN DE SEGURIDAD: Proceso de establecer y mantener la seguridad en un sistema o red de sistemas informáticos. Las etapas de este proceso incluyen la prevención de

problemas de seguridad, detección de intrusiones, investigación de intrusiones, y resolución.

INTEGRIDAD: Requisito de seguridad que indica que la información deberá ser protegida ante alteraciones no autorizadas.

POLÍTICA DE SEGURIDAD: Conjunto de reglas que ponen en práctica los requisitos de seguridad del sistema.

PRIVACIDAD: Estar libre de accesos no autorizados.

PRIVILEGIO: Nivel de confianza perteneciente a un objeto de sistema.

VULNERABILIDADES: Debilidades en un sistema que pueden ser utilizadas para violar las políticas de seguridad.

RIESGO: Efecto de la incertidumbre sobre la consecución de los objetivos.
NOTA 1 – Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto.
NOTA 2 – Los objetivos pueden tener diferentes aspectos (tales como financieros, de salud y seguridad, o ambientales) y se pueden aplicar a diferentes niveles (tales como nivel estratégico, nivel de un proyecto, de un producto, de un proceso o de una organización completa).

NOTA 3 – Con frecuencia, el riesgo se caracteriza por referencia a sucesos potenciales y a sus consecuencias, o a una combinación de ambos.

NOTA 4 – Con frecuencia, el riesgo se expresa en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) y de su probabilidad.

NOTA 5 – La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad.

PROCESO DE GESTIÓN DEL RIESGO: Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.

DUEÑO DEL RIESGO: Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo.

TRATAMIENTO DEL RIESGO: Proceso destinado a modificar el riesgo.

NOTA 1 – El tratamiento del riesgo puede implicar:

Evitar el riesgo, decidiendo no iniciar o continuar con la actividad que motiva el riesgo;

Aceptar o aumentar el riesgo con objeto de buscar una oportunidad;

Eliminar la fuente de riesgo;

Cambiar la probabilidad;

Cambiar las consecuencias;

Compartir el riesgo con otra u otras partes [incluyendo los contratos y la financiación del riesgo; y

Mantener el riesgo en base a una decisión informada.

NOTA 2 – Los tratamientos del riesgo que conducen a consecuencias negativas, en ocasiones se citan como "mitigación del riesgo", "eliminación del riesgo", "prevención del riesgo" y "reducción del riesgo".

NOTA 3 – El tratamiento del riesgo puede originar nuevos riesgos o modificar los riesgos existentes.1

TRÁMITES: Solicitudes de los ciudadanos ante la Administración que se resuelven de manera inmediata (Certificaciones, Permisos, Consultas)

INVESTIGACIONES: Procesos que ameritan seguimiento por violación a las normas administrativo laborales.

EXPEDIENTES: Compilación de la investigación en documentos físicos y/o Digitales

CONCILIACIÓN: Audiencias para lograr acuerdo entre partes en conflicto, Trabajador – Empleador.

DT BOGOTÁ: Denominación abreviada de la Dirección Territorial de Bogotá del Ministerio del Trabajo.

[1] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método

RESUMEN

En este Trabajo se describen los riesgos y vulnerabilidades que surgen del flujo de información en la red, Bases de datos, Servidores y Aplicaciones de la Dirección Territorial de Bogotá (DT Bogotá), la cual es una dependencia del Ministerio del trabajo, donde se atienden trámites, audiencias de conciliación y se adelantan investigaciones dentro del ámbito administrativo laboral. Se plantea una solución para evitar ataques informáticos con objetivos poco éticos, y para desarrollar mecanismos de seguridad diseñados para regular y proteger la confidencialidad de los datos, prevenir e intentar detectar tentativas de intrusión para así poder llevar a cabo la reparación del daño más adelante. Actualmente se manejan una precaria interpretación de la normatividad como política de seguridad informática, sin que exista la debida documentación y difusión en la entidad. Los usuarios del sistema informático desconocen los cuidados de seguridad informática que se deben tener y realizan acciones inseguras propiciando riesgo con los daños consecuentes que pueden afectar el normal desarrollo de las actividades.

Palabras Claves: Amenaza, Detección, Hacking, Prevención, Riesgo, Seguridad, Técnica, VLAN, Segmentación, PHVA

ABSTRACT

This document describes the risks and vulnerabilities that arise from the information flow in the Network, Databases, Servers and Applications of the Bogotá Territorial Direction (DTBogotá), which is a department of the Ministry of Labour where processes, conciliation hearings, and investigations related to the administrative labour environment take place. A solution is proposed to avoid computer attacks with unethical aims, and to develop security mechanisms designed to regulate and protect the confidentiality of data, and to prevent any attempt of intrusion in order to avoid system damage. Nowadays exists a precarious interpretation of normativity as a policy of computer security, with lack of documentation and dissemination of information in the department. Computer users are unaware of the system security precautions that must be taken and carry out unsafe actions, causing risk, with the consequent damages that can affect the normal operations of the department.

Keywords: Access, threaten, Detection, Hacking, Prevention, Risk, Security, Technical, VLAN, Segmentation, PHVA

INTRODUCCIÓN

De manera sencilla y con el propósito de ser asertivo se describe el estado actual y se propone desarrollar un sistema de gestión de seguridad de la información para la DT BOGOTÁ del Ministerio del Trabajo. El planteamiento de la necesidad de gestión del riesgo y luego la propuesta de aplicar medidas preventivas y correctivas surgen de la particular situación de que radica en que no cuenta con un sistema de gestión de seguridad de la información y que en él, sea posible brindar el conocimiento a las personas que trabajan en las diferentes áreas de la DT BOGOTÁ del Ministerio del Trabajo para la protección de la información, el cual es el activo más valioso de la empresa. Esto se debe a que en esta dependencia, que es la presenta el mayor flujo de expedientes de investigaciones administrativo laborales atiende las audiencias de Resolución de Conflictos y Conciliaciones y gestiona trámites directamente las solicitudes de trámites de los Ciudadanos, las empresas de servicios Temporales, los sindicatos y las asociaciones de Pensionados. Se pretende estructurar un sistema de gestión de la seguridad de la información para garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la entidad de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías, La carencia de este diseño representa inminentes riesgos rutinarios con la información que allí se maneja.

Lo anterior, hace que se establezca como prioridad un sistema de gestión de seguridad de la información como parte relevante de una Dirección Territorial donde la información está concentrada en un alto volumen de documentos físicos y una naciente consolidación en

bases de datos que todavía se manejan de manera dispersa y varios aplicativos elementales que operar de manera aislada. El respaldo y la salvaguarda de estos recursos son precarios por tanto en el SGSI a diseñar se asume una de las medidas más importantes para gestionar los riesgos y minimizar su impacto.

1. PRESENTACIÓN DEL PROYECTO

1.1. NOMBRE DEL PROYECTO

DISEÑO DE UN SISTEMA DE SEGURIDAD INFORMÁTICA PARA LA DIRECCIÓN TERRITORIAL DE BOGOTÁ DEL MINISTERIO DEL TRABAJO

1.2.TEMA DE ESTUDIO

Diseño de un Sistema de Seguridad de la Información para la Dirección Territorial de Bogotá que forma parte del Ministerio del Trabajo y es el área de contacto con los ciudadanos y las empresas con domicilio en el Distrito Capital.

1.3. LÍNEA DE INVESTIGACIÓN

Línea: Gestión de Sistemas – Área de Modelos y Estándares de Seguridad Informática.

1.4.PLANTEAMIENTO DEL PROBLEMA

La Dirección Territorial de Bogotá del Ministerio del trabajo, ubicada en el piso 2 de la carrera 7 No.32 63 de la ciudad de Bogotá, se conecta a la red principal del ministerio,

mediante fibra óptica, aquí en el data center local se distribuye en 194 puntos de los cuales diez están reservados para Access Point (Actualmente siete en funcionamiento), así se habilita un segmento de red para el trabajo y la navegación de 116 equipos de escritorio, cincuenta equipos portátiles, sendas tablets asignados a funcionarios, telefonía IP, los equipos de ciudadanos que acuden a adelantar sus diligencias en esta sede y se suma un número no definido de SmartPhones. Actualmente no existen políticas ni controles de seguridad propios de la entidad claramente definidos, se reciben soporte del nivel central a cargo de una empresa contratista, sin tener directrices documentadas que sean de rigurosa aplicación.

Se evidencia la recurrente caída de la señal de los puntos de acceso de la red inalámbrica, lo que causa el "intercambio" de información y algunas veces de contraseñas entre los funcionarios que están fuera de la wifi y los equipos conectados a los puntos fijos. Esto en el afán de acceder a los servidores, las impresoras, scanner y correo institucional.

Además de la probabilidad de acceso a la red por parte de personas ajenas a la entidad (intrusos desde las proximidades del edificio), el intercambio de datos se realiza por medios físicos con gran exposición a infección por virus informáticos, pérdida de información y suplantación de usuarios.

Las Bases de datos están expuestas a manipulación de muchos usuarios tratando de optimizar los procesos, la información se encuentra dispersa y tanto los bancos de datos como los aplicativos son independientes unos de otros y muy elementales.

Se hace obvio el malestar, el retraso y algunas veces hasta la suspensión de actividades, generando confusión, agravada si se tiene en cuenta que se atienden audiencias y trámites a los que acuden clientes externos (ciudadanos).

Ante la evidente necesidad de proteger los recursos informáticos de esta Importante

Ante la evidente necesidad de proteger los recursos informáticos de esta Importante dependencia del Ministerio del trabajo se plantea la siguiente premisa:

¿Es factible diseñar un Sistema de Gestión de Seguridad Informática, para solventar los problemas evidenciados en el análisis de riesgos y vulnerabilidades, focalizado en la Dirección territorial de Bogotá del Ministerio del Trabajo, y así poder prevenir y minimizar el daño que puedan causar un eventual Ataque interno o Externo?

1.5. JUSTIFICACIÓN DEL PROYECTO

Teniendo en cuenta que la Información es activo importante y valioso para la entidad, y que se evidencian inminentes riesgos y amenazas contra los principios de seguridad, se hace indispensable establecer la Protección Adecuada para que de manera estructurada se abarquen todos los niveles de certidumbre garantizando la continuidad de los trámites y el manejo de expedientes, se minimicen potenciales daños causados por cualquier contingencia y se optimice la inversión que representa el Sistema de Seguridad Informática.

Se debe hacer un reconocimiento del panorama de la legislación nacional e internacional en contra de los delitos informáticos para dimensionar la problemática que está afectando a la entidad, a los ciudadanos y al estado Colombiano.

La implementación del Sistema de gestión de Seguridad Informático en la DT Bogotá es esencial para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen institucional necesarios para lograr los objetivos del Ministerio del Trabajo y asegurar beneficios propios y para la comunidad vinculada.

1.6. OBJETIVOS

1.6.1. GENERAL.

Diseñar un sistema de gestión de seguridad información para la Dirección Territorial del Ministerio del Trabajo en Bogotá.

1.6.2 ESPECÍFICOS.

Identificar y evaluar las vulnerabilidades y riesgos asociados al sistema de información existente en la Dirección Territorial de Bogotá del Ministerio del Trabajo.

Definir y documentar un plan de tratamiento del riesgo de Seguridad Informática que permita brindar un mayor nivel de seguridad de la información dentro de la Dirección Territorial de Bogotá del Ministerio del Trabajo.

Crear un manual de sensibilización que permita la revisión periódica de controles para mantener las buenas prácticas de Seguridad de la Información en el MT.

1.7. ALCANCE DEL PROYECTO

El estudio estará focalizado en la gestión de tecnología e Informática en la Dirección Territorial de Bogotá del ministerio del trabajo para la cual se elaborará el diseño de un Sistema de Gestión de Seguridad de la Información, utilizando como guía principal la norma NTC-ISO-IEC 27001 que adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA) y MAGERIT como metodología de análisis y gestión de riesgos para estructurar todos los procesos del SGSI.

2. MARCO REFERENCIAL

Se ha seleccionado esta entidad para hacer un acercamiento a sus procesos para aplicar la conceptualización Seguridad de la Información y proponer una solución que permitirá reducir problemas y facilitar el desempeño de las actividades propias de cada dependencia dentro del Ministerio.

2.1 MARCO CONTEXTUAL

El Ministerio del trabajo es la entidad de orden nacional encargada de construir acuerdos, promover el empleo digno, proteger los derechos de los colombianos en capacidad de trabajar, construir más y mejores empresas, fomentar la calidad del talento humano y buscar que en Colombia no haya un solo trabajador sin protección social.

El Ministerio del trabajo está integrado por 51 Dependencias del nivel central, 32 Direcciones territoriales correspondientes a los departamentos administrativos, dos oficinas especiales las de Urabá y Barrancabermeja y un total de 141 inspecciones municipales.
La dirección territorial de Bogotá está ubicada en la calle 32 No. 32 63

Fig. No. 1 Ubicación de la DT Bogotá en el D.C.

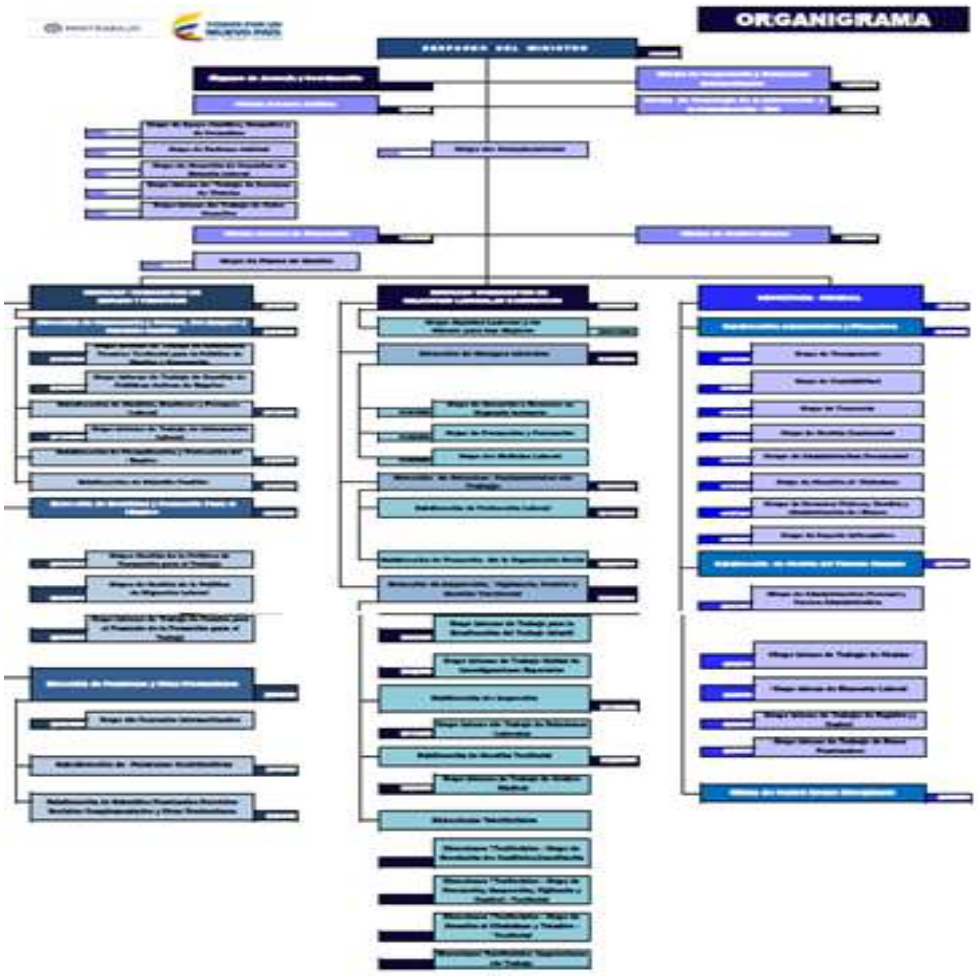
Fuente: https://www.google.com.co/maps/place/Oficina+De+Trabajo/@4.622156,-74.0771792,14z/data=!4m5!3m4!1s0x0:0xefcdefe43e81bd0c!8m2!3d4.619675!4d-74.0680811

Figura No. 2 DT Bogotá Entrada cra 7 Bogotá

La dirección territorial de Bogotá a su vez está conformada por los grupos de trabajo del Despacho, Riegos Laborales, Grupo de Prevención Inspección Vigilancia y Control (PIVC), Grupo de Resolución de Conflictos y Conciliaciones (RCC), y el grupo de Atención al Ciudadano y Trámites (GACT). En las inspecciones de los diferentes grupos se atienden ciudadanos y/o se gestionan expedientes de investigaciones Administrativo laborales y algunos trámites.

Organigrama del Ministerio del Trabajo

Figura No. 3 Organigrama Mintrabajo



Fuente: www.Mintrabajo.gov.co

Esta dependencia tiene un población promedio de 150 funcionarios, más personal de apoyo, si se suman los ciudadanos y representantes de los empleadores que generan un alto flujo de personas y tareas, causa mayores requerimientos de atención en cuanto a seguridad y manejo de la información, lo cual conlleva necesariamente a que se adecuen escenarios

que presentan vulnerabilidades de seguridad en los sistemas informáticos, de cuyo análisis nos ocuparemos en este trabajo.

Misión

Formular, adoptar y orientar la política pública en materia laboral que contribuya a mejorar la calidad de vida de los colombianos, para garantizar el derecho al trabajo decente, mediante la identificación e implementación de estrategias de generación y formalización del empleo; respeto a los derechos fundamentales del trabajo y la promoción del diálogo social y el aseguramiento para la vejez.

Visión

Para 2018, ser reconocidos como el Ministerio que promueve la protección, vinculación, formalización y el acceso al trabajo de los colombianos en las diferentes etapas de su ciclo de vida laboral, en el marco del trabajo decente; gestionando la consolidación del Sistema de Protección para la vejez y la articulación intersectorial.[2]

Mapa De Procesos

Aquí se plasman los procesos misionales y de apoyo del Ministerio.

[2] http://www.mintrabajo.gov.co/el-ministerio/quienes-somos/mision-vision-y-objetivos.html

Fig. No. 4 Mapa de Procesos Mintrabajo

Fuente: www.mintrabajo.gov.co\SIG

La Dirección Territorial, los procesos se adelantan en Grupos de trabajo de la siguiente manera:

Dirección (Despacho del Director) – Riesgos Laborales

Dirección: resolver recursos de reposición de accidentes de accidentes laborales, apelación grupos IVC, RCC, Atención al ciudadano, apoyos y respuestas acciones de tutela, respuestas derechos de petición, traslado documentación, cierre de empresas temporal o definitivo y despidos colectivos.

Riesgos Laborales: investigación accidentes de trabajo, visitas de carácter general, visitas a petición de los ciudadanos.

Resolución de Conflictos y Conciliaciones – RCC

RCC: audiencias de conciliaciones, atentos atentatorios al derecho de asociación sindical (persecución sindical, violación al derecho de asociación), negativa a negociar, acoso laboral, responder derechos de petición, resolver recursos de reposición, apoyo acción de tutela.

Prevención Investigación Vigilancia y control – PIVC

Adelanta investigaciones por presunta violación a los derechos laborales, apoyo acción de tutela, visitas de carácter de inspección general, visitas solicitadas por los ciudadanos, responder derechos de petición, resolver recursos de reposición, investigación posibles violaciones a las convenciones colectivas (sindicatos).

Atención al Ciudadano y Trámites – GACT

Autorización despido de trabajadores en estado de embarazo, discapacitados, cierre de empresas temporales, declaración de siniestro en las empresas temporales, autorización funcionamiento horas extras, registros sindicales.

2.2 ESTADO DEL ARTE

De estudios sobre la seguridad de la información y el diseño de políticas para ser aplicados en diferentes sistemas de información tanto de entidades públicas como de empresas privadas se ha asimilado información y conocimiento ha a partir del cual se han generado comparaciones que ofrecen diferentes posibilidades de comprensión del problema tratado debido a que posibilitan alternativas en torno al caso de estudio. Así que algunos de los resultados, conclusiones o, respuestas se han consultado en trabajos ya realizados sobre seguridad informática, así como proyectos de grado relacionados con el tema. En la siguiente se relación se describen algunos de estos que han servido como material de referencia para el presente trabajo de investigación aplicada al Ministerio del Trabajo en su sede de La DT Bogotá.

Tabla No. 1 Estado del Arte

Titulo/ Autores	Resumen
Implementación De Sistema De Gestión De Seguridad De La Información Aplicada Al Área De Recursos Humanos De La Empresa Decevale S.A. Calderón Onofre Diana Estrella Ochoa Martín Flores Villamarín Manuel Www.Espol.Edu.Ec/	Plantea La Reorganización Del Departamento De Recursos Humanos Para Mejorar Sus Procedimientos Y Aplicarlos A La Seguridad De La Información, Tomando Esta Última Como Un Activo Más De La Empresa E Indispensable Para El Desarrollo De Sus Actividades

Metodología De Implantación De Un SGSI En Un Grupo Empresarial Jerárquico Ing. Gustavo Pallas Mega	Implantar, Operar Y Mantener De Forma Evolutiva, Un Sistema De Gestión De Seguridad De La Información (SGSI) Para Una Empresa U Organización Perteneciente A Un Grupo Empresarial, En Una Relación De Subordinación Con Otra Empresa Principal. Es Decir, Existe Un Orden Jerárquico Establecido Que No Será Ajeno A La Seguridad De La Información.
"Aplicación De La Metodología Magerit Para El Análisis Y Gestión De Riesgos De La Seguridad De La Información Aplicado A La Empresa Pesquera E Industrial Bravito S.A. En La Ciudad De Machala" Karina Del Rocío Gaona Vásquez	Seguridad Y Gestión De Riesgos De Los Activos De La Empresa "Pesquera E Industrial Bravito S.A.". Proponiendo La Metodología Magerit Para Realizar El Análisis De Riesgos
Análisis Y Diseño De Un Sistema De Gestión De La Seguridad De La Información Basado En El Criterio De La Norma Nte Inen-Iso/Iec 27001:2011, De Un Modelo De Negocio Aplicado En La Comercialización Y Distribución De Productos Químicos. Xavier Alejandro Águila Plaza	Adopción De Un Sgsi (Sistema De Gestión De Seguridad De Información) Basado En La Norma Homologada Para Ecuador Nte Inen-Iso/Iec 27001:2011 Ha Despertado Interés En Organizaciones Que Se Dedican A La Comercialización Y Distribución De Productos Químicos, Con La Finalidad Mejorar La Gestión De La Seguridad De Información, En Sus Procesos Y La Gestión De Riesgo En Sus Activos De Información.
Diseño De Una Metodología Para La Implementación Del Sistema De Gestión De Seguridad De La Información - Sgsi, En El Sector De Laboratorios De Análisis Microbiológicos, Basado En Iso 27001. Johanna Carolina Buitrago Estrada Diego Hernando Bonilla Pineda Carol Estefanie Murillo Varón	Diseño Metodológico Para La Implementación De Un Sistema De Seguridad De La información Sgsi En El Sector De Laboratorios De Análisis Microbiológicos Que Garantice El Nivel De Seguridad Y Permita Obtener La Certificación Iso/Iec 27001:2005; Se Adopta Como Referencia Las Normas Iso 27001 Y 27002. Finalmente, Se Concluye Que La Seguridad Es Un Proceso De Implantación Que Exige Un Cambio Cultural Y Organizativo En Las Empresas.
Diseño De Un Sistema De Gestión De Seguridad De La Información (Sgsi) Para El Departamento De Informática De La Superintendencia De Notariado Y Registro	Diseño Del Sistema De Gestión De Seguridad De La Información, Para La Superintendencia De Notariado Y Registro Considerando Fundamente Los Conceptos Y Planteamientos De Los Estándares Internacionales De La Iso,

Loileiman Enrique Quintero Parra	Específicamente Las Normas Iso/Iec 27001 E Iso/Iec 27002. Así Como La Aplicación De La Metodología Magerit Para La Ejecución De La Tarea De Análisis De Riesgo Respectivo, Metodología Diseñada Por El Gobierno Español Para La Ejecución De Análisis De Riesgo.
Propuesta De Actualización, Apropiación Y Aplicación De Políticas De Seguridad Informática En Una Empresa Corporativa, Propolsinecor. Luis Olmedo Patiño Alpala	Se Diseña Una Propuesta De Actualización, Apropiación E Implementación De Políticas Claras De Seguridad De La Información, Acordes Al Negocio Y Actividades De La Compañía, Para Ser Aprobadas Por La Alta Gerencia, Difundidas E Implementación Por Propolsinecor., Se Valoran Los Activos Informáticos, Se Analizan Las Vulnerabilidades, Amenazas Y Riesgos Existentes En La Seguridad Informática, Que Puedan Afectar Los Recursos Y Prestigio De La Compañía Para Contrarrestar Y Mitigar Los Riesgos En Seguridad Informática,
Diseño De Un Sistema De Gestión De La Seguridad Informática – Sgsi–, Para Empresas Del Área Textil En Las Ciudades De Itagüí, Medellín Y Bogotá D.C. A Través De La Auditoría Ing. Alexander Guzmán García Ing. Carlos Alberto Taborda Bedoya	Desarrollo De Un Sistema De Gestión De La Seguridad Informática (Sgsi) Para Empresas Del Sector Textil De Las Pymes En Las Ciudades De Medellín, Bogotá D.C. He Itagüí (Colombia): Basados En La Norma Iso 27001, Estableciendo Las Fases, Documentación Y Procedimientos Requeridos Y Exigidos En El Estándar.

Fuente: Autor

2.2 MARCO TEÓRICO

Como guía y marco de ordenamiento para este proyecto, ISO 27001, es un estándar internacional publicado en octubre de 2005, para gestionar y garantizar la selección de

controles de seguridad adecuados y proporcionales la organización de la información. Es una norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI), contribuye a la protección de los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI. Es una norma adecuada para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo, además es una norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI), contribuye a la protección de los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes.

2.2.1 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Seguridad Informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

Considerar aspectos de seguridad significa conocer el peligro, clasificarlo y protegerse de los impactos o daños de la mejor manera posible. Esto significa que solamente cuando estamos conscientes de las potenciales amenazas, agresores y sus intenciones dañinas (directas o indirectas) en contra de nosotros, podemos tomar medidas de protección adecuadas, para que no se pierda o dañe nuestros recursos valiosos.

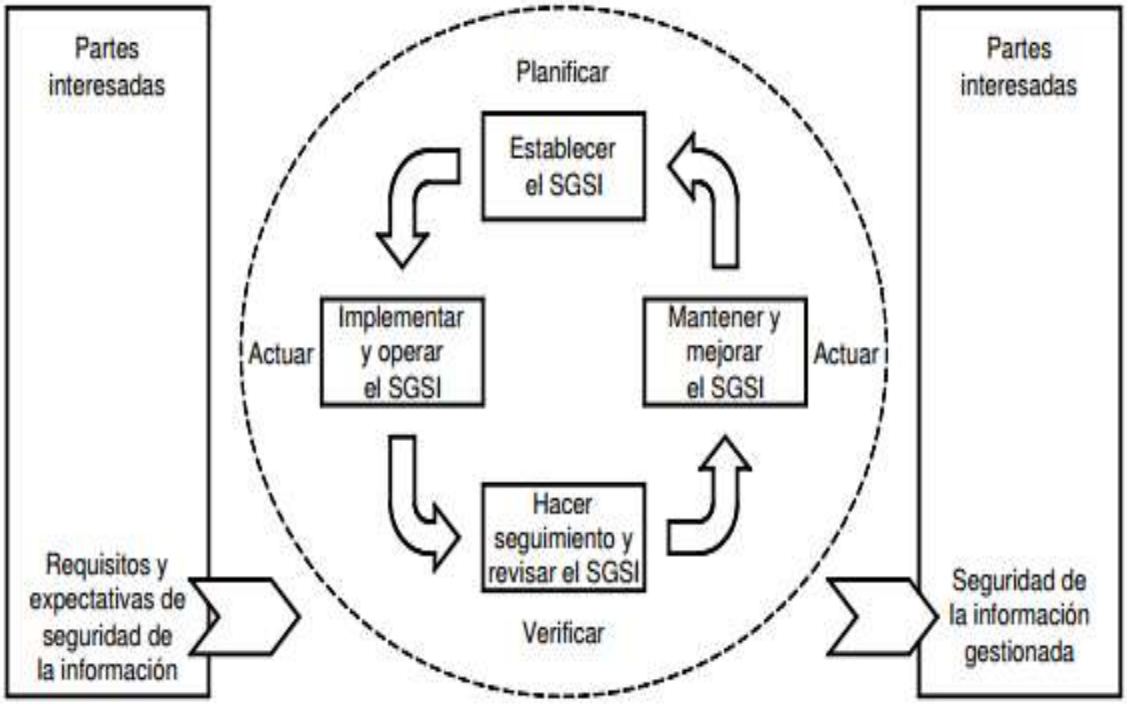
En este sentido, la Seguridad Informática sirve para la protección de la información, en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella.

Gestión De La Seguridad hace referencia a los aspectos relacionados con la concepción del sistema de seguridad y su implantación, especialmente la determinación de las necesidades de protección, el análisis y la gestión de los riesgos que gravitan sobre los sistemas informáticos y los controles a implementar, que incluyen políticas, procesos, procedimientos, estructuras organizativas, mecanismos y funciones de seguridad que requieren ser supervisados sistemáticamente y mejorados cuando fuera necesario para asegurar que se cumplan los objetivos de seguridad de la organización. Igualmente se describe el contenido de las etapas en que se estructura el proceso de diseño, implementación y operación de un Sistema de Gestión de la Seguridad Informática (SGSI), y se apoya para ello en el modelo definido por la NC-ISO-IEC 27001 referida al establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un SGSI. En su elaboración se han utilizado conceptos expresados en las normas ISO-IEC de la serie 27000, en particular las normas cubanas NC-ISO-IEC 27001

Sistema De Gestión De La Seguridad

El SGSI se compone de cuatro procesos básicos:

Fig. No. 5 Modelo PHVA aplicado a los procesos del SGSI



Fuente:

https://www.google.com.co/search?q=Modelo+PHVA+aplicado+a+los++procesos+del+SGSI&source=lnms&tbm=isch&sa=X&ved=0ahUKEwj6upO7h57TAhUDYiYKHZKyBFcQ_AUIBigB&biw=1293&bih=545&dpr=1#imgrc=6Osw038ia9bNzM:&spf=215

Tabla 2. PHVA aplicado a los procesos del SGSI

Planificar	Establecer las políticas, los objetivos, procesos y procedimientos de seguridad necesarios para gestionar el riesgo y mejorar la seguridad informática, con el fin de
Hacer (Implementar y	Tiene como objetivo fundamental garantizar una adecuada implementación de los controles seleccionados y la

Verificar (Revisar y dar	Evaluar y, en donde sea aplicable, verificar el desempeño de los procesos contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los
Actuar (Mantener y mejorar el	Emprender acciones correctivas y preventivas basadas en los resultados de la verificación y la revisión por la

Fuente: http://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

Las redes de datos transmiten información valiosa y confidencial de tal manera que las regulaciones de conformidad obligan a las organizaciones a hacer auditorías para el manejo y protegerla de los ataques y del mal uso. Aunque cualquier característica podría representar un riesgo, no todos los riesgos son iguales, algunos requieren un cambio de procedimiento, otros de configuración. Busca mantener la integridad, disponibilidad y confidencialidad de la información dentro de la red, para que la organización mantenga la continuidad en sus procesos.

Cuando hablamos de integridad queremos decir que los objetos del sistema sólo pueden ser modificados por personas autorizadas y en forma controlada.

Por otro lado disponibilidad significa que los objetos del sistema deben permanecer accesibles a las personas autorizadas. Por último, podemos definir confidencialidad en el sistema cuando la información contenida en el mismo no es brindada hacia entidades externas. Para alcanzar dicho Objetivo debemos plantearnos y definir los recursos se quieren proteger dentro de una red, dimensionar las amenazas y vulnerabilidades. De igual

manera se visualizan las medidas y herramientas que se implementarán para alcanzar un óptimo nivel de seguridad sin perder de vista la relación costo/beneficio.

Definidos estos puntos se pueden diseñar las políticas de seguridad adecuadas a implementar y crear un perímetro de defensa que permita proteger las fuentes de información.

Para identificar amenazas se dan a conocer los más conocidos tipos de ataques, el tipo de acceso, la forma operacional y sus objetivos.

2.2.2 NORMA ISO27001 - CICLO PHVA

Norma ISO27001 es un estándar ISO que proporciona un modelo para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en el ciclo de

Vida PDCA (Planear-Hacer-Verificar-Actuar; o ciclo de Deming) de mejora continua, al igual que otras normas de sistemas de gestión (ISO 9001 para calidad, ISO 14001 para medio ambiente, etc.).

Este estándar es certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo, puede solicitar una auditoria externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

El origen de la Norma ISO27001 está en el estándar británico BSI (British Standards Institution) BS7799- Parte 2, estándar que fue publicado en 1998 y era certificable desde entonces. Tras la adaptación pertinente, ISO 27001 fue publicada el 15 de Octubre de 2005.

Es una norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI), contribuye a la protección de los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI. Es una norma adecuada para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo, además es una norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI), contribuye a la protección de los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI. Es una norma adecuada para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo.

La Tabla 2 corresponde a las directivas de aplicabilidad según la norma 27001, define los controles que debe implementar una organización para tratar los riesgos. (Ver Anexo A)

2.2.3 METODOLOGÍA MAGERIT

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno.

Esta metodología, está en una guía completa y paso a paso de cómo llevar a cabo el análisis de riesgos. Esta metodología está dividida en tres libros. El primero de ellos hace referencia

al Método, donde se describe la estructura que debe tener el modelo de gestión de riesgos. Este libro está de acuerdo a lo que propone ISO para la gestión de riesgos.

El segundo libro es un Catálogo de Elementos, el cual es una especie de inventario que puede utilizar la empresa para enfocar el análisis de riesgo. Es así como contiene una división de los activos de información que deben considerarse, las características que deben tenerse en cuenta para valorar los activos identificados y además un listado con las amenazas y controles que deben tenerse en cuenta.

Finalmente el tercer libro es una Guía de Técnicas, lo cual lo convierte en un factor diferenciador con respecto a otras metodologías. En este tercera parte se describen diferentes técnicas frecuentemente utilizadas en el análisis de riesgos. Contiene ejemplos de análisis con tablas, algoritmos, árboles de ataque, análisis de costo beneficio, técnicas gráficas y buenas prácticas para llevar adelante sesiones de trabajo para el análisis de los riesgos.

Objetivos de MAGERIT

- ✓ Sensibilizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de controlarlos a tiempo.
- ✓ Ofrecer un método sistemático para analizar tales riesgos.
- ✓ planificar las medidas oportunas para mantener los riesgos bajo control.

- ✓ Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Inventarios de utilidad en la aplicación de la metodología:

- ✓ Tipos de activos
- ✓ Dimensiones y criterios de valoración
- ✓ Amenazas
- ✓ Salvaguardas

Algunas de técnicas a utilizar en las distintas fases del análisis de riesgos son:

- ✓ Análisis mediante tablas
- ✓ Técnicas generales o
- ✓ Análisis coste-beneficio
- ✓ Diagramas de flujo de datos (DFD)
- ✓ Diagramas de procesos
- ✓ Técnicas gráficas
- ✓ Planificación de proyectos
- ✓ Sesiones de trabajo: entrevistas, reuniones y presentaciones
- ✓ Valoración Delphi

2.3. MARCO CONCEPTUAL

La información que hace parte de la Dirección Territorial de Bogotá es fundamental para el correcto desempeño dentro de las políticas del Ministerio del trabajo, sus procesos

misionales y su relación con el ciudadano, esta será parte primordial en el cumplimiento de los objetivos, es por ello que resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de la Entidad y el mismo Estado colombiano.

Así, dentro de Marco de Seguridad algunos aspectos decisivos son:

Seguridad de la información

Hace referencia a la seguridad de activos de forma general, incluyendo la seguridad informática, la seguridad TIC y la seguridad de los datos.

Seguridad informática

Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información segura y confiable."[3]

Mecanismos de seguridad

Todo aquello de naturaleza hardware como software que se utiliza para crear, reforzar y mantener la seguridad informática. Se clasifican en:

- ✓ Preventivos: Actúan antes de que se produzcan ataques. Su misión es evitarlos.

[3] https://books.google.com.co/books?id=Mgvm3AYIT64C&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

- ✓ Detectores: Actúan cuando el ataque se ha producido y antes que cause daños en el sistema.
- ✓ Correctores: Actúan después de que haya habido un ataque y se hayan producido daños. Su misión es la de corregir las consecuencias del daño.

Seguridad pasiva

"Está construida por el conjunto de medidas que se implementan con el fin de minimizar la repercusión debida a un incidente de seguridad y permitir la recuperación del sistema. A estas medidas podemos llamarlas de corrección." (Aguilera López, Purificación, 2010).

Seguridad activa

"Los mecanismos y procedimientos que permiten prevenir y detectar riesgos para la seguridad del sistema de información constituyen la seguridad activa del mismo." (Aguilera López, Purificación, 2010).

Seguridad física

"Se utiliza para proteger el sistema informático utilizando barreras y mecanismos de control. Se emplea para proteger físicamente el sistema informático.
Las amenazas físicas se pueden producir provocadas por el hombre, de forma accidental o voluntaria, o bien por factores naturales." (Aguilera López, Purificación, 2010).

Seguridad lógica

"Se encarga de asegurar la parte del software de un sistema informático, que se compone de todo lo que no es físico, es decir, los programas y los datos." (Aguilera López, Purificación, 2010).

Arquitectura de seguridad OSI

La arquitectura de seguridad OSI (Estándares ISO 7498-2 y ITU-T X.800) hace distinción entre los conceptos de servicio y mecanismos de seguridad. Un servicio de seguridad es una característica que debe tener un sistema para satisfacer una política de seguridad. Un mecanismo de seguridad es un procedimiento concreto utilizado para implementar el servicio de seguridad. En otras palabras, un servicio de seguridad identifica lo que es requerido; mientras el mecanismo describe cómo lograrlo. La arquitectura OSI identifica las clases de servicios de seguridad: Confidencialidad, autenticidad, integridad, control de acceso, y no repudio.

Servicios de seguridad

- ✓ Confidencialidad: se refiere a la protección de la información respecto al acceso no autorizado, sea en los elementos computarizados del sistema o en elementos de almacenamiento.

- ✓ Integridad: Protección de la información respecto a modificaciones no autorizadas, tanto a la almacenada en los elementos computarizados de la organización como la usada como soporte. Estas modificaciones pueden llevarse a cabo de manera accidental, intencional, o por errores de hardware-software.

- ✓ Autenticidad: Garantía que el usuario autorizado tiene para usar un recurso y que no sea suplantado por otro usuario.

- ✓ Control de Acceso: Posibilidad de controlar los permisos a cualquier usuario para acceder a servicios o datos de la organización.

- ✓ No Repudio: Al ser transferido un conjunto de datos, el receptor no puede rechazar la transferencia, y el emisor debe poder demostrar que envió los datos correspondientes.

Disponibilidad de los recursos y de la información

Protección de los elementos que poseen la información de manera que en cualquier momento, cualquier usuario autorizado pueda acceder a ella, sin importar el problema que ocurra.

Consistencia

Capacidad del sistema de actuar de manera constante y consistente, sin variaciones que alteren el acceso a la información.

Auditoría

Capacidad para determinar todos los movimientos del sistema, como accesos, transferencias, modificaciones, etc., en el momento en que fueron llevados a cabo (fecha y hora).

Vulnerabilidad

Consiste en cualquier debilidad que puede explotarse para causar pérdida o daño del sistema. De esta manera, el punto más débil de seguridad de un sistema consiste en el punto de mayor vulnerabilidad de ese sistema.

Amenaza

Es cualquier circunstancia con el potencial suficiente para causar pérdida o daño al sistema. De esta manera, el punto más débil. La presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que de tener la oportunidad atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad. Las amenazas en función del tipo de alteración, daño o intervención que podrían producir sobre la información se clasifican en:

- ✓ De interrupción: El objetivo de la amenaza es deshabilitar el acceso a la información; por ejemplo, destruyendo componentes físicos como el disco duro, bloqueando el acceso a los datos, o cortando o saturando los canales de comunicación.

- ✓ De interpretación: Personas, programas o equipos no autorizados podrían acceder a in determinado recurso del sistema y captar información confidencial de la organización, como pueden ser datos, programas o identidad de personas.

- ✓ De modificación: Personas, programas equipos no autorizados no solamente accederían a los programas y datos de un sistema de información sino que además los modificarían.

- ✓ De fabricación: Agregarían información falsa en el conjunto de información del sistema.

Según su origen las amenazas se clasifican en:

- ✓ Accidentales: accidentes meteorológicos, incendios, inundaciones, fallos en equipos, en las redes, en los sistemas operativos o en el software, errores humanos.

- ✓ Intencionadas: Son debidas siempre a la acción humana, como a introducción de software malicioso, malware, intrusión informática, robos o hurtos.

Ataques

Se define como cualquier acción que explota una vulnerabilidad. Se clasificación de la siguiente manera:

- ✓ Ataques Pasivos: Consiste en sólo observar comportamientos o leer información, sin alterar sin alterar el estado del sistema ni la información. En este sentido, un ataque pasivo sólo afecta la confidencialidad o privacidad del sistema o de la información.

- ✓ Ataques Activos: Por el contrario, tiene la capacidad de modificar o afectar la información o el estado del sistema o ambos. En consecuencia, un ataque activo afecta no sólo la confidencialidad o privacidad sino también la integridad y la autenticidad de la información o del sistema.

Riesgos

Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. El elemento de riesgo está siempre presente independiente de las medidas que tomemos, por lo que debemos hablar de niveles de seguridad, la seguridad absoluta no es posible y en adelante entenderemos que la seguridad informática es un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas

informáticos. Así que lo importante es proteger la información si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (hardware, software y datos) son los datos y la información los sujetos principales de protección de las técnicas de seguridad.

2.4. MARCO LEGAL

Para implementar sistema de gestión los estándares ISO son aplicables a cualquier tipo y tamaño de empresa, El ISO (International Organization for Standardization, Organización Internacional para la Estandarización) es un organismo internacional que se dedica a desarrollar reglas de normalización en diferentes ámbitos, entre ellos la informática.

El IEC (International Ellectrotechnical Commision) es otro organismo que publica normas de estandarización en el campo de la electrónica.

ISO 27000

La serie de normas ISO/IEC 27000 se denomina requisitos para la especificación de sistemas de gestión de la seguridad de la información (SGSI), proporciona un marco de estandarización para la seguridad de la información para que sea aplicado en una organización o empresa y comprende un conjunto de normas sobre las siguientes materias:

- Sistema de gestión de la seguridad de la información
- Valoración de riesgos

ISO 27001

De acuerdo a La normatividad internacional ISO/IEC, las organizaciones en Colombia están sujetas a cumplir parámetros para certificarse, el estándar para la seguridad de la información ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información y el ICONTEC, previa preparación y solicitud realiza la auditoria correspondiente. Esta norma está dividida en once dominios de control, 39 objetivos y 133 controles. Los dominios presentados abarcan: política de seguridad, organización de la seguridad de la información, gestión de activos, control de acceso, seguridad de los recursos humanos, cumplimiento, seguridad física y del entorno, adquisición, desarrollo y mantenimiento de sistemas de información, gestión de las comunicaciones y operaciones, gestión de la continuidad del negocio y gestión de incidentes de seguridad de la información.

ISO/IEC 27002

Antes ISO 17799, es una guía de buenas prácticas, describe los controles a seguir dentro del marco de la seguridad de la información; enmarcados en 11 dominios, 39 objetivos de control y 133 controles.

ISO/IEC 27003

Proporciona ayuda y orientación sobre la implementación de un SGSI, incluye el método PHVA (planear, hacer verificar y actuar) contribuyendo con revisiones y mejora continua.

ISO/IEC 27004

Especificará las métricas y técnicas de medición para determinar la eficacia de un SGSI y de sus controles. Aplicable específicamente en la fase del hacer (Do); de acuerdo con el método PHVA.

ISO/IEC 27005

Suministra directrices para la gestión del riesgo en la seguridad de la información.

Ley 1273 de 2009

"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"

Ley 1712 del 6 de marzo del 2014

"Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones".

Decreto Nacional N° 2573

"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones."

Ley 1341 de 2009

"Por la cual se definen 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[4]

3. DISEÑO METODOLÓGICO

Los riesgos asociados con la información y los sistemas de la Dirección territorial de Bogotá del ministerio del trabajo serán analizados utilizando metodología estructurada de análisis de riesgos mediante MAGERIT, para cubrir cubre la fase Análisis y Gestión de Riesgos, herramienta adecuada para el caso que nos ocupa que corresponde a la Gestión global de un Sistema de Seguridad de la Información basado en ISO 27001.

3.1. FUENTES DE INFORMACIÓN

Las fuentes de información son instrumentos para el conocimiento, búsqueda y acceso a la información acerca de la investigación que nos ocupa.

[4] http://www.mintic.gov.co/portal/604/w3-article-3705.html

Fuentes de información primaria. Suministran información directamente de los funcionarios involucrados en la administración de las aplicaciones y las Bases de Datos de la Dirección territorial.

Fuentes de información secundaria. Es la información documental que orienta al análisis y evaluación de la seguridad informática y que se encuentra consignada en documentos Como: normas: NTC- ISO-IEC-27001 y Metodología MAGERIT y documentos del Ministerio del Trabajo.

TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Entrevista: En este caso se dirigieron algunas entrevistas haciendo preguntas concretas a algunos funcionarios.

Encuestas: Usando la herramienta limesurvey se realizó dos encuestas, una sobre tecnología, para detectar necesidades y otra para levantar el inventario físico. (VER ANEXO A)

Observación: De manera continua se ha hecho un monitoreo que ha permitido registrar patrones de conducta de los usuarios y del sistema informático.

Revisión documental: para ello se revisaron documentos que brindan soporte a la seguridad informática y el control de los mismos como son: normas NTC-ISO-IEC- 27001, Metodología MAGERIT y contenidos del SIG del Ministerio del trabajo a través del portal institucional.

3.2. ESTADO ACTUAL - DIAGNÓSTICO

El Ministerio ha delegado el manejo de servidores y mantenimiento de la red una empresa contratista, mediante convenio interinstitucional, proyecto supervisado por un ingeniero coordinador o interventor del proyecto, quien depende de la subdirección Administrativa y Financiera con sede en el nivel central Ubicado en la calle 100 No. 33 – 99 de Bogotá.

Esta interventoría está apoyada en cada sede por un técnico administrativo que tiene funciones de soporte.

En la misma sede coexiste la Oficina de tecnologías de la Información y las comunicaciones (Oficina de TIC), que se encarga de generar lineamientos, políticas y proyectos de mejora para gestionar los procesos informáticos.

Recientemente y en cumplimiento de los lineamientos del Gobierno en Línea se estableció el grupo que se está encargando del levantamiento del componente de seguridad.

Actualmente se aplican las políticas de uso recomendado por la normatividad general y las que tiene a su disposición la empresa contratista.

En el caso de la sede de la calle 32 del Ministerio del Trabajo, está conectada mediante un canal dedicado de fibra óptica de 20MB con 143 puntos lógicos, cableado estructura categoría 5E, planta telefónica (Branch) para el mismo número de usuarios, provee además el direccionamiento DHCP El Router da el DHCP para los equipos de cómputo de la DT. El proveedor de servicios informáticos es UNE telecomunicaciones, se incluye mesa de servicio para soparte

3.3. TIPO DE INVESTIGACIÓN

Esta es una monografía de investigación sobre el estado de la seguridad informática en la Dirección Territorial de Bogotá, Dependencia del Ministerio Del Trabajo que plantea la necesidad de gestión del riesgo informático, para ello, se evalúan y cuantifican los bienes a proteger, y en función de estos análisis, se propone diseñar medidas preventivas y correctivas que eliminen los riegos asociados o que los reduzcan hasta niveles manejables.[5]

La investigación está orientada al apoyo de toma de desiciones decisiones porque no se centra en hacer aportes teóricos si no que su objetivo es buscar solución a un problema planteado, que es la necesidad de diseñar e implementar un SGSI.

Para este caso concreto de la Dirección territorial de Bogotá del Ministerio del Trabajo, se tomará como referencia lo indicado en "la norma ISO/IEC 27001 que especifica los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI documentado dentro del contexto global de los riesgos de negocio de la organización, además especifica los requisitos para la implantación de los controles de seguridad hechos a medida de las necesidades de organizaciones individuales o partes de las mismas".[6]

Se adopta el modelo PHVA para todos los procesos de la Dirección Territorial.

[5] http://www.monografias.com/trabajos94/que-seguridad-informatica/que-seguridad-informatica.shtml#ixzz4eDuHEqG0
[6] http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/isoirc_27001_pdca.html

De igual manera y tomando como base para ello el modelo de referencia de seguridad de la norma ISO/IEC 27001:2013 se utilizará como herramienta para determinar los riesgos existentes, analizarlos y evaluarlos la metodología MAGERIT.

3.4. METODOLOGÍA MAGERIT - ISO 27001

El sistema de seguridad en la información requiere de una metodología adecuada para su implementación, para evaluar la información de una forma consistente se deben tener en cuenta los elementos existentes que hacen parte de la misma. Enmarcados en la normatividad internacional ISO/IEC, las organizaciones en Colombia están sujetas a cumplir parámetros para certificarse, el estándar para la seguridad de la información ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información y el ICONTEC.

Este estándar internacional adopta el modelo de mejora continua PHVA: Planificar, Hacer, Verificar y Actuar aplicado a toda la estructura de procesos del SGSI, el modelo PHVA establece que no es suficiente con el diseño e implementación del SGSI sino que es necesario garantizar la revisión periódica y continua actualización y mejora del mismo, permitiendo a la entidad utilizar los instrumentos que consideren oportunos para medir y controlar la mejora del sistema.

Es así como para la entidad se deben fijar los estándares y el modelo que mejor se ajuste a su esquema de requerimientos para garantizar la seguridad y continuidad de sus procesos.

Las fases de este modelo son:

Planificación (Plan) [establecer el SGSI]

El Ministerio tiene en el SIG un documento centralizado que contiene políticas de seguridad en redes de datos y las estrategias para prevenir posibles incidentes que amenacen o vulneren la infraestructura y demás recursos de la red del Ministerio del Trabajo. Para el Ministerio del Trabajo los recursos de red son considerados un activo valioso que debe ser aprovechado y utilizado en beneficio de la operación y eficiencia de la entidad, estas políticas se aplicarán en la gestión de las Dirección Territorial de Bogotá, para mejorar la seguridad de la información de la organización, para ofrecer resultados de acuerdo con las políticas y objetivos generales de la organización.

Se incluirán los procesos que se adelantan el dependencia la DT Bogotá y en esta fase de

Planeación del ciclo PHVA

Se tendrán en cuentas los siguientes aspectos:

- ✓ Apoyar y divulgar las buenas prácticas y el diseño de un modelo de gestión de seguridad sus políticas y controles.

- ✓ Plantear las políticas y controles que harán parte del Modelo de Seguridad de la información.

- ✓ Proveer el apoyo para asesorar a los usuarios y administradores de la DT Bogotá

- ✓ Gestionar y obtener aprobación y soporte de la Dirección (Equivale a la gerencia en una entidad privada), Junto con la dirección definir el alcance y límites del SGSI y su aplicabilidad en la Dirección Territorial.

- ✓ La Realización del inventario de orientado a los activos que soportan los procesos de negocio que componen el alcance del SGSI, es decir, que activos soportan los sistemas de información y aplicaciones, adicionalmente, se calificará el grado de criticidad o importancia de cada activo en relación con el apoyo al método de evaluación del riesgos.

- ✓ La evaluación del riesgo en seguridad: Una vez el levantamiento de información de los activos parte del alcance del SGSI está realizado, se debe hacer la evaluación del riesgo asociado a dichos activos, especificando las áreas de preocupación, amenazas, vulnerabilidades, escenarios de riesgo, probabilidad de ocurrencia de la amenaza e impacto si llega a materializarse la amenaza a los activos que soportan los sistemas de información y las aplicaciones

- ✓ Uso de la metodología de gestión, evaluación y análisis del riesgo que se considere conveniente, lo importante es que tenga los elementos recomendados en la norma ISO27001. Par el caso de la metodología Magerit propuesta.

- ✓ El Plan de Tratamiento del Riesgo: Una vez la entidad ha definido el alcance del SGSI, y la Declaración de Aplicabilidad.

- ✓ Revisión de los controles propuestos y el grado de implementación de los mismos.

- ✓ Acciones, prioridades, recursos, responsables y fecha de compromiso para la implementación de los controles.

- ✓ Mitigación der los riesgos en seguridad de la información implementando dichos controles

Hacer - Ejecutar [implementar y gestionar el SGSI]

- ✓ Diseñar el SGSI de acuerdo a su política, controles, procesos y procedimientos. FASE

- ✓ Aceptar y afianzar las recomendaciones propuestas como Modelo SGSI
- ✓ Definir una política de seguridad que apoye los la gestión de los diferentes procesos en la DT Bogotá.
- ✓ La política de seguridad tendrá la siguiente estructura básica:
- ✓ Políticas Objetivos de Control y Controles de Justificación
- ✓ Estructura del Modelo de Seguridad, es decir, la política de seguridad que apoya los objetivos de control.

- ✓ Se establecen controles asociados a cada objetivo de control para que la entidad los verifique e implemente.
- ✓ Acatar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad en las actividades.

Verificar - Seguimiento [monitorizar y revisar el SGSI]

En la fase VERIFICAR del ciclo PHVA, en el que se realizará la revisión y seguimiento de la implementación y cumplimiento del Modelo de Seguridad para resolver las brechas de seguridad de la información encontradas fueron efectivas.

- ✓ Revisar regularmente la efectividad del Modelo SGSI, atendiendo al cumplimiento de la política, objetivos y revisión de los controles de seguridad.

- ✓ Evaluar la efectividad de los controles para verificar que se cumple con los Requisitos de seguridad, para esto se tendrá una visión orientada a niveles de Madurez.

- ✓ Revisar regularmente en intervalos/periodos planificados, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en las entidades, la tecnología, los objetivos y procesos misionales, las amenazas identificadas, la efectividad de los controles implementados y el ambiente.

- ✓ Requerimientos legales y obligaciones contractuales, entre otros.

Verificar.

- ✓ Medir y revisar las prestaciones de los procesos del SGSI. Comprobar que las medidas adoptadas han surtido efecto, para ello se debe volver a recopilar datos y monitorizar el comportamiento del sistema.

- ✓ Adoptar acciones correctivas y preventivas basadas en auditorías y revisiones internas con el objetivo de mejorar el SGSI.

- ✓ Evidenciar ajustes, nuevos controles, procesos, lineamientos y políticas que serán puestos a consideración
- ✓ Analizar, consolidar y publicar los indicadores, métricas y estadísticas del Sistema y del Modelo de Seguridad implementado en las entidades de acuerdo al MECI

- ✓ Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de seguimiento y revisión.
- ✓ Verificar que el que se integren con las mejoras identificadas.
- ✓ Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.
- ✓ Comunicar las acciones y mejoras a las partes interesadas

El ciclo PHVA es un ciclo de vida continuo, lo cual quiere decir que la fase de Actuar lleva de nuevo a la fase de Planear para iniciar un nuevo ciclo de cuatro fases, no es necesario llevar una secuencia estricta de las fases, sino que, pueden haber actividades de

implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado o que se monitoreen controles que aún no están implantados en su totalidad.

DEFINICION DE POLITICAS

Se plantean reglas generales de comportamiento para la interacción entre los usuarios y los activos informáticos. Las políticas son independientes de los ambientes propios de la entidad y representan la base de un modelo de seguridad, dependen de la cultura de la organización.

Las políticas y procedimientos deben estar hechos a la medida, según los requerimientos específicos de cada organización. Para la definición de las políticas y procedimientos se realiza un proceso de validación en conjunto con la organización con el fin de generar políticas y procedimientos que se ajusten a esta. La definición de las políticas teniendo como referencia el análisis de riesgo realizado, los controles del ISO 1 7799/ISO 27001.

Las políticas cubrirán la Seguridad en la Organización, Clasificación de la Información, Seguridad en el recurso Humano, y Seguridad Física.

DEFINICION DE PROCEDIMIENTOS

Los procedimientos son la descripción detallada de la manera como se implementa una política, el procedimiento incluye todas las actividades requeridas, los roles y responsabilidades de las personas encargadas de llevarlos a cabo, se deben definir por lo menos los siguientes procedimientos: Administración de cuentas de usuario, Manejo de

Incidentes, Manejo de Virus, Administración de cuentas privilegiadas, Procedimiento de respaldo.

DEFINICION DE ESTANDARES

Es la definición cuantitativa o cualitativa de un valor o parámetro determinado que puede estar incluido en una política o procedimiento. Algunos de los principales estándares a definir son: Longitudes de contraseñas, Histórico de contraseñas, Eventos a registrar en logs, Switches, Routers, Firewall, VPNs y Sistemas Operativos.

4. DESARROLLO METODOLOGICO

La metodología MAGERIT – versión 3.0, contiene los siguientes pasos para realizar el análisis de riesgos:

Fase 1. Determinación de los *activos* relevantes para la organización, su interrelación y su valor.

Fase 2. Determinar *amenazas* a las que están expuestos los activos.

Fase 3. Determinar las *salvaguardas* actuales y su eficacia, frente a los riesgos.

Fase 4. Determinar el *impacto*, definido como el daño sobre el activo derivado de la materialización de la amenaza.

Fase 5. Estimar el *riesgo*, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

ANÁLISIS MEDIANTE TABLAS:

Mediante el análisis de la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos. En el análisis de riesgos hay que trabajar con múltiples elementos que hay que combinar en un sistema para ordenarlo por importancia sin que los detalles, muchos, perjudiquen la visión de conjunto. La experiencia ha demostrado la utilidad de métodos simples de análisis llevados a cabo por me-dio de tablas que, sin ser muy precisas, sí aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas. Sea la escala siguiente útil para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

• MB: muy bajo • B: bajo • M: medio • A: alto • MA: muy alto [7]

4.1 IDENTIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS CRITICOS DE LA ORGANIZACIÓN

Son el conjunto de componentes o funcionalidades del sistema de información susceptibles de ser atacados deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

4.1.1 EQUIPOS DE CÓMPUTO REDES Y COMUNICACIONES

[7] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas

Figura No.6. Vista actual del cuarto de cableado

Fuente: El Autor

Tabla No. 3 Inventario Equipos Centro De Cómputo

INVENTARIO EQUIPOS CENTRO DE COMPUTO								
ROUTER CISCO	No.	1						
	REFERENCIA	CISCO 2900 SERIES						
	SERIAL	FTX1545 82CA						
	PROPIEDAD							
SWITCH	No.	1	2	3	4	5	6	7
	REFERENCIA	HP 2920-48G POE	CISCO 3560-X SERIES	CISCO 3560-G SERIES POE-24	CISCO 2950 SERIES	CISCO 2950 SERIES	CISCO 3560G SERIES	HUAWEI
	SERIAL	SG38FLZ0SZ	FD01526V10E	F0C135Y2KU	FOC0801W3RU	FOC0801X3WG	FOC1533Z0UW	372702
	PROPIEDAD						UNE	UNE
	PUERT	24	0	0	0	0	1	22

	OS LIBRES							
	PUERTOS OCUPADOS	24	48	24	48	48	23	2
	SE REQUIEREN PTOS ADICIONALES CUANTOS	NO	NO	NO	NO	NO	NO	NO
ACCESS POINT	No.							
	MARCA							
	SERIAL							
	PROPIEDAD							
BRANCH	REFERENCIA	SIEMENS BRANCH SYS-2USM02-6M01E						
	SERIAL	F31505-E12-B7						
	PROPIEDAD	UNE						
AIRE ACONDICIONADO	FUNCIONA	SI	SI					
	MARCA	YORK	YORK					
	MODELO	YSEC09FS-ADG	YSEC09FS-ADG					
	CAPACIDAD	9000 Btu/h	12000 Btu/h					
	FECHA ULTIMO MTO							
	PROPIEDAD							
UPS	FUNCIONA	SI						
	MARCA	TITAN						
	MODELO	TITAN EA9930						

	CAPACIDAD	30KVA cabinet						
	FECHA ULTIMO MTO							
	PROPIEDAD							
PATCH PANEL	EXISTE	SI						
	ESTADO (B-R-M)	B						
	TIENE PUNTOS LIBRES	22						

Fuente: El Autor

4.1.2 RECURSOS HUMANOS

Todos los funcionarios y contratistas que laboran para la DTBOGOTÁ deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades, Los responsables de la información deben autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, Las claves de acceso compartidas asignadas a los funcionarios de los sistemas información en la Dirección Territorial de Bogotá del Ministerio del Trabajo de la Entidad tienen únicamente carácter de consulta, estas no permiten modificación de la información, no deben divulgarse hacia el exterior de la entidad, se cambiarán periódicamente.

La Dirección Territorial cuenta con los siguientes tipos de Funcionarios:

Director: Que posee acceso al sistema de información en su totalidad funcional.

Profesionales especializados: Poseen acceso a algunos formularios y consultas en las aplicaciones y correo de la red institucional.

Profesionales Universitarios: acceden a las aplicaciones ofimáticas, correo y consultas de Bases de Datos.

Técnicos Administrativos: Acceden a las aplicaciones ofimáticas, correo y consultas de Bases de Datos.

Auxiliares Administrativos: Acceden a las aplicaciones ofimáticas, correo y consultas de Bases de Datos.

Ingeniero de Sistemas: para soporte en sitio, prestador de servicios contratado por UNE Telecomunicaciones como técnico de la mesa de ayuda, administra y opera la infraestructura para garantizar la funcionalidad y disponibilidad para los funcionarios del Ministerio.

Estudiantes Universitarios: Prestan apoyo como requisito para obtener título profesional (pasantías en temas administrativo laborales).

Personal de Servicios Generales: Empresas de prestación de servicios.

Tabla No. 4 # Funcionarios Y Equipos

FUNCIONARIOS Y EQUIPOS	[Funcionarios]	153
	[Contratistas]	1
	[Computadores de escritorio]	124
	[Portátiles]	35
	[Teléfonos IP	138
	[Total Impresoras]	14

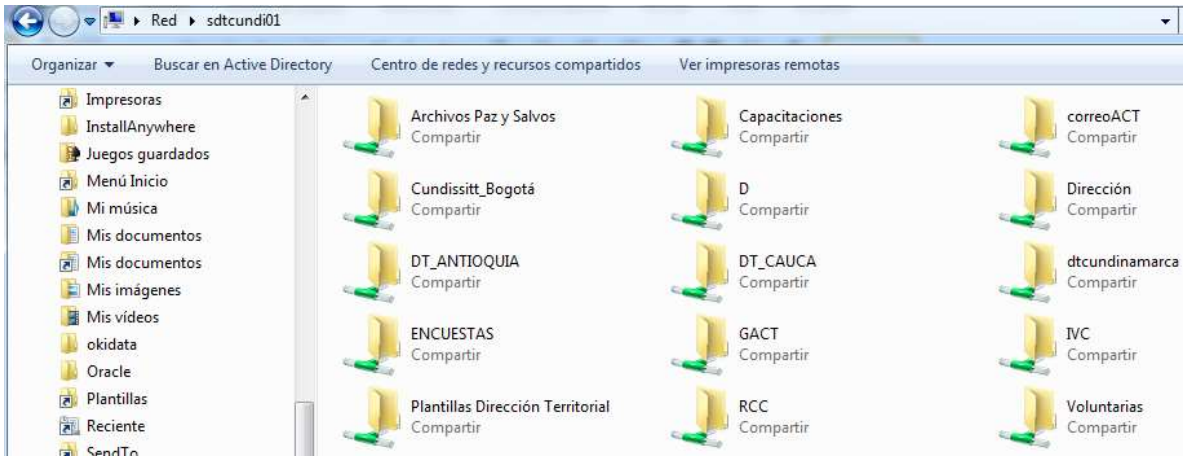
Fuente: El Autor

4.1.3 DATOS E INFORMACIÓN

La Dirección, deberá designar un responsable del manejo de las Bases de Datos, en cada grupo de trabajo y mantener centralizada y protegida la información. De igual manera hacer copias de respaldo y velar por el cabal diligenciamiento de las plantillas que contienen la información.

Los funcionarios de la sede acceden a la página web y algunas aplicaciones que se encuentran alojadas en los servidores ubicados en el nivel central edificio ubicado en la calle 100. Las Bases de Datos propias de la Dirección territorial de Bogotá, se encuentran alojadas en el servidor SDTCUNDI01, en el mismo datacenter.

Fig. No. 7 Servidor SDTCUNDI01



Fuente: El Autor

4.1.4 SOFTWARE Y APLICACIONES

La Dirección debe desarrollar revisar y actualizar una política de administración de la configuración formalmente definida y documentada que sean para facilitar la implantación de la política de administración de la configuración y delos controles asociados, documentar y mantener actualizada la configuración básica que por defecto deben manejar cada uno de los usuarios en todos los sistemas de información computarizados y los controles de acceso.

Tabla 5 Aplicaciones y BD

	NOMBRE	TIPO_APLICATIVO	LENGUAJE	MOTOR_BD	SERVICIO	AREA_USUARIO

Apoyo	4	**BABEL**	WEB	JAVA	ORACLE 12C	Nuevo sistema para el manejo y gestión documental de la entidad.	Nivel central-DTBogotá_DTAntioquia_DTSantander
Misional	7	**CERTIDIRECTOR**		ACCESS	ACCESS	Generación certificaciones de No Reclamaciones Laborales en la Dirección Territorial de Bogotá	Despacho Director - DTBogotá
Misional	9	**CONSTANCIAS TEMPORALES**		ACCESS	ACCESS	Registro de Empresas temporales y generación de Constancias_DTBogotá	G. Atención al Ciudadano y Trámites - DTBogotá
Misional	10	**CONSTANCIAS DISCAPACIDAD**		ACCESS	ACCESS	Registro de expedición de constancias de Discapacidad	G. Atención al Ciudadano y Trámites - DTBogotá
Misional	11	**CONSTANCIAS DISCAPACIDAD HEROES DE LA NACION**		ACCESS	ACCESS	Generación de Constancias de discapacidad para miembros de las Fuerzas Armadas	G. Atención al Ciudadano y Trámites - DTBogotá
Misional	15	**CUNDISIIT**		ACCESS	ACCESS	Generación de citaciones inspecciones RCC	G. Atención al Ciudadano y Trámites - DTBogotá
Misional	16	**CUNDIVOL**		ACCESS	ACCESS	Numeración y registro de Actas Mutuo Acuerdo Grupo RCC_DTBOGOTÁ	G. Resolución de Conflictos y Conciliaciones - DTBogotá
Misional	17	**DISCAPACIDAD**	Cliente_Servidor		SQLSERVER 2012	BD, convenio Min Salud	Bd_MT. Subd. Análisis, Monitoreo y Prospectiva Laboral

Misional	31	**NUMERADOR ACTAS**		ACCESS	ACCESS	Numeración Actas conciliadas, no conciliadas, parcialmente Concialiadas y no comparecencias	G. Resolución de Conflictos y Conciliaciones - DTBogotá
Apoyo	49	**SISTEMA DE CORRESPONDENCIA_WEB (MELBA)**	WEB	Visual Basic.NET	SQL Server	Correspondencia y gestión de documentos	Depencias del nivel Central, DTBogotá, DTCundinamarca

Fuente: El Autor

4.1.5 SERVICIOS

En la DT Bogotá y demás dependencias del Ministerio del Trabajo se ofrece a los funcionarios los siguientes servicios Informáticos:

- ✓ Acceso a la Red: Cada funcionario del Ministerio de Trabajo, tendrá un usuario con contraseña que será de uso personal e intransferible.

- ✓ Uso de Servicio de Internet: El uso de Internet (envío, descarga o visualización de información)

- ✓ Asignación y uso Equipos de Cómputo e infraestructura del Ministerio

- ✓ Correo electrónico institucional: El correo electrónico institucional es el medio que se utiliza para enviar y recibir comunicaciones asociadas a las funciones del cargo desempeñado y de la Entidad.

4.1.6 EXPEDIENTES EN CURSO

Las actuación en la Jurisdicción Administrativo Laboral Administración queda evidenciada mediante la creación del expediente donde se consignan entre otra información las averiguaciones preliminares, el acto administrativo de formulación de cargos y sucesiva probatoria.[8]

4.1.7 VALORACIÓN DE LOS ACTIVOS

La experiencia ha demostrado la utilidad de métodos simples de análisis llevados a cabo por medio de tablas que, sin ser muy precisas, sí aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas.[9]

De acuerdo a las cinco dimensiones de la metodología: Confidencialidad, Disponibilidad, Autenticidad y Trazabilidad se han calificado los activos así:

Tabla No. 6 Escala Valoración de Activos

VALOR	**CRITERIO**	
ALTO (A)	3	Daño Grave a Dirección territorial
MEDIO (M)	2	Daño Importante a Dirección territorial
BAJO (B)	1	Daño Menor a Dirección territorial

[8] Manual del Inspector de Trabajo y de la Seguridad Social
[9] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas

Fuente: El Autor

Tabla No. 7 Valoración de Activos

ACTIVO	VALOR
ÉQUIPOS DE CÓMPUTO REDES Y COMUNICACIONES	2
DATOS E INFORMACIÓN	3
SOFTWARE Y APLICACIONES	3
SERVICIOS	2
EXPEDIENTES EN CURSO	3
PERSONAL	3

Fuente: El Autor

4.2 DETERMINACIÓN DE AMENAZAS

Las amenazas pueden ser de origen Natural**,** industrial, por Errores y fallos no intencionados o por Ataques intencionados.

Son eventos que pueden dañar cualquiera de las dimensiones consideradas para la valoración de los activos de información. Se deben fijar los estándares y el modelo que mejor se ajuste a los requerimientos de cada entidad para garantizar la seguridad y continuidad de sus los procesos propios. Las vulnerabilidades identificadas son:

_ Privilegios excesivos e inutilizados. Cuando a alguien se le otorgan privilegios de base de datos que exceden los requerimientos de su puesto de trabajo se crea un riesgo innecesario. Los mecanismos de control de privilegios de los roles de trabajo han de ser bien definidos o mantenidos.

_Abuso de Privilegios. Los usuarios pueden llegar a abusar de los privilegios legítimos de bases de datos para fines no autorizados, por ejemplo, sustraer información confidencial. Una vez que los registros de información alcanzan una máquina cliente, los datos se exponen a diversos escenarios de violación.

_Malware y spearphising. Se trata de una técnica combinada que usan los cibercriminales, hackers patrocinados por estados o espías para penetrar en las organizaciones y robar sus datos confidenciales.

_Exposición de los medios de almacenamiento para backup. Éstos están a menudo desprotegidos, por lo que numerosas violaciones de seguridad han conllevado el robo de discos y de cintas. Además, el no auditar y monitorizar las actividades de acceso de bajo nivel por parte de los administradores sobre la información confidencial puede poner en riesgo los datos.

_Explotación de vulnerabilidades y bases de datos mal configuradas. Los atacantes saben cómo explotar estas vulnerabilidades para lanzar ataques contra la Entidad.

_Datos sensibles mal gestionados. Los datos sensibles en las bases de datos estarán expuestos a amenazas si no se aplican los controles y permisos necesarios.

_Denegación de servicio (DoS). En este tipo de ataque se les niega el acceso a las aplicaciones de red o datos a los usuarios previstos.

_Limitado conocimiento y experiencia en seguridad y educación. Falta de conocimientos para poner en práctica controles de seguridad, políticas y capacitación.

Cuando se define la seguridad de la información como prioridad, estableciendo medidas que ayuden a conseguirla, de manera inmediata se plantea la necesidad de instalar mecanismos, que permitan controlar los riesgos asociados a la seguridad entre los que se

encuentran desde las medidas físicas aplicables al espacio en el que se ubican los sistemas que contienen la información hasta los aspectos muy relevantes, protegiendo así los activos físicos y garantizando una verdadera "seguridad de la información".

Garantizar un nivel de protección total es imposible, de manera que el propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

4.3 VALORACIÓN DE AMENAZAS

Para la degradación que pueda causar a un activo de la magnitud se mide del 1 al 100%,

La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción". Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela cualitativamente por medio de alguna escala nominal se establece una escala de acuerdo a la frecuencia de ocurrencia del evento así:

Tabla No. 8. Escala Valoración de Amenazas

VALOR		CRITERIO	
10	FRECUENTE	F	MENSUALMENTE
1	NORMAL	FN	UNA VEZ AL AÑO
1/10	POCO FRECUENTE	PF	CADA VARIOS AÑOS

Fuente: El Autor

Tabla No. 9. Valoración de Amenazas

AMENAZA	FRECUENCIA	DIMENSIONES DE SEGURIDAD		
		DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
DE ORIGEN INDUSTRIAL	1	80		
ERRORES DE USUARIO	10	50	80	10
ERRORES DE ADMINISTRADOR	1	70	50	10
ESCAPES Y FUGAS DE INFORMACIÓN	10			90
PÉRDIDA Y ROBO DE EQUIPOS	1	10		10
ABUSO DE PRIVILEGIOS	1	10	50	90
ACCESO NO AUTORIZADO	10		50	90
MODIFICACIÓN DELIBERADA DE LA INFORMACIÍN	10		50	

Fuente: El Autor

4.3 ESTIMACIÓN DEL IMPACTO

Se hace conforme a la valoración de los activos y las amenazas, se puede calcular el impacto en base a tablas sencillas de doble entrada:

Tabla No. 10. Escala Estimación del Impacto

impacto		***degradación***		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: MAGERIT – versión 3.0 Libro III - Guía de Técnicas

Tabla No.11. Estimación del Impacto

ESCENARIO	**ACTIVO**	**RIESGO**	**VULNERABILIDAD**	**IMPACTO**
Comunicaciones	ÉQUIPOS DE CÓMPUTO REDES Y COMUNICACIONES	Falla De Conexión– Tiempos Muertos	Ataques Servicios Web	Alta
		Penetración Del Firewall – Virus, Intrusos	Bajo Nivel De Detección	
Seguridad Física	EXPEDIENTES EN CURSO	Abuso De Procesos De Tramitación, Incremento Del Número De Posibles	No Se Controla La Autenticación E Identificación De Usuarios, Áreas De Trabajo Del Personal	Alta

		Atacantes, Suplantación De Usuarios, Etc.		
Funcionarios	PERSONAL	Suplantación, Accesos No Autorizados, Errores, Manipulación Indebida De Información	Escaso Análisis De Las Personas Involucradas En El Proceso	Alta

Fuente: El Autor

4.4 CÁLCULO DEL RIESGO

El riesgo se calcula multiplicando la frecuencia de la amenaza por el Impacto.

Tabla No. 12. Cálculo del riesgo

ESCENARIO	ACTIVO	RIESGO	VULNERABILIDAD	IMPACTO	FRECUENCIA	RIESGO
Comunicaciones	ÉQUIPOS DE CÓMPUTO REDES Y COMUNICACIONES	Falla De Conexión– Tiempos Muertos	Ataques Servicios Web	3	1	3
		Penetración Del Firewall – Virus, Intrusos	Bajo Nivel De Detección			
Seguridad Física	EXPEDIENTES EN CURSO	Abuso De Procesos De Tramitación, Incremento Del Número De Posibles Atacantes, Suplantación De Usuarios, Pérdida de Expedientes	No Se Controla La Autenticación E Identificación De Usuarios, Áreas De Trabajo Del Personal	3	1	3

Funcionarios	PERSONAL	Suplantación, Accesos No Autorizados, Errores, Manipulación Indebida De Información	Escaso Análisis De Las Personas Involucradas En El Proceso	3	10	30
Bases De Datos	DATOS E INFORMACIÓN	Accesos No Autorizados, Escape, Alteración O Divulgación De La Información	Fragilidad En Las Políticas De Uso, Dispersión De La Información, Formatos Elementales Y Almacenamiento Precario	3	10	30
Aplicaciones Y Sistemas Operativos	SOFTWARE Y APLICACIONES	Inestabilidad – Incompatibilidad	Errores Irrecuperables	3	1	3

Fuente: El Autor

Aquellos activos que han recibido calificación de impacto muy alto (MA) deberían ser objeto de atención inmediata. En el caso de estudio de la DT Bogotá del ministerio del trabajo todos los activos tienen escala Alta o Muy Alta de riesgo.

4.5 SALVAGUARDAS

La Guía de Aproximación señalaba una serie de salvaguardas, denominadas mínimas, vigentes:

1. Documentación de la política de seguridad

2. Asignación de funciones y responsabilidades

3. Responsabilidades del usuario en el acceso

4. Proceso de selección

5. Comportamiento ante incidentes

6. Controles físicos de seguridad

7. Seguridad del equipamiento

8. Cumplimiento de obligaciones jurídicas

9. Protección, transporte y destrucción

10. Gestión externa de servicios

Todos ellos recogidos en el catálogo de salvaguardas que se incluye en el "Catálogo de Elementos". [10]

5. POLÍTICAS Y CONTROLES

Las comparaciones del análisis de riesgo realizadas sobre diferentes procesos y grupos de trabajo permiten priorizar los riesgos sobre los cuales se ha de centrar la atención para definir una opción de tratamiento. Se ha elaborado una lista a partir de la evaluación de riesgos identifica las amenazas, vulnerabilidades y riesgos de la información, sobre la plataforma tecnológica con el fin de generar un plan de implementación de los controles

[10] MAGERIT – versión 2 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información I - Método

que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Perfiles de usuario: con el propósito de garantizar la seguridad del sistema es imprescindible que los perfiles de usuario se encuentren definidos conforme a su rol dentro de la compañía, con lo cual se garantiza un adecuado uso de los recursos y evita inconvenientes en la administración del sistema. Se deben probar los privilegios de acceso individuales y establecer restricciones de acceso lógico y físico asociados con cambios al sistema de información.

Control: Otorgar los mínimos privilegios de acceso a servicios que requieren mayor nivel de seguridad, se requiere minimizar el daño potencial causado por usuarios autorizados lo cual implica establecer segregación de funciones para separar usuarios de los servicios y usuarios con roles

Gestión de contraseñas: implementar las políticas necesarias y suficientes para garantizar que los usuarios del sistema acojan y adopten en sus máquinas "contraseñas fuertes", con lo cual se evita accesos no autorizados de usuarios ajenos a la máquina o a lo que es más preocupante ajenos a la empresa.

Control: creación de contraseñas seguras

Licencias: La falta de licencias originales no permite tener resultados satisfactorios pueden existir módulos, componentes o utilitarios del sistema que pueden estar presentando inconvenientes que no pueden ser subsanados por las actualizaciones que regularmente el sistema aplica. Tener licenciado nuestros productos es indispensable para que se efectúen las actualizaciones que necesitan nuestros recursos informáticos en especial nuestro sistema operativo.

Control: Usar software protegido con las debidas licencias.

Configuración de los sistemas: el administrador del sistema debe propender porque el sistema se encuentre correctamente configurado, con lo cual obtendremos un adecuado funcionamiento del sistema y evitaremos posibles ataques de diversos tipos.

Control: Definir e implementar un estándar para configurar los equipos del Centro de Servicios de manera que controle la descarga e instalación de software y los cambios en la configuración del sistema.

Sistemas de autenticación: Adicionalmente al proceso de autenticación mediante usuario y contraseña es necesario estudiar la posibilidad de implementar controles más avanzados tales como como dispositivos biométricos.

Control: Definir servicio de controles de Seguridad para Identidad, Autenticación y Cifrado.

Copias de Seguridad: Monitoreo del rendimiento de las copias de seguridad, buscando verificar la configuración ideal para su desarrollo.

Control: Las copias de respaldo deben ser protegidas contra pérdida, daño y acceso no autorizado mediante su almacenamiento en sitios seguros, la disposición de copias alternas fuera de las instalaciones y la restricción de acceso a personas autorizadas

Control de Red: es necesario garantizar una configuración adecuada la red, como medio relevante de protección del sistema operativo y las Bases de datos, controlando el flujo de información a través de dicho medio, en consecuencia es pertinente verificar y evaluar las diversas configuraciones establecidas para la protección de los protocoles de red. Regularmente el firewall controla los flujos de datos, razón por la cual es necesario verificar su configuración y los permisos implementados para la red.

Control: De haber personal suficiente, competente para operar la red en condiciones normales, capacitado para hacer frente a los errores, las condiciones de excepción y de emergencia.

Herramientas para el control de amenazas: como parte fundamental de la protección del sistema operativo, las Bases de datos y demás recursos tenemos la utilización aplicaciones

que controlan las posibles amenazas informáticas a las que está expuesto el sistema, la cuales pueden ser entre otros antivirus, antispyware y antispam, herramientas que deben ser actualizadas permanentemente efectuando monitoreo constante para garantizar su efectividad.

Control: El análisis de riesgos debe determinar los riesgos evaluando el nivel del impacto potencial de las amenazas asociadas, las amenazas accidentales y deliberadas a la confidencialidad, integridad y disponibilidad de la información, las vulnerabilidades debidas a deficiencias de control y las vulnerabilidades debidas a las circunstancias que aumentan la probabilidad de ocurrencia de un grave incidente de seguridad de la información.

Control de registro de aplicaciones: es necesario instalar y configurar esta utilidad a fin de que el sistema realice control sobre el software que se instala en el computador, es necesario realizar monitoreo al estado de los registros. Las aplicaciones que se eliminan del sistema y que no tienen una gestión adecuada pueden ocasionar inconvenientes de rendimiento por lo cual se necesita efectuar control sobre dicho registro.

Control: Los sistemas de información y las aplicaciones, deben ser diseñados e implementados de manera que se minimicen las vulnerabilidades y los ataques externos e internos se reduzcan a un nivel aceptable.

Esquema de copias de seguridad: es importante revisar la funcionalidad y operatividad de las copias de seguridad realizadas, para lo cual se hace necesario efectuar pruebas de recuperación que garanticen la efectividad de los respaldos.

Control: Los acuerdos para las copias de seguridad deben permitir que la red y los sistemas sean restaurados dentro de los plazos críticos.

Preservación logs del sistema: la implementación de los mecanismos de almacenamiento y protección de los archivos "logs" es fundamental a fin de evitar su eliminación, por cuanto por medio de la revisión de estos documentos podemos determinar las causas de los problemas que afectan nuestro sistema, así como la ocurrencia de posibles ataques.

Control: Se deben adoptar medidas para asegurar la prestación continua de los servicios en caso de una falla prolongada.

Puertos de red: Se deben identificar los puertos que hacen parte del servicio, a fin de efectuar el cerrado de aquellos que no están siendo usados, por otra parte realizar cambio de los puertos que son usados por default por el sistema a fin de garantizar mayor nivel de seguridad.

Control: Se deben proteger los puertos de diagnóstico de la red implementando controles de acceso.

Aplicaciones: Mantener actualizado el inventario de los aplicativos de ejecución en los servidores, así como el registro de los usuarios con permisos para su uso

Control: El sistema de información protege la integridad y disponibilidad de la información y aplicaciones disponibles.

Periféricos: Es pertinente identificar los periféricos (unidades de Backup, impresoras, scanner y discos externos, entre otros) se encuentran instalados y configurados, a fin de garantizar el control de E/S de la información contenida en el servidor.

Control: Se deben establecer restricciones para el uso y una guía de implementación para los dispositivos, autorizar, monitorear y controlar el acceso de los dispositivos.

Soporte: la continuidad de los contratos de soporte técnico es de gran importancia, este debe incluir como mínimo el mantenimiento preventivo y correctivo para hardware y software de servidores y las demás máquinas de la empresa, ello garantiza amparo para los casos de daños físicos, así como el adecuado soporte para los casos en que sea requerido para solucionar problemas o fallos del sistema operativo.

Control: Definir estándares para los servicios infraestructura de soporte y generar guías para el uso de la entidad y el personal.

6. PLAN DE SENSIBILIZACIÓN

Se diseñó para incluir en el plan de mejoramiento por parte del Grupo de Soporte informático un plan de sensibilización para despertar conciencia y responsabilidad acerca del cuidado de los elementos, la seguridad de la información y el buen uso de los servicios informáticos. Básicamente se trabajan dos frentes:

- ✓ Aplicación de la circular 076 del 30 de diciembre del 2016 con directrices sobre el manejo y operación de las herramientas tecnológicas disponibles en el Ministerio del Trabajo (VER ANEXO B)
- ✓ Divulgación de boletines campaña de apoyo a las buenas prácticas de uso y seguridad de los recursos informáticos. (VER ANEXO)
- ✓ Se hizo un refuerzo en las siguientes aspectos:
- ✓ Se están promoviendo charlas por parte de la Oficina TIC, que incluyen los siguientes temas:

  Principios seguridad de la información

  Políticas de seguridad de la información

  Seguridad interno

7. PLAN DE REVISIÓN PERIODICA Y ACTUALIZACIÓN DEL SGSI

A la fecha se realiza como parte de un nuevo proyecto, la caracterización del proceso de Soporte Informático que se presentará como propuesta a la Oficina asesora de Planeación del Ministerio del trabajo para que esta considere la incorporación de las actividades del grupo de trabajo dentro del mapa de procesos de la entidad como subsistema de apoyo a la gestión Misional del Ministerio. Este trabajo incluye la documentación de las actividades del grupo encargado de garantizar la disponibilidad y el desempeño de la infraestructura tecnológica y los servicios tecnológicos. En esta gestión se incluye la elaboración de procedimientos, el plan Revisión Periódica y Actualización del Sistema de Gestión de Seguridad Informática.

8. CONCLUSIONES Y RECOMENDACIONES

La Dirección Territorial de Bogotá, del ministerio del trabajo no cuenta con medidas de seguridad guiados y documentados, por lo cual este estudio será de gran beneficio para minimizar riesgos en el futuro.

La metodología Magerit permitió seguir una serie de pasos de pasos estructurados para el análisis y gestión de los riesgos para obtener datos realistas del estado de riesgo actual en la Entidad donde y permitió seleccionar que medidas serán necesarias para mitigar el riesgo.

Se identificó un alto riesgo de que se divulgue información y que usuarios no autorizados accedan a los expedientes tanto físicos como digitalizados.

Se identificó un alto riesgo de usuarios no autorizados accedan a la información, que funcionarios abucen de sus privilegios o de que intencionalmente se altere la información almacenada.

Este proyecto servirá de base para que en la entidad se establezca un manual de sensibilización que permita la revisión periódica de controles para mantener las buenas prácticas de Seguridad de la Información en el MT, de igual manera será punto de partida para la creación de normativas de seguridad para los recursos informáticos y para los empleados que laboran en la empresa.

Recomendaciones

Se debe hacer revisión periódica de las amenazas y riesgos acordes con los cambios tecnológicos y deben ser controlados para evitar problemas a futuro.

Se deben implementar las salvaguardas escogidas en el análisis de riesgos para la Entidad.

Para reducir los riesgos que existen en los activos se debe capacitar por lo menos un funcionario que se responsabilice de la Gestión de Seguridad a nivel de Dirección Territorial.

El recurso humano con que cuenta la DT Bogotá, se debe capacitar para cumplir las normas de seguridad que se mencionaron en la gestión de riesgos.

Además de controlar los riesgos identificados en el proyecto, el equipo se estar atento a los nuevos riesgos o las que estén todavía sin identificar.

Para el desarrollo y revisión se debe seguir un proceso y orden lógico de identificación de nuevo riesgos en el transcurso, asignación de responsabilidades, medidas a tomar por cada decisión y avance.

BIBLIOGRAFÍA

[1] raulosj. (2014). proyectos-de-seguridad-informática. 2015, de raulosj Sitio web: http://es.slideshare.net/raulosj/proyectos-de-seguridad-informática

[2] Groups.google.com. (2017). Google Groups. [online] Available at: https://groups.google.com/forum/#!topic/seguridad-de-la-informacion/uP5OprmdiLw [Accessed 13 Apr. 2017].

[3] Ccn-cert.cni.es. (2017). Citar un site web - Cite This For Me. [online] Available at: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html [Accessed 10 Apr. 2017].

[4] Mujica Manuel. (2009). estándares-de-seguridad-informática. Mérida: slideshare.http://es.slideshare.net/fullscreen/mmujica/estndares-de-seguridad-informtica/13

[5] Martinez Morales Maria De Los Ángeles. (2012). ejemplo-anteproyecto-investigación Ddisponible en internet enhttp://es.slideshare.net/ariamgel/ejemplo-anteproyecto-investigacion?related=1

[6] Google Books. (2017). Seguridad informática. [online] Disponible en: https://books.google.com.co/books?id=Mgvm3AYIT64C&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false [último acceso 10 Abril 2017].

[7] Andreu, Fernando. Fundamentos Y Aplicaciones De Seguridad – Izaskun, Barcelona 2006. Disponible en internet en http://books.google.com.co/books?id=k3JuVG2D9lMC&printsec=frontcover&dq=Redes+Inalambricas&hl=es&sa=X&ei=FSN0Usl1x5HZBcCPgOgG&ved=0CFUQ6AEwBg#v=onepage&q=Redes%20Inalambricas&f=false

[8] I. (2006, 03). REQUISITOS SGSI. intranet.bogotaturismo. Obtenido 11, 2016, de http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

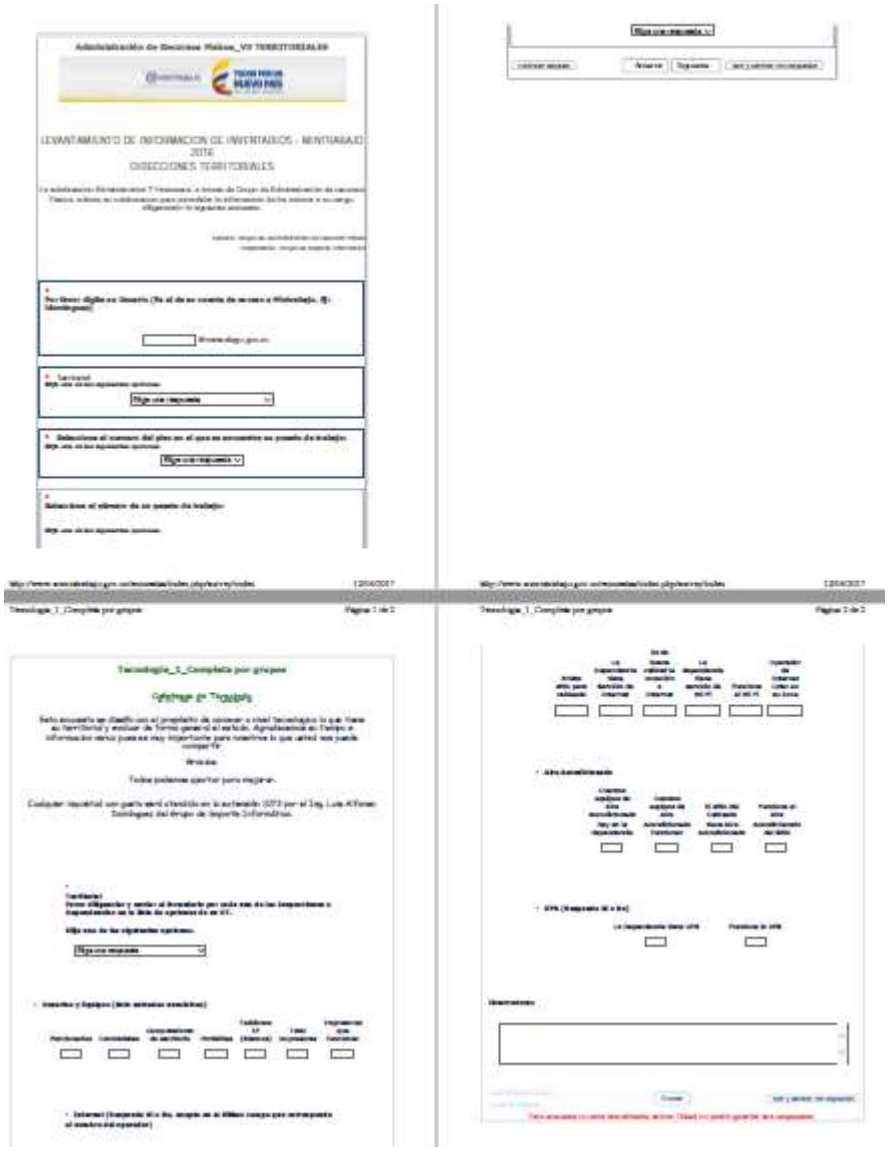
[9] Gutiérrez Amaya, C. (2013, 05). MAGERIT: metodología práctica para gestionar riesgos. welivesecurity. Obtenido 11, 2016, de http://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

[10] Guía del PMBOK (2013). Fundamentos para la dirección de proyectos. Global Standard. Recuperado el 28 de octubre de 2016, de http://datateca.unad.edu.co/contenidos/104004/GESTION_DE_LA_CALIDAD_2016-1/libros_pmbok_guide5th_spanish.pdf

ANEXOS

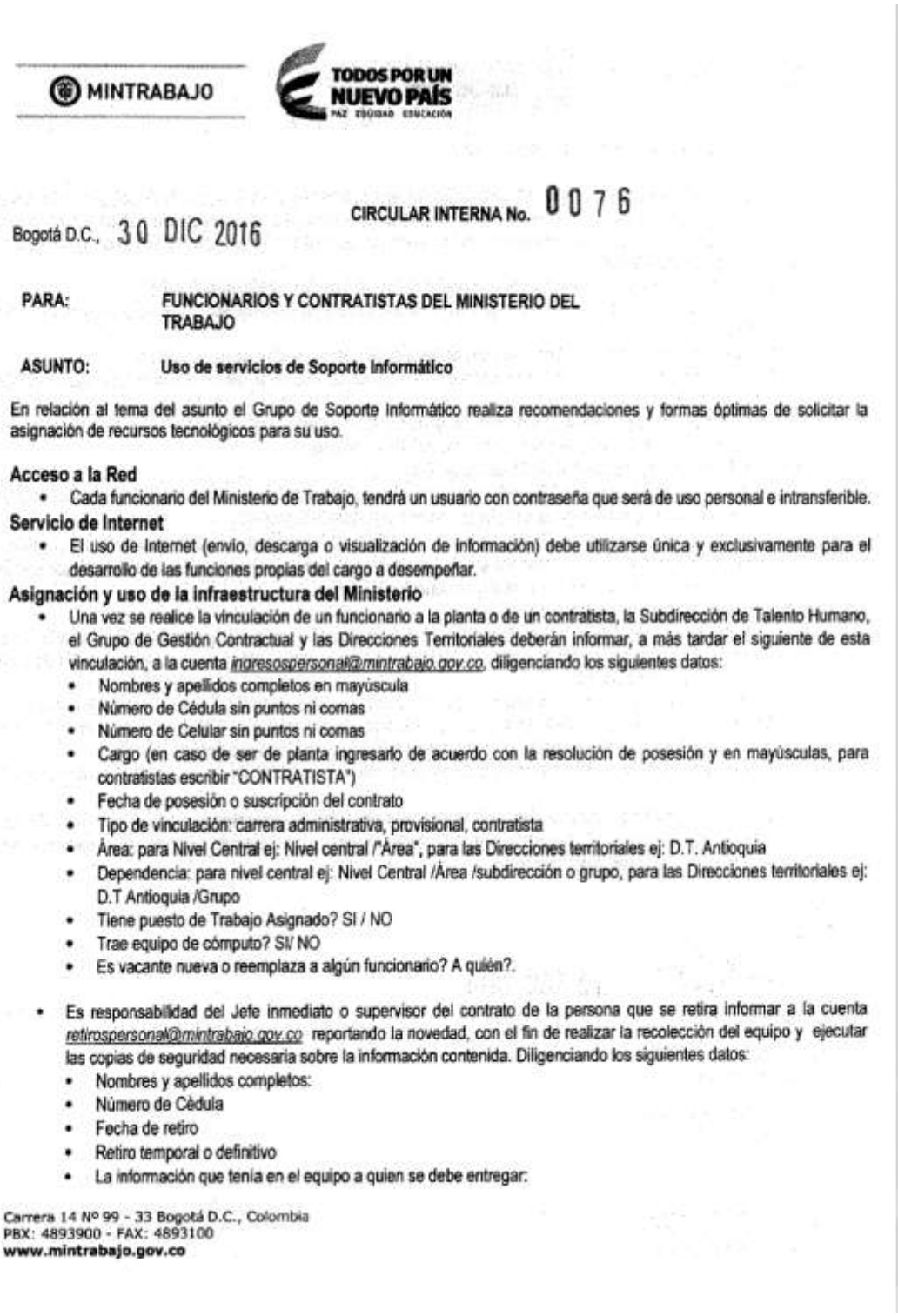
Vista encuestas digitales de Inventario y tecnología

ANEXO A



ANEXO B

Circular Uso de servicios Informáticos



MINTRABAJO

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

Bogotá D.C., 30 DIC 2016

CIRCULAR INTERNA No. 0076

PARA: **FUNCIONARIOS Y CONTRATISTAS DEL MINISTERIO DEL TRABAJO**

ASUNTO: **Uso de servicios de Soporte Informático**

En relación al tema del asunto el Grupo de Soporte Informático realiza recomendaciones y formas óptimas de solicitar la asignación de recursos tecnológicos para su uso.

Acceso a la Red

- Cada funcionario del Ministerio de Trabajo, tendrá un usuario con contraseña que será de uso personal e intransferible.

Servicio de Internet

- El uso de Internet (envío, descarga o visualización de información) debe utilizarse única y exclusivamente para el desarrollo de las funciones propias del cargo a desempeñar.

Asignación y uso de la infraestructura del Ministerio

- Una vez se realice la vinculación de un funcionario a la planta o de un contratista, la Subdirección de Talento Humano, el Grupo de Gestión Contractual y las Direcciones Territoriales deberán informar, a más tardar el siguiente de esta vinculación, a la cuenta *ingresospersonal@mintrabajo.gov.co*, diligenciando los siguientes datos:
  - Nombres y apellidos completos en mayúscula
  - Número de Cédula sin puntos ni comas
  - Número de Celular sin puntos ni comas
  - Cargo (en caso de ser de planta ingresarlo de acuerdo con la resolución de posesión y en mayúsculas, para contratistas escribir "CONTRATISTA")
  - Fecha de posesión o suscripción del contrato
  - Tipo de vinculación: carrera administrativa, provisional, contratista
  - Área: para Nivel Central ej: Nivel central /"Área", para las Direcciones territoriales ej: D.T. Antioquia
  - Dependencia: para nivel central ej: Nivel Central /Área /subdirección o grupo, para las Direcciones territoriales ej: D.T Antioquia /Grupo
  - Tiene puesto de Trabajo Asignado? SI / NO
  - Trae equipo de cómputo? SI/ NO
  - Es vacante nueva o reemplaza a algún funcionario? A quién?.

- Es responsabilidad del Jefe inmediato o supervisor del contrato de la persona que se retira informar a la cuenta *retirospersonal@mintrabajo.gov.co* reportando la novedad, con el fin de realizar la recolección del equipo y ejecutar las copias de seguridad necesaria sobre la información contenida. Diligenciando los siguientes datos:
  - Nombres y apellidos completos:
  - Número de Cédula
  - Fecha de retiro
  - Retiro temporal o definitivo
  - La información que tenía en el equipo a quien se debe entregar:

Carrera 14 Nº 99 - 33 Bogotá D.C., Colombia
PBX: 4893900 - FAX: 4893100
www.mintrabajo.gov.co

ANEXO C

Boletines Campaña de sensibilización


Sabías que…
El Grupo de Soporte Informático se apoya en:
Impresión
Internet
Escaner
Teléfonos
Equipos
Soporte técnico
Mesa de ayuda
TIPS para dar nombre a los Archivos y carpetas en nuestro computador
Si practicamos esto evitaremos daño en nuestros archivos.


Sabías que…
El Grupo de Soporte Informático se apoya en:
Impresión
Internet
Escaner
Teléfonos
Equipos
Soporte técnico
Mesa de ayuda
La contraseña de tu equipo de trabajo es el pasaporte para ingresar a ver tus correos, tus documentos y la información que tienes dentro de él.
Por esta razón, cuando el sistema solicite cambio de contraseña, no coloques el mes con el año presente porque tu equipo queda vulnerable y expuesto. Utiliza contraseñas personalizadas como: un nombre con una letra mayúscula y un número, y que sea de fácil recordación.
¡ Recuerda la seguridad de tus archivos está en tus decisiones!


Sabías que…
El Grupo de Soporte Informático se apoya en:
Impresión
Internet
Escaner
Teléfonos
Equipos
Soporte técnico
Mesa de ayuda


Sabías que…
El Grupo de Soporte Informático se apoya en:
Impresión
Internet
Escaner
Teléfonos
Equipos
Soporte técnico
Mesa de ayuda
Cuando se realice el aseo de los elementos electrónicos como teclados, teléfonos de tu casa u oficina, debes procurar o indicar usar compresas húmedas y no mojadas, para evitar que caigan gotas de agua dentro de los circuitos ocasionando humedad y a veces daño de dichos elementos.
¡ El buen funcionamiento de los equipos depende de todos!

1. Información General	
Tipo de documento	Trabajo de Grado - Monografía
Acceso al documento	Universidad Nacional Abierta y a Distancia - UNAD
Título del documento	DISEÑO DE UN SISTEMA DE SEGURIDAD INFORMÁTICA PARA LA DIRECCIÓN TERRITORIAL DE BOGOTÁ DEL MINISTERIO DEL TRABAJO
Autores	DOMÍNGUEZ, Luis
Director	GONZALEZ, Yina
Publicación	Bogotá. Universidad Nacional Abierta y a Distancia, 2017.
Unidad Patrocinante	Ministerio del Trabajo
Palabras Claves	Seguridad de la Información, Seguridad informática, Activos, Amenaza, Detección, Hacking, Prevención, Riesgo, Seguridad, VLAN, PHVA, MAGERIT

2. Descripción

Se identifican los riesgos y vulnerabilidades que surgen del flujo de información en la Red, Bases de Datos, Servidores y Aplicaciones de la Dirección Territorial de Bogotá (DT Bogotá), que es un departamento del Ministerio de Trabajo donde se llevan a cabo procesos, audiencias de conciliación e investigaciones Relacionados con el entorno laboral administrativo. Se propone una solución para evitar ataques informáticos con fines poco éticos y para desarrollar mecanismos de seguridad diseñados para regular y proteger la confidencialidad de los datos e impedir cualquier intento de intrusión para evitar daños en el sistema. Hoy en día existe una precaria interpretación de la normatividad como política de seguridad informática, con falta de documentación y difusión de información en el departamento. Los usuarios informáticos desconocen las precauciones de seguridad del sistema que deben tomarse y llevan a cabo acciones inseguras, causando riesgo, con los consiguientes daños que pueden afectar las operaciones normales de esta y demás dependencias del Ministerio.

3. Fuentes

Raulosj. (2014). proyectos-de-seguridad-informática. 2015, de raulosj Sitio web: http://es.slideshare.net/raulosj/proyectos-de-seguridad-informática

Groups.google.com. (2017). Google Groups. [online] Available at: https://groups.google.com/forum/#!topic/seguridad-de-la-informacion/uP5OprmdiLw [Accessed 13 Apr. 2017].

Ccn-cert.cni.es. (2017). Citar un site web - Cite This For Me. [online] Available at: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[Accessed 10 Apr. 2017].

Mujica Manuel. (2009). estándares-de-seguridad-informática. Mérida: slideshare.http://es.slideshare.net/fullscreen/mmujica/estndares-de-seguridad-informtica/13

Martinez Morales Maria De Los Ángeles. (2012). ejemplo-anteproyecto-investigación Ddisponible en internet enhttp://es.slideshare.net/ariamgel/ejemplo-anteproyecto-investigacion?related=1

Google Books. (2017). Seguridad informática. [online] Disponible en: https://books.google.com.co/books?id=Mgvm3AYIT64C&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false [último acceso 10 Abril 2017].

Andreu, Fernando. Fundamentos Y Aplicaciones De Seguridad – Izaskun, Barcelona 2006. Disponible en internet en http://books.google.com.co/books?id=k3JuVG2D9lMC&printsec=frontcover&dq=Redes+Inalambricas&hl=es&sa=X&ei=FSN0Usl1x5HZBcCPgOgG&ved=0CFUQ6AEwBg#v=onepage&q=Redes%20Inalambricas&f=false

I. (2006, 03). REQUISITOS SGSI. intranet.bogotaturismo. Obtenido 11, 2016, de http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

Gutiérrez Amaya, C. (2013, 05). MAGERIT: metodología práctica para gestionar riesgos. welivesecurity. Obtenido 11, 2016, de http://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Guía del PMBOK (2013). Fundamentos para la dirección de proyectos. Global Standard. Recuperado el 28 de octubre de 2016, de http://datateca.unad.edu.co/contenidos/104004/GESTION_DE_LA_CALIDAD_2016-1/libros_pmbok_guide5th_spanish.pdf

4. Contenido

El documento consta de 8 capítulos en su contenido, distribuido de la siguiente manera:

1. PRESENTACIÓN DEL PROYECTO : este capítulo contiene el nombre del proyecto, el tema de estudio, la línea de investigación y en él se plantean la pregunta de investigación, el alcance y los siguientes objetivos:

GENERAL: Diseñar un sistema de gestión de seguridad información para la Dirección Territorial del Ministerio del Trabajo en Bogotá.

ESPECÍFICOS:

Identificar y evaluar las vulnerabilidades y riesgos asociados al sistema de información existente en la Dirección Territorial de Bogotá del Ministerio del Trabajo.

Definir y documentar un plan de tratamiento del riesgo de Seguridad Informática que permita brindar un mayor nivel de seguridad de la información dentro de la Dirección Territorial de Bogotá del Ministerio del Trabajo.

Crear un manual de sensibilización que permita la revisión periódica de controles para mantener las buenas prácticas de Seguridad de la Información en el MT.

2. MARCO REFERENCIAL

Se ha seleccionado la DT Bogotá del ministerio del Trabajo para hacer un acercamiento a sus procesos para aplicar la conceptualización Seguridad de la Información y proponer una solución que permitirá reducir problemas y facilitar el desempeño de las actividades propias de cada dependencia dentro del Ministerio.

3. DISEÑO METODOLÓGICO

Gestión de Riesgos informáticos con aplicabilidad de la Norma ISO 27001 y La metodología MAGERIT.

4. DESARROLLO METODOLOGICO

Contiene el análisis y valoración de los activos de la entidad, identificación y Valoración de Amenazas, la Estimación del impacto y cálculo del riesgo

5. POLÍTICAS Y CONTROLES

6. PLAN DE SENSIBILIZACIÓN

7. PLAN DE REVISIÓN PERIODICA Y ACTUALIZACIÓN DEL SGSI

8. CONCLUSIONES Y RECOMENDACIONES

5. Metodología

Los riesgos asociados con la información y los sistemas de la Dirección territorial de Bogotá del ministerio del trabajo serán analizados utilizando metodología estructurada de análisis de riesgos mediante MAGERIT, para cubrir cubre la fase Análisis y Gestión de Riesgos, herramienta adecuada para el caso que nos ocupa que corresponde a la Gestión global de un Sistema de Seguridad de la Información basado en ISO 27001.

Para el diagnóstico se recogió información directamente de algunos funcionarios, para el estudio se recopiló de los funcionarios de la DT Bogotá, alguna de la observación complementada con el análisis documental

6. Resultados

Se identificaron entre otras vulnerabilidades:

_ Privilegios excesivos e inutilizados. se otorgan privilegios que exceden los requerimientos de su puesto de trabajo se crea un riesgo innecesario.

_Abuso de Privilegios. Los usuarios pueden llegar a abusar de los para fines no autorizados, por

_Exposición de los medios de almacenamiento para backup.
.
_Vulnerabilidad y bases de datos mal configuradas.

_Datos sensibles mal gestionados.

_Limitado conocimiento y experiencia en seguridad desconocimiento de práctica de controles de seguridad, políticas y capacitación.

7. Conclusiones
Se identificó un alto riesgo de que se divulgue información y que usuarios no autorizados accedan a los expedientes tanto físicos como digitalizados y un alto riesgo de que usuarios no autorizados accedan a la información, que funcionarios abucen de sus privilegios o de que intencionalmente se altere la información almacenada. Este proyecto servirá de base para que en la entidad se establezca un manual de sensibilización que permita la revisión periódica de controles para mantener las buenas prácticas de Seguridad de la Información en el Ministerio del Trabajo, de igual manera será punto de partida para la creación de normativas de seguridad para los recursos informáticos y para los empleados que laboran en la Entidad.

Elaborado por:	Luis Alfonso Domínguez Barreto
Revisado por:	Yina Alexandra Gonzalez Sanabria

Fecha de elaboración del Resumen:	18	04	2017