DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (S.G.S.I.) PARA EL CENTRO DE DATOS DE LA PERSONERÍA DE BOGOTÁ D.C. BAJO LAS NORMAS NTC-ISO-IEC 27001:2013 Y NTC-ISO-IEC 27002:2013

NUBIA ESPERANZA ACOSTA UBAQUE
TANIA KRUSKAYA LEÓN PATIÑO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (S.G.S.I) PARA EL CENTRO DE DATOS DE LA PERSONERÍA DE BOGOTÁ D.C. BAJO LAS NORMAS NTC-ISO-IEC 27001:2013 Y GTC-ISO-IEC 27002:2013

NUBIA ESPERANZA ACOSTA UBAQUE
TANIA KRUSKAYA LEON PATIÑO

Trabajo de grado para optar por el título:
Especialista En Seguridad Informática

Director de Proyecto:
MSc. Alexander Larrahondo Nuñez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2017

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 10 de marzo de 2017

Este trabajo está dedicado a Dios que nos dio la vida, la oportunidad y los medios para realizar nuestros estudios, a todas aquellas personas que en nuestras vidas nos motivaron para seguir adelante y aún están a nuestro lado, a todas aquellas personas que fueron nuestro pilar para llegar hasta aquí y hoy nos ven desde el cielo, y especialmente, a nuestros amadísimos hijos pues han sido nuestra inspiración para alcanzar esta meta que nos trazamos y para quienes esperamos seguir siendo ejemplo.

AGRADECIMIENTOS

Agradecemos al director de proyecto de grado, a los asesores, por su pulcritud y diligencia en las retroalimentaciones para que este trabajo se formulara adecuadamente, agradecemos a los tutores que con su laboriosidad nos orientaron en esta difícil tarea y por los cuales no nos sentimos trabajando en solitario y por último agradecemos al Director de Tecnologías de la información y las comunicaciones de la Personería de Bogotá, quien nos dio vía libre para tomar como punto de partida la entidad en la cual laboramos.

CONTENIDO

pág.

INTRODUCCIÓN 15

1. PLANTEAMIENTO DEL PROBLEMA 16
1.1. FORMULACIÓN DEL PROBLEMA 16
1.2. DELIMITACIÓN DE LA INVESTIGACIÓN 16
1.3. OBJETIVOS 17
1.3.1. Objetivo general 17
1.3.2. Objetivos específicos 17
1.4. JUSTIFICACIÓN 18

2. MARCO REFERENCIAL 20
2.1. MARCO TEÓRICO 20
2.1.1. Seguridad de la información 20
2.1.2. Sistema de Gestión de la Seguridad de la Información (SGSI) 24
2.1.3. Norma ISO/IEC 27000 25
2.1.4. Estándar 26
2.1.5. Metodologías de evaluación de riesgo 26
2.2. MARCO CONTEXTUAL 28
2.3. MARCO LEGAL 30

3. METODOLOGÍA 34

4. RESULTADOS 35
4.1. ETAPA 1 PLANIFICACIÓN 35
4.1.1. Alcance del Sistema de Gestión de Seguridad de la Información (SGSI) 35
4.1.2. Metodología MAGERIT 35
4.1.3. Inventario de activos 35
4.1.4. Valoración de activos 40
4.1.5. Identificación de amenazas 43
4.1.6. Impacto del riesgo 48
4.1.7. Identificación de riesgos 52
4.1.8. Riesgo Promedio 62
4.1.9. Resumen de riesgos 62
4.1.10 Políticas de seguridad 63
4.1.11 Objetivos de control 93
4.2. ETAPA 2 EJECUCIÓN 101
4.2.1. Plan de Tratamiento de Riesgos 101
4.2.2. Declaración de aplicabilidad 106
4.2.3. Plan de continuidad 113
4.2.4. Implementación 166
4.2.5. Documentación 167

4.3. ETAPA 3 SEGUIMIENTO.....169
4.3.1. Procedimientos de monitorización y revisión.....169
4.3.2. Instrumentos para registro de acciones y eventos 172
4.4. ETAPA 4 MANTENIMIENTO Y MEJORA 173

5. CONCLUSIONES.....175

BIBLIOGRAFÍA.....176

ANEXOS.....178

LISTA DE CUADROS

pág.

Cuadro 1. Metodología del proyecto 34
Cuadro 2. Activos centro de datos 36
Cuadro 3. Escala de valores para los activos 40
Cuadro 4. Valoración de activos 41
Cuadro 5. Frecuencia de amenazas 44
Cuadro 6. Identificación y valoración de amenazas 44
Cuadro 7. Impacto del riesgo 48
Cuadro 8. Matriz identificación de riesgos.....53
Cuadro 9. Análisis de riesgo promedio 62
Cuadro 10. Resumen de riesgos.....62
Cuadro 11. Objetivos de control.....93
Cuadro 12. Tratamiento de los riesgos 103
Cuadro 13. Declaración de aplicabilidad.....106
Cuadro 14. Documentos Requeridos Norma ISO 27001- 2013 168
Cuadro 15. Etapas de un proceso de auditoría.....170

LISTA DE FIGURAS

pág.

Figura 1. Amenazas informáticas 22
Figura 2. Aspectos que abarca un SGSI 24
Figura 3. ¿Para qué sirve el SGSI? 25
Figura 4. Organigrama 29
Figura 5. Organización interna 30
Figura 6. El riesgo en función del impacto y la probabilidad. 48
Figura 7. Matriz riesgo 52
Figura 8. Gestión de riesgos 102
Figura 9. Comité de seguridad informática 116
Figura 10. Comité de emergencias (COE) 117
Figura 11. Organización plan de continuidad 121
Figura 12. Flujo para la Activación Plan de Continuidad 140
Figura 13. Prioridades Plan de Continuidad de Negocio 143
Figura 14. Pasos para realizar auditoría 169
Figura 15. Recolección y verificación de información 171
Figura 16. Formato programas de auditoría 171

LISTA DE ANEXOS

pág.

Anexo A. Codificación de grupos ……..……..……..…177
Anexo B. Amenazas metodología MAGERIT……..……..……180
Anexo C. Verificación de cumplimiento ISO 27002:2013…….…… 201
Anexo D. Lista chequeo de auditoría interna ……..207
Anexo E. Formato para registro de visita de auditoría…….….215

GLOSARIO

ACTIVO: "En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización"[1].

AMENAZA: "Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización"[2].

AUDITORÍA: Serie de pasos organizados de una manera lógica, para obtener y analizar evidencia de una manera crítica y objetiva, con el objetivo de dar la dictamen del proceso o gestión evaluado.

BACKUP: "Copia adicional de los archivos de la computadora que generalmente se guarda en un lugar físicamente separado de los originales. Resulta fundamental para la recuperación cuando se dañan o se pierden los archivos originales."[3]

CIFRADO: Método por el cual se esconde el contenido de archivo o mensaje, de manera que solo pueda ser leído por la persona autorizada.

CLAVE PRIVADA: "Un cifrado de clave privada (o simétrico), se basa en un algoritmo/método/cifrado que usa una única clave para cifrar/descifrar los mensajes/criptogramas."[4]

CLAVE PÚBLICA: Se encuentra en la criptografía asimétrica, basada en la generación de dos claves para un mismo mensaje, donde la clave pública puede ser entregada a cualquier persona.

COBIT: Es un modelo utilizado para valorar los sistemas de información de una entidad.

CONTRASEÑA: Es una palabra o frase secreta, utilizada para acceder a ciertas funciones informáticas.

COSO: "Documento que contiene las principales directivas para la implantación, gestión y control de un sistema de control" [5]

---

[1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Norma ISO 27000 en español. [En línea]. [17 marzo de 2016]. Disponible en: http://www.iso27000.es/glosario.html#section10a

[2] Ibíd., Disponible en: http://www.iso27000.es/glosario.html#section10a

[3] SYMANTEC, Norton. Glosario de seguridad de internet [En línea]. [17 marzo de 2016]. Disponible en: http://co.norton.com/security-glossary/article

[4] Guassianos. Criptografía: Cifrado de clave privada. Disponible en: http://gaussianos.com/criptografia-cifrado-de-clave-privada/

[5] Consultora Sur. Auditoria, Contabilidad & Economía. Disponible en: https://blogconsultorasur.wordpress.com/2011/09/06/que-es-coso/

CRIPTOGRAFÍA: La Real academia de la lengua española, descompone etimológicamente la palabra, indicando ser derivada del griego kryptós que significa oculto y grafía que significa escritura[6], significando en conjunto el arte de escribir con clave secreta de forma enigmática; también representa escritura escondida. En este sentido se entiende la criptografía como la técnica que permite proteger los documentos e información, utilizando códigos que alteran la transmisión de un mensaje, de manera que no pueda ser leído por una persona diferente al destinatario, y pueda ser transformado o descifrado solo por la persona autorizada con el conocimiento de las llaves correspondientes.

DECLARACION DE APLICABILIDAD: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del ISO 27001. (ISO/IEC[7]27000).

IMPACTO: Cálculo de las consecuencias que pueden ocurrir al concretarse un riesgo o una amenaza.

MAGERIT: Es una metodología de análisis y gestión de riesgos.

PLAN: Enmarcado en el contexto de un SGSI, es la fase donde se define cuando, como y donde se realizaran los objetivos de seguridad propuestos, el tiempo que llevara su realización, se define el alcance para la implementación del SGSI.

POLÍTICA: La política del SGSI es un documento, con aprobación de las altas directivas enmarcado en la necesidad de un sistema de gestión para la seguridad de la información, contiene un conjunto de normas y prácticas para lograr los objetivos de seguridad de información de una entidad.

RIESGO: Riesgo se puede definir como la posibilidad de que ocurra un evento que perturba el cumplimiento de un objetivo.

SALVAGUARDA: Es un mecanismo, política o cualquier otro medio utilizado para minimizar un riesgo.

SEGURIDAD: 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[8]

[6] Real Academia de la Lengua Española, Diccionario de la lengua española. Disponible en: http://dle.rae.es/?id=BHcfHjo
[7] MINTIC. Modelo de Seguridad y Privacidad de la Información. [03 marzo de 2015]. Disponible en: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html
[8] Markus Erb. Gestión de Riesgo en la Seguridad Informática. Disponible en: https://protejete.wordpress.com/gdr_principal/definicion_si/

VULNERABILIDAD: La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño, según se puede deducir de lo expresado en la información contenida en el Observatorio Tecnológico de España [9]

[9] Ministerio de educación, cultura y deporte. Observatorio tecnológico. Gobierno de España. Disponible en: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

RESUMEN

El presente documento contiene una propuesta de diseño de un sistema de gestión de seguridad de la información SGSI, diseñado específicamente para el centro de datos de la Personería de Bogotá D.C., con él se quiere dar un manejo adecuado a la seguridad de la Entidad, diseñando un SGSI, tomando como base el estándar ISO 27001:2013.

Se realiza un análisis de los riesgos existentes en la personería de Bogotá, aplicado específicamente en los servicios, infraestructura y aplicativos que se encuentran en el centro de datos, que son base para la función misional de la entidad.

Se realiza una identificación de los riesgos, amenazas y vulnerabilidades a los que están expuesto los activos relacionados en el Centro de Datos, una vez evaluados los mismos se proponen controles de seguridad y el de plan de tratamiento del riesgo, para una respuesta oportuna ante algún incidente de seguridad.

Se complementa el diseño de las políticas de seguridad enfocadas al Centro de datos, con los soportes documentales adecuados para tener un registro de actividades.

Adicionalmente se propone las etapas de implementación del SGSI en el Centro de Datos, como una base fundamental y primera etapa para la implementación del SGSI en toda la entidad.

INTRODUCCIÓN

El auge de la tecnología, ha implicado que las empresas deban estar preparadas para proteger adecuadamente la información, siendo esta uno de los activos más importantes de una organización. La gestión de la seguridad debe ser un proceso de mejora continua y de constante adaptación a los cambios en la organización, en cuanto a procesos de negocio y a la tecnología implicada.

La seguridad de la información se desarrolla atendiendo a tres dimensiones principales, las cuales son, confidencialidad entendida como la garantía del acceso a la información únicamente de los usuarios autorizados, integridad como la preservación de la información de forma completa y exacta y disponibilidad como la garantía del acceso a la información en el instante en que el usuario la necesita; la dedicación para una adecuada formulación de un SGSI debe ser establecida teniendo en cuenta la naturaleza de la entidad.

El presente proyecto tiene como propósito formular un diseño del Sistema de Seguridad de la Información -SGSI- para el Centro de Datos de la Personería de Bogotá D. C. y así contribuir y garantizar la adecuada gestión de la seguridad en la entidad.

En el centro de datos de la Personería de Bogotá se concentran los servidores, aplicativos y dispositivos críticos que soportan el eje funcional de la entidad; la no disponibilidad de los mismos, puede causar consecuencias graves para la imagen institucional y el cumplimiento de su misión.

Teniendo en cuenta que su labor principal se fundamenta en tres ejes fundamentales sobre los cuales opera y son su razón de ser, resulta crucial, que la entidad fortalezca la seguridad informática con la que cuenta y provea de mecanismos adecuados para resguardar adecuadamente datos personales, información de procesos disciplinarios, información de veedurías e información de víctimas entre otros.

La Personería de Bogotá cumple una misión muy loable en favor de los ciudadanos; por ende, es importante velar porque sus herramientas informáticas cuenten con un óptimo funcionamiento y estén protegidas, especialmente las que se encuentran en el área del centro de datos pues allí se acopian los principales dispositivos.

En el desarrollo de la presente propuesta, se aprecian los resultados producto del desglose de las etapas de Planificación, Ejecución, Seguimiento y Mantenimiento y se formulan varias oportunidades de mejora, dentro de las cuales se destacan como estrategias de continuidad del proyecto el autodiagnóstico del cumplimiento de compromisos, simulacros de materialización de riesgos y contratación de consultorías para realizar mediciones objetivas de la ejecución del sistema.

1. PLANTEAMIENTO DEL PROBLEMA

La Personería de Bogotá D.C., ha acumulado mucha información sensible con el paso de los años, en el ejercicio de sus funciones como ente de control y como garante de derechos. El resguardo de esa información y su gestión, es vital para su funcionamiento, por lo cual, creó el centro de cómputo y se ha venido adecuando y modernizando en infraestructura así como en sus procesos internos.

La readecuación del centro de cómputo se ha dado de forma paulatina, sin embargo, frente a los cambios suscitados, la reestructuración de la Personería mediante el acuerdo 514 del Concejo de Bogotá y a la expansión de la entidad al realizar en esta administración una atención de 24 horas para el ciudadano, ampliando la atención no solamente a sedes externas sino a centros comerciales, no se han delimitado claramente los nuevos riesgos y vulnerabilidades de manera formal, lo que conlleva a la no formulación de controles adecuados, quedando la entidad más expuesta a enfrentar alteraciones en el funcionamiento, pudiendo redundar en el retraso en la prestación del servicio.

Adicionalmente, la entidad está en proceso de verificación de cumplimiento de las normas técnicas colombianas en materia de seguridad de la información, por lo cual necesita contar con un Sistema de Gestión de Seguridad de la Información que cobije toda la entidad tanto en su sede central como en los puntos externos. Para formular dicho sistema, se debe iniciar con un reconocimiento general del manejo de la información en la entidad y una propuesta clara para el centro de cómputo, la cual sería la base para la posterior formulación de los demás aspectos que cobija un SGSI institucional.

1.1.FORMULACIÓN DEL PROBLEMA

¿Cómo contribuir a mejorar la seguridad del centro de datos de la Personería de Bogotá D.C., cumpliendo con la NTC-ISO-IEC 27001:2013 y GTC-ISO-IEC 27002:2015?

1.2. DELIMITACIÓN DE LA INVESTIGACIÓN

El tipo de investigación del proyecto, es Investigación de Campo, para comprender y resolver alguna situación, necesidad o problema en un contexto determinado. El tipo de proyecto es de aplicación, con tipo de intervención de Investigación Acción.

Se trabaja en el ambiente real de la Personería, interactuando con las personas, tanto colaboradores como funcionarios.

En la cadena de formación de sistemas de la UNAD, se encuentran dos líneas de acción, de las cuales se seleccionó la línea de Gestión de sistemas (Área: Ciencias de la Computación), involucrando por ende, la seguridad informática; dentro de esa línea, se plasma el presente proyecto de aplicación.

Teniendo en cuenta que no se registran antecedentes en la entidad de una formulación completa, detallada y formal de un Sistema de Gestión de Seguridad Informática para el centro de datos, el presente proyecto comprende una etapa de selección de metodología para detección de riesgos y análisis de vulnerabilidades, el análisis mismo de los riesgos y vulnerabilidades, pasando por la formulación del plan de tratamiento de riesgos con sus correspondientes controles y métricas, correctamente documentados, continuando con el seguimiento sobre los controles que la entidad tenga implementados y los que haya podido implementar fruto de la presente propuesta; culmina con el reporte completo de actividades de mantenimiento y mejora que se podrían llevar a cabo para el perfeccionamiento del mencionado sistema. Los únicos antecedentes encontrados son un conjunto de lineamientos generales sobre cultura informática, el establecimiento de algunos procedimientos internos y formatos de uso interno en el Centro de Cómputo y la formulación básica de un plan de contingencias.

1.3.OBJETIVOS

1.3.1.Objetivo general

Diseñar un sistema de gestión de seguridad de la información, que contribuya a reducir los riesgos existentes en la Personería de Bogotá, aplicado a los servicios, productos e infraestructura que se encuentran en el Centro de Datos y que soportan los aplicativos críticos de la entidad.

1.3.2.Objetivos específicos

- Realizar el análisis de riesgos, amenazas y vulnerabilidades a las que están expuestos los activos de información ubicados en el Centro de Datos de la Personería de Bogotá, bajo la norma NTC-ISO-IEC 27001:2013.

- Recomendar controles de seguridad de acuerdo al entorno del manejo de la información de la entidad, bajo la norma NTC-ISO-IEC 27002:2013.

- Definir un plan de tratamiento de riesgos en el cual se formulen los diferentes procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

- Diseñar una política de seguridad específica para el centro de cómputo y sugerir los correspondientes instrumentos para registro de actividad.

- Proponer las etapas de formulación del SGSI en el Centro de Datos, que sirva de base a la posterior consolidación de un SGSI para toda la entidad.

- Plantear la creación de un Plan de Continuidad del Negocio estableciendo las fases que deberían ser tenidas en cuenta.

1.4.JUSTIFICACIÓN

La personería de Bogotá, creó hace varios años un Área de Sistemas aprovechando los conocimientos de algunos profesionales con los que contaba, los cuales, tenían habilidades en informática, con el fin de sistematizar procesos que se desarrollaban al interior de la entidad. Se invirtieron recursos para la adecuación del centro de datos, dotándolo con herramientas básicas de seguridad y de redes, las cuales han sido actualizadas paulatinamente según las necesidades de la entidad, pero no de forma suficiente; por lo anterior, en ocasiones se han presentado algunos intentos de intrusiones y ataques, afectando el funcionamiento de algunos aplicativos.

La dependencia que tiene a cargo el Centro de Datos, antes Área de Informática, ha cambiado su estructura y se ha convertido en la Dirección de Tecnologías de la Información y las Comunicaciones; dicha reestructuración, ha implicado varias fases de modernización de la entidad en lo que a parque computacional y cableado se refiere, sin embargo, algunos recursos aún no se han renovado y varios procesos no se encuentran plenamente estructurados y fortalecidos, dando lugar a debilidades que pueden desencadenar accesos indebidos a la información confidencial, modificación de la información existente, o daños en los aplicativos, provocando conmoción temporal en la prestación de los servicios, perjudicando a los miles de usuarios.

Tanto los servidores, las aplicaciones y las bases de datos que soportan la gestión diaria de la entidad, deben encontrarse habilitados y en óptimo estado, para poder garantizar de forma permanente la atención a los usuarios las 24 horas del día; esta última es una meta institucional, por lo cual, la Dirección de Tecnologías de la Información y las Comunicaciones debe estar a la altura, contribuyendo a su

cumplimiento y buscando formular y ejecutar las acciones necesarias para garantizar la disponibilidad, confidencialidad e integridad de la información.

El primer beneficiario de la implementación de un adecuado SGSI en el Centro de Datos es la entidad pues brinda garantías para que la gestión de las dependencias sea más ágil y segura, impactando de igual forma la atención al usuario final propendiendo por la prestación del servicio 24 horas y la reserva de información de forma adecuada.

2. MARCO REFERENCIAL

2.1. MARCO TEÓRICO

El campo de la Seguridad Informática es bastante extenso y de vital importancia en cualquier empresa por cuanto permite realizar de manera sistemática una serie de actividades para proteger uno de los activos más importantes, es decir, la información; por lo anterior, es necesario clarificar tanto la definición de este término, como la semántica básica que se emplea en el transcurso del desarrollo de la presente propuesta, tanto para delimitar el alcance, como para permitir la comprensión total de la propuesta aquí contenida. A continuación se explica en detalle cada uno de los conceptos empleados y desarrollados:

2.1.1. Seguridad de la información

Para comenzar el análisis de la Seguridad Informática, se deberán conocer las características de lo que se pretende proteger: Se entiende por Dato "la unidad mínima con la que se compone cierta información. La Información "es una agregación de datos que tiene un significado específico más allá de cada uno de éstos"[10] y tendrá un sentido particular según cómo y quién la procesa.

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso, que en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación. Existe Información que debe o puede ser pública: puede ser visualizada por cualquier persona (por ejemplo, índice de analfabetismo en un país); y aquella que debe ser privada: sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella (por ejemplo, antecedentes médicos).

En caso de la información privada, se deben maximizar los esfuerzos para preservarla y reconocer las siguientes características en la Información:

Es Crítica: Es indispensable para garantizar la continuidad operativa.
Es Valiosa: Es un activo con valor en sí misma.
Es Sensitiva: Debe ser conocida por las personas que la procesan y sólo por ellas.

Se deduce del texto de López-Polín[11] que la seguridad de la información se obtiene mediante la preservación de los siguientes principios básicos:

[10] CALVO, Rafael. Glosario de términos. Disponible en: http://www2.ati.es/novatica/glosario/buscador/glosario_internet_busca.html.
[11] LÓPEZ-POLÍN, Ignacio. Confidencialidad, integridad y disponibilidad de la información. Disponible en: http://www.belt.es/expertos/experto.asp?id=2245

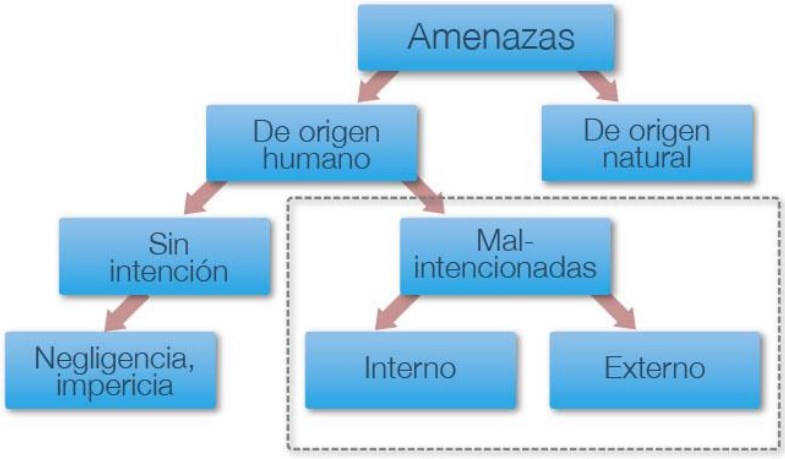
La Integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorías. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.
La Disponibilidad u Operatividad de la Información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.
La Confidencialidad o Privacidad de la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño (por ejemplo, conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo, los planes de desarrollo de un producto que se filtran a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).
El Control sobre la información permite asegurar qué sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma.
La Autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Además, pueden considerarse algunos aspectos adicionales según el documento de la Universidad de Cantabria[12], relacionados con los anteriores, pero que incorporan otros matices particulares:

- Protección a la Réplica: Mediante la cual, se asegura que una transacción sólo pueda realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.
- No Repudio: Hace referencia a evitar que cualquier entidad que envió o recibió información, demande ante terceros, que no la envió o recibió.
- Consistencia: Asegurar que el sistema se comporte como se supone que debe hacerlo, ante los usuarios que corresponda.
- Auditoría: Es la capacidad de determinar, qué acciones o procesos se están llevando a cabo en el sistema, así como quién y cuándo las realiza.
- Amenaza, En el entorno informático, se define como cualquier elemento que comprometa al sistema.

[12] Universidad de Cantabria. La gestión del riesgo operacional. Disponible en: https://books.google.com.co/books?id=kR33ej859OEC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Figura 1. Amenazas informáticas



Fuente: http://www.magazcitum.com.mx/?p=2193#.VuGsMfnhDIU

Las amenazas, pueden ser analizadas en tres momentos: antes del ataque, durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad del sistema informático.

La Prevención (antes): Conjunto de mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo, el cifrado de información para su posterior transmisión.

La Detección (durante): Mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.

La Recuperación (después): Son los mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo, recuperación desde las copias de seguridad (backup) realizadas.

Es importante definir el Riesgo como “la proximidad o posibilidad de daño sobre un bien”[13]. Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo debería ser atacado de las siguientes maneras:

- Minimizando la posibilidad de su ocurrencia.
- Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
- Diseño de métodos para la más rápida recuperación de los daños experimentados.

[13] BORGHELLO, Cristian. "Seguridad Informática: Sus Implicancias e Implementación" Argentina, 2001. [4 enero de 2016]. Disponible en: http://www.academia.edu/10446995/SEGURIDAD_DE_LA_INFORMACION

- Corrección de las medidas de seguridad en función de la experiencia recogida.

El Daño es el resultado de la amenaza; puede producirse porque no se supo identificar adecuadamente la amenaza, se deben detectar las Vulnerabilidades (debilidades) del sistema y que pueden ser explotadas y empleadas, por la amenaza, para comprometerse y aplicar las técnicas de protección adecuadas.

La Seguridad indicará el índice en que un Sistema Informático está libre de todo peligro, daño o riesgo, esta característica es muy difícil de conseguir en un 100%, por lo que sólo se habla de Fiabilidad y se la define como "la probabilidad de que un sistema se comporte tal y como se espera de él[14]", y se habla de Sistema Fiable en vez de sistema seguro.

Las distintas funciones que se deben asegurar en un sistema informático, son descritas a continuación a nivel general.

Reconocimiento: Cada usuario deberá poseer una identificación y autenticarse con ella al ingresar en el sistema, cada operación que este efectué debe ser registrada y monitoreada. Con lo que se persigue que no se produzca un acceso y/o manipulación no autorizado de los datos o información y toda actividad quede registrada en caso de algún suceso.

Aislamiento: Los datos utilizados deben ser independientes para cada usuario, tanto de manera física como lógica existen diferentes técnicas que pueden ser utilizadas para este fin. También se debe lograr tener separados con accesos independientes los datos accesibles y los datos que son considerados críticos, además permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo

Auditabilidad: Procedimiento utilizado en la elaboración de pruebas, validaciones, controles, evidencias, verificaciones o demostraciones del sistema.

Controlabilidad: Se debe tener un control continuo de todos los sistemas y subsistemas.

Administración y Custodia: la vigilancia permite conocer, en todo momento, cualquier suceso, para luego realizar un seguimiento de los hechos y permitir una retroalimentación del sistema de seguridad, de forma tal de mantenerlo actualizado contra nuevas amenazas.[15]

[14] MENTOR, Aula. Gobierno de España, Ministerio de Educación, Cultura y Deporte. [En línea]. [18 diciembre de 2015]. Disponible en : http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/bases_de_la_seguridad_informtica.html

[15] BORCHEGO, Cristian. Seguridad informática sus implicancias e implementación, Universidad Tecnológica Nacional, Tesis de licenciatura en Sistemas, Septiembre 2001

2.1.2.Sistema de Gestión de la Seguridad de la Información SGSI

Un Sistema de Gestión de la Seguridad de la Información SGSI es un instrumento de gestión que mediante una serie de acciones organizadas, permite conocer, tramitar y disminuir los riesgos que atenten contra la entidad.

Este sistema debe realizarse mediante procesos sistemáticos, documentados y conocidos por una organización o entidad'[16].

Figura 2. Aspectos que abarca un SGSI

Fuente: http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

Un SGSI contribuye a identificar y evaluar los riesgos que afectan a la entidad, con el objetivo de implantar medidas, procesos y procedimientos para su apropiado control, tratamiento y mejora continua.

Las políticas y procedimientos que se establezcan atendiendo al SGSI son adaptados específicamente para cada empresa, y, para su aplicabilidad, deben ser adoptados por todos los estamentos de la misma para procurar la mayor reducción de los riesgos posible y reducir su impacto en caso de que se materialicen.

[16] MINTIC. Informe final-Modelo de seguridad de la información-Sistema SANSI [En línea]. [10 diciembre de 2015]. Disponible en: http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf

Para que el SGSI se formule, implemente y apropie debe ser direccionado desde las directivas y materializado posteriormente por los diferentes estamentos de la entidad por categorías. Es así como para poder delimitar los aspectos que se contemplan dentro de la seguridad organizativa, se involucran aspectos como las políticas de seguridad, organización de la seguridad de la información, manejo adecuado y gestión de los diferentes activos, incidentes y continuidad del negocio. Dentro de la categoría de la seguridad lógica cobran importancia los controles de acceso, la gestión de comunicaciones y operaciones, adquisición, desarrollo y mantenimiento de sistemas de información. Es un complemento la seguridad física y del entorno, y, finalmente, para poder establecer conformidad sobre el sistema, se debe realizar una verificación minuciosa sobre la normatividad legal vigente y diferentes directivas.

Figura 3. ¿Para qué sirve el SGSI?

Fuente: http://www.iso27000.es/download/doc_sgsi_all.pdf

Un SGSI incluye un manual de seguridad, procedimientos que indican claramente cómo se debe llevar a cabo la operación y control de la seguridad, listas de chequeo e instrumentos complementarios de los procedimientos en los cuales se especifiquen en detalle las actividades ejecutadas, relacionadas con la seguridad de la información y registros que permitan dar cuenta de lo efectivamente ejecutado y sirvan de herramienta de análisis para mejoramiento de procesos.

2.1.3.Norma ISO/IEC 27000

Esta serie proporciona un marco de referencia para la gestión de la seguridad de la información. La ISO desarrolla estándares requeridos por el mercado acerca de

productos, tecnologías, sistemas y métodos de gestión, entre otros. Estos estándares, por naturaleza, son de aplicación voluntaria.

27000 Términos y Definiciones usados en toda la Serie 27000.
27001Requisitos de un SGSI.
27002 Objetivos de Control y Controles de Seguridad de la Información.
27003 Guía para implantar un SGSI según el Modelo PDCA y los requerimientos de sus diferentes fases.
27004 Métricas y Técnicas de Medida para determinar la eficacia de un SGSI y de los Controles de Seguridad aplicados.
27005 Directrices para la Gestión de Riesgos en la Seguridad de la Inform.
27006 Requisitos para la Acreditación de Entidades de Auditoría y Certificación de SGSI. (Min. Comunicaciones, 2008, p.14)

2.1.4.Estándar

Los estándares son publicaciones que recopilan el trabajo en común de los comités de fabricantes, usuarios, organizaciones y consumidores, que contiene especificaciones técnicas y mejores prácticas en la experiencia profesional con el objeto de ser utilizada como guía para las necesidades demandadas por la sociedad y tecnología. Suministra un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información.

Existen estándares internacionalmente aceptados relacionados con seguridad de la información (COBIT3, NIST4, AS/NZ43605, entre otros), que la enfocan desde diferentes puntos de vista como controles de seguridad, buen gobierno, gestión de riesgo, etc.

2.1.5.Metodologías de evaluación de riesgo

El objetivo principal de esta actividad es realizar una selección asertiva de la metodología para la evaluación de riesgos, por lo cual, se rastrea información sobre diferentes metodologías de las cuales se establecen algunos aspectos importantes de cada una así:

MAGERIT: Formula un proceso de gestión de riesgos en el cual se incorpora la norma ISO-31000 de Gestión de riesgo, detallando los pasos que van desde la identificación del contexto, identificación del riesgo, análisis del riesgo, evaluación del riesgo y tratamiento del riesgo, con sus correspondientes actividades paralelas de monitoreo y revisión. Es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica, implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los

riesgos derivados del uso de tecnologías, según lo descrito en el libro 3 de la metodología Magerit.[17]

Magerit toma la gestión del riesgo como pilar para una buena administración, recalcando la importancia que los directivos de la organización y los responsables de la misma, tengan conciencia de que existen riesgos y que estos deben ser gestionados, ofrece un método ordenado para analizar los riesgos que se originan del uso de tecnologías de la información y comunicaciones (TIC), esta metodología da pautas para ayudar a identificar los riesgos, buscando el tratamiento oportuno para mantenerlos bajo control.

Esta metodología también pretende que las entidades tomen medidas adecuadas para procesos de certificación, evaluación o auditorias según sea el caso. La versión 3 de Magerit, está organizada en dos libros uno de método y el otro de Catalogo de elementos y en una guía de técnicas para ser utilizadas en la aplicación de esta metodología.

OCTAVE: Esta metodología fue desarrollada por la Universidad de Carnegie Melon y se centra principalmente en una evaluación de la organización y una identificación de vulnerabilidades mediante la construcción de perfiles de amenazas basada en la identificación de activos, sobre los cuales se realizan medidas de probabilidad por rangos de frecuencias y se analizan los límites. Se complementa con la formulación de planes y definición de estrategias de seguridad lo cual constituye el plan y estrategia de seguridad. Deriva de Melissa (creada en 1984 para un entorno militar francés) y Marion (creada en Francia en 1985 actualizada por CLUSIF).

MEHARI: Creada en 1995 por CLUSIF, basada en Melissa y Marion. Evalúa riesgos y proporciona una guía para implementación de la seguridad en una empresa; evalúa riesgos según la disponibilidad, confidencialidad e integralidad. El impacto se determina en la medida de afectación de la calidad de los servicios de seguridad.

DAFP: Se presenta de forma detallada como una guía elaborada por el Departamento Administrativo de la Función Pública en el año 2011, mediante la cual se orienta sobre la gestión del riesgo, el análisis del contexto, identificación del riesgo, análisis del riesgo, valoración del riesgo y definición de políticas de administración del riesgo.

EBIOS: Creada en Francia, está compuesta por el desarrollo en código abierto en el cual se siguen fases de análisis de contexto, análisis de necesidades e identificación de puntos de conflicto, identificación de objetivos de control y riesgos residuales. Compatible con las normas internacionales ISO13335, ISO15408, ISO17799.

[17] MAGERIT .3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WMs9dm_hCzd

CRAMM: Desarrollado por el gobierno del Reino Unido por primera vez en 1987, orientado a la administración pública británica, contempla la identificación de activos físicos y lógicos, análisis de amenazas, análisis de materialización de riesgos teniendo en cuenta una escala de clasificación de exigencia de seguridad según el activo, lista completa de tratamiento de riesgos y cálculo de riesgos en caso de materialización de amenazas.

NIST SP-800-30: Desarrollada en el 2002 por el Instituto Nacional de Estándares y Tecnología, se basa en la caracterización del sistema, identificación de amenazas, y vulnerabilidades, análisis de controles, definición de probabilidad, pérdida de integridad, disponibilidad y confidencialidad, determinación de riesgos e impacto, recomendaciones de controles y documentación de resultados.

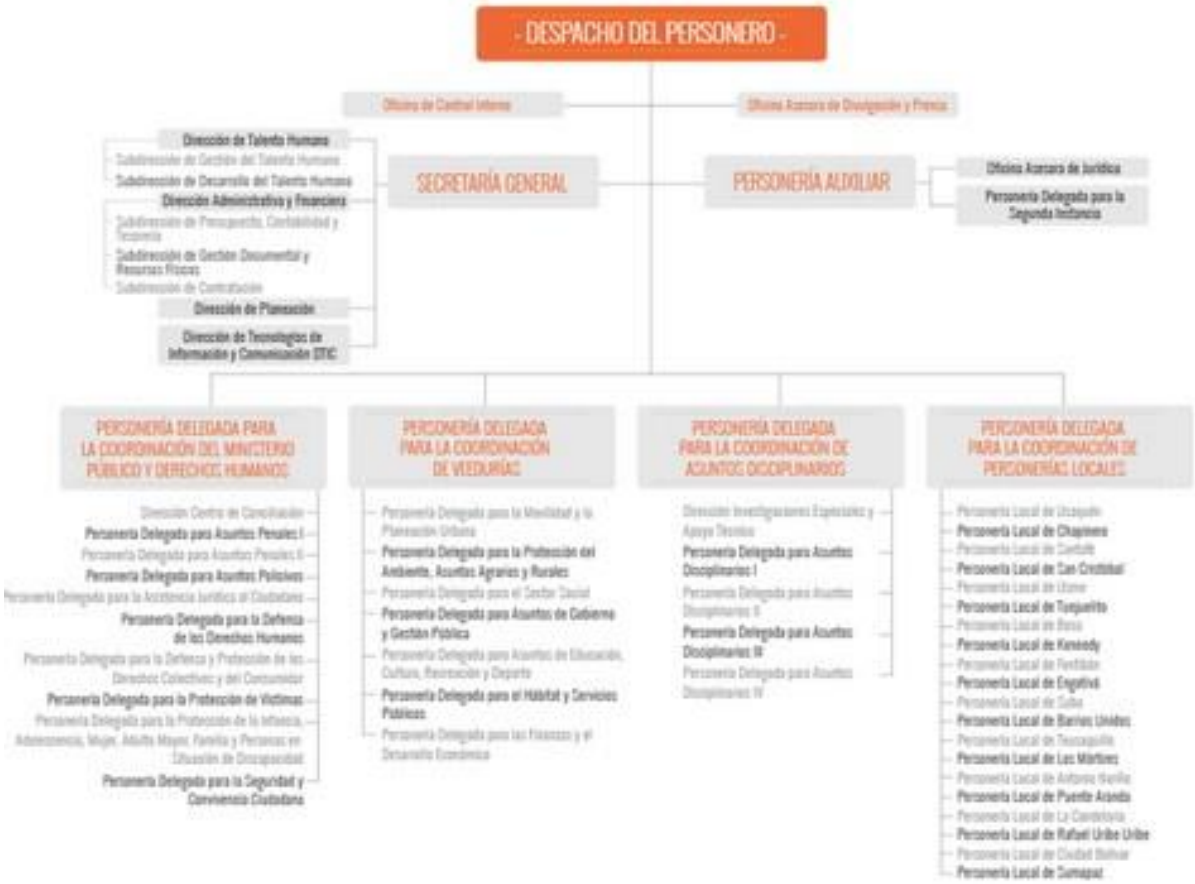
COBIT 5: Incorpora a sus lineamientos Risk IT. En este enfoque se establecen porcentajes específicos para las amenazas como hacking, pérdida de datos, ataques informáticos, satisfacción del personal, o errores no intencionados entre otros. Cuenta con una herramienta diseñada y desarrollada por ISACA para su cabal aplicación. Por ser un lineamiento de mejores prácticas indica la ruta a seguir pero deja a libre elección la metodología apropiada a cada organización.

2.2. MARCO CONTEXTUAL

La Personería de Bogotá es un órgano de control que cumple las funciones de Ministerio Público, vigilante de la conducta de los funcionarios públicos, ejerce Veedurías y promueve la defensa de los Derechos Humanos de los ciudadanos. Su naturaleza está establecida en los artículos 117 y 118 de la Constitución Política y en el artículo 104 del Decreto ley 1421 de 1993 (Estatuto Orgánico de Bogotá). Recientemente fue reestructurada mediante el Acuerdo 514 de 2012 del Concejo de Bogotá. Hay tres fuentes de funciones adicionales para la Personería resultantes de la Ley 1448 de 2011 (de víctimas), la Ley 1480 de 2011 (del consumidor) y la Ley 1551 de 2012 (modificatoria de la Ley 136 de 1994).

Por ser una entidad de control, le corresponde la guarda y promoción de los Derechos Humanos, la protección del interés público y la vigilancia de la conducta de los funcionarios públicos. Por lo anteriormente expuesto, es fundamental velar por la seguridad de su información, buscando mecanismos, equipos y procedimientos que contribuyan a minimizar los riesgos informáticos.

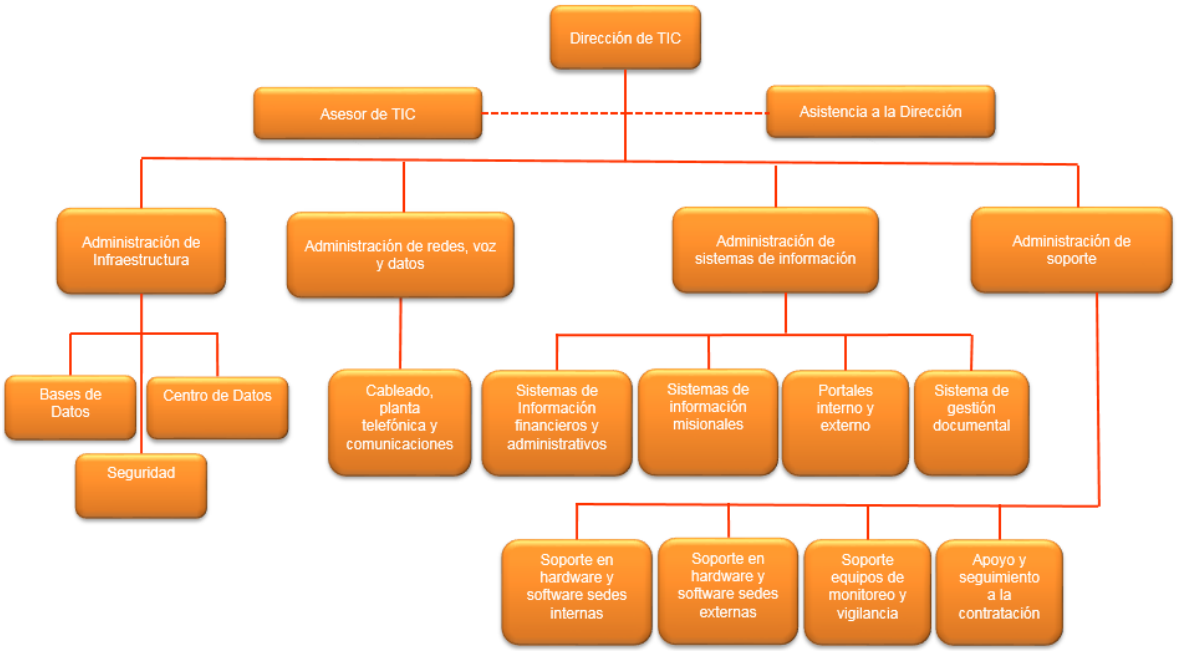
Figura 4. Organigrama



Fuente: Primer versión publicada en Intranet conforme al Acuerdo 514

La Dirección de TIC cuenta con una subdivisión de procesos internamente la cual se presenta a continuación:

Figura 5. Organización interna



Fuente: Las autoras

El centro de datos de la Personería concentra los servidores, aplicativos y administración de procesos y dispositivos críticos que soportan el eje funcional de la entidad; la no disponibilidad de los mismos puede causar consecuencias graves para la imagen institucional y el cumplimiento de su misión.

En los últimos años la Personería ha realizado avances para ofrecer mejorar los servicios prestados al ciudadano, por tal motivo es fundamental contar con una arquitectura de gestión de la seguridad que identifique y evalúe los riesgos que afectan al negocio, con el objetivo de implementar medidas de contraataque, procesos y procedimientos para su apropiado control, tratamiento y mejora.

2.3. MARCO LEGAL

Decreto 1360 de 1989: Por el cual se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor. Se define programa de computador, descripción de programa y material auxiliar.

Constitución Política de Colombia de 1991 (artículos 61 y 74): Es considerada como la carta magna de la República de Colombia y se le conoce como la Constitución de los Derechos Humanos. En sus artículos 61 y 74 hace referencia a la protección de la propiedad intelectual y al derecho que les asiste a todas las personas a acceder a los documentos públicos.

Ley 527 de 1999 (artículo 12): Define y reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y firmas digitales y dentro de ella en el artículo 12 se hace alusión a la conservación de los mensajes de datos y documentos.

Ley 594 de 2000 (artículos 19 y 21): Dicta la ley general de archivos y en su artículo 19 hace referencia a la incorporación de tecnologías de avanzada en la administración y conservación de archivos y en el 21 habla sobre los programas de gestión documental.

Ley 599 de 2000: Criterios adoptados para el cálculo de aumentos de penas.

Ley 1032 de 2006: De la prestación, acceso o uso ilegales de los servicios de telecomunicaciones. Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal.

Acuerdo 279 de 2007: Dicta los lineamientos para la política de promoción y uso del software libre en el sector central, el sector descentralizado y el sector de las localidades del distrito capital.

Ley 1273 de 2009: Modifica el código penal creando un bien tutelado, el de protección de la información y de los datos y se preservan los sistemas que utilizan las tecnologías de la información y las comunicaciones.

Ley 1286 de 2009: Modificatoria de la Ley 29 de 1990, se transforma a Colciencias en Departamento Administrativo, se fortalece el Sistema Nacional de Ciencia, Tecnología e Innovación en Colombia 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.

Ley 1288 de 2009: Fortalece el marco legal para llevar a cabo actividades de inteligencia y contrainteligencia.

Decreto 235 de 2010: Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.

Ley 1437 de 2011 (artículos 3 y 8): Es el código de procedimiento administrativo y en sus artículos 3 y 8 hace referencia a los principios y deber de información al público.

Ley 1474 de 2011: Medidas administrativas de lucha contra la corrupción. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública

Decreto Ley 19 de 2012: Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

Ley 1581 de 2012: Mediante la cual se dictan disposiciones generales para la protección de datos personales. Reglamentada parcialmente por el decreto nacional 1377 de 2013.

Decreto 2693 de 2012: Establece los lineamientos generales de la Estrategia de Gobierno en Línea.

Decreto 1377 de 2013: Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Decreto 886 de 2014: Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política.

Decreto 2573 de 2014: 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 1712 de 2014: Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Especialmente lo contenido en el Artículo 3º, en la lista de principios a aplicar, se tienen: Principio de transparencia, de buena fe, de gratuidad y de la calidad de la información.

Decreto 103 de 2015: Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Este decreto tiene por objeto reglamentar la Ley 1712 de 2014, en lo relativo a la gestión de la información pública.

Decreto 1494 de 2015: Corrige yerros de la Ley 1712 de 2014. Artículos 5, 18, 21 y 26.

Decreto 2199 de 2015: Corrige yerros de la Ley 1712 de 2014. Artículos 1 y 18.

3.METODOLOGÍA

Se toma como base la norma NTC-ISO-IEC 27001, la que utiliza el ciclo PDCA: Planear – Hacer- Verificar - Actuar. Divido en las siguientes etapas: Planificación, Ejecución, Seguimiento, Mantenimiento y Mejora y la metodología a emplear para realizar el análisis y formular un plan para gestionar los riesgos.

Cuadro 1. Metodología del proyecto

Etapa	Ciclo	Actividad
Planificación	Establecer el SGSI	Definir el alcance del SGSI Definir políticas de seguridad Definir la metodología de evaluación del riesgo Realizar inventario de activos Valoración de activos Identificar amenazas Identificar los riesgos Resumen de riesgos Seleccionar objetivos de control
Ejecución	Implementar y utilizar el SGSI	Definir un plan de tratamiento de riesgos en el cual se formulen los diferentes procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad Definir documento de declaración de aplicabilidad Proponer un Plan de Continuidad Sugerir documentación
Seguimiento	Monitorear y revisar el SGSI	Proponer procedimientos de monitorización y revisión
Mantenimiento y Mejora	Mantener y mejorar el SGSI	Sugerir acciones preventivas y correctivas sobre el SGSI

Fuente: Las autoras

La evaluación de riesgo se lleva a cabo mediante la evaluación empleando NTC-ISO-IEC 27001:2013, de igual forma se sustenta en la metodología Magerit[18].

[18] CONSEJO SUPERIOR DE ADMINISTRACION ELECTRÓNICA, MAGERIT V3., Metodología de análisis y gestión de riesgos de los sistemas de información. Ed. Ministerio de Hacienda y Administraciones

4. RESULTADOS

4.1.ETAPA 1 PLANIFICACIÓN

4.1.1.Alcance del Sistema de Gestión de Seguridad de la Información (SGSI)

El SGSI formulado se aplica a todo el conjunto de activos físicos tangibles e intangibles ubicados en el centro de datos de la Personería de Bogotá D.C. La presente, es una propuesta que inicialmente se delimita en una ubicación concreta, pero constituye la base para la formulación secuencial, meticulosa y ordenada de un SGSI institucional.

4.1.2.Metodología MAGERIT

De las metodologías analizadas se selecciona la metodología MAGERIT por ser bastante completa y detallada, incorporar la norma ISO-31000, se dirige principalmente a cualquier tipo de administración pública, ha sido mejorada hasta la versión 3, no deja margen a la improvisación, uno de los objetivos es concienciar a los miembros de la entidad sobre la existencia de los riesgos y la importancia de su gestión y, por último, porque al ser tan meticulosa en su desarrollo, ayuda a la entidad para poder afrontar los permanentes procesos de auditoría pues es una entidad de control.

4.1.3.Inventario de activos

La identificación de los activos es necesaria para poder evaluar su valor y el riesgo al que están expuestos.

Los activos que se encuentran en el centro de datos de la Personería de Bogotá, se relacionan en el cuadro 2., se clasificaron por datos de información, servicios, aplicaciones, equipamiento informático, redes y comunicaciones, equipo auxiliar, personal, e instalaciones, basados en la metodología Magerit, en su libro II Catálogo de elementos[19].

[19] Públicas, España, octubre de 2012. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Cuadro 2. Activos centro de datos

TIPO	CODIGO	NOMBRE DEL ACTIVO	DESCRIPCION DEL ACTIVO
DATOS / INFORMACION	BD_INT	Base de Datos INTRANET	Base de Datos Oracle de la página web interna de la entidad.
	BD_WEB	Base Datos Mysql	Bases de datos Mysql de la página web.
	BD_ORCL	Base Datos ORCL	Bases de datos Oracle portal
	BD_SICAPITA	Base Datos SICAPITA	Sistema Administrativo y Financiero
	BD_WEBOIDO	Base Datos WEBOIDO	Bases de datos Oracle de los aplicativos de centros comerciales, radar, Sinproc, requerimientos ciudadanos
	BD_SIAFI2	Base de datos SIAFI2	Bases de datos Oracle de aplicativo de correspondencia
	BD_RAD	Base de datos radar	Base de datos Postgresql del aplicativo rutas de soluciones
	BD_CVIS	Base de datos Control de visitantes	Registro de todos los visitantes a las oficinas en la sede Central
	BD_DIG	Base de datos Digiturno 4.5	Registro de todos los visitantes atendidos por Digiturno
	ANT_DIG	Datos digitales Antecedentes firmados digitalmente	Archivos de expedición de antecedentes vía web con firma digital
	DAT_CORR	Datos Digitales Correspondencia externa recibida escaneada	Archivos de carga de documentos escaneados
	INF	Información	Audiencias públicas grabadas en salas y pasadas a CDs
	FTE_SINPROC	Código fuente SINPROC	Fuentes y compilados de la aplicación Sistema Integrado de procesos
	FTE_SICAPITA	Código fuente SICAPITA	Fuentes y compilados de la aplicación Sistema Administrativo y Financiero
	FTE_ANTEC	Código fuentes antecedentes digitales	Fuentes antecedentes digitales
	FTE_RCIU	Código fuente Sistema Requerimientos Ciudadanos	Fuentes aplicativo Sistema Requerimientos Ciudadanos
	DOC	Documentación	Documentación

Cuadro 2. (Continuación)

TIPO	CODIGO	NOMBRE DEL ACTIVO	DESCRIPCION DEL ACTIVO
DATOS / INFORMACION	FTE_RAD	Código Fuente de Radar	Fuentes del aplicativo rutas de soluciones
	REG_VIR	Registros de consola de antivirus	Registro de estaciones matriculadas en la base de datos y repositorio distribuido de las descargas de DATS
	FTE_INT	Código Fuente de la Intranet	Fuentes de la página web interna de la entidad
	FTE_WEB	Código Fuente del Portal Web	Fuentes de la página web de la entidad
SERVICIOS	WEB	Portal Web	Página web de la entidad
	CORDIS	CORDIS	Aplicativo de manejo de correspondencia
	SINPROC	SINPROC	Sistema integrado de procesos
	INTRANET	INTRANET	Página web interna
	PERNO	PERNO	Aplicativo manejo de la nomina
	CEN_COM	Centros Comerciales	Aplicativo centros comerciales
	REQ_CIU	Requerimientos Ciudadanos	Aplicativo requerimientos ciudadanos
	GLASS	Glassfish	Servicio para la interacción de los servicios de intranet.
	ANT_DISC	Antecedentes Disciplinarios	Consulta de antecedentes disciplinarios
	DESP	Desprendibles	Desprendibles de pago funcionarios de planta
	RADAR	Radar	Aplicativo rutas de soluciones
	SICAPITA	SICAPITA	Aplicativo Sistema Administrativo y Financiero
APLICACIONES	CORREO	Correo electrónico	Correo electrónico Google
	DHCP	SAMBA (DHCP)	Servicio de asignación de direcciones IP

Cuadro 2. (Continuación)

TIPO	CODIGO	NOMBRE DEL ACTIVO	DESCRIPCION DEL ACTIVO
APLICACIONES	CORREO	Correo electrónico	Correo electrónico Google
	DHCP	SAMBA (DHCP)	Servicio de asignación de direcciones IP
	SO_WIN	Sistema Operativo Windows Server	Sistema operativo Windows Server
	SO_LINUX	Sistema Operativo Linux	Sistema operativo Linux distribuciones: Debian, ubuntu, Redhat, Centos
	SO_AIX	Sistema Operativo Unix AIX	Sistema operativo AIX
	LDAP	LDAP	Sistema de Autenticación
	NAGIOS	Nagios	Sistema de monitoreo servidores, router, locales y servicios
	DIGIT	Digiturno	Sistema para el control de atención de los visitantes
	CACCES	Control de acceso	Control de acceso al Centro de Computo y dirección de TIC
	DNS	DNS Interno	Resolución de nombres interno
	A_VIRUS	Antivirus	Sistema control de virus McAfee
	PCSEG	PCSecure	Software Seguridad
EQUIPAMIENTO INFORMATICO	FW	Firewall	Apliance para el control de contenidos, reglas de acceso lógico y zonificación de la red (DMZ. LAN, WAN, Externa)
	RED	Servidores de red	Servidores por los cuales se presta el servicio de red a los usuarios
	BD	Servidor de Base de datos	Manejo de Bases de datos
	SER_WEB	Servidor de WEB	Página WEB
	SER_INT	Servidor de Intranet	Intranet
	SER_ANT	Servidor de Consola Antivirus	Consola antivirus McAfee
	SER_RADAR	Servidor Radar	Servidor aplicativo rutas de soluciones
	SER_APP	Servidor Aplicativos	Servidor principal de Aplicaciones misionales de la entidad
	SER_MON	Servidor de Monitoreo	Monitoreo servicios, conexión a locales, servidores, swtiches
	SER_ARC	Servidor de Archivos	Información almacenada y compartida para usuarios internos

Cuadro 2. (Continuación)

TIPO	CODIGO	NOMBRE DEL ACTIVO	DESCRIPCION DEL ACTIVO
EQUIPAMIENTO INFORMATICO	SER_ACC	Servidor control de acceso	Control de acceso al Centro de Computo y dirección de TIC
	SER_TEL	Servidor de Telefonía.	Sistema que controla la comunicación vía VOZ IP en la entidad
	SER_NOM	Servidor de Nomina	Servidor nomina
	SER_DIG	Servidor Digiturno	Servidor control atención a usuarios
REDES DE COMUNICACIONES	INTERNET	Conexión a internet canal dedicado	Permite la conexión a Internet
	TEL	Conexión telefonía IP	Conexión Telefonía a través de Voz IP
	LOCAL	Conexión dedicado locales	Canal dedicado a locales
	SWITCH	Switches	Dispositivos de comunicación
	CORE	Core	Dispositivo principal de red local
	WIREL	Red inalámbrica	Conexión inalámbrica
	LAN	Red de área local	Conexión de la red interna
EQUIPAMIENTO AUXILIAR	CAB_RED	Cableado de Red	Ayuda a la comunicación del centro de cableado principal con los demás centros de datos
	CAB_ELEC	Cableado eléctrico	Provee energía a las instalaciones del centro de computo
	TARJETAS	Tarjeta de identificación	Tarjeta para permitir el ingreso
	RACK	Racks	Alojamiento de servidores y dispositivos
	USO	UPS	Provee energía temporal, en caso de interrupción del fluido eléctrico
	AIRE	Aire Acondicionado	Ayuda a mantener la temperatura adecuada en el centro de computo
INSTALACIONES	CC	Centro de Computo	Área dentro de computo
	DTIC	Dirección de Tecnología	Área de la dirección de TIC
PERSONAL	DIRECTOR	Director de sistemas	Jefe dirección
	DBA	Administrador de BD	Administradores de Base de datos
	ADMIN	Administradores del Sistema	Administradores de infraestructura
	SOPORTE	Técnicos soporte	Funcionarios soporte técnico

Cuadro 2. (Continuación)

TIPO	CODIGO	NOMBRE DEL ACTIVO	DESCRIPCION DEL ACTIVO
PERSONAL	ADMIN_RED	Administradores de Red	Administradores servicio de comunicaciones
	ADMIN_AP	Ingenieros administradores aplicativos	Administradores de aplicativos
	ADMIN_TEL	Administrador telefonía	Administración servicios Voz IP
	SEGUR	Administrador Seguridad	Oficial de seguridad
	PROVEE	Proveedores	Proveedores de servicios

Fuente. Las autoras

4.1.4.Valoración de activos

Para valorar los activos tomaremos las siguientes dimensiones de seguridad:

[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos

- Confidencialidad: ¿qué daño causaría que lo conociera quien no debe?
- Integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto?
- Disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?
- Autenticidad: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
- Trazabilidad del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? ¿quién hace qué y cuándo?

En el siguiente cuadro se presenta la escala de valores que se utilizará para la evaluación de los activos.

Cuadro 3. Escala de valores para los activos

Valor			Criterio
10	Muy alto	MA	Daño muy grave a la entidad.
7-9	Alto	A	Daño grave a la entidad.
4-6	Medio	M	Daño importante a la entidad.
1-3	Bajo	B	Daño menor a la entidad.
0	Despreciable	D	Irrelevante

Fuente. Metodología Magerit

Cuadro 4. Valoración de activos

TIPO	NOMBRE DEL ACTIVO	D	I	C	A	T
DATOS / INFORMACION	Base de Datos INTRANET	M	A	A	A	A
	Base Datos Mysql	MA	A	A	MA	A
	Base Datos ORCL	M	A	A	M	M
	Base Datos SICAPITA	MA	MA	A	MA	MA
	Base Datos WEBOIDO	MA	MA	A	A	A
	Base de datos SIAFI2	A	A	A	A	A
	Base de datos radar	B	A	M	B	B
	Base de datos Control de visitantes	A	A	B	D	B
	Base de datos Digiturno 4.5	B	A	A	M	A
	Datos digitales Antecedentes firmados digitalmente	MA	MA	MA	A	A
	Datos digitales Correspon externa recibida escan.	A	A	A	A	A
	Datos Digitales videos Ministerio Publico	MA	A	A	A	A
	Código fuente SINPROC	A	M	M	A	A
	Código fuente SICAPITA	B	MA	A	A	A
	Código fuentes antecedentes digitales	A	MA	MA	M	M
	Código fuente Sistema Requerimientos Ciudadanos	A	A	A	A	A
	Documentación	A	M	A	A	MA
	Código Fuente de Radar	M	A	A	M	M
	Registros de consola de antivirus	D	B	A	B	A
	Código Fuente de la Intranet	M	A	A	A	M
	Código Fuente del Portal Web	B	A	A	B	B
SERVICIOS	Portal Web	A	A	A	M	M
	CORDIS	A	A	MA	MA	A
	SINPROC	A	MA	A	A	A
	INTRANET	M	A	A	M	M
	PERNO	MA	MA	MA	MA	MA
	Centros Comerciales	A	A	MA	A	A
	Requerimientos Ciudadanos	A	MA	MA	A	A
	Glassfish	B	M	M	M	B
	Antecedentes Disciplinarios	A	MA	MA	MA	MA
	Desprendibles	MA	A	B	A	A
	Radar	B	A	B	B	B
	SICAPITA	A	MA	MA	A	A

Cuadro 4. (Continuación)

TIPO	NOMBRE DEL ACTIVO	D	I	C	A	T
APLICACIONES	Correo electrónico	MA	A	A	MA	A
	SAMBA (DHCP)	B	MA	MA	M	M
	Sistema Operativo Windows Server	M	M	M	B	B
	Sistema Operativo Linux	M	MA	MA	M	M
	Sistema Operativo Unix AIX	M	M	M	M	M
	LDAP	M	MA	MA	B	B
	Nagios	D	B	B	B	B
	Digiturno	B	A	A	A	M
	Control de acceso	B	M	B	B	B
	DNS Interno	B	A	A	B	B
	Antivirus	D	A	A	D	D
	PCSecure	B	A	A	M	M
EQUIPAMIENTO INFORMATICO	Firewall	B	MA	MA	A	A
	Servidores de red	B	MA	MA	B	B
	Servidor de Base de datos	MA	MA	MA	A	A
	Servidor de WEB	A	A	A	M	M
	Servidor de Intranet	M	M	M	B	B
	Servidor de Consola Antivirus	D	A	A	D	D
	Servidor Radar	B	A	B	B	B
	Servidor Aplicativos	A	MA	MA	A	A
	Servidor de Monitoreo	B	B	B	B	D
	Servidor de Archivos	A	MA	MA	A	A
	Servidor control de acceso	D	B	B	B	B
	Servidor de Telefonía	B	MA	MA	A	A
	Servidor de Nomina	MA	MA	MA	A	A
	Servidor Digiturno	M	A	A	M	M
REDES DE COMUNICACIONES	Conexión a internet canal dedicado	M	MA	MA	A	A
	Conexión telefonía IP	M	MA	MA	A	A
	Conexión dedicado locales	D	A	A	M	M
	Switches	A	A	MA	A	A
	Core	A	MA	MA	A	A
	Red inalámbrica	M	M	M	B	B
	Red de área local	M	A	MA	A	A

Cuadro 4. (Continuación)

TIPO	NOMBRE DEL ACTIVO	D	I	C	A	T
EQUIPAMIENTO AUXILIAR	Cableado de Red	B	A	MA	B	B
	Cableado eléctrico	B	A	MA	B	B
	Tarjeta de identificación	M	M	M	M	M
	Racks	D	B	B	B	B
	UPS	D	A	MA	B	B
	Aire Acondicionado	D	A	MA	B	B
INSTALACIONES	Centro de Computo	D	A	MA	A	A
	Dirección de Tecnología	D	M	M	B	B
PERSONAL	Director de sistemas	A	A	A	A	A
	Administrador de BD	A	MA	MA	A	A
	Administradores del Sistema	A	MA	MA	A	A
	Técnicos soporte	M	M	M	M	M
	Administradores de Red	A	MA	MA	A	A
	Ingenieros administradores aplicativos	A	MA	MA	A	A
	Administrador telefonía	A	MA	MA	A	A
	Administrador Seguridad	A	A	A	A	A
	Proveedores	A	A	A	A	A

Fuente. Las autoras

De acuerdo al cuadro 4 podemos determinar que los activos más significativos para la entidad son las Bases de datos misionales: Sicapita, Weboido, Siafi2 y las de los antecedentes digitales los cuales están ligados con la misión de la entidad. En cuanto al equipamiento informático son transcendentales los servidores de red, firewall, de base de datos, nómina y aplicativos. En equipos de comunicación son importantes el core, el canal de internet, la telefonía, y en prioridad también se encuentran las personas en especial los administradores de los diferentes sistemas y los servicios que afectan el desarrollo de la misión de la entidad como son los de requerimientos ciudadanos, antecedentes disciplinarios, correo, sinproc y cordis. La falla en cualquiera de estos activos afectaría la operación de la Personería y la correcta realización de las labores misionales.

4.1.5.Identificación de amenazas

Las siguientes amenazas se tomaron del Catálogo de Elementos de la metodología MAGERIT, los cuales son mostrados en el Anexo B. Tipos de amenazas según la metodología MAGERIT.

Cuadro 5. Frecuencia de amenazas

Valor		Criterio
MA	muy alta	casi seguro
A	alta	muy alto
M	media	posible
B	baja	poco probable
MB	muy baja	muy raro

Fuente. Las autoras

Cuadro 6. Identificación y valoración de amenazas

Tipo	Amenazas	Frecuencia	Dimensiones de Seguridad				
			D	I	C	A	T
[DA] DATOS / INFORMACION							
E.1	Errores de los usuarios	A	B	M	B	B	B
E.2	Errores del administrador del sistema/ de la seguridad	M	M	M	B	M	M
E.15	Alteración de la información	M	B	M	M	B	M
E.18	Destrucción de la información	B	B	B	B	B	B
E.19	Fugas de información	M	M	M	M	B	M
A.5	Suplantación de la identidad	B	B	B	M	B	B
A.6	Abuso de privilegios de acceso	M	M	M	M	B	B
A.11	Acceso no autorizado	M	M	M	M	M	M
A.15	Modificación de la información	M	M	M	M	B	B
A.18	Destrucción de la información	B	B	B	B	MB	B
A.19	Revelación de información	M	M	M	M	B	M
[SI]SERVICIOS INTERNOS							
E.1	Errores de los usuarios	MA	M	MA	MA	M	MA
E.2	Errores del administrador del sistema/ de la seguridad	M	M	M	B	M	M
E.15	Alteración de la información	M	B	M	M	B	M
E.18	Destrucción de la información	M	MA	M	M	M	M
E.19	Fugas de información	M	M	M	M	B	M
E.24	Caída del sistemas por agotamiento de recursos	A	MA	A	A	A	A
A.5	Suplantación de la identidad	A	MA	A	MA	A	A
A.6	Abuso de privilegios de acceso	A	M	MA	A	A	A
A.7	Uso no previsto	A	A	M	MA	A	A
A.11	Acceso no autorizado	M	M	A	M	M	M
A.13	Repudio (negación de actuaciones)	A	A	A	A	A	A

Cuadro 6. (Continuación)

Tipo	Amenazas	Frecuencia	Dimensiones de Seguridad				
			D	I	C	A	T
[SI]SERVICIOS INTERNOS							
A.15	Modificación de la información	M	M	B	M	B	M
A.18	Destrucción de la información	B	B	B	B	B	B
A.19	Revelación de información	A	A	MA	A	B	B
A.24	Denegación de servicio	M	M	A	M	M	A
[E] EQUIPAMIENTO							
[SW] APLICACIONES							
I.5	Avería de origen físico o lógico	A	A	A	A	B	B
E.1	Errores de los usuarios	M	M	M	M	MB	MB
E.2	Errores del administrador del sistema/ de la seguridad	M	A	M	M	M	M
E.8	Difusión de software dañino	A	A	A	A	M	M
E.15	Alteración de la información	M	M	M	M	MB	MB
E.18	Destrucción de la información	M	M	M	M	MB	MB
E.19	Fugas de información	M	M	M	M	MB	MB
E.20	Vulnerabilidades de los programas (software)	M	M	M	M	B	MB
E.21	Errores de mantenimiento /actualización de programas	A	A	A	A	A	A
A.5	Suplantación de la identidad	M	MB	M	M	MB	M
A.6	Abuso de privilegios de acceso	A	A	A	A	M	M
A.7	Uso no previsto	M	M	M	M	M	M
A.11	Acceso no autorizado	M	M	M	MA	B	M
A.15	Modificación de la información	M	M	M	M	MB	M
A.18	Destrucción de la información	M	MA	M	M	M	M
A.19	Revelación de información	M	M	MA	M	MB	M
A.22	Manipulación de programas	MA	A	MA	MA	A	MA
[HW] EQUIPOS							
N.1	Fuego	B	B	B	B	B	B
N.2	Daños por agua	B	B	B	B	B	B
N.3	Desastres naturales	B	B	B	B	B	B
I.3	Desastres industriales	B	B	B	B	B	B
I.5	Avería de origen físico o lógico	M	M	M	M	B	B
I.7	Corte del suministro eléctrico	M	A	A	M	M	M
E.2	Errores de mantenimiento /actualización de equipos	M	M	M	M	M	M

Cuadro 6. (Continuación)

Tipo	Amenazas	Frecuencia	Dimensiones de Seguridad				
			D	I	C	A	T
E.24	Caída del sistemas por agotamiento de recursos	A	A	A	A	M	A
E.25	Perdida de equipos	B	B	B	B	B	B
A.6	Abuso de privilegios de acceso	M	M	M	M	M	M
A.7	Uso no previsto	M	M	M	M	M	M
A.11	Acceso no autorizado	M	M	M	M	M	M
A.23	Manipulación de hardware	A	A	A	A	M	M
A.24	Denegación de servicio	M	M	M	M	MB	MB
A.25	Robo de equipos	B	B	B	B	B	B
A.26	Ataque destructivo	B	B	B	B	B	B
[COM] REDES DE COMUNICACIONES							
I.8	Fallo de servicio de comunicaciones	M	M	M	M	M	M
E.2	Errores del administrador del sistema/ de la seguridad	M	M	M	M	MB	MB
E.9	Errores de [re]encaminamiento	M	M	M	M	M	M
E.10	Errores de secuencia	M	M	M	M	MB	MB
E.15	Alteración de la información	M	M	M	M	M	M
E.19	Fugas de información	M	M	M	MA	M	M
E.24	Caída del sistemas por agotamiento de recursos	A	A	A	A	M	M
A.5	Suplantación de la identidad	M	M	M	M	M	M
A.6	Abuso de privilegios de acceso	A	A	A	A	A	A
A.7	Uso no previsto	M	M	M	M	M	M
A.9	[Re-]encaminamiento de mensajes	M	M	MA	M	A	M
A.10	Alteración de secuencia	M	M	M	M	M	M
A.11	Acceso no autorizado	M	M	M	M	M	MB
A.12	Análisis de tráfico	A	M	A	MA	A	A
A.14	Interceptación de información (escucha)	A	A	A	A	MB	A
A.15	Modificación de la información	M	M	MA	M	M	M
A.18	Destrucción de la información	M	M	MA	M	M	M
A.19	Revelación de información	M	M	MA	M	M	M
A.24	Denegación de servicio	M	MA	M	M	M	M
A.26	Ataque destructivo	B	B	B	B	B	B
[AUX] EQUIPAMIENTO AUXILIAR							
N.*	Desastres naturales	B	B	B	B	B	B

Cuadro 6. (Continuación)

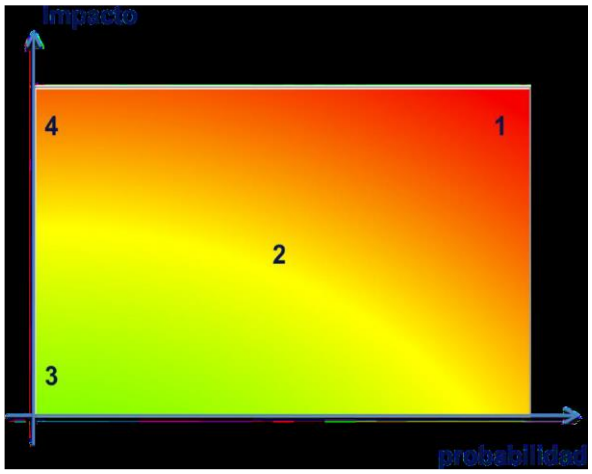
Tipo	Amenazas	Frecuencia	Dimensiones de Seguridad				
			D	I	C	A	T
E.23	Errores de manteniendo / actualización de equipos (hardware)	B	B	B	B	B	B
A.7	Uso no previsto	B	B	B	B	B	B
A.23	Manipulación del hardware	M	M	M	M	M	M
A.26	Ataque destructivo	B	B	B	B	B	B
A.11	Acceso no autorizado	M	M	M	M	B	B
I.3	Contaminación medioambiental	B	B	B	B	B	B
I.2	Daños por agua	B	B	B	B	B	B
N.1	Fuego	B	B	B	B	B	B
[I] INSTALACIONES							
N.1	Fuego	B	B	B	B	B	B
N.2	Daños por agua	B	B	B	B	B	B
N.*	Desastres naturales	B	B	B	B	B	B
I.1	Fuego	B	B	B	B	B	B
I.2	Daños por agua	B	B	B	B	B	B
I.*	Desastres industriales	B	B	B	B	B	B
I.3	Contaminación electromagnética	B	B	B	B	B	B
A.5	Suplantación de la identidad	M	M	M	M	M	M
A.6	Abuso de privilegios de acceso	M	M	M	M	MB	M
A.7	Uso no previsto	M	M	M	M	M	M
A.11	Acceso no autorizado	M	M	M	M	M	M
A.26	Ataque destructivo	B	B	B	B	B	B
[P] PERSONAL							
E.15	Alteración de la información	M	M	M	M	M	M
E.18	Destrucción de la información	M	A	M	M	M	M
E.19	Fugas de información	A	A	A	A	A	A
E.28	Indisponibilidad de la información	B	B	B	MB	B	B
A.15	Modificación de la información	M	M	MA	M	M	M
A.19	Revelación de información	A	A	A	A	M	M
A.28	Indisponibilidad del personal	A	A	A	A	M	M
A.29	Extorsión	B	B	B	B	B	B
A.30	Ingeniería social	M	M	M	M	M	A

Fuente. Las autoras

4.1.6. Impacto del riesgo

- MB: muy bajo
- B: bajo
- M: medio
- A: alto
- MA: muy alto

Figura 6. El riesgo en función del impacto y la probabilidad.



Zonas:

•Zona 1 – riesgos muy probables y de muy alto impacto; posiblemente nos planteemos sacar-los de esta zona

•Zona 2 – riesgos de probabilidad relativa e impacto medio; se pueden tomar varias opciones

•Zona 3 – riesgos improbables y de bajo impacto; o los dejamos como están, o permitimos que suban a mayores si ello nos ofreciera alguna ventaja o beneficio en otro terreno

•Zona 4 – riesgos improbables pero de muy alto impacto; suponen un reto de decisión pues su improbabilidad no justifica que se tomen medidas preventivas, pero su elevado impacto exige que tengamos algo previsto para reaccionar.

Fuente. MAGERIT versión 3.0- Libro I Método

Cuadro 7. Impacto del riesgo

Tipo	Amenaza	Frecuencia Residual	Impacto	Proba-bilidad	Zona Riesgo
[DA] DATOS / INFORMACION					
E.1	Errores de los usuarios	A	MA	M	4
E.2	Errores del administrador del sistema/ de la seguridad	M	MA	M	4
E.15	Alteración de la información	M	MA	M	4
E.18	Destrucción de la información	B	MA	B	4
E.19	Fugas de información	M	MA	M	4
A.5	Suplantación de la identidad	B	MA	B	4
A.6	Abuso de privilegios de acceso	M	MA	M	4
A.11	Acceso no autorizado	M	MA	M	4
A.15	Modificación de la información	M	MA	M	4
A.18	Destrucción de la información	B	MA	B	4
A.19	Revelación de información	M	MA	M	4

Cuadro 7. (Continuación)

Tipo	Amenaza	Frecuencia Residual	Impacto	Proba-bilidad	Zona Riesgo
[IS]SERVICIOS INTERNOS					
E.1	Errores de los usuarios	MA	MA	MA	1
E.2	Errores del administrador del sistema/ de la seguridad	M	MA	M	4
E.15	Alteración de la información	M	MA	M	4
E.18	Destrucción de la información	M	A	M	4
E.19	Fugas de información	M	A	M	4
E.24	Caída del sistemas por agotamiento de recursos	A	MA	A	1
A.5	Suplantación de la identidad	A	MA	A	1
A.6	Abuso de privilegios de acceso	A	A	MA	1
A.7	Uso no previsto	A	A	M	4
A.11	Acceso no autorizado	M	A	M	4
A.13	Repudio (negación de actuaciones)	A	A	M	4
A.15	Modificación de la información	M	A	B	2
A.18	Destrucción de la información	B	A	B	2
A.19	Revelación de información	A	A	MA	1
A.24	Denegación de servicio	M	A	A	4
[E] EQUIPAMIENTO					
[SW] APLICACIONES					
I.5	Avería de origen físico o lógico	A	A	A	4
E.1	Errores de los usuarios	M	MA	A	1
E.2	Errores del administrador del sistema/ de la seguridad	M	MA	A	1
E.8	Difusión de software dañino	A	MA	A	1
E.15	Alteración de la información	M	MA	M	4
E.18	Destrucción de la información	M	A	M	4
E.19	Fugas de información	M	A	M	4
E.20	Vulnerabilidades de los programas (software)	M	MA	M	4
E.21	Errores de mantenimiento /actualización de programas	A	A	A	4
A.5	Suplantación de la identidad	M	A	M	4
A.6	Abuso de privilegios de acceso	A	A	A	4
A.7	Uso no previsto	M	A	M	4
A.11	Acceso no autorizado	M	A	M	4

Cuadro 7. (Continuación)

Tipo	Amenaza	Frecuencia Residual	Impacto	Proba-bilidad	Zona Riesgo
[SW] APLICACIONES					
A.15	Modificación de la información	M	A	M	4
A.18	Destrucción de la información	M	MA	M	4
A.19	Revelación de información	M	M	MA	1
A.22	Manipulación de programas	MA	A	MA	1
[HW] EQUIPOS					
N.1	Fuego	B	A	B	2
N.2	Daños por agua	B	A	B	2
N.3	Desastres naturales	B	MA	B	4
I.3	Desastres industriales	B	A	B	2
I.5	Avería de origen físico o lógico	M	MA	M	4
I.7	Corte del suministro eléctrico	M	A	A	4
E.2	Errores de mantenimiento /actualización de equipos	M	A	M	4
E.24	Caída del sistemas por agotamiento de recursos	A	A	A	4
E.25	Perdida de equipos	B	A	B	2
A.6	Abuso de privilegios de acceso	M	A	M	4
A.7	Uso no previsto	M	A	M	4
A.11	Acceso no autorizado	M	A	M	4
A.23	Manipulación de hardware	A	A	A	4
A.24	Denegación de servicio	M	MA	M	4
A.25	Robo de equipos	B	A	B	2
A.26	Ataque destructivo	B	A	B	2
[COM] REDES DE COMUNICACIONES					
I.8	Fallo de servicio de comunicaciones	M	MA	M	4
E.2	Errores del administrador del sistema/ de la seguridad	M	A	M	4
E.9	Errores de [re]encaminamiento	M	A	M	4
E.10	Errores de secuencia	M	A	M	4
E.15	Alteración de la información	M	A	M	4
E.19	Fugas de información	M	MA	M	4
E.24	Caída del sistemas por agotamiento de recursos	A	A	A	4
A.5	Suplantación de la identidad	M	A	M	4

Cuadro 7. (Continuación)

Tipo	Amenaza	Frecuencia Residual	Impacto	Proba-bilidad	Zona Riesgo
A.6	Abuso de privilegios de acceso	A	A	A	4
A.7	Uso no previsto	M	A	M	4
A.9	[Re-]encaminamiento de mensajes	M	A	A	4
A.10	Alteración de secuencia	M	A	M	4
A.11	Acceso no autorizado	M	MA	M	4
A.12	Análisis de tráfico	A	A	A	4
A.14	Interceptación de información (escucha)	A	A	A	4
A.15	Modificación de la información	M	MA	M	4
A.18	Destrucción de la información	M	MA	M	4
A.19	Revelación de información	M	MA	M	4
A.24	Denegación de servicio	M	MA	M	4
A.26	Ataque destructivo	B	A	B	2
[AUX] EQUIPAMIENTO AUXILIAR					
N.*	Desastres naturales	B	A	B	2
E.23	Errores de mantenimiento / actualización de equipos (hardware)	B	MA	B	4
A.7	Uso no previsto	B	A	B	2
A.23	Manipulación del hardware	M	MA	M	4
A.26	Ataque destructivo	B	A	B	2
A.11	Acceso no autorizado	M	MA	M	4
I.3	Contaminación medioambiental	B	A	B	2
I.2	Daños por agua	B	A	B	2
N.1	Fuego	B	A	B	2
[I] INSTALACIONES					
N.1	Fuego	B	A	B	2
N.2	Daños por agua	B	MA	B	4
N.*	Desastres naturales	B	A	B	2
I.1	Fuego	B	A	B	2
I.*	Desastres industriales	B	M	B	2
I.3	Contaminación electromagnética	B	M	B	2
A.5	Suplantación de la identidad	M	M	M	2
A.6	Abuso de privilegios de acceso	M	A	M	4
A.7	Uso no previsto	M	M	M	2
A.11	Acceso no autorizado	M	A	M	4

Cuadro 7. (Continuación)

Tipo	Amenaza	Frecuencia Residual	Impacto	Proba-bilidad	Zona Riesgo
A.26	Ataque destructivo	B	A	B	2
[P] PERSONAL					
E.15	Alteración de la información	M	A	M	4
E.18	Destrucción de la información	M	MA	M	4
E.19	Fugas de información	A	MA	A	1
E.28	Indisponibilidad de la información	B	A	B	2
A.15	Modificación de la información	M	MA	MA	1
A.19	Revelación de información	A	MA	A	1
A.28	Indisponibilidad del personal	A	MA	A	1
A.29	Extorsión	B	A	B	2
A.30	Ingeniería social	M	MA	M	4

Fuente. Las autoras

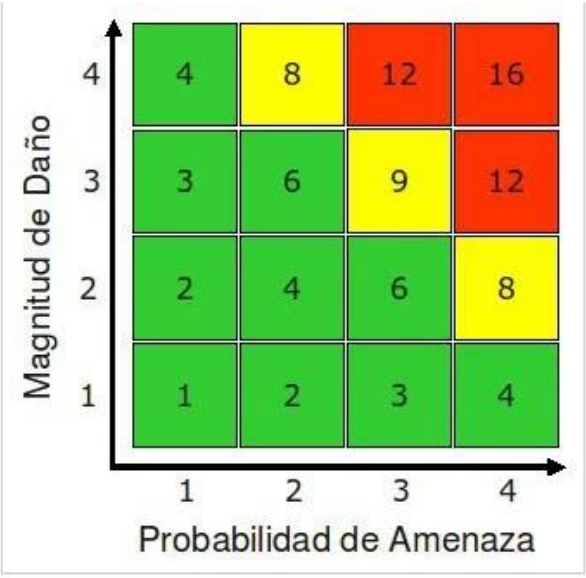
4.1.7.Identificación de riesgos

El resultado de la matriz es el resultado de la valoración de la magnitud de daño para cada activo multiplicado con la probabilidad de amenaza: Riesgo = Probabilidad de Amenaza x Magnitud de Daño

Figura 7. Matriz riesgo

Valores probabilidad de amenaza y de magnitud del daño:
1=Insignificante
2=Baja
3=Mediana
4=Alta

Riesgo bajo: 1- 6
Riesgo medio: 8 -9
Riesgo alto: 12- 16



Fuente: https://protejete.wordpress.com/gdr_principal/matriz_riesgo/

Cuadro 8. Matriz identificación de riesgos

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]										
Datos e Información	Clasificación			Magnitud de Daño:	DATOS / INFORMACIÓN										
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)	1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto	Errores de los usuarios	Errores del administrador del sistema/ de la seguridad	Alteración de la información	Destrucción de la información	Fugas de información	Suplantación de la identidad	Abuso de privilegios de acceso	Acceso no autorizado	Modificación de la información	Destrucción de la información	Revelación de información
					3	3	3	2	3	2	3	2	2	3	2
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	x	x	x	3	9	9	9	6	9	6	9	6	6	9	6
Base de Datos INTRANET	x		x	3	9	9	9	6	9	6	9	6	6	9	6
Base Datos Mysql	x		x	4	12	12	12	8	12	8	12	8	8	12	8
Base Datos ORCL			x	1	3	3	3	2	3	2	3	2	2	3	2
Base Datos SICAPITA	x	x	x	4	12	12	12	8	12	8	12	8	8	12	8
Base Datos WEBOIDO	x	x	x	4	12	12	12	8	12	8	12	8	8	12	8
Base de datos SIAFI2	x	x	x	4	12	12	12	8	12	8	12	8	8	12	8

Base de datos radar	x		x	3	9	9	9	6	9	6	9	6	6	9	6
Base de datos Control de visitantes	x	x	x	3	9	9	9	6	9	6	9	6	6	9	6

Cuadro 8. (Continuación)

Datos e Información	Clasificación			Magnitud de Daño: 1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto	DATOS / INFORMACIÓN										
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)		Errores de los usuarios	Errores del administrador del sistema/ de la seguridad	Alteración de la información	Destrucción de la información	Fugas de información	Suplantación de la identidad	Abuso de privilegios de acceso	Acceso no autorizado	Modificación de la información	Destrucción de la información	Revelación de información
					3	3	3	2	3	2	3	2	2	3	2
Base de datos Digiturno 4.5	x		x	3	9	9	9	6	9	6	9	6	6	9	6
Datos digitales Antecedentes firmados digitalmente	x	x		4	12	12	12	8	12	8	12	8	8	12	8
Datos Digitales Correspondencia externa recibida escaneada	x	x	x	3	9	9	9	6	9	6	9	6	6	9	6
Datos Digitales videos Ministerio Publico	x	x	x	4	12	12	12	8	12	8	12	8	8	12	8
Código fuente SINPROC			x	4	12	12	12	8	12	8	12	8	8	12	8
Código fuente SICAPITA			x	4	12	12	12	8	12	8	12	8	8	12	8
Código fuentes antecedentes digitales		x	x	3	9	9	9	6	9	6	9	6	6	9	6
Código fuente Sistema Requerimientos Ciudadanos			x	2	6	6	6	4	6	4	6	4	4	6	4
Código Fuente de Radar			x	3	9	9	9	6	9	6	9	6	6	9	6

Registros de consola de antivirus			x	2	6	6	6	4	6	4	6	4	4	6	4
Código Fuente de la Intranet			x	3	9	9	9	6	9	6	9	6	6	9	6
Código Fuente del Portal Web			x	3	9	9	9	6	9	6	9	6	6	9	6

Cuadro 8. (Continuación)

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]														
Datos e Información	Clasificación			Magnitud de Daño: 1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto	SERVICIOS INTERNOS														
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material,		Errores de los usuarios	Errores del administrador del sistema/ de la seguridad	Alteración de la información	Destrucción de la información	Fugas de información	Caída del sistemas por agotamiento de recursos	Suplantación de la identidad	Abuso de privilegios de acceso	Uso no previsto	Acceso no autorizado	Repudio (negación de actuaciones)	Modificación de la información	Destrucción de la información	Revelación de información	Denegación de servicio
					3	3	2	3	2	3	2	3	2	3	2	2	3	2	2
Portal Web		x	x	3	9	9	6	9	6	9	6	9	6	9	6	6	9	6	6
CORDIS	x		x	4	12	12	8	12	8	12	8	12	8	12	8	8	12	8	8
SINPROC	x		x	4	12	12	8	12	8	12	8	12	8	12	8	8	12	8	8
INTRANET	x		x	3	9	9	6	9	6	9	6	9	6	9	6	6	9	6	6
PERNO	x	x	x	3	9	9	6	9	6	9	6	9	6	9	6	6	9	6	6
Centros Comerciales	x		x	2	6	6	4	6	4	6	4	6	4	6	4	4	6	4	4
Requerimientos Ciudadanos	x		x	3	9	9	6	9	6	9	6	9	6	9	6	6	9	6	6
Glassfish			x	2	6	6	4	6	4	6	4	6	4	6	4	4	6	4	4

Antecedentes Disciplinarios	x		x	4	12	12	8	12	8	12	8	12	8	12	8	8	12	8	8
Desprendibles	x	x	x	2	6	6	4	6	4	6	4	6	4	6	4	4	6	4	4
Radar			x	2	6	6	4	6	4	6	4	6	4	6	4	4	6	4	4
SICAPITA	x	x	x	4	12	12	8	12	8	12	8	12	8	12	8	8	12	8	8

Cuadro 8. (Continuación)

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																
Datos e Información	Clasificación			Magnitud de Daño:	APLICACIONES																
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen,	1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto	Errores de los usuarios	Errores del admin del sistema/ de la seguridad	Alteración de la información	Destrucción de la información	Fugas de información	Caída del sistemas por agotamiento de recursos	Suplantación de la identidad	Abuso de privilegios de acceso	Uso no previsto	Acceso no autorizado	Repudio (negación de	Modificación de la	Revelación de	Denegación de servicio	Difusión de software dañino	Errores de mantenimiento	Vulnerabilidades de los programas	Manipulación de programas
					3	3	3	3	2	4	3	2	2	2	2	2	3	2	3	3	3	2
Correo electrónico			x	4	12	12	12	12	8	16	12	8	8	8	8	8	12	8	12	12	12	8
SAMBA (DHCP)			x	4	12	12	12	12	8	16	12	8	8	8	8	8	12	8	12	12	12	8
Sistema Operativo Windows Server			x	3	9	9	9	9	6	12	9	6	6	6	6	6	9	6	9	9	9	6
Sistema Operativo Linux			x	3	9	9	9	9	6	12	9	6	6	6	6	6	9	6	9	9	9	6
Sistema Operativo Unix AIX			x	2	6	6	6	6	4	8	6	4	4	4	4	4	6	4	6	6	6	4
LDAP			x	2	6	6	6	6	4	8	6	4	4	4	4	4	6	4	6	6	6	4
Nagios			x	1	3	3	3	3	2	4	3	2	2	2	2	2	3	2	3	3	3	2

Digiturno			x	2	6	6	6	6	4	8	6	4	4	4	4	4	6	4	6	6	6	4
Control de acceso			x	2	6	6	6	6	4	8	6	4	4	4	4	4	6	4	6	6	6	4
DNS Interno			x	2	6	6	6	6	4	8	6	4	4	4	4	4	6	4	6	6	6	4
Antivirus			x	3	9	9	9	9	6	12	9	6	6	6	6	6	9	6	9	9	9	6
PCSecure			x	2	6	6	6	6	4	8	6	4	4	4	4	4	6	4	6	6	6	4

Cuadro 8. (Continuación)

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]															
Datos e Información	**Clasificación**			**Magnitud de Daño:**	**EQUIPOS**															
	Confidencial, Privado, Sensitivo	**Obligación por ley / Contrato / Convenio**	**Costo de recuperación (tiempo, económico, material, imagen, emocional)**	**1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto**	Fuego	Daños por agua	Desastres naturales	Desastres industriales	Avería de origen físico o lógico	Corte del suministro eléctrico	Errores de mantenimiento /actualización de	Caída del sistemas por agotamiento de	Perdida de equipos	Abuso de privilegios de acceso	Uso no previsto	Acceso no autorizado	Manipulación de hardware	Denegación de servicio	Robo de equipos	Ataque destructivo
					3	2	3	2	3	2	3	3	2	2	2	2	2	2	2	1
Firewall	x		x	4	12	8	12	8	12	8	12	12	8	8	8	8	8	8	8	4
Servidores de red	x		x	4	12	8	12	8	12	8	12	12	8	8	8	8	8	8	8	4
Servidor de Base de datos	x		x	4	12	8	12	8	12	8	12	12	8	8	8	8	8	8	8	4
Servidor de WEB		x	x	3	9	6	9	6	9	6	9	9	6	6	6	6	6	6	6	3
Servidor de Intranet		x	x	3	9	6	9	6	9	6	9	9	6	6	6	6	6	6	6	3
Servidor de Consola Antivirus	x		x	2	6	4	6	4	6	4	6	6	4	4	4	4	4	4	4	2
Servidor Radar		x	x	3	9	6	9	6	9	6	9	9	6	6	6	6	6	6	6	3
Servidor Aplicativos		x	x	4	12	8	12	8	12	8	12	12	8	8	8	8	8	8	8	4

Servidor de Monitoreo	x		x	2	6	4	6	4	6	4	6	6	4	4	4	4	4	4	4	2
Servidor de Archivos	x		x	3	9	6	9	6	9	6	9	9	6	6	6	6	6	6	6	3
Servidor control de acceso	x		x	2	6	4	6	4	6	4	6	6	4	4	4	4	4	4	4	2
Servidor de Telefonía	x		x	4	12	8	12	8	12	8	12	12	8	8	8	8	8	8	8	4
Servidor de Nomina	x		x	4	12	8	12	8	12	8	12	12	8	8	8	8	8	8	8	4
Servidor Digiturno	x		x	3	9	6	9	6	9	6	9	9	6	6	6	6	6	6	6	3

Cuadro 8. (Continuación)

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																			
Datos e Información	Clasificación			Magnitud de Daño:	REDES DE COMUNICACIONES																			
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)	1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto	Fallo de servicio de comunicaciones	Errores del administrador del sistema/ de la seguridad	Errores de [re]encaminamiento	Errores de secuencia	Alteración de la información	Fugas de información	Caída del sistemas por agotamiento de recursos	Suplantación de la identidad	Abuso de privilegios de acceso	Uso no previsto	[Re-]encaminamiento de mensajes	Alteración de secuencia	Acceso no autorizado	Análisis de tráfico	Interceptación de información (escucha)	Modificación de la información	Destrucción de la información	Revelación de información	Denegación de servicio	Ataque destructivo
	3	2	2	2	2	2	3	2	3	2	2	2	3	3	3	2	2	2	3	3
Conexión a internet canal dedicado		x	x	4	12	8	8	8	8	8	12	8	#	8	8	8	12	12	12	8	8	8	12	12

Conexión telefonía IP		x	x	4	12	8	8	8	8	8	12	8	#	8	8	8	12	12	12	8	8	8	12	12
Conexión dedicado locales		x	x	3	9	6	6	6	6	6	9	6	9	6	6	6	9	9	9	6	6	6	9	9
Switches	x		x	3	9	6	6	6	6	6	9	6	9	6	6	6	9	9	9	6	6	6	9	9
Core	x		x	4	12	8	8	8	8	8	12	8	#	8	8	8	12	12	12	8	8	8	12	12
Red inalámbrica		x	x	2	6	4	4	4	4	4	6	4	6	4	4	4	6	6	6	4	4	4	6	6
Red de área local		x	x	4	12	8	8	8	8	8	12	8	#	8	8	8	12	12	12	8	8	8	12	12

Cuadro 8. (Continuación)

Matriz de Análisis de Riesgo					Probabilidad de Amenaza								
	Clasificación			Magnitud de Daño:	EQUIPAMIENTO AUXILIAR - INSTALACIONES								
Datos e Información	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)	1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto	Desastres naturales	Errores de manteniendo / actualización de equipos (hardware)	Uso no previsto	Manipulación del hardware	Ataque destructivo	Acceso no autorizado	Contaminación medioambiental	Daños por agua	Fuego
					3	2	2	3	2	2	2	2	3
Cableado de Red	x		x	3	9	6	6	9	6	6	6	6	9

Cableado eléctrico	x		x	3	9	6	6	9	6	6	6	6	9
Tarjeta de identificación	x			2	6	4	4	6	4	4	4	4	6
Racks	x		x	3	9	6	6	9	6	6	6	6	9
UPS	x		x	4	12	8	8	12	8	8	8	8	#
	x		x	4	12	8	8	12	8	8	8	8	#
Centro de Computo	x		x	4	12	8	8	12	8	8	8	8	#
Oficina Dirección de Tecnología		x	x	2	6	4	4	6	4	4	4	4	6

Cuadro 8. (Continuación)

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]											
Datos e Información	Clasificación			Magnitud de Daño:	PERSONAL											
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)	1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto	Errores de los usuarios	Errores del administrador del sistema/ de la seguridad	Alteración de la información	Destrucción de la información	Fugas de información	Caída del sistemas por agotamiento de recursos	Suplantación de la identidad	Abuso de privilegios de acceso	Uso no previsto	Acceso no autorizado	Repudio (negación de	Modificación de la información
					3	3	3	3	2	4	3	2	2	2	2	2

Director de sistemas	x			3	9	9	9	9	6	12	9	6	6	6	6	6
Administrador de BD		x		4	12	12	12	12	8	16	12	8	8	8	8	8
Administradores del Sistema		x		3	9	9	9	9	6	12	9	6	6	6	6	6
Técnicos soporte		x		2	6	6	6	6	4	8	6	4	4	4	4	4
Administradores de Red		x		3	9	9	9	9	6	12	9	6	6	6	6	6
Ingenieros administradores aplicativos		x		3	9	9	9	9	6	12	9	6	6	6	6	6
Administrador telefonía		x		3	9	9	9	9	6	12	9	6	6	6	6	6
Administrador Seguridad		x		3	9	9	9	9	6	12	9	6	6	6	6	6
Proveedores			x	2	6	6	6	6	4	8	6	4	4	4	4	4

Fuente: Las autoras

4.1.8.Riesgo Promedio

Cuadro 9. Análisis de riesgo promedio

		Probabilidad de Amenaza		
		1	**2**	**3**
Magnitud de Daño	**Datos e Información**	8.1	7.4	6.5
	Sistemas e Infraestructura	7.2	6.9	7.3
	Personal	7.4	7.6	7.6

Fuente. Las autoras

4.1.9.Resumen de riesgos

Cuadro 10. Resumen de riesgos

Riesgo	Recurso afectado
Abuso de privilegios de acceso	DATOS, SW, COMUNICACIONES
Acceso con clave ajena	SW, DATOS
Acceso no autorizado	DATOS, SW, COMUNICACIONES
Alteración de la información	SW, DATOS
Alteración de la información	SW, DATOS
Análisis de tráfico	SW, COMUNICACIONES
Ataque destructivo	DATOS, SW, COMUNICACIONES
Avería de origen físico o lógico	HW, EQUIPOS AUX, COMUNICACIONES
Bajo rendimiento	SW, HW
Caída del sistemas por agotamiento de recursos	SW, COMUNICACIONES
Corte del suministro eléctrico	HW
Daño por fuego	DATOS, SW, COMUNICACIONES
Daños por agua	DATOS, SW, COMUNICACIONES

Cuadro 10. (Continuación)

Riesgo	Recurso afectado
Denegación de servicio	PERSONAL, COMUNICACIONES
Desastres naturales	DATOS, SW, COMUNICACIONES, EQUIPOS
Destrucción de la información	DATOS, SW, COMUNICACIONES
Difusión de software dañino	SW, DATOS
Equipos obsoletos	EQUIPOS
Error de acceso	SW
Errores de los usuarios	PERSONAL, DATOS
Errores de mantenimiento / actualización de equipos (hardware)	PERSONAL, EQUIPOS
Errores de mantenimiento /actualización de equipos	PERSONAL, SW
Errores del administrador del sistema/ de la seguridad	PERSONAL, DATOS
Extorsión	PERSONAL
Fallo de servicio de comunicaciones	COMUNICACIONES
Fuego	EQUIPOS, HW
Fugas de información	PERSONAL, DATOS
Interceptación de información (escucha)	COMUNICACIONES
Revelación de información	PERSONAL
Suplantación de la identidad	PERSONAL
Vulnerabilidades de los programas (software)	SW

Fuente. Las autoras

4.1.10.Políticas de seguridad

Las políticas de seguridad forman la base de la normatividad que regula la administración de los recursos informáticos de la Personería de Bogotá. Se participó en la formulación y revisión de la primera versión de políticas de seguridad institucionales como parte del grupo de tres ingenieros encargados del tema, dando como resultado la Resolución 318 del 17 de julio de 2015, mediante la cual se adopta oficialmente la Política de Seguridad de la entidad.

Las políticas de seguridad han sido divulgadas a través de diferentes medios como son la Intranet, el correo institucional y charlas, buscando que todos los servidores de la entidad, funcionarios tanto de planta como contrato y terceros conozcan esta normatividad, la apliquen operando niveles convenientes de seguridad.

A continuación se relaciona el contenido de las políticas de seguridad de la entidad:

Titulo 1. Definiciones

Para los efectos de la política de seguridad, se adoptarán las siguientes definiciones:

Activo: Es todo aquel elemento que compone el proceso de la comunicación, desde hardware, software, datos y documentación (Microsoft).

Acuerdo de Nivel de Servicio: Un Acuerdo de Nivel de Servicio (ANS) es un convenio entre un proveedor de servicios de TI y un cliente. Describe las características del servicio de TI, los niveles de cumplimiento y las sanciones, y especifica las responsabilidades del proveedor y del cliente. Un ANS puede cubrir múltiples servicios de TI o múltiples clientes (Marco de Referencia - Mintic, 2014)

Aplicaciones o aplicativos: Las aplicaciones son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares (MINTIC - Ecosistema Digital).

Autenticación: Proceso utilizado entre un emisor y un receptor, con el fin de asegurar la integridad de los datos y proporcionar la autenticidad de los datos originales **(**ICONTEC **I**nternacional, 2004)

Copia de respaldo: Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.

Contenido: Todos tipos de información o datos que se divulga en la intranet y/o página web, entre los que se encuentran: textos, imágenes, fotos, logos, diseños, animaciones (Personeria de Bogotá, 2015)

Clave de autenticación o Contraseñas: Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.

Copyright: Derecho exclusivo de un autor o editor a explotar una obra física o digital, literaria, científica o artística.

Dominio: Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red. Es la parte principal de una dirección en la Web, que usualmente indica la organización o compañía que administra dicha página (personeriabogota.gov.co).

Información personal: Es aquella suministrada por el usuario o el visitante para el registro o consulta de información, la cual incluye datos como nombre, identificación, edad, género, dirección, correo electrónico y teléfono, entre otros (Personería de Bogotá, 2015)

Internet: Herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP/IP.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos. (NTC 5411-1:2006)

Intranet: Es una red de ordenadores privados que utiliza tecnología Internet para compartir, dentro de una organización, parte de sus sistemas de información y sistemas operacionales.

Log: Uno o más ficheros de texto automáticamente creados y administrados por un servidor, en donde se almacena toda la actividad que se hace sobre dicho servidor o aplicación.

Medios de almacenamiento físico: Se considera como medio de almacenamiento físico las cintas, los disco extraíbles, los discos compactos - CD y los DVD entre otros.

Nombres de Grupos: Seudónimos utilizados para la clasificación de conjuntos de computadoras dentro del dominio.

Portal web: Es un sitio compuesto por varias páginas web, el cual, permite al usuario el fácil acceso a diferentes recursos y servicios que tienen relación con un mismo tema.

Publicar: Es la acción de hacer visible un contenido o documento desde un portal o sitio web.

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad según la NTC-ISO/IEC 27001,2006

Servicio al ciudadano: Es la asistencia, orientación o intervención que actualmente suministra la Personería de Bogotá, D.C. en línea o que proveerá en el futuro, por medio de su portal, como publicación de información, registro, certificados, asistencia, noticias, entre otros.

Servidor: Computadora central en un sistema de red que provee servicios a otras

computadoras (ALEGSA - Definición de Servidor, 2015)

Sistema Informático o de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna forma mensajes de datos (Diario Oficial - Ley 527 de 1999, 1999)

Usuario: Es cualquier persona que utiliza una computadora o cualquier otro mecanismo para acceder y/o hacer uso de los sistemas informáticos de la entidad. (Alegsa - Definición de Usuario, 2015). Se considera usuario interno, todo funcionario y contratista, que haga uso de los recursos informáticos de la entidad. A su vez, se considera usuario externo, todo ciudadano que haga uso del portal web y acceda previa autorización, a servicios de internet a través de la red wifi de la entidad.

Titulo 2. Documentos de referencia - Fundamento legal

Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.

Ley 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones .

Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

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 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales .

Ley 1712 de 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 .

Ley 594 de 2000: Por medio de la cual se dicta la Ley General de Archivos y se dictan otras .

Ley 599 de 2000: Por la cual se expide el Código Penal .

Ley 962 de 2005: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos .

Ley 1150 de 2007: Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.

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 de Espectro y se dictan otras disposiciones

Ley 1343 de 2009: Por medio de la cual se aprueba el Tratado sobre el Derecho de Marcas y su Reglamento , adoptados el 27 de octubre de 1994.

Ley 1437 de 2011: Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo .

Decreto 2609 de 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Decreto 2578 de 2012: Por el cual se reglamenta el Sistema Nacional de Archivos, se establece la Red Nacional de Archivos, se deroga el Decreto número 4124 de 2004 y se dictan otras disposiciones relativas a la administración de los archivos del Estado .

Decreto 2693 de 2012: Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones

Decreto 943 de 2014: En ejercicio de las facultades legales y, en especial las conferidas por el artículo 189 numeral 11 de la Constitución Política y en desarrollo de las normas generales señaladas en la Ley 87 de 1993 .

Decreto 2573 de 2014: 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

Resolución No. 038 del 06 de febrero de 2015: Por la cual se crea el Comité de Seguridad Informática de la Personería de Bogotá D.C.

Norma ISO 27001: Tecnología de la Información. Técnicas de Seguridad. Sistemas

de Gestión de la Seguridad de la Información.

Titulo 3. Alcance

Artículo 1. La política de seguridad informática rige para la gestión, el uso adecuado y seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la Personería de Bogotá, D.C. Esta política debe ser conocida y cumplida tanto por funcionarios como contratistas y terceros que utilicen la información generada y custodiada por la entidad, y hagan uso de los servicios tecnológicos de la misma.

Titulo 4. Responsables

Comité de seguridad informática: Responsable de aprobar las políticas de seguridad de la información aplicables al interior de la entidad, emitiendo las directrices y recomendaciones que considere pertinentes para uso y aplicación por parte de todos los usuarios. Debe realizar la verificación del cumplimiento de dichas directrices como mínimo en cada una de sus sesiones ordinarias, o de manera extraordinaria, cuando surja algún cambio significativo en la infraestructura tecnológica.

Líderes de los procesos o directores de las dependencias: Responsables por informar a la Dirección de Tecnologías de Información y Comunicación –DTIC-las novedades en vinculación y contratación de los colaboradores de la entidad y los permisos de las carpetas o recursos compartidos para los cuales están autorizados. Así mismo, deben conocer y asegurar la implementación de las políticas de seguridad informática, dentro de sus áreas de responsabilidad y asegurar su cumplimiento por parte de su equipo de trabajo.

Dirección de Tecnologías de Información y Comunicación – DTIC –: Deberá garantizar la divulgación, y el seguimiento de las políticas de seguridad de la información al interior de la Entidad, estableciendo los procedimientos que permitan su operatividad y cumplimiento. Adicionalmente, recomendará al Comité de Seguridad Informática para su aprobación los nuevos sistemas de información y/o los requerimientos de desarrollo, actualizaciones y nuevas versiones.

Dirección Administrativa y Financiera – DAF –: Responsable del inventario de equipos y su actualización según se establezca en las normas vigentes y de proporcionar los suministros que permitan la operación adecuada de los sistemas de información de la entidad por medio de los procesos contractuales necesarios tanto para la ampliación de la red como para su mantenimiento. Adicionalmente, debe informar a la DTIC las novedades referidas a los contratistas que en el desarrollo de sus actividades requieran acceso a información de la entidad, relacionando claramente los datos de los usuarios entrantes y salientes de acuerdo con lo establecido en el procedimiento Administración de cuentas de usuario, Código: 11-PT-01

Dirección de Talento Humano: Debe informar a la Dirección de Tecnologías de Información y Comunicación toda novedad de personal de acuerdo con lo establecido en el procedimiento Administración de cuentas de usuario, Código: 11-PT-01.

Funcionarios y contratistas: Todo funcionario o contratista de la entidad es responsable del reporte oportuno de debilidades e incidentes de seguridad que detecte o que sean de su conocimiento y de proteger el ingreso a los recursos informáticos a los cuales se les permite el acceso mediante la utilización de contraseñas confidenciales; para tal fin, debe cerrar las sesiones activas al finalizar las tareas, y/o dejar los equipos bloqueados mediante protector de sesión protegido por contraseña. De la misma forma es responsable por el manejo del espacio en disco en su equipo de trabajo, realizando revisiones periódicas y eliminación de archivos no necesarios.

Titulo 5. Lineamientos generales

Artículo 2. Todo contrato o convenio relacionado con servicios de tecnología y/o acceso a información, debe contener una obligación o cláusula donde el contratista o tercero acepte el conocimiento de las políticas de seguridad y acuerde mantener confidencialidad de la información con la suscripción de un acuerdo o compromiso de confidencialidad de la información, el cual se hará extensivo a todos sus colaboradores.

Artículo 3. Las actualizaciones, modificaciones o novedades en materia de seguridad se comunicarán mediante los medios tecnológicos habilitados para tal fin.

Artículo 4. Todas las acciones realizadas bajo un nombre de usuario y contraseña de acceso, quedaran registradas y sus consecuencias legales son responsabilidad del usuario titular.

Artículo 5. La entidad podrá divulgar información personal de los ciudadanos registrada en sus sistemas de información, tal como está establecido en las normas legales vigentes.

Titulo 6. Asignación de roles y responsabilidades

Artículo 6. El (la) líder del proceso y/o los Jefes de Dependencias definirán los roles de usuario que se estimen pertinentes en cada uno de sus equipos y los niveles de operación siguiendo lo establecido en el procedimiento Administración de cuentas de usuario, Código: 11-PT-01

Titulo 7. Clasificación de los roles

Los roles asociados a cada servicio o sistema de información serán identificados y clasificados por su tipo y uso teniendo como base los siguientes criterios:

Artículo 7. Internos:

- Grupo Tecnología (GT): Usuarios que por su actividad directa con los sistemas de información y de tecnología necesitan accesos especiales a los sistemas tecnológicos de la entidad.
- Grupo VIP: Usuarios que por su actividad gerencial necesitan accesos con niveles básicos de seguridad para cumplir con sus labores designadas.
- Funcionario Activo: Usuarios que requieren diferentes niveles de acceso de acuerdo con los niveles de servicio asociados basados en sus funciones.

Artículo 8. Externos: Ciudadano con acceso a la página web y/o terceros con acceso a la red mediante redes inalámbricas dentro de la entidad.

Titulo 8. Políticas operativas

Capítulo 1. Administración de activos físicos

Artículo 9. La administración de hardware conectado a la red y la atención de requerimientos de desarrollos y adecuaciones, debe realizarse de acuerdo con lo establecido en el Protocolo para la Administración de redes y Comunicaciones, Código: 11-PC-01. En consecuencia, no pueden conectarse computadores, servidores, dispositivos de comunicaciones como switches, enrutadores o cualquier otro hardware a la red sin la aprobación y supervisión de la DTIC.

Artículo 10. El cableado de energía eléctrica y de comunicaciones, deberá cumplir con los estándares vigentes según el reglamento interno de instalaciones eléctricas RETIE, RITEL y norma de cableado EIA/TIA 568. Cualquier cambio en las instalaciones eléctricas o ramales adicionales a los establecidos por la entidad debe hacerse presentando previa solicitud y con aprobación y supervisión técnica de la DTIC.

Artículo 11. El suministro de energía eléctrica deberá estar regulado a 110 voltios con polo a tierra, salvo especificación contraria del fabricante o proveedor de los equipos. Adicionalmente se debe contar con suministro de energía interrumpible (UPS) para asegurar la ejecución continua o el apagado regulado y sistemático del parque tecnológico que sustenta las operaciones críticas de la entidad.

Para efectos de la conservación física de los equipos se debe prevenir interferencia eléctrica o magnética, riesgo de contaminación por alimentos, bebidas o golpes con objetos que perjudiquen o pongan en riesgo el funcionamiento de los mismos o

deterioren la información almacenada en ellos.

Artículo 12. Se debe evitar colocar encima o cerca de los computadores ganchos, clips u otros elementos que puedan caer accidentalmente dentro del equipo. Adicionalmente se deberá apagar la pantalla si se retira de su puesto de trabajo y apagar el equipo al finalizar la jornada laboral.

Capítulo 2. Mantenimiento preventivo y correctivo

Artículo 13. La Dirección DTIC deberá elaborar el cronograma de mantenimiento preventivo y correctivo el cual será notificado a las dependencias con mínimo una semana de antelación con el fin de asegurar la prestación del servicio a los usuarios. Adicionalmente, deberá informarse el nombre e identificación del personal autorizado para realizar las actividades de mantenimiento con el fin de evitar el riesgo de hurto y/o pérdida de equipos.

Artículo 14. Toda solicitud de mantenimiento correctivo o asistencia técnica, debe realizarse siguiendo el Procedimiento Soporte técnico, Código: 11-IN-01. Cuando los equipos requieran de cambio de partes y no haya disponibilidad de las mismas, la DTIC deberá provisionar al usuario afectado con un equipo de alterno destinado para tal fin en el Plan de Contingencia de acuerdo con la disponibilidad de equipos.

Artículo 15. Ningún funcionario(a) está autorizado(a) para efectuar ningún tipo de intervención, reparación y/o modificación en un equipo a su cargo. El mantenimiento preventivo y correctivo debe ser realizado por técnicos de DTIC, quienes deben contar con el entrenamiento y las herramientas necesarias siguiendo lo establecido en el Protocolo para la ¨administración de Redes y Comunicaciones¨ Código. 11-PC- 01.

Capítulo 3. Retiro y traslado de equipos

Artículo 16. Para efectuar el traslado y/o retiro de equipos (incluidos la información y el software) por cambio del funcionario responsable o cambio en la ubicación del equipo se debe seguir lo establecido en el procedimiento Egreso y/o Traslado de Bienes, Código: 09-PT-06.

Artículo 17. Si para el cumplimiento de una actividad específica el funcionario y/o contratista requiere temporalmente el uso de un equipo debe solicitarlo por medio de la intranet ¨Préstamo Elementos Informáticos¨ Código. 11-RE-08 a la Dirección de TIC quien autorizara mediante un oficio dirigido a la Dirección Administrativa y Financiera, la cual debe ser firmada por su Director(a) y luego entregado al personal de vigilancia y seguridad del edificio, quien a su vez registrará en la bitácora (libre de salida de elementos) con Nombre, cedula, fecha, hora, oficina que entrega y firma), para el proceso de retiro del equipo.

Artículo 18. Para el caso de personerías locales y demás puntos de atención a la comunidad, los equipos serán responsabilidad de los funcionarios y/o contratistas según inventario de la entidad.

Capítulo 4. Seguridad física y del entorno

Artículo 19. Las áreas para la gestión, almacenamiento y procesamiento de información de la Personería de Bogotá, D.C. (centro de cómputo y cuartos de comunicaciones), deben ser aseguradas y en lo posible monitoreadas con cámaras de video con el fin de prevenir o impedir accesos no autorizados, adulteración, perdida, consulta, daños e interferencia en el funcionamiento de los aplicativos e información de la entidad.

Artículo 20. Todos los servidores y equipos de comunicaciones de voz y datos deben estar localizados en lugares seguros para prevenir el uso o acceso no autorizado. De igual forma, deberá contarse con protecciones físicas y ambientales para los activos críticos, incluyendo perímetros de seguridad, controles de acceso físicos, controles especiales en áreas de mayor sensibilidad, seguridad de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales de operación y sistemas de contención, detección y extinción de incendios.

Capítulo 5. Seguridad para áreas de acceso restringido

Artículo 21. Constituyen áreas de acceso restringido el Centro de Cómputo, los cuartos de potencia (recursos eléctricos, Unidades de poder ininterrumpida UPS y cuartos de electricidad) y centros de cableado, por lo que solo el personal autorizado por Dirección de Tecnologías puede acceder a él. Este personal debe portal el carnet de la entidad que lo acredita como funcionario del área en mención.

Artículo 22. Toda persona que ingrese al Centro de Cómputo debe estar acompañada por un funcionario de DTIC. Los administradores del Centro de Cómputo mantendrán un registro de todas las visitas autorizadas a esta área, en el que se identifique nombre del visitante, documento de identificación, fecha, hora de entrada y salida de las instalaciones, la actividad por la cual ingresaron y la persona que autorizo su ingreso. A su vez, todo equipo informático ingresado al Centro de Cómputo deberá ser registrado. El Administrador del Centro de Cómputo maneja una bitácora de ingreso a esta área para el registro y control. No se permite ingerir alimentos o bebidas en las instalaciones del Centro de Cómputo.

Artículo 23. El Centro de Cómputo debe contar con equipos vigilancia (cámaras) y sistemas de protección contra incendios, control de temperatura (Aire acondicionado) y sistema eléctrico de respaldo (UPS) de acuerdo con lo establecido en norma ISO 27001-2013 estándar ANSI/BICSI 002.

Artículo 24. Cualquier cambio que se realice en el Centro de Cómputo o centros de

cableado, y que potencialmente afecte los sistemas de información de la entidad, debe estar previamente autorizado y debe registrarse en bitácora de aplicaciones Código: 11 -RE- 05

Titulo 9. Seguridad de la información

Capítulo 1. Información sensible

Artículo 25. Todo funcionario o contratista deberá devolver los activos informáticos que tiene a su cargo si por cualquier motivo existe retiro ya sea definitivo o temporal, cambio de puesto de trabajo, licencias, vacaciones, suspensión y/o finalización del contrato, haciendo entrega formal de los activos a su cargo y claves de acceso; de ser necesario, instruir a su reemplazo en la utilización de la aplicación que opera, también debe solicitar la toma de la copia de respaldo del equipo a la Dirección de Tecnologías de la Información y Comunicación.

Adicionalmente es necesario garantizar que todos los funcionarios de la entidad, contratistas y terceros deben recibir formación adecuada en concientización y actualización sobre las políticas y los procedimientos de seguridad informática de la entidad, según sea pertinente para sus funciones laborales.

Artículo 26. Los sistemas de información de la entidad que contengan información reservada, se deben mantener con niveles de protección más estrictos con el fin de velar por su reserva.

Capítulo 2. Protección contra el código malicioso y descargable

Artículo 27. La dirección de TIC designará el (la) funcionario (a) responsable (Estándar Internacional ISO/IEC 17799, 2005) de supervisar la consola de antivirus para que administre la plataforma y regule el uso y despliegue de la herramienta en toda la Personería. Para tal fin se deben realizar las siguientes tareas:

- Revisión periódica de las últimas definiciones en la consola.
- Descarga de últimas actualizaciones de Internet.
- Corregir posibles alertas de virus.
- Registrar en la bitácora los resultados de este proceso.

Artículo 28. Todos los equipos y dispositivos móviles deben tener software de antivirus. Por lo tanto todo equipo debe ser incluido dentro del dominio de la red persobogota.gov.co, para que se puedan ejercer los controles y apliquen las actualizaciones y detecciones correspondientes.

Artículo 29. El software de instalación en los servidores debe ser protegido contra escritura de tal manera que se prevenga su posible infección.

Artículo 30. Antes de distribuir datos a otros usuarios, tanto internos como externos, se debe hacer una revisión a los mismos usando el software de Antivirus.

Artículo 31. Está prohibido intentar desinstalar o deshabilitar el software antivirus de los computadores por parte de los usuarios de la entidad. Si los usuarios sospechan la infección de un virus informático, deben vacunar sus archivos y verificar su eliminación mediante el software de Antivirus, si el problema persiste se debe comunicar de inmediato a la Dirección de TIC a la extensión 5316.

Artículo 32. Todo medio de almacenamiento, como cinta, discos duros removibles, USB y discos compactos que ingresen a la entidad, deben ser previamente revisados y/o vacunados como media preventiva de infección antes de su uso.

Artículo 33. Está prohibido el uso de software ilegal o de libre distribución so pena de acción disciplinaria. En caso de necesitar la instalación de algún software adicional, el funcionario (a) responsable debe solicitarlo a la Dirección de TIC.

Se revisará periódicamente el contenido de software y datos de los equipos de cómputo, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas. Cualquier anomalía será reportada al Jefe Inmediato del funcionario involucrado.

Artículo 34. Los ambientes de prueba y producción de software estarán separados físicamente (diferente hardware) siempre que sea posible, y se definirán y documentarán las reglas para la transferencia de software desde el estado de prueba hacia el estado producción.

Capítulo 2. Gestión de la provisión de servicios por terceros

Artículo 35. Se deben establecer con los proveedores Acuerdos de Niveles de Servicio con sus respectivas penalizaciones en caso de incumplimiento de los niveles acordados.

Se debe monitorear el cumplimiento de los acuerdos de niveles de servicio establecidos usando herramientas o mecanismos comprobados de verificación tales como software u otros.

Artículo 36. Las excepciones en los niveles del servicio y las incidencias presentadas en el servicio, deberán ser revisadas con especial cuidado, para evitar reportes que carezcan de veracidad.

Artículo 37. Los proveedores de servicio deberán cumplir las políticas de seguridad informática en cuanto a la reserva de la información de la entidad o lo que les aplique.

Titulo 10. Políticas de copias de seguridad

Capítulo 1. Respaldo de los servicios centro de cómputo

Artículo 38. La Dirección TIC realizará los procedimientos de copia, recuperación y pruebas de la información, estandarizando los medios y mecanismos para el registro de tareas y eventualidades de manera que se garantice la continuidad de prestación de los servicios de la entidad y la atención oportuna de contingencias.

Artículo 39. Los medios de almacenamiento físico y de red estarán instalados en el Centro de Cómputo, a los cuales tendrán acceso únicamente los funcionarios indicados por la Dirección TIC para ser administrados.

Artículo 40. En el caso de copias de respaldo a medios de almacenamiento físico, éstas se harán mediante software especializado y/o programado o con el uso comandos de transferencia con seguridad, que permitan el uso de protocolos como FTP, SSH y/o WInScp y con comandos de tarea como RCP, tar y/o cpio, con posibilidad de compresión.

Los funcionarios de la Dirección TIC, encargados de la infraestructura tecnológica, deberán seguir los procedimientos de respaldo de la información establecidos internamente, en los que se especifican: Periodicidad, tipo, jerarquía, generación y ubicación de las copias generadas.

Artículo 41. Se considera como información a respaldar aquella que es exclusivamente de carácter institucional.

Este respaldo contempla los archivos compartidos de carácter documental, propios de la gestión encomendada por la misión de la entidad en su diaria marcha, sistemas de información críticos y misionales (ejecutables y compilados de menús, librerías, formas, packages, objetos, etc), bases de datos de los sistemas de información, bases de datos de los servicios corporativos como el correo, portales web e Intranet, programas específicos de servicio (Eje. Consola ePo, Appliances y otras consolas de monitoreo), y IOS de equipos de telecomunicaciones (firewalls, switches, servidores, microcomputadoras, Appliance y sistemas de virtualización).

Artículo 42. La Dirección TIC delegará los administradores de cada sistema informático, los cuales son los responsables de informar y registrar la toma de la copia de respaldo, estos son:

- Administrador de bases de datos de sistemas de información
- Administrador de Centro de Cómputo, servidores y servicios
- Administrador de Sistemas de información y Portales

- Administrador de las Redes y comunicaciones.

Capítulo 2. Respaldo de información de usuarios

Artículo 43. Cada usuario es responsable de generar copia de seguridad de la información en el servidor de archivos que la Dirección de Tecnologías de Información y Comunicaciones asigne para tal fin, respetando las cuotas de espacio asignadas.

El servicio de recursos y activos informáticos compartidos de la Personería están disponibles para todos los funcionarios y contratistas que lo requieran. Para su solicitud se debe seguir el procedimiento publicado en la intranet Código: 11-PT-02, el cual requiere diligenciamiento del Formato para el uso de recursos compartidos código 11- RE- 04.

Artículo 44. La Dirección TIC, brindará las instrucciones y capacitaciones necesarias a los usuarios que requieran guardar información o compartir archivos en espacio del servidor.

Artículo 45. Es responsabilidad de los usuarios la manipulación de los archivos compartidos, solo se permite archivos que estén directamente ligados a su función (no se permiten archivos personales), cualquier modificación a los mismos deberá atender los permisos otorgados y previamente solicitados.

Artículo 46. Es responsabilidad de cada funcionario y/o contratista identificar, clasificar y definir la información relevante a respaldar en los medios de almacenamiento autorizados, con el fin de mantener una copia original de los datos importantes y/o relevantes. Archivos no autorizados serán eliminados.

Artículo 47. Todos los usuarios de los activos y recursos informáticos deberán acatar las políticas de respaldo impartidas por la Dirección TIC, y deberán conocer las responsabilidades y/o consecuencias que generan el uso de las herramientas y las copias de respaldo no autorizadas.

Titulo 11. Gestión de seguridad de las redes

Capítulo 1. Controles y procedimientos

Artículo 48. La Dirección TIC definirá controles para garantizar la seguridad de los datos y los servicios conectados a las redes de la entidad contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

- Establecer los procedimientos para la administración de los equipos remotos, incluyendo los equipos en las áreas restringidas.

- Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.
- Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.
- Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

Capítulo 2. Controles de red

Artículo 49. Los equipos de acceso a la red estarán protegidos contra accesos no autorizados.

La Entidad proporcionará tecnologías de acceso remoto a sus funcionarios (VPN) y autorizará su uso de forma particular cuando así se requiera. La Dirección TIC garantizará un adecuado esquema de seguridad informática para los mismos.

Artículo 50. Las direcciones IP internas, configuraciones e información relacionada con la topología y diseño de los sistemas de comunicación y redes de la entidad serán restringidas, de tal forma que no sean conocidas por funcionarios, contratistas, ciudadanos o personas ajenas a la entidad sin la previa autorización de la Dirección TIC.

Artículo 51. Todos los computadores de la entidad que sean autorizados para ser accedidos remotamente a través de mecanismos como Internet, enlaces dedicados, y otros, deben ser protegidos con mecanismos de control de acceso aprobados por la Dirección TIC.

Artículo 52. La conexión directa entre los sistemas de información de la entidad y otra organización vía redes públicas de datos como Internet requieren de la aprobación de la Dirección TIC, estos deberán cumplir como mínimo las políticas de seguridad informática de la entidad y estarán sujetos a otros mecanismos de seguridad que la dirección TIC considere.

Artículo 53. Como requisito para interconectar las redes de la entidad con las de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos se seguridad dispuestos por este documento, que deberán ser igual o mayores.

Artículo 54. Los funcionarios, contratistas o colaboradores que desarrollen actividades para la entidad de manera remota, deben utilizar equipos de cómputo autorizados por dirección TIC y que no afecten la seguridad de la red.

Artículo 55. El acceso remoto a la red de datos de la Personería de Bogotá, D.C., se brindará para recursos como el correo electrónico de la entidad y el acceso a

otros sistemas de información que por su carácter descentralizado requiera usuarios externos y en este caso se seguirá el procedimiento establecido para tal fin.

Artículo 56. La entidad se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos de seguridad y confidencialidad establecidos.

Artículo 57. El acceso a la red de la Personería está controlado mediante un dispositivo de seguridad perimetral Firewall, que permite la segregación de redes y el manejo de políticas de acceso a cada una de ellas. La modificación de estas reglas establecidas en el Firewall, debe ser aprobada por la Dirección de Tecnologías de Información y Comunicaciones.

Artículo 58 Los usuarios que requieran conexión a internet o a los sistemas de información de la entidad a través de la red WIFI de la Personería de Bogotá, D.C. deberán cumplir las presentes políticas de seguridad informática.

Artículo 59. Los puntos de acceso a la red WIFI deberán contar con contraseñas de autenticación para evitar accesos no permitidos.

Titulo 12. Manipulación de los soportes de copia de información

Capítulo 1. Gestión de soportes extraíbles

Artículo 60. Se recomienda para el uso de medios informáticos removibles las siguientes acciones:

- En lo posible almacenar la información en los medios dispuestos para tal fin (pc, carpetas compartidas)
- Eliminar de forma segura los contenidos no requeridos del medio reutilizable que ha de ser retirado o reutilizado en la entidad (discos duros, etc).
- Almacenar todos los medios en un ambiente seguro y protegido.
- Si por alguna razón, información reservada y clasificada de la entidad es retirada de las instalaciones de la personería en uno de estos medios, se deben utilizar sistemas de encriptación para proteger la misma en caso de pérdida. Para ello se debe solicitar soporte a la dirección TIC.

Capítulo 2. Seguridad de la documentación del sistema

Artículo 61. La documentación del sistema debe ser almacenarla en forma segura, permitiendo el acceso solo a personal debidamente autorizados.

Titulo 13. Servicios electrónicos de información

Capítulo 1. Gobierno en línea

Artículo 62. La Personería de Bogotá, D.C., pone a disposición de la ciudadanía y los usuarios en general, los recursos del portal web de la entidad y la intranet respectivamente, los cuales incluyen información pertinente, veraz, oportuna y accesible en línea de forma segura, en los procesos de prestación de servicios relacionados con la misión de la entidad, de acuerdo con los lineamientos establecidos en el manual para la implementación de la Estrategia Gobierno en Línea de la República de Colombia.

Capítulo 2. Transacciones en línea

Artículo 63. Para el uso y acceso a los trámites en línea con que cuenta la Personería de Bogotá, D.C., en su portal web e intranet. Los trámites y servicios que puede acceder el ciudadano son:

- Solicitud Antecedentes.
- Orientación Jurídica.
- Reconocimiento e inscripción Veedurías Ciudadanas.

Titulo 14. Manejo de la información

Capítulo 1. Clasificación de la información

Artículo 64. La información resultante de los procesos misionales y de apoyo de la Entidad se tratará conforme a los lineamientos y parámetros establecidos en el Manual de Gestión Documental de la entidad. Código: 12-MN-01

Artículo 65. Los activos informáticos asociados a cada sistema de información, serán identificados y clasificados por su tipo y uso siguiendo lo establecido en las tablas de retención documental vigentes, de acuerdo con los siguientes criterios:

- Pública: Datos misionales y críticos
- Interna: Aplicativos, archivos de software, archivos de usuarios, herramientas y programas de desarrollo. Manuales, procedimientos internos, guías y formatos.
- Reservada y clasificada: Bases de Datos, Documentación, procedimientos operativos, configuraciones

Capítulo 2. Salvaguarda de la información

Artículo 66. Los medios de almacenamiento transportados fuera de las

instalaciones de entidad, deberán cumplir con los controles de seguridad establecidos para tal fin.

Artículo 67. Toda la información que sea objeto de intercambio entre los diferentes sistemas de información estará controlada en cuanto a su acceso, envío, uso, almacenamiento y eliminación, de acuerdo a los controles de seguridad establecidos.

Artículo 68. Todos los cambios que se hagan en la página web de la entidad debe seguir la guía para publicación o actualización de información de la página Código: 11-GU-01

Artículo 69. Todos los sistemas y/o aplicativos de producción que la dirección TIC estime pertinentes y que contengan información misional de la entidad deben generar logs o trazas de auditoría; igualmente, los sistemas que operen y administren información misional, valiosa o critica para la entidad deben tener archivos de log que contengan evidencia sobre todos los eventos relevantes que sucedan con la información, y con las seguridades necesarias relacionadas con la consulta, modificación o borrado.

Artículo 70. Todos los log del sistema y de las aplicaciones deben mantenerse en forma segura, de tal forma que evite el acceso no autorizado a esta información.

Artículo 71. Todo software aplicativo habilitado en ambiente de producción de la entidad debe incluir archivos logs que registren como mínimo la siguiente información:

- La actividad realizada en la sesión abierta por el usuario incluyendo la identificación del código del usuario, fecha hora de la entrada y de la salida de cada sesión del sistema, aplicaciones invocadas.
- Cambios de información en los archivos de las aplicaciones críticas.
- Adiciones y/o cambios a los privilegios de los usuarios, fecha y hora de iniciación y terminación de ingreso al sistema de información.

Titulo 15. Uso de internet

Artículo 72. Las conexiones que acceden a Internet están protegidas por un Firewall, el cual está localizado entre la red privada y el proveedor de servicios de Internet, este controla (aplica seguridad) y supervisa las salidas hacia Internet.

Artículo 73. Todos los usuarios conectados a red con equipos que posean las condiciones mínimas para el acceso a Internet, tendrán derecho a su instalación y podrán navegar conforme a los lineamientos establecidos por este documento.

Artículo 74. Los recursos y servicios de Internet se usarán primordialmente para asuntos institucionales. El uso personal no debe interferir con la operación eficiente de los sistemas de la entidad, ni con los deberes y obligaciones de los funcionarios y/o contratistas establecidas en las funciones de su cargo.

Artículo 75. No se debe descargar y/o distribuir virus, gusanos, troyanos. La trasmisión de imágenes, sonidos y video pueden saturar el canal (ancho de banda) y disminuyen la velocidad de transmisión. (Tales como: Real Audio, eMule, eDonkey, o similares.)

Artículo 76. La Dirección TIC se reserva el derecho de bloquear sitios que se detecten como peligrosos (con contenidos no autorizados) para la seguridad de los recursos informáticos.

Artículo 77. El uso indebido del canal de Internet por parte de un usuario puede ocasionar la suspensión temporal del servicio y en caso de reincidencia, a la suspensión del mismo.

Artículo 78. No se puede descargar archivos o instalar programas de sítios web desconocidos o gratuito.

Artículo 79. El canal de internet será monitoreado periodicamente, para revisar el tráfico de paquetes, verificando el uso de este servicio.

Artículo 80. El incumplimiento de las presentes normas acarreará las sanciones correspondientes según sea el caso.

Titulo 16. Uso de la intranet

Capítulo 1. Usuario administrador

Artículo 81. El administrador del servicio debe:

- Definir la prioridad de las diferentes solicitudes y dar el trámite respectivo, teniendo en cuenta las directrices impartidas y los procedimientos vigentes.
- Asignar cuenta de usuario y contraseña a cada funcionario o contratista de la entidad.
- Asignar grupo y perfil, de acuerdo con las funciones asignadas dentro de la intranet.
- Efectuar cambio de roles y responsabilidades (Estándar Internacional ISO/IEC 17799, 2005) de los usuarios para efectuar cambio de privilegios.
- Mantener la base de datos de usuarios con sus respectivos roles actualizados.

Capítulo 2. Gestión de contenido

Artículo 82. Los cambios directos sobre la información contenida en las diferentes dependencias los realiza el gestor de contenido de la misma, previa capacitación y configuración de usuario.

Artículo 83. Los cambios solicitados que requieran modificación de la estructura básica de las páginas o creación de otras nuevas, sólo los podrá gestionar la Dirección de Tecnologías.

Capítulo 3. Usuario final

Artículo 84. El usuario puede navegar libremente a través de las diferentes páginas de la intranet, y tiene acceso a los diferentes documentos allí publicados.

Artículo 85. El acceso a la información se encuentra habilitado para uso exclusivo del personal de la entidad, por lo cual cada usuario está obligado a no divulgar a personal ajeno a la institución su cuenta de usuario, contraseña ni la información allí contenida.

Artículo 86. La contraseña del usuario del servicio no puede ser cambiada, por cuanto se encuentra asociada a un código interno asignado a cada funcionario, por lo cual se recomienda no compartirla ni revelarla, puesto que el usuario del servicio, propietario de la misma, es el único responsable de todas las acciones que se realicen con su usuario.

Artículo 87. Cada usuario es responsable del adecuado manejo su usuario de autenticación y contraseña asignadas; En caso de que el usuario digite de forma errónea la contraseña en tres intentos consecutivos, el sistema bloqueará automáticamente la cuenta, caso en el cual el funcionario deberá solicitar el desbloqueo.

Artículo 88. Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en lugares donde personas no autorizadas puedan ubicarlas fácilmente.

Artículo 89. Se consideran violaciones graves el robo, daño o divulgación de información reservada o clasificada publicada en la intranet.

Artículo 90. No se permite la publicación de ningún tipo de información de texto o audiovisual que no haya sido aprobado por el jefe inmediato y cuyo contenido no esté relacionado con las funciones que cumple la Personería de Bogotá.

Titulo 17. Portal web

Capítulo 1. Contenido

Artículo 91. La actualización de la información contenida en la página web debe hacerse como lo determina la Guía para la actualización del Portal Web Código: 11-GU-01

Artículo 92. En caso de que algún componente o servicio del portal se encuentre en mantenimiento o no disponible por falla, se debe publicar una imagen o texto que informe al usuario sobre dicho evento.

Artículo 93. La redacción de cada uno de los contenidos, está a cargo de los gestores de contenido asignados por cada de dependencia, y deberá producirse conforme a lo establecido en la mencionada Guía.
Toda publicación de documentos deberá estar de acuerdo con lo establecido en el Manual de Imagen Corporativa, Código: 11-MN-01.

Capítulo 2. Gestión de contenido

Artículo 94. Los cambios directos sobre la información contenida en las diferentes dependencias los realiza el gestor de contenido de la misma, previa capacitación y configuración de usuario.

Artículo 95. Los cambios solicitados que requieran modificación de la estructura básica de las páginas o creación de otras nuevas, sólo los podrá gestionar la Dirección de Tecnologías.

Titulo 18. Uso del correo electrónico

Capítulo 1. Directrices generales

Artículo 95. Todo funcionario o contratista de la Personería de Bogotá, D.C., dispondrá de una cuenta de correo electrónico activa.

Artículo 96. La vigencia de la cuenta para contratistas comprende el periodo de contratación que inicia el primer día de ingreso y finaliza el último día de contratación laboral, de acuerdo con la información del contrato.

Artículo 97. El uso de su cuenta de correo es con fines laborales y su uso es de carácter obligatorio, en ella llegará información oficial de conocimiento necesario para los funcionarios de la entidad.

Artículo 98. Se prohíbe el uso de cuentas de correo gratuito con propósitos institucionales o cuentas de suscripción gratuita a otros proveedores.

Artículo 99. La cuenta y contraseña es personal e intransferible. No debe permitir que personas diferentes hagan uso de su cuenta de correo.

Artículo 100. La clave o contraseña de correo debe poseer un mínimo de seis (6) caracteres y debe contener al menos una letra mayúscula, una letra minúscula y un número.

Artículo 101. El usuario es el único y directo responsable de todas las acciones y mensajes que se lleven a cabo en su nombre.

Artículo 102. La Entidad no se hace responsable por lo que se haga o diga en nombre de una cuenta particular y por lo tanto está prohibido el uso de cuentas por personas ajenas a su titular.

Artículo 103. Cada cuenta tendrá un espacio de almacenamiento básico de 30 Gb. Cuando, debido a las necesidades de las funciones que desempeñe el funcionario, requiera de su amplitud, deberá hacerse una solicitud a la cuenta de servicios admin@personeriabogota.gov.co.

Artículo 104. Es responsabilidad del funcionario o contratista depurar su cuenta periódicamente siendo él el único responsable de respaldar sus correos (Copia de respaldo).

Artículo 105. El usuario debe leer diariamente su correo y borrar aquellos mensajes obsoletos, para liberar espacio en su buzón de correo.

Artículo 106. Solo podrán enviar correos masivos aquellas oficinas que por su naturaleza de socialización y sensibilización lo requieran; esto se hará a través de listas de distribución, las cuales tienen unos moderadores que aprueban o deniegan los mensajes. Estos moderadores deben ser autorizados previamente por los directores de la dependencia.

Artículo 107. Se desactivarán las cuentas de correo que estén inactivas por un periodo de dos meses sin ninguna justificación.

Artículo 108. El incumplimiento por parte del funcionario o contratista de los lineamientos o el mal manejo de su cuenta, puede ocasionar la suspensión temporal del servicio y en caso de reincidencia, la suspensión del mismo y en un último caso la notificación a la Dirección de Talento humano y/o Dirección Administrativa para que adopten las medidas pertinentes.

Artículo 109. Se considera como conductas de mal manejo:

- Exceder los servicios para los cuales se autorizó la cuenta.

- Enviar mensajes para la difusión de noticias, mensajes políticos, religiosos, correos sin identificar plenamente a su autor o autores o enviar anónimos.
- Difundir «cadenas» de mensajes que saturen el servicio entre otros problemas.
- Perturbar el trabajo de los demás enviando mensajes que puedan interferir con sus actividades laborales.
- Agredir o lesionar directa o indirectamente a otras personas.
- Suscribir las cuentas de correo institucional en servicios externos (comerciales) con fines no gubernamentales o afines a la misión institucional.

Artículo 110. No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca atractivos premios o temas provocativos. Mucho menos si estos archivos tienen doble extensión.

Artículo 111. No se debe confiar en los archivos gratuitos que se descargan de sitios web desconocidos, ya que son una potencial vía de propagación de virus.

Artículo 112. De ninguna manera se deben ejecutar archivos de las siguientes características:

- Archivos que contienen más de un punto por ejemplo (diagrama.noticias.532.txt)
- Archivos que contienes doble extensión, por ejemplo (loganaste.txt.exe)
- Archivos que contienen alguna de las siguientes extensiones ejecutables (No permitidas): exe, vbs, pif, com, bat, dll, ocx

Artículo 113. No contestar los mensajes SPAM, ni mensajes con falsos contenidos (Hoaxes), tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, bloqueo de cuentas bancarias, etc.

Artículo 114. No responder correos donde soliciten ratificación de contraseñas de cualquier cuenta que posee, la Dirección TIC nunca solicitara por esta media esta clase de información.

Artículo 115. No suscribir el correo institucional en sitios desconocidos y/o comerciales, ya que generan la acumulación en los buzones de entrada de mensajes basura.

Artículo 116. El sobrepaso de tamaño de archivos adjuntos por encima de 20MB, puede provocar que los destinatarios no reciban el mensaje. Es importante tomar en consideración el tamaño de los archivos enviados como adjuntos en el correo (attachments). Si se envían comprimidos, se ahorra tiempo de conexión y se evita saturar la red.

Artículo 117. La aparición y desaparición de archivos, incluso temporales injustificadamente, lentitud del sistema, bloqueos o re-inicios continuos,

inicialización o finalización de programas o procesos sin justificación, la bandeja del CD/DVD se abre y cierra sin motivo alguno, el teclado, mouse u otro periférico dejan de funcionar, son evidencias de que nuestro equipo está siendo controlado por un hacker que ha ingresado a nuestro sistema con un troyano/backdoor, comunicarse a la dirección TIC - área de soporte para informar el evento, extensión 5316.

Artículo 118. Verificar siempre la procedencia de los correos antes de abrirlos. Procure colocar siempre en la línea de Asunto:, un contenido conciso que tenga significado para el destinatario y le motive a leer el contenido del correo.

Capítulo 2. Listas de correo

Artículo 119. Cada oficina puede solicitar la creación de estas listas de correo, enviando un correo a admin@personeriabogota.gov.co donde se especifique el nombre de la lista, la justificación, el responsable de su actualización, el nombre de los integrantes de la lista con sus respectivos buzones de correo.

Artículo 120. Las Listas de correo que incluyen todos los usuarios de la entidad, debe ser moderada y aprobada con el visto bueno del área administrativa, prensa o Directivo autorizado.

Titulo 19. Controles de acceso a los servicios

Capítulo 1. Políticas de usuario

Artículo 121. Para el registro de usuarios de acceso a los aplicativos, bases de datos y servicios de información de la entidad, se debe proceder de acuerdo con lo establecido en el procedimiento Administración de Cuentas de usuario, Código: 11-PT-01.

Artículo 122. Cuando se crea un nombre de usuario de red se debe seguir las siguientes especificaciones:

- Primera letra del nombre
- Primera letra del segundo, de no tener segundo nombre se continuara con el siguiente ítem.
- Primer apellido
- De coincidir con otro nombre de usuario se agrega un número consecutivo.

Artículo 123. Toda solicitud de acceso a los servidores debe ser enviada por escrito usando el formato establecido Código 11-PT-02, y enviarlo al correo electrónico por la persona responsable de la información al buzón admin@personeriabogota.gov.co, donde se debe especificar como mínimo:

- Nombre de la carpeta a la cual se le va permitir el acceso,
- Nombre del usuario al cual se le va dar permiso
- Clase de permiso que se le otorgo (lectura o acceso total)

Artículo 124. La dirección TIC se reserva el derecho de realizar revisiones periódicas con el objeto de cancelar cuentas de usuario redundantes o inactivas.

Capítulo 2. Nombres de grupos

Artículo 125. Los grupos globales se crearan teniendo en cuenta el recurso de red y el área o dirección a la que pertenecen los usuarios que ingresan a red, como se presenta en el anexo A.

Capítulo 3. Seguridad de las contraseñas

Artículo 126. Se requiere que los usuarios cambien las contraseñas iníciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas temporales, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.

Artículo 127. Para prevenir los ataques contra los intentos de adivinar la clave, la cuenta será desactivada después tres (3) intentos erróneos consecutivos.

Artículo 128. Solamente puede solicitar cambio de contraseña el funcionario al cual pertenece dicho usuario o el jefe inmediato mediante correo al buzón de admin@personeriabogota.gov.co.

Artículo 129. Los sistemas están configurados de tal manera que requieran contraseñas fuertes, no repetibles en un periodo de tiempo o en cambios anteriores, bloqueo de cuentas y solicitud de cambio de tiempo después de cumplido un periodo de tiempo de seis meses

Artículo 130. Se recomienda cambiar las contraseñas si se sospecha que han sido empleadas por otras personas, solicitándolo a los administradores de red.

Artículo 131. Bajo ninguna circunstancia las contraseñas de los usuarios deben ser compartidas o reveladas a otra persona porque de lo contrario el usuario está asumiendo la responsabilidad de las acciones que la otra persona toma con su contraseña.

Artículo 132. Los administradores podrán restablecer las contraseñas solamente en el evento que el usuario haya olvidado su contraseña, no sin antes haber verificado su identidad.

Capítulo 4. Contraseñas de administración

Artículo 133. Las contraseñas de administración de servicios (aplicaciones, bases de datos, dispositivos, servidores, controles de acceso, programas especiales y gestores), deben ser guardadas en documento por el Director de la Dirección TIC, y solo será entregada en momentos de aplicación de las contingencias o para propósitos específicos de instalación y configuración a los ingenieros delegados para tal fin.

Artículo 134. Las contraseñas de administración deben ser cambiadas cuando se haga uso de estas de manera regular y deben cumplir con todos los demás lineamientos generales de políticas de contraseñas establecidos en este documento.

Artículo 135. Los administradores del sistema tendrán contraseñas de administración personal las cuales están conformadas por las iniciales del nombre y la palabra admin, con la cual ingresarán a los servidores cuando necesiten realizar labores administrativas, de manera que en el log se registren los eventos realizados por cada administrador.

Artículo 136. Las contraseñas estarán bajo la responsabilidad del administrador de la red delegado por el director TIC y deben ser cambiadas bajo circunstancias normales cada 3 meses por la persona que sea delegada por la Oficina de Sistemas.

Artículo 137. Para las contraseñas administrativas se recomienda una longitud no menor a 8 caracteres.

Artículo 138. La dirección TIC se reserva el derecho de verificar el cumplimiento de seguridad de contraseñas y deshabilitar las que no cumplen con lo establecido en este documento.

Capítulo 5. Contraseñas de Administrador Local

Artículo 139. La contraseña de administrador local de una estación de trabajo nunca caduca. Esta contraseña en general para todas las estaciones de trabajo y se usa para efectos de Soporte en cada una de estas estaciones.

Artículo 140. Se recomienda la duplicidad de cuentas administrativas locales para estaciones de trabajo, la cuenta Administrador solo podrá definir el Administrador de la Red, la otra cuenta puede ser modificada y manejada por los grupos de soporte de la red.

Titulo 20. Gestión de incidentes en la seguridad de la información.

Artículo 141. Todo funcionario, contratista o tercero que haga uso de los sistemas informáticos de la Entidad deberá reportar a: admin@personeriabogota.gov.co de manera oportuna las debilidades e incidentes de seguridad que detecte o que sean de su conocimiento.

Las incidencias pueden provenir de diversas fuentes tales como usuarios, gestión de aplicaciones, soporte técnico, entre otros.

Artículo 142. El responsable de seguridad informática designado por el director TIC tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados así como su comunicación al Comité de Seguridad Informática y a los propietarios de la información.

Artículo 143. El responsable de seguridad informática junto con la Dirección de Tecnologías de Información y Comunicaciones son los responsables de establecer el proceso, procedimientos e instructivos para la gestión de incidentes de seguridad de la Información.

Artículo 144. El responsable de seguridad informática, una vez en conocimiento de un incidente, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

Artículo 145. La Entidad adoptará métodos probados, como por ejemplo el marco de referencia de ITIL, para la implementación del proceso de gestión de incidentes, el cual debe incluir los incidentes de seguridad.

El proceso debe contemplar el reporte, registro, clasificación, diagnóstico, resolución y cierre del incidente, así como el monitoreo y seguimiento del incidente.

Artículo 146. La solución de un incidente se registrará en una base de conocimientos de errores conocidos, con el fin de que pueda ser consultada y sirva de apoyo oportuno cuando un incidente se presente de manera recurrente o de pistas de solución en incidentes similares.

La recurrencia de un incidente deberá ser tratada como un problema.

Artículo 147. La entidad desarrollará un procedimiento formal de comunicaciones, que incluya el reporte, verificación, escalamiento, seguimiento, acciones de mejoras y cierre de vulnerabilidades, riesgos o incidente de seguridad que se detecten o sucedan.

Artículo 148. Se deberá documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Identificará aquellos que sean recurrentes,

con su respectivo de nivel de impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

Titulo 21. Gestión de la continuidad del negocio

Artículo 149. La Dirección TIC participará en la definición, documentación, prueba y actualización de los planes de contingencia.

Artículo 150. El Personero Distrital, el Personero Auxiliar, los Personeros Delegados para las Coordinaciones, los Personeros Delegados, los Directores y Subdirectores, así como los Jefes de Oficina, identificaran las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la entidad, evaluaran los riesgos para determinar el impacto de dichas interrupciones, identificaran los controles preventivos, y recomendaran ajustes a los planes de contingencia necesarios para garantizar la continuidad de las actividades.

Artículo 151. Los planes deben incluir procedimientos de emergencia, escenarios de contingencia, responsabilidades asignadas, directorio de contacto, plan de capacitación, plan de comunicaciones, plan de adquisiciones, pan de pruebas, entre otros aspectos.

Artículo 152. Los administradores y/o responsables de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

Artículo 153. La Dirección TIC tendrá a cargo la coordinación del proceso de administración de la continuidad de la operación de los sistemas de información de la Entidad frente a interrupciones imprevistas.

Artículo 154. Se debe realizar pruebas de cada plan de contingencia, para minimizar el riesgo de fallas por cambios en la infraestructura, por errores o malas apreciaciones y definiciones.

Titulo 22. Propiedad intelectual

Artículo 155. Se implementarán procedimientos para garantizar el cumplimiento de las normas de propiedad intelectual. El incumplimiento de las normas de propiedad intelectual puede derivar en sanciones penales, fiscales y disciplinarias.

Artículo 156. Cuando el personal de soporte técnico encuentre programas instalados en los equipos, sin el respectivo licenciamiento, procederá con la desinstalación de los mismos, efectuando el registro correspondiente e informando, según sea el caso, a la Dirección Administrativa y Financiera, y la Dirección de Talento Humano para tomar las medidas pertinentes.

Artículo 157. Las licencias de uso de software estarán bajo custodia de la Dirección de Tecnología de la Información y Comunicación. Así mismo, los manuales y los medios de almacenamiento (CD, cintas magnéticas u otros medios) que acompañen a las versiones originales de software.

Artículo 158. La Dirección TIC es la única dependencia autorizada para realizar copia de seguridad del software original. Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

El software adquirido por la Personería de Bogotá, D.C., no puede ser copiado o suministrado a terceros.

Artículo 159. Se prohíbe el uso e instalación de juegos, software pirata y pornografía en los computadores de la Personería de Bogotá, D.C.

Artículo 160. Los funcionarios, contratistas o terceros responsables de la publicación de la información en el sitio WEB de la entidad, deberán atender el cumplimiento a las normas en materia de propiedad intelectual.

Artículo 161. La entidad efectuará constantes revisiones al cumplimiento de las normas en materia de propiedad intelectual Registro de Auditoría.

Artículo 162. La Dirección de Tecnologías de Información y Comunicaciones podrá autorizar el uso de material o software declarado como de libre uso, el producido por ella misma o el producido por el titular cuando medie autorización de este, en los términos y condiciones acordados y lo dispuesto en la normatividad vigente.

Los usuarios únicamente podrán utilizar material o software autorizado por la Entidad.

Artículo 163. En el caso de requerir software adicional se deben tener en cuenta los siguientes lineamientos:

- Evaluar las necesidades de la oficina que va a ser uso del mismo
- Verificar con el proveedor los requerimientos mínimos a nivel de hardware y software donde será instalado el aplicativo
- Establecer en la contratación de desarrollo de software aplicativo a la medida, que la propiedad intelectual es de la Personería de Bogotá, D.C., por lo cual el proveedor deberá entregar el código fuente y documentación de todos los módulos, que permita a nuestros usuarios realizar los ajustes en forma autónoma. Durante el periodo de garantía del software la Entidad no deberá realizar modificaciones, porque contractualmente estas corresponden al

proveedor.

- Comprobar los niveles de conocimientos requeridos del usuario final quién manejará el aplicativo.
- En la generalidad de los casos, sólo se adquirirán las últimas versiones liberadas de los productos de software comercial seleccionados, salvo situaciones específicas que se deberán justificar ante la Autoridad de Informática y Sistemas. Todos los productos de software que se adquieran deberán contar con su licencia de uso, documentación y garantía respectivos.
- Se debe definir en los términos de contratación, los casos cuando el proveedor de equipos de cómputo, debe suministrar el software pre instalado, las respectivas licencias de uso, medios con instaladores y fuentes, los manuales de usuario, técnico y de código de errores.

Titulo 23. Comunicación y socialización de las políticas

Artículo 164. Todo funcionario o contratista que ingrese a prestar funciones o servicios deberá recibir capacitación sobre las políticas de seguridad de la información y demás aplicaciones de que dispone la Entidad en el momento de su inducción, durante la cual se darán a conocer las obligaciones para con los usuarios y las sanciones que puede acarrear su incumplimiento, y los documentos en las que están consignadas.

Artículo 165. La inducción en el puesto de trabajo referida al uso de las herramientas tecnológicas será impartida por la Dirección TIC, previa concertación de hora y lugar.

Artículo 166. La Dirección de Talento Humano remitirá a la Dirección TIC la relación de aquellos usuarios que requieran inducción sobre intranet.

Titulo 24. Supervisión y auditoria

Artículo 167. La Dirección TIC podrá acceder a la infraestructura para la inspección de todos los dispositivos informáticos conectados o no a la red para propósitos de auditoría, resolución de problemas o para investigar violaciones a las políticas establecidas toda vez que lo necesite y sin previo trámite.

Titulo 25. Cumplimiento de las políticas de seguridad informática

Artículo 168. El Personero Distrital, el Personero Auxiliar, los Personeros Delegados para las Coordinaciones, los Personeros Delegados, los Directores y Subdirectores, así como los Jefes de Oficina y el Comité de Seguridad Informática, son responsables de conocer y asegurar la implementación de las políticas de seguridad informática, dentro de sus áreas de responsabilidad, así como del cumplimiento de las políticas por parte de su equipo de trabajo.

Artículo 169. La Dirección TIC se reserva el derecho de realizar revisiones periódicas (previamente aprobadas por el Comité de Seguridad Informática) para garantizar el cumplimiento de la Política de Seguridad informática.

Todos los funcionarios y contratistas de apoyo prestarán el soporte necesario para adelantar está revisión periódica.

Artículo 170. Las revisiones periódicas se podrán realizar de manera manual o mediante el uso de herramientas de software especializadas en pruebas de penetración, detección de vulnerabilidades y verificación de controles.

En caso de ser necesario, las revisiones podrán realizarse mediante la contratación de una asistencia técnica especializada.

El resultado de las revisiones se presentará en un informe técnico para su interpretación por parte de los responsables de la seguridad informática de la Entidad.

4.1.11.Objetivos de control

Los objetivos de control son pronunciamientos donde se esboza el resultado que se desea alcanzar implementando procedimientos de control de una actividad en particular, con el fin de mitigar los riegos que se puedan presentar.

La selección de controles se basa en la Norma ISO 27001-2013 de acuerdo al análisis de riesgo realizado, como se detallan en el cuadro 11.

Cuadro 11. Objetivos de control

A5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION	
A5.1	Orientación de la dirección para la gestión de la seguridad de la información	
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.

Cuadro 11. (Continuación)

A6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION	
A6.1	Organización interna	
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A6.2	Dispositivos móviles y teletrabajo	
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A7	SEGURIDAD DE LOS RECURSOS HUMANOS	
A7.1	Antes de asumir el empleo	
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A7.2	Durante la ejecución del empleo	
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
A7.3	Terminación y cambio de empleo	

Cuadro 11. (Continuación)

A7	SEGURIDAD DE LOS RECURSOS HUMANOS	
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
A8	**GESTION DE ACTIVOS**	
A8.1	Responsabilidad por los activos	
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A8.2	Clasificación de la información	
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A8.3	Manejo de medios	
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

Cuadro 11. (Continuación)

A9	CONTROL DE ACCESO	
A9.2	Gestión de acceso de usuarios	
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
A9.3	Responsabilidades de los usuarios	
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A9.4	Control de acceso a sistemas y aplicaciones	
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
A10	**CRIPTOGRAFIA**	
A10.1	Controles criptográficos	
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
A11	**SEGURIDAD FISICA Y DEL ENTORNO**	
A11.1	Áreas seguras	
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.

Cuadro 11. (Continuación)

A11	SEGURIDAD FISICA Y DEL ENTORNO	
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A11.2	Equipos	
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso.
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A12	SEGURIDAD DE LAS OPERACIONES	
A12.1	Procedimientos operacionales y responsabilidades	
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A12.2	Protección contra códigos maliciosos	
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A12.3	Copias de respaldo	

Cuadro 11. (Continuación)

A12	SEGURIDAD DE LAS OPERACIONES	
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
A12.4	Registro y seguimiento	
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
A12.5	Control de software operacional	
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
A12.6	Gestión de la vulnerabilidad técnica	
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A12.7	Consideraciones sobre auditorias de sistemas de información	
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A13	SEGURIDAD DE LAS COMUNICACIONES	
A13.1	Gestión de la seguridad de las redes	
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A13.2	Transferencia de información	

Cuadro 11. (Continuación)

A13	SEGURIDAD DE LAS COMUNICACIONES	
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	
A14.1	Requisitos de seguridad de los sistemas de información	
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones, se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A14.2	Seguridad en los procesos de Desarrollo y de Soporte	
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.

Cuadro 11. (Continuación)

A14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.
A14.3	Datos de prueba	
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
A15	**RELACIONES CON LOS PROVEEDORES**	
A15.1	Seguridad de la información en las relaciones con los proveedores.	
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A15.2	Gestión de la prestación de servicios de proveedores	
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**	
A16.1	Gestión de incidentes y mejoras en la seguridad de la información	
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

Cuadro 11. (Continuación)

A17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	
A17.1	Continuidad de Seguridad de la información	
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A18	CUMPLIMIENTO	
A18.1	Cumplimiento de requisitos legales y contractuales	
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A18.2	Revisiones de seguridad de la información	
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Fuente: Las autoras

4.2. ETAPA 2 EJECUCIÓN

4.2.1.Plan de Tratamiento de Riesgos

El plan de tratamiento del riesgo, se definen las acciones que se van a realizar, de acuerdo a los riesgos encontrados, utilizando los controles adecuados para su detección y prevención. Conforme a la norma ISO 27001-2013, se pueden tomar cuatro diferentes acciones:

Mitigar el riesgo: Con la que se quiere disminuir el riesgo, aplicando medidas o controles adecuados.

Asumir el riesgo: Se acepta el riesgo si está dentro de los valores aceptables por la entidad, estos riesgos deben ser verificados y controlados de manera que no pasen el umbral admitido.

Transferir el riesgo a un tercero: Se traslada el riesgo a otra parte ya sea asegurando activos.

Evitar el riesgo: Esta es una de las opciones más costosas Aunque no suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo

Figura 8. Gestión de riesgos

Fuente. www.Iso27000.es

Cuadro 12. Tratamiento de los riesgos

Riesgo	Alternativa de tratamiento	Controles asociados	Acciones a Ejecutar
Abuso de privilegios de acceso	Mitigar	A.9.1.1 A.9.1.2	Establecer política de control de acceso, definir los usuarios autorizados para el acceso a la información
Acceso con clave ajena	Mitigar	A.9.2.5 A.9.3.1	Se debe establecer procedimientos para revisar los derechos de usuario, implementar políticas de seguridad
Acceso no autorizado	Mitigar	A.9.4.2 A.9.4.3	Realizar procedimientos de control de acceso, mecanismo de autenticación.
Aceleración de nuevas tecnologías generando discontinuidad de las mismas en un corto periodo de tiempo	Mitigar	A.12.1.3	Crear un grupo especial para la investigación de nuevas tecnologías, y la renovación de equipos obsoletos
Alteración de la información	Mitigar	A.9.4.1 A.12.3.1	Documentar e implementar un procedimiento de copias de respaldo.
Análisis de tráfico	Aceptar	A.13.1.1 A.13.1.2	Implementar sistemas de monitoreo de red.
Ataque destructivo	Mitigar	A.12.6.1	Implementar herramientas como firewall, para identificar vulnerabilidades
Avería de origen físico o lógico	Mitigar	A.17.1.1 A.17.1.2	Se debe establecer procedimientos para la gestión de la continuidad de la organización.
Bajo rendimiento	Mitigar	A.12.1.3	Se debe realizar un plan de gestión de la capacidad, implementando controles que indiquen problemas antes que sucedan.
Caída del sistemas por agotamiento de recursos	Mitigar	A.12.1.4 A.11.2.4	Se deben separar los ambientes de desarrollo, pruebas y producción. Se debe realizar mantenimiento de los equipos en periodos definidos
Corte del suministro eléctrico	Mitigar	A.11.2.2	Mantenimiento de UPS, y planta eléctrica
Daño por fuego	Mitigar	A.11.2.1	Sistema detección de incendios
Daños por agua	Mitigar	A.11.1.4	Mantenimiento de instalaciones físicas
Daños presentados en los equipos de comunicaciones	Mitigar	A.12.6.1	Generar un procedimiento para la gestión de vulnerabilidades
Denegación de servicio	Mitigar	A.14.2.5	Se deben establecer, documentar y mantener principios para la construcción de ambientes seguros
Desastres naturales	Mitigar	A.11.1.4 A.17.1.2	Establecer procesos y procedimientos para gestión de la continuidad del negocio. Y planes de contingencia

Cuadro 12. (Continuación)

Riesgo	Alternativa de tratamiento	Controles asociados	Acciones a Ejecutar
Destrucción de la información	Mitigar	A18.1.3	Reforzar los mecanismos de detección de intrusos y de investigación de incidentes, los registros de actividad de los sistemas se centralizan en un sistema para preservar los registros y poder investigarlos.
Difusión de software dañino	Mitigar	A.12.2.1	Actualización y administración del software de antivirus
Equipos obsoletos	Mitigar	A.12.1.3	Plan de renovación y adquisición de un buen parque de equipos tecnológicos
Error de acceso	Mitigar	A.9.1.1	Generar políticas de control de acceso, establecer herramientas que permitan su adecuado control
Errores de los usuarios	Mitigar	A.7.2.2 A.9.3.1	Se debe exigir a los usuarios el cumplimiento de las políticas de seguridad, realizar planes de capacitación
Errores de mantenimiento / actualización de equipos (hardware)	Mitigar	A.7.1.1	Contratación de personal especializado en el tema
Errores del administrador del sistema/ de la seguridad	Mitigar	A.7.1.1 A.7.1.2	Capacitación en nuevas tecnologías a los administradores.
Extracción de datos no autorizados	Mitigar	A.9.2.4 A.9.2.5 A.9.2.6	Se debe tener procedimientos formales para la asignación y retiro de derechos de acceso
Fallo de servicio de comunicaciones	Mitigar	A.11.2.3	Implementar directrices de seguridad para los elementos de comunicaciones, adquirir canales redundantes
Falta capacitación	Mitigar	A.7.2.2	Realizar planes de inducción y capacitación a usuarios
Falta de personal que brinde soporte a los aplicativos	Mitigar	A.7.1.1	Contratar el personal necesario para el correcto soporte y mantenimiento de los aplicativos.
Fugas de información	Mitigar	A.7.2.2	Implementar políticas de seguridad
Indisponibilidad del personal	Mitigar	A.12.1.1	Procedimientos de operación probados y roles de backup bien preparados
Ingeniería social	Mitigar	A.7.2.2	Sensibilizar a los usuarios sobre la seguridad de la información

Cuadro 12. (Continuación)

Riesgo	Alternativa de tratamiento	Controles asociados	Acciones a Ejecutar
Ingreso Personas no autorizadas	Mitigar	A.11.1.5	Implementar mecanismos de ingresos a las instalaciones y zonas seguras
Instalación de programas innecesarios	Mitigar	A.12.5.1 A.12.6.2	Implementar procedimientos para el control de software tanto en los servidores como de usuario
Interceptación de información (escucha)	Mitigar	A.10.1.1	Implementar controles criptográficos para la protección de la información
Modificación de la información	Mitigar	A.9.1.1	Establecer políticas de control de acceso
Modificación del sistema de archivos	Mitigar	A.9.1.1 A.9.1.2	Establecer políticas de control de acceso
Perdida de información	Mitigar	A.12.3.1	Establecer políticas de copias de respaldo.
Problemas en la configuración de los parámetros de seguridad del servidor del sistema de información	Mitigar	A.14.2.8	Definir procedimientos de pruebas de funcionalidad de la seguridad
Re-encaminamiento de mensajes	Mitigar	A.13.2.3	Fortalecer el sistema de autenticación, implementar mecanismos para acceso no autorizado
Revelación de información	Mitigar	A.13.2.4	Realizar acuerdos de confidencialidad de la información
Sabotaje	Mitigar	A.9.2.6 A.7.2.3	Realizar verificación de los derechos de acceso. Aplicar procesos disciplinarios formales en caso de violación a la seguridad
Suplantación de la identidad	Mitigar	A.7.2.2 A12.4.1	Implementar mecanismos de detección de intrusos y para la investigación de incidentes, los registros de actividad de os sistemas se centralizan en un sistema para preservar los registros y poder investigarlos
Uso no previsto	Mitigar	A18.1.3	Llevar un control de los registros de log, para análisis y fortalecimiento del sistema
Utilización indebida	Mitigar	A.14.1.2	Se debe proteger las actividades fraudulentas de la información de los servicios que utilizan redes públicas.

Fuente. Las autoras

4.2.2.Declaración de aplicabilidad

En este documento se especifican los controles que aplican, de acuerdo a las necesidades de la entidad, algunos controles de la norma no aplican a la personería de Bogotá.

Cuadro 13. Declaración de aplicabilidad

Controles y razones de selección	
RL (LR)	Requerimientos legales
OC (CO)	Obligaciones Contractuales
RN/MP (BR/BP)	Requerimientos de negocio/Adoptar mejores prácticas
RAR (RRA)	Resultados del análisis de riesgos

Control ref	Nombre control	Descripción del control	Control seleccionado				Descripción aplicación	Aplicación, Justificación de exclusión o doc referencia
			RL	OC	RN /MP	RAR		
A.5.1.1	Políticas de seguridad	Documentación de las políticas de seguridad de la información			x		Se cuenta con la documentación pero se deben aplicar las mejores prácticas para su perfeccionamiento	SI
A.5.1.2	Revisión de políticas de seguridad en la información	Las políticas de seguridad de la información se revisarán a intervalos		x			Las políticas de seguridad tiene planeadas revisiones anuales por el responsable de la seguridad	SI
A.6.1.1	Responsabilidad sobre activos	Inventario de activos	x				Se cuenta con la identificación clara de activos	SI

Cuadro 13. (Continuación)

Control ref	Nombre control	Descripción del control	Control seleccionado				Descripción aplicación	Aplicación, Justificación de exclusión o doc referencia
			RL	OC	RN	RAR		
A.6.1.2	Distribución de tareas	Las actividades se dividen para reducir oportunidades de modificaciones sin intención				x	Se tienen definidos roles de acuerdo a las taras realizadas	SI
A.6.1.3	Contacto con las autoridades	Se deben mantener contactos con las autoridades pertinentes			x		Se tienen definidos niveles jerárquicos de autoridad	SI
A.6.1.4	Contacto con grupos de interés especial	Se deben mantener contactos apropiados con grupos de interés especial y asociaciones de profesionales especializadas en seguridad						NO
A.6.1.5	Seguridad de la información en proyectos	Direccionar la seguridad en la gestión de proyectos sin importar el tipo de proyecto		x			Existe pero debe ser actualizado	SI
A.6.2.1	Políticas de dispositivos móviles	Políticas para soportar el uso de dispositivos móviles debido al riesgo que conlleva su uso			x		Complementar la Política de Seguridad, dispositivos periféricos de seguridad con reglas preestablecidas	SI
A.6.2.2	Teletrabajo	Se deben implementar políticas y medidas de seguridad para proteger la información a la que se tiene acceso						NO

Cuadro 13. (Continuación)

Control ref	Nombre control	Descripción del control	Control seleccionado				Descripción aplicación	Aplicación, Justificación de exclusión o doc referencia
			RL	OC	RN	RAR		
A.7.1.1	Selección	Clasificación del tipo de perfil y antecedentes que deben tener los empleados de acuerdo con la información a acceder			x	x	Verificación de los antecedentes de todos los candidatos a un empleo	SI
A.7.1.2	Términos y condiciones de empleo	Acuerdo de responsabilidad sobre la información		x	x		Los acuerdos contractuales con empleados y contratistas estableciendo responsabilidades conforme al uso de la información	SI
A.7.2.1	Responsabilidades de administración	Obligación contractual de aplicar las políticas y procedimientos establecidos en materia de seguridad informática		x			Se cuenta con el comité de seguridad para la coordinación de la misma	SI
A.7.2.2	Manejo de la seguridad de la información y entrenamiento	Todos los empleados cuyos contratos ameriten recibirán entrenamiento y actualización regularmente conforme a los procedimientos y políticas organizacionales	x				Implica educación y toma de conciencia	SI
A.7.2.3	Proceso disciplinario	Instauración y comunicación formal de proceso disciplinario para aquellos empleados que atenten contra la seguridad de la información				x	Se debe contar con procesos disciplinarios, claros y conformes con la normatividad vigente	SI

Cuadro 13. (Continuación)

Control ref	Nombre control	Descripción del control	Control seleccionado				Descripción aplicación	Aplicación, Justificación de exclusión o doc referencia
			RL	OC	RN	RAR		
A.7.3.1	Finalización o cambio de empleo	Las responsabilidades y deberes continuarán siendo válidos hasta la culminación del contrato de forma forzosa		x			Se informa al área responsable de la seguridad el retiro de los funcionarios	SI
A.8.1.1	Inventario de activos	Activos asociados con la información o procesamiento de la misma deben ser identificados para su conservación y mantenimiento			x		Se tiene un inventario y clasificación de los Activos de Información.	SI
A.8.1.2.	Propiedad sobre los inventarios	Mientras los activos se mantengan en el inventario constituyen propiedad de la empresa			x		Existe un inventario actualizado con los activos de información de la compañía y su respectivo responsable.	SI
A.8.1.3	Uso sobre los activos	Establecimiento de reglas sobre usos aceptables tanto de la información como de los activos asociados				x	Se debe contar con cláusulas y con guías para la clasificación y uso de Activos de Información	SI
A.8.1.4.	Regreso de activos	Con motivo de la terminación de la vinculación laboral de un empleado debe retornar todos los activos a su cargo		x			Procedimiento gestión de inventarios	SI

Cuadro 13. (Continuación)

Control ref	Nombre control	Descripción del control	Control seleccionado				Descripción aplicación	Aplicación, Justificación de exclusión o doc referencia
A.8.2.1.	Clasificación de la información	La información debe ser clasificada conforme a la normatividad vigente, valor, criticidad y sensitividad para evitar su adulteración				x	Se debe establecer un procedimiento para clasificación de la información	SI
A.8.2.2	Identificación de la información	Procedimientos apropiados para la clasificación de la información de acuerdo con el esquema adoptado por la organización			x		Se debe establecer procedimiento de etiquetado de la información	SI
A.8.2.3.	Manejo de activos	Procedimientos de manejo de activos a ser desarrollados e implementados de acuerdo con la clasificación adoptada			x		Establecer procedimiento para el manejo de activos	SI
A.8.3.1	Manejo de medios removibles	Procedimientos que deben ser implementados para el manejo de medios removibles acorde con el esquema adoptado				x	Establecer e implementar procedimiento para el manejo de medios removibles.	SI
A.8.3.2	Disposición de medios de comunicación	Medios de comunicación deben ser dispuestos tan pronto como sean requeridos usando procedimientos formales			x		Procedimiento para la eliminación de medios	SI
A.8.3.3	Transferencia de medios físicos	Los medios se deben protegidos de un eventual ingreso no autorizado			x		Procedimiento control de acceso, dispositivos de protección	SI
A.9.1	Requisitos del negocio para control de acceso	Definición de políticas de control de acceso y restricción de acceso a redes	x			x	Documento políticas de seguridad, ítem control de acceso	SI
A.9.2	Gestión de acceso de usuarios	Proceso de generación de cuentas de usuario con aviso	x		x		Se cuenta con un procedimiento para la creación, modificación y eliminación de cuentas de usuario	SI
A.9.3.	Responsabilidades de los usuarios	Uso de información de autenticación secreta	x				Documento políticas de seguridad de obligatorio cumplimiento	SI
A.9.4	Control de acceso a sistemas y aplicaciones	Se establecen procedimientos de ingreso seguro y restricción a códigos fuente	x		x		Restricción y control de uso de programas utilitarios con capacidad de anular el sistema	SI

Cuadro 13. (Continuación)

Control ref	Nombre control	Descripción del control	Control seleccionado				Descripción aplicación	Aplicación, Justificación de exclusión o doc referencia
A.10.1	Controles Criptográficos	Políticas de uso de controles criptográficos y gestión de llaves	x		x		Desarrollo e implementación de políticas sobre el uso y vida útil de llaves criptográficas	SI
A.11.1	Áreas seguras	Procedimiento para prevención y restricción de acceso a oficinas o recintos no autorizados					Se definen controles y se usan perímetros de seguridad así como la implementación de controles de acceso y de puntos de acceso	SI
A.11.2	Tratamiento de equipos	Definición y aplicación de procedimientos de ubicación, protección, mantenimiento y retiro de equipos	x		x		Medidas de seguridad que aseguran los equipos no sólo físicamente sino se previenen sesiones desatendidas	SI
A.12.1	Procedimientos operacionales y responsabilidades	Gestión de cambios e implementación de ambientes separados			x		La implementación de ambientes separados garantiza las características de la información al no ponerla en peligro	SI
A.12.2	Protección contra códigos maliciosos	Controles de detección y protección			x		Dispositivos para control de código malicioso	SI
A.12.3	Copias de respaldo	Realización de copias de respaldo tanto de la información como del software	x				Establecer procedimiento para backup y recuperación	SI
A.12.4	Registro de seguimiento	Generación de logs, sincronización de relojes y protección de la información de registro			x		Activar el registro de log y su conservación	SI
A.12.6	Gestión de la vulnerabilidad técnica	Establecer reglas de instalación de software por parte de los usuarios						NO
A.13	Seguridad de las comunicaciones	Se establecen procedimientos para la gestión de la seguridad en las redes, transferencia de la información	x		x		Seguridad periférica, documentación y procedimientos	SI
A.14	Adquisición, desarrollo y mantenimiento de sistemas	Requisitos de seguridad de los sistemas de información y seguridad en los procesos de desarrollo y soporte		x	x		Metodología para la gestión de requerimientos	SI

Cuadro 13. (Continuación)

Control ref	Nombre control	Descripción del control	Control seleccionado				Descripción aplicación	Aplicación, Justificación de exclusión o doc referencia
A.15	Relaciones con los proveedores	Seguridad de la información con los proveedores gestión de la prestación de servicios						NO
A.16	Gestión de incidentes de seguridad de la información	Procedimientos de reporte de eventos, responsabilidades, evaluación de eventos y respuesta a incidentes			x		Documento plan de contingencia	SI
A.17	Aspectos de seguridad de la información y de la gestión de continuidad del negocio	Planificación de la continuidad, Verificación, Redundancias y aseguramiento de la disponibilidad de instalaciones de procesamiento de información	x	x	x		Establecer el plan de continuidad del negocio	SI
A.18	Cumplimiento	Verificación de cumplimiento de requisitos legales y contractuales así como cumplimiento de las políticas de seguridad de la información	x	x	x		Verificación de las leyes y normatividad aplicables a la seguridad de la información	SI

Fuente. Las autoras

4.2.3.Plan de continuidad

En el último año la Personería de Bogotá a través de la Dirección de Tecnologías de Información y Telecomunicaciones incursionó en la operación de los servicios de Infraestructura en la Nube, como mecanismo de protección de los servicios más críticos de la entidad (más adelante se relacionan como identificación de procesos), lo que permitió la puesta en marcha del concepto de Data Center alterno, dando una mayor seguridad en cuanto a la continuidad de negocio, gracias a los acuerdos de niveles de seguridad NSL, concepto que enuncia que los servicios deben prestarse 99.9% del tiempo sin interrupción alguna y con replicación de la infraestructura en diferentes lugares geográficos del mundo.

No obstante, algunos recursos de la infraestructura tecnológica de la entidad siguen en producción en el Centro de Cómputo de la entidad y quedan relacionados como es debido; otros sirven de respaldo a los servicios, en caso de alguna falla de comunicación se presente, permitiendo la continuidad de operación. Aún existen vulnerabilidades informáticas que pueden poner en riesgo la gestión institucional, debido a los incidentes por fallos técnicos u operativos que podrían dejar los sistemas fuera de servicio. Así las cosas, se hace necesario conseguir una mayor redundancia de las comunicaciones internas y externas y seguir respaldando las unidades de poder y las instalaciones donde estos sistemas tienen su tablado tecnológico.

Por lo anterior y teniendo en cuenta la renovación de las comunicaciones internas, las ampliaciones de las redes y la adquisición de unidades especiales de respaldo, este Plan de Contingencias se debe renovar de acuerdo a la actual coyuntura y beneficiará la operación de las aplicaciones, los servicios, las bases de datos y los portales, entre otros procesos.

La presente actualización se refiere al tema propuesto para la aplicación de una práctica profesional en donde se desarrolle de la forma más compendiosa posible, rescatando aspectos teóricos relevantes y dejando sólo lo necesario en materia de operaciones informáticas, para hacerlo entendible, práctico y acertado a nuestra realidad. En ese orden de ideas, se reducen responsables y tareas, se condensa el procedimiento de mitigación, continuidad y recuperación y se limita a restaurar la operación y el funcionamiento normal de cualquier actividad tras la afectación producida por sucesos, previniendo la pérdida de operaciones de uno o varios servicios de infraestructura informática de la entidad.

Para implementar medidas, se evalúa a cuáles servidores no se les ha aplicado un plan de recuperación, para ejecutar la distribución de cargas y redistribución actualizada y así conocer el estado de los servicios asociados a éstos, para hacerles pruebas de tolerancia a fallos. Se formula un cronograma para llevar a cabo los planes a seguir y así evaluar el debido y correcto funcionamiento de la

infraestructura, tal y como se planeó que se estuvieran ejecutando sus correspondientes funciones desde el momento en que fueron instalados y configurados; posteriormente, se analiza viabilidad de la realización de pruebas evitando la interrupción del servicio y por ultimo registrar conclusiones y mejorar los servicios si es el caso.

4.2.3.1 Objetivo

Diseñar el plan de continuidad de la Entidad, que enuncie el procedimiento y mecanismos de prevención, mitigación y recuperación de incidentes y/o siniestros, a partir del establecimiento de gestión y controles para la protección de los procesos críticos en materia de servicios Informáticos.

4.2.3.2 Información general del plan de continuidad

4.2.3.2.1 Siniestros

Referente a los acontecimientos que rara vez se presentan como terremotos, incendios, inundaciones, atentados, robo, pérdida masiva de comunicaciones y fallas eléctricas de proporciones graves; en cuyo caso se deben aplicar las prevenciones y correcciones, con sus correspondientes etapas, solamente a las estructuras patrimoniales como demanda la ley en este aspecto.

Para este caso la Personería ya cuenta con un plan de mitigación de desastres y para el caso de la contingencia informática se aplicaran las medidas de recuperación de operaciones, contando con las actividades desarrolladas en este plan para cada uno de los responsables, previa declaración de la emergencia.

Como no existe un Centro de Datos alterno, se propone que la nube reciba las operaciones necesarias para la atención integral al ciudadano, ya que las bases de datos y aplicaciones están allí y así cumplir con la mitigación o prevención, continuidad y recuperación de negocio.

4.2.3.2.2 Incidentes que ocurren con los servicios informáticos

Incluye el respaldo de los elementos referidos a los sistemas de información, infraestructura (dispositivos, servidores y servicios), personal a cargo, y otros recursos de apoyo, y esta direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de la entidad. Infraestructura de respaldo que también es vulnerable como por ejemplo las unidades de potencia ininterrumpida (UPS) y el sistema de refrigeración del Centro de Cómputo

Los sistemas de comunicaciones (hardware y software, sistema de cableado, canales de datos y medios de transmisión) también están constantemente expuestos a riesgos por latencias, caídas o hasta perdidas de paquetes, pudiendo ser la principal fuente de problemas. Entonces el Hardware y el Software asociado a esto, también están expuestos a diversos factores de riesgo lógico y Físico, aunque no se descartan incidentes o errores humanos.

Para la contingencia en este caso, se efectuarán los procedimientos relacionados solamente en este plan, que involucran respaldo inmediato del bien afectado para la continuidad de operaciones.

4.2.3.2.3 Actividades asociadas

El plan de continuidad de operaciones es un plan de procedimientos alternativos a la forma acostumbrada de operar de la entidad, constituye una herramienta que ayuda a que los procesos críticos de la entidad continúen funcionando en una situación de desastre, aun cuando el desastre sea incontrolable en el entorno.

La realización de un plan de continuidad está conformada por cuatro fases:

Fase 1: Análisis del negocio
Fase 2: Evaluación de riesgos e impacto
Fase 3: Plan de respuesta y recuperación
Fase 4: Pruebas y mantenimiento

4.2.3.3 Fase I: Análisis del negocio

4.2.3.3.1 Organización

Según el acuerdo 514 de 2012, la entidad está conformada por el Despacho del Personero, asesorado directamente por la Oficina de Control Interno y la Oficina Asesora de Divulgación y Prensa; le acompañan tres personerías delegadas con sus correspondientes oficinas y un eje de apoyo, los cuales se muestran en la figura Nro. 4. Organigrama.

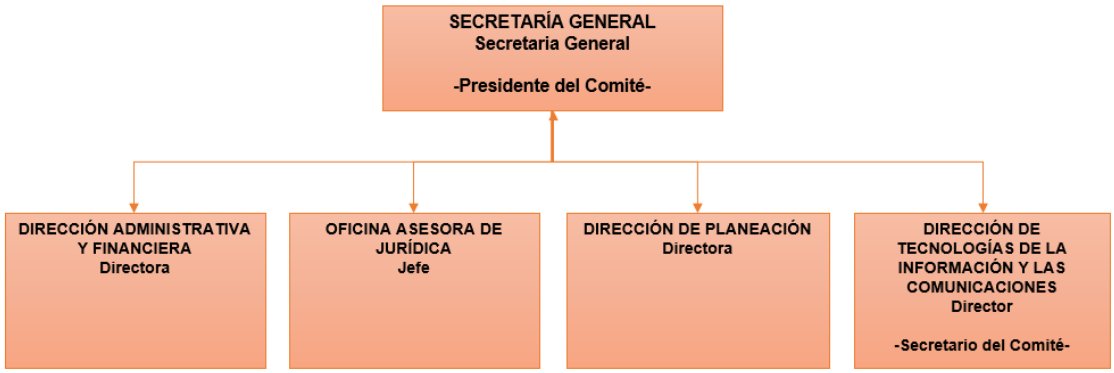
4.2.3.3.2 Compromiso de la dirección

La dirección debe comprometerse tanto para la planeación como para la implementación y pruebas del plan de continuidad, así como proveer los recursos que se requieran para su realización. De igual forma, atendiendo a las necesidades del plan en contraste con los diferentes perfiles del personal con el que cuentan, liderar la conformación de diferentes comités que faciliten el seguimiento y materialización del plan.

4.2.3.3.3 Comité de Seguridad

Para direccionar los aspectos relacionados con la seguridad informática, se ha conformado el Comité de Seguridad Informática, el cual, se encuentra integrado por personal directivo de la entidad; tiene como misión la aprobación y actualización de políticas informáticas de la entidad, revisión del Plan Estratégico de Tecnología y Comunicaciones de la entidad, definir y aprobar las normas de acceso a los servicios informáticos, recomendar políticas y definir niveles de acceso a diferentes aplicaciones, aprobación del plan de contingencias y seguridad de la Información aprobar el informe semestral y entre otras funciones. Su conformación se muestra en la figura Nro. 9

Figura 9. Comité de seguridad informática



Fuente. Las autoras

Se deben conformar los grupos de desarrollo con la anuencia del comité de seguridad. Se sugiere la estructuración del grupo técnico-profesional encargado del desarrollo, implantación y mantenimiento del plan de continuidad, quedando conformado como se relaciona a continuación

4.2.3.3.4 Comité de Sistema Integrado de Gestión

La finalidad principal de este comité es integrar y articular los sistemas de gestión de calidad con el sistema de control interno como instrumento gerencial que contribuya al mejoramiento de los servicios que ofrece la entidad y propenda por el logro de los objetivos institucionales así como la implementación de procesos con altos niveles de calidad.

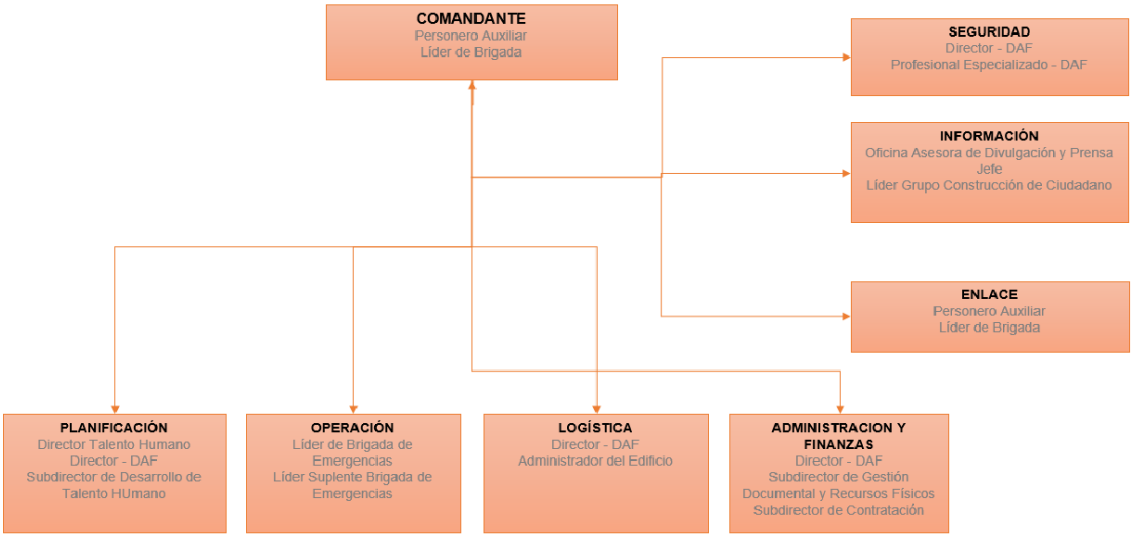
El Comité está integrado por:

- Personero de Bogotá
- Personero delegado para la coordinación de veedurías
- Secretario General
- Director de Planeación
- Jefe oficina asesora de divulgación y prensa
- Jefe de oficina de Control interno

4.2.3.3.5 Comité de Emergencias

Cada una de las dependencias tiene funciones específicas que cumplir para el normal funcionamiento de la entidad, sin embargo, en la eventualidad de que se llegara a presentar algún tipo de emergencia de grandes magnitudes, la entidad cuenta con un Plan de Emergencias general que permite la conformación de un equipo de trabajo colaborativo que atiende la emergencia, se denomina COE (Comité de Emergencias) y se compone como se muestra en la figura 10.

Figura 10. Comité de emergencias (COE)



Fuente. Las autoras

A pesar de que el comité de emergencias cumple con unas funciones institucionales generales para la aplicación del presente plan, cumple con funciones específicas asociadas a seguridad de la información, las cuales se relacionan a continuación:

Funciones

- Ordenar la documentación inherente y las evidencias de trabajo del proyecto.
- Diseñar planes de entrenamiento para los funcionarios de la entidad, a todo nivel, para que se involucren en las tareas del plan.
- Diseñar cronogramas y apoyar logísticamente las pruebas de cada segmento del plan.
- Mantener operativo el plan de contingencias.
- Coordinar las pruebas y simulacros.
- Dar orientación y apoyo en caso de emergencias mayores.

4.2.3.3.6 Coordinador del Plan de Continuidad

El coordinador del Plan es el canal de comunicación entre el grupo de Comité Técnico Operativo y el Comité de Seguridad, a través del cual se transmitirán las decisiones tomadas en torno a las acciones del Plan, los niveles de ejecución del Plan y el estado de los recursos informáticos que cubre el Plan. Debe encargarse de monitorear y asegurar el cumplimiento estricto del Plan y del mantenimiento de los canales de comunicación entre los diferentes grupos de trabajo. Proveer los recursos necesarios y notificar las decisiones a los funcionarios delegados.

El Director de Tecnologías, coordinador del Plan, junto con el oficial de la seguridad informática, elaborará el plan de trabajo para el desarrollo e implantación del proyecto y conformará subgrupos de trabajo para la ejecución de cualquier incidente.

4.2.3.3.7 Comité técnico operativo

Funciones generales

- Coordinar el desarrollo, implantación y mantenimiento del Plan para la recuperación del Sistema de Información o la utilización de sistemas alternos.
- Efectuar el seguimiento a los costos en que se incurre en el desarrollo e implantación del Plan.
- Aprobar y formular recomendaciones ante el Comité de Seguridad acerca del establecimiento de convenios, contratos o compras de elementos para el desarrollo del Plan.
- Manejar los convenios y/o contratos que se hayan firmado para el desarrollo del Plan.
- Recomendar acerca de la compra y/o mantenimiento de hardware, software o instalaciones, si se requieren.
- Efectuar las pruebas que garanticen la plena operatividad del Plan.
- Mantener operativo el Plan.
- Verificar que se estén realizando los backup internos y externos.

- Realizar simulacros periódicos, por lo menos una vez al año, con los sistemas alternos, con el fin de mantener activos a los miembros del equipo y vigente el Plan.
- Garantizar que existan personas que puedan reemplazar a los funcionarios claves en los procesos de recuperación.
- Verificar que la infraestructura de respaldo, siempre esté disponible y listo para atender la contingencia.

La conformación y funciones específicas de cada uno de los miembros del comité se detallan a continuación:

Ingeniero Documentador

- Se encargará de mantener la información actualizada y el Plan
- Elaborar el plan de trabajo para el desarrollo e implantación del Plan.
- Documentar el Plan para la recuperación del servicio.
- Resguardar la documentación de procesos y procedimientos informáticos, protocolos y guías necesarias para la ejecución de planes respectivos.
- Control periódico de los estándares, protocolos y procedimientos Informáticos
- Disponer de acceso inmediato a los documentos en caso de una contingencia.

Ingeniero encargado Soporte Técnico

- Se encargará de mantener los inventarios de los bienes informáticos actualizados.
- Garantizar la operatividad de los equipos de cómputo y en coordinación con las Redes mantenerlas operativos.
- Efectuar el monitoreo permanente de los componentes de Hardware.
- Coordinar la instalación de nuevos equipos.
- Garantizar mantenimiento preventivo y correctivo de los equipos y medios de transmisión.
- Proveer soporte técnico a los usuarios
- Instalar equipos de cómputo y los elementos de soporte eléctrico.

Ingeniero encargado de la Infraestructura

- Se encargará de mantener los inventarios de su infraestructura actualizados.
- Actualizar bitácora correspondiente.
- Garantizar la operatividad de la Infraestructura (servidores y Servicios).
- Coordinar la instalación de nuevos equipos relacionados con el Comité Técnico Operativo.

- Elaborar Copias de Respaldo (backups)
- Disponer de acceso inmediato a los backups cuando se requieran.

Ingeniero encargado de bases de datos

- Velar por que los procedimientos establecidos para proveer los backups se apliquen.
- Actualizar bitácora correspondiente.
- Mantener actualizados los manuales de procedimientos para backup.
- Garantizar que los backups disponibles para los sistemas alternos de respaldo estén actualizados.
- Atender a los usuarios y prestar la asesoría que le sea requerida.

Ingeniero encargado de Sistemas de Información

- Revisar los procedimientos para la actualización de archivos y las bases de datos.
- Actualizar bitácora correspondiente.
- Revisar, implementar y actualizar los procedimientos de instalación de software operativo y aplicativo.
- Modificar procesos e instruir a los usuarios sobre el manejo de los sistemas.
- Garantizar la existencia de copias de respaldo del software Operativo, Aplicativo y utilitario.
- Coordinar las tareas que deben ejecutar los responsables de los aplicativos críticos en el momento de la contingencia.

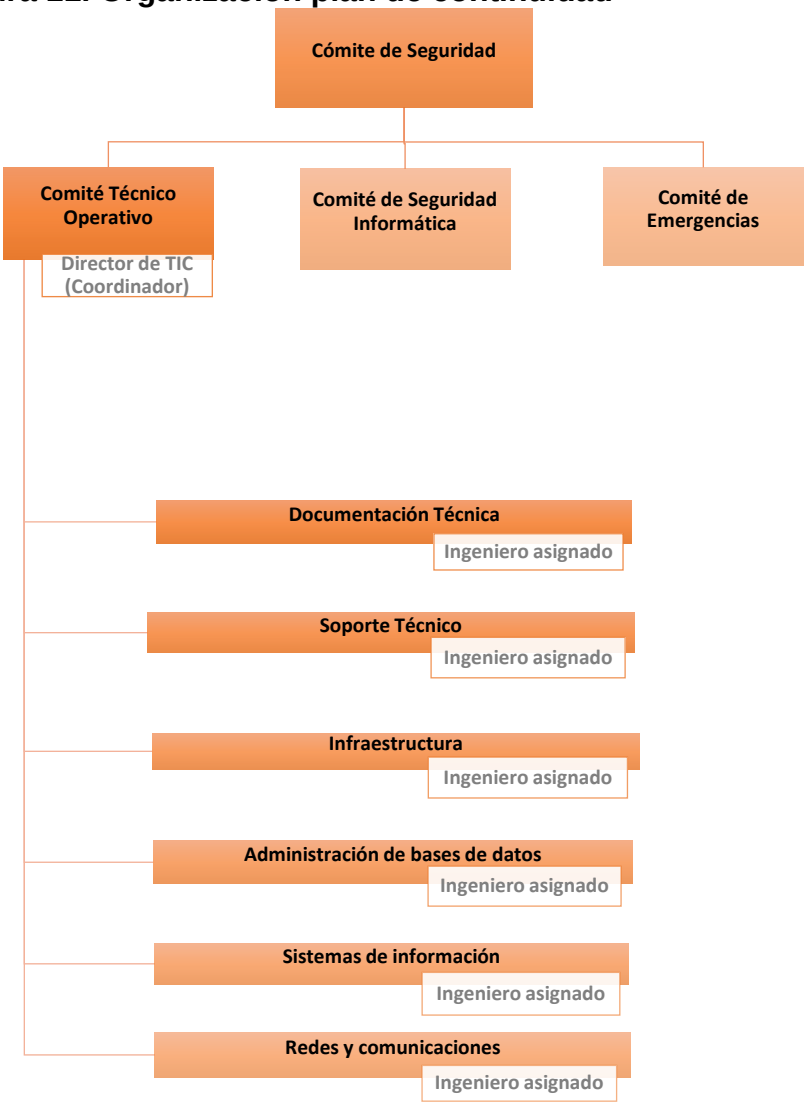
Ingeniero encargado de Redes y Comunicaciones

- Garantizar la operatividad de la Infraestructura (Servicios sistemas de información de la Personería), desde el punto de vista de las comunicaciones.
- Actualizar la bitácora correspondiente.
- Efectuar el monitoreo permanente de los componentes involucrados en la red de transmisión de datos.
- Adecuar el equipo de comunicación y reconfiguración de la red de transmisión de datos.
- Mantener contacto permanente con proveedor de Internet.

Un funcionario de la Dirección de TIC cumple las funciones de oficial de seguridad y vela constantemente por el cumplimiento de las políticas de seguridad institucionales, haciendo permanentemente recomendaciones para optimizar tanto su cumplimiento como la actualización permanente del presente plan. De igual forma, un Asesor con conocimiento en seguridad informática, es la mano derecha del Director de TIC y le brinda el apoyo suficiente como para saber qué estamento

del Comité de Contingencia y Seguridad debe ser activado según la situación y apoya en la formulación de estrategias de mejoramiento permanente sobre las acciones ejecutadas por cada uno.

Figura 11. Organización plan de continuidad



Fuente: Las autoras

4.2.3.4 Fase II: Evaluación de riesgos e impacto

Para realizar un análisis de los riegos, se procede a identificar los objetos que deben ser protegidos, los riesgos residuales, los potenciales riesgos secundarios, su impacto en la entidad, y su importancia dentro del funcionamiento.

Subsiguientemente se procede a realizar los pasos necesarios para minimizar o anular la ocurrencia de eventos que faciliten los daños, y en caso de ocurrencia de estos, se procede a fijar un plan de ejecución para su recomposición o minimización de las pérdidas y/o los tiempos de reemplazo o mejoría.

4.2.3.4.1 Identificación de Riesgos

A continuación se presenta la lista de los riesgos más comunes ocurridos en la entidad, sobre los cuales se priorizará una acción de mitigación, que se debe plasmar en el plan de prevención

Datos / Información

- Errores de los usuarios
- Errores del administrador del sistema/ de la seguridad
- Alteración de la información
- Destrucción de la información
- Fugas de información
- Suplantación de la identidad
- Abuso de privilegios de acceso
- Acceso no autorizado
- Modificación de la información
- Destrucción de la información
- Revelación de información

Servicios

- Errores de los usuarios
- Errores del administrador del sistema/ de la seguridad
- Alteración de la información
- Destrucción de la información
- Fugas de información
- Caída del sistemas por agotamiento de recursos
- Suplantación de la identidad
- Abuso de privilegios de acceso
- Uso no previsto
- Acceso no autorizado
- Repudio (negación de actuaciones)
- Modificación de la información
- Destrucción de la información
- Revelación de información
- Denegación de servicio

Aplicaciones

- Avería de origen físico o lógico
- Errores de los usuarios

- Errores del administrador del sistema/ de la seguridad
- Difusión de software dañino
- Alteración de la información
- Destrucción de la información
- Fugas de información
- Vulnerabilidades de los programas (software)
- Errores de mantenimiento /actualización de programas
- Suplantación de la identidad
- Abuso de privilegios de acceso
- Uso no previsto
- Acceso no autorizado
- Modificación de la información
- Destrucción de la información
- Revelación de información
- Manipulación de programas

Equipamiento Informático

- Fuego
- Daños por agua
- Desastres naturales
- Desastres industriales
- Avería de origen físico o lógico
- Corte del suministro eléctrico
- Errores de mantenimiento /actualización de equipos
- Caída del sistemas por agotamiento de recursos
- Perdida de equipos
- Abuso de privilegios de acceso
- Uso no previsto
- Acceso no autorizado
- Manipulación de hardware
- Denegación de servicio
- Robo de equipos
- Ataque destructivo

Redes de comunicaciones

- Fallo de servicio de comunicaciones
- Errores del administrador del sistema/ de la seguridad
- Errores de [re]encaminamiento
- Errores de secuencia
- Alteración de la información
- Fugas de información
- Caída del sistemas por agotamiento de recursos
- Suplantación de la identidad
- Abuso de privilegios de acceso

- Uso no previsto
- [Re-]encaminamiento de mensajes
- Alteración de secuencia
- Acceso no autorizado
- Análisis de tráfico
- Interceptación de información (escucha)
- Modificación de la información
- Destrucción de la información
- Revelación de información
- Denegación de servicio
- Ataque destructivo

Equipamiento Auxiliar

- Desastres naturales
- Errores de mantenimiento / actualización de equipos (hardware)
- Uso no previsto
- Manipulación del hardware
- Ataque destructivo
- Acceso no autorizado
- Contaminación medioambiental
- Daños por agua
- Fuego

Instalaciones

- Fuego
- Daños por agua
- Desastres naturales
- Fuego
- Desastres industriales
- Contaminación electromagnética
- Suplantación de la identidad
- Abuso de privilegios de acceso
- Uso no previsto
- Acceso no autorizado
- Ataque destructivo

Personal

- Alteración de la información
- Destrucción de la información
- Fugas de información
- Indisponibilidad de la información
- Modificación de la información
- Revelación de información
- Indisponibilidad del personal

- Extorsión
- Ingeniería social
- Errores humanos
- Falta capacitación

4.2.3.4.2 Probabilidad de riesgo

Para que un riesgo sea considerado como amenaza al servicio, su probabilidad de ocurrencia debe ser superior a cero. De igual forma, la probabilidad de riesgo debe ser inferior al 100% pues en caso contrario correspondería a una certeza de ocurrencia de un evento. La probabilidad se puede entender también como la posibilidad de lograr un efecto, porque si la condición se produce, se supone que la posibilidad de que suceda será del 100%. Esta probabilidad la clasificaremos así:

Cuadro 14. Matriz de riesgo

MATRIZ DE RIESGOS		
PROBABILIDAD		
EFECTO	**VALORACIÓN**	**CRITERIO**
Raro	15%	Puede ocurrir excepcionalmente.
Posible	22%	Puede ocurrir en cualquier momento del futuro.
Probable	27%	Ocurre ocasionalmente
Casi cierto	36%	Ocurre en la mayoría de las circunstancias.

Fuente: https://protejete.wordpress.com/

4.2.3.4.3 Impacto de riesgos

El impacto del riesgo mide la gravedad de los efectos adversos, o la magnitud de una pérdida, causados por la ocurrencia. Es una valoración aplicada al riesgo, para describir su impacto relacionado con la prestación del servicio normal. Cuanto mayor sea el número, mayor es el impacto.

Cuadro 15. Impacto del Riesgo

IMPACTO		
IMPACTO	**VALORACIÓN**	**CRITERIO**
Insignificante	1	Pérdida de control, operaciones, Información y/o equipamiento no sensibles.
Moderado	2	Pérdida de control, operaciones, Información y/o equipamiento medianamente sensibles.

Fuente: https://protejete.wordpress.com/

Cuadro 15. (Continuación)

		IMPACTO
IMPACTO	**VALORACIÓN**	**CRITERIO**
Mayor	3	Pérdida de control, operaciones, información y/o equipamiento medianamente sensibles que pueden causar retraso o interrupción de servicios.
Catastrófico	4	Pérdida de control, operaciones, Información y/o equipamiento críticos que puede causar daño serio de infraestructura o destrozo patrimonial

Fuente: https://protejete.wordpress.com/

4.2.3.4.4 Exposición a riesgos

La exposición al riesgo es el resultado de multiplicar la probabilidad por el impacto. En ocasiones, un riesgo de alta probabilidad tiene un bajo impacto y se puede ignorar sin inconvenientes; otras veces, un riesgo de alto impacto tiene una baja probabilidad, por lo que también se podría pensar en ignorarlo, en cuyo caso habrá que considerar también la criticidad de dicho evento. Los riesgos que tienen un alto nivel de probabilidad y de impacto son los que más necesidad tienen de administración, pues son los que producen los valores de exposición más elevados.

Cuadro 16. Exposición al riesgo

EXPOSICION					
Probabilidad	15%	0,15	0,3	0,45	0,6
	22%	0,22	0,44	0,66	0,88
	27%	0,27	0,54	0,81	1,08
	36%	0,36	0,72	1,08	1,44
		1	2	3	4
		Impacto			

Fuente: https://protejete.wordpress.com/

Cuadro 17. Ponderación del riesgo

PONDERACIÓN	
Prioridad A	Riesgo Alto:Requiere medidas a tomar de manera urgente. (Igual o mayor a 1)
Prioridad B	Riesgo Moderado: Requiere medidas necesarias a tomar. (Entre 0,5 y 0,99)
Prioridad C	Riesgo Bajo: No requiere medias a tomar, aunque se tendrá en permanente vigilancia. (Entre 0 y 0,49)

Fuente: https://protejete.wordpress.com/

4.2.3.4.6 Sistemas de información

De acuerdo con la prioridad de los riesgos y el impacto generado, se arroja como resultado la siguiente relación de procesos críticos, con prioridad alta, media y baja, procesos que deben estar disponibles 99.9%.

Cuadro 18. Prioridad A – Sistemas de Información

SISTEMA INTEGRADO DE PROCESOS SINPROC	
Objetivo: Sistema para el registro, consulta y modificación de procesos Misionales	
RESPONSABLES	COMPONENTES CRITICOS
Encargado del sistemas de información Ingeniero de área Ingeniero Junior – Ing Desarrolladores	Antecedentes disciplinarios
	Firma Digital de antecedentes (Hilopas)
	Modulo Quejas por internet QRSD
SISTEMA INTEGRADO DE PROCESOS SINPROC	
RESPONSABLES	COMPONENTES CRITICOS
Encargado del sistemas de información Ingeniero de área Ingeniero Junior Ingenieros desarrolladores	Módulo Procesos disciplinarios
	Módulo de Requerimiento Ciudadano (Personal y Escrito)
	Módulo de fallos
	Módulo de Querellas
	Modulo Centros Comerciales
	Módulo de Tutelas
	Módulo de Ministerio Publico (Familia)
	Modulo Grupo Pas (Pendientes por asignar y Visita a Hospitales)
	Módulo de Conciliaciones
BASE DE DATOS	Weboido , Siafi2
DEPENDENCIAS DEL SERVICIO	Servidor de Aplicaciones App, Ficha Técnica Servidores Servidor de Base de datos BDPerso Servicio DNS´s, EXTERNO Servicio de Internet Red LAN, Diagrama de Red Interna y Externa
Uso: 7X24	
Usuarios: Delegadas Disciplinarios I, II, III, IV.	

Policivo, C.A.C., Oficina Jurídica, Ministerios Públicos, Finanzas, Asuntos de Gobierno, Línea 143, Grupo Req. Ciudadano, Oficina de Conciliaciones, Grupo PAS, Derechos Humanos,Operadores: Asesores y Secretarias

Cuadro 19. (Continuación)

SISTEMA PERNO	
Objetivo: Sistema para el registro, consulta y modificación de Novedades de la Nómina de la Entidad	
RESPONSABLES	COMPONENTES CRITICOS
Encargado del sistemas de información Ingeniero de área Ingeniero Junior Grupo - Subdirección De Gestión De Talento Humano	Hojas de Vida
	Liquidación
	Consultas de Nómina
	Novedades
BASE DE DATOS	Sicapita
DEPENDENCIAS DEL SERVICIO	Servidor de Aplicaciones App03, Servidor de Base de datos BDPERSO Servicios DNS´s Servidor Persobogota1 Servicio de Internet Red LAN
Uso: 5X8 Usuarios: Todos los funcionarios de Planta de la Personería Operadores: Grupo de Subdirección de Gestión de Talento Humano	
SISTEMA CORDIS	
Objetivo: Sistema para el registro y consulta de la Correspondencia Interna y Externa de la Entidad	
RESPONSABLES	COMPONENTES CRITICOS
Encargado del sistema de información Ingeniero Junior Ingeniero de área Grupo - Secretaria General Correspondencia	Registro de correspondencia Interna y Ext.
	Seguimiento documental
	Etiquetas para el envío y recepción
BASE DE DATOS	Siafi2
DEPENDENCIAS DEL SERVICIO	Servidor de Aplicaciones App02, Ficha técnica Servidores de Respaldo y Contingencia Servidor de Base de datos DBCONTI, Servicios DNS´s Servidor Persobogota1 Servicio de Internet Red LAN
Uso: 5X8	

Usuarios: Todas las dependencias de la Personería
Operadores: Secretarias de dependencias

Cuadro 20. Prioridad B - Sistemas de Información

SISTEMAS EMERGENTES	
Objetivo: Sistema para el registro de información relacionada con el requerimiento ciudadano en los Centros Comerciales, mapa de procesos más críticos y agenda xxx	
RESPONSABLES	COMPONENTES CRITICOS
Ingeniero encargado del sistema de información	 Sistema Radar
BASE DE DATOS	Weboido
DEPENDENCIAS DEL SERVICIO	Servidor de Aplicaciones App Servidor de Base de datos BDPERSO Servicios DNS´s Servidor Persobogota1 Servicio de internet Red LAN
Uso: 7X24 Usuarios: usuarios externos Operadores: Línea 143	
SISTEMAS DIGITURNO	
Objetivo: Sistema para el llamado de turnos en el Centro de Atención a la Ciudadanía y Delegada para Protección de Víctimas del Conflicto Armado	
RESPONSABLES	COMPONENTES CRITICOS
Encargado del sistema Ingeniero Junior	Módulos de atención Módulos virtuales de selección Módulo de tableros de llamados
BASE DE DATOS	DIGITURNO4.5
DEPENDENCIAS DEL SERVICIO	Servidor Digiturno-pc, Servicio de Canal de datos Sedes externas, Interconexión sedes externas Red LAN Impresora EPSON Monitores de turnos
Uso: 5X8 Usuarios: Ciudadano que visita la entidad para la solución de temas relacionados con:Servicios Públicos, Atención Prioritaria en Salud, Consultas de Tutelas,	

Consultas por Servicios Públicos, Derecho al Trabajo, Derecho Consumidor, Impugnación y Desacatos, Orientación Jurídica, Otros Servicios, Pensiones, Salud, Tutelas, Restitución de tierras, Víctimas del conflicto armado, Operadores: Funcionarios Asesores del centro de Atención y de Delegada de victimas

Cuadro 20. (Continuación)

SISTEMA ADMINISTRATIVO Y FINANCIERO EXTRANET	
Objetivo: Es una herramienta informática creada por la Secretaría Distrital de Hacienda (SDH) para satisfacer las necesidades de administración de la información en entidades del sector público, de los niveles nacional, territorial y distrital. Está integrada por componentes administrativos, financieros, tributarios y pensionales.	
RESPONSABLES	COMPONENTES CRITICOS
Ingeniero de Soporte Técnico encargado Funcionarios de Secretaria De Hacienda ETB	Presupuesto (Modulo Predis)
	Cronograma de presupuesto (Modulo Opget)
	Planillas de Pagos (Modulo Opget)
	Plan de cuentas (Modulo PAC)
DEPENDENCIAS DEL SERVICIO	Enrutador de Hacienda Red LAN Configuración especial del HOST de las estaciones Instructivo para instalar un cliente Secretaria de Hacienda o Planeación
BASE DE DATOS	10.168.13.7
Uso: 7X24 Usuarios: Dirección administrativa y Financiera Dirección de Talento Humano Sub Dirección Administrativa y Financiera Operadores:	

Fuente: Las autoras

Cuadro 21. Prioridad C - Sistemas de Información

SISTEMA DE CONTROL DE VISITANTES	
Objetivo: Es una herramienta encargada de administrar, ordenar, dirigir o regular el control de acceso a la entidad de agentes externos o visitantes	
RESPONSABLES	COMPONENTES CRITICOS
Subdirección de Gestión Documental y Recursos Físicos - Admón. Edificio	Software Base de datos
	Módulo de captura
DEPENDENCIAS DEL SERVICIO	Red LAN

BASE DE DATOS	Visitantes
Uso: 5X8 Usuarios: Sub Dirección Administrativa y Financiera Operadores:	

Fuente: Las autoras

4.2.3.4.7 Servicios

Cuadro 22. Prioridad A – Servicios

CORREO ELECTRONICO	
Consideración	**Observación**
Nivel de importancia de la aplicación en la entidad	Alto
Impacto operativo, financiero o contable	4
Oportunidad de servicio	Trabajo colaborativo otorgado por la Alcaldía de Bogotá
Programas críticos	Agenda
	Herramientas colaborativas
	Drive
	Chat
	Listas de distribución
Usos críticos	Comunicación interna y externa de los funcionarios de la entidad, envío y recepción de información y archivos de carácter urgente Notificaciones a los investigados, etc. Dispositivos Móviles. Compartición de documentos y trajo simultáneo desde cualquier lugar. Comunicación en tiempo real y realización de video conferencias, entre equipos de trabajo. Creación Sitios web.
Comunicaciones: Entrada y salida de datos	Ingreso de información archivos y temas
	Envío de información archivos y temas
	Backup de correos y archivos
	Mensajería Instantánea
	Compartición de Archivos
Dependencias del Servicio	Servicio de Internet Canal de Datos

	Red LAN Convenio Interadministrativo anual.

Cuadro 22. (Continuación)

INTRANET	
Consideración	**Observación**
Nivel de importancia de la aplicación en la entidad	Medio
Impacto operativo, financiero o contable	2
Oportunidad de servicio	Trabajo colaborativo que día tras día se convierte en la herramienta primordial de acceso a operaciones y procesos críticos
Programas críticos	Portal de Oracle
	Java Run time
	WorkFlow
	Digifile
Usos críticos	Acceso a los servicios en línea Acceso a los procedimientos de la entidad Acceso a los formularios Acceso a temas de interés de los funcionarios
Comunicaciones: entrada y salida de datos	Documentos
	Servicios
	Normativas
	Información de interés general interno
Dependencia	DNS Interno, Servidor Persobogota1 Base de datos INTRANET Red de datos LAN Servidor App Servidor INTRANET.SRV,
PAGINA WEB	

Consideración	Observación
Nivel de importancia de la aplicación en la entidad	Alto
Impacto operativo, financiero o contable	4

Cuadro 22. (Continuación)

Consideración	Observación
Oportunidad de servicio	Imagen corporativa; servicios al ciudadano, antecedentes disciplinarios en línea
Programas críticos	JOOMLA
	Java
	PHP
	MySqL
	Servicios Intranet
	Indagar
Usos críticos	Portal de acceso a la información para el ciudadano Expedición de antecedentes Disciplinarios WEB Quejas por internet
Comunicaciones: entrada y salida de datos	Correos en línea
	Chat
	Foros
Dependencia	DNS Interno y Externo Servicio de Internet Base de datos *DBPERSONERIA* Red de datos LAN Servidor WEB,

Fuente: Las autoras

Cuadro 23. Prioridad B – servicios

ACCESO A INTERNET	
Consideración	**Observación**
Nivel de importancia de la aplicación en la entidad	Alta

Impacto operativo, financiero o contable	3
Oportunidad de servicio	Contacto con Proveedores, otros agentes de ministerio público, acceso a los portales de Gestión, Renovación Tecnológica, Investigación
Programas críticos	Portal de contratación Sivicof
	Acceso a ACUEDUCTO
	Indagar

Cuadro 23. (Continuación)

Consideración	**Observación**
Usos críticos	Normativa
	Noticias relacionadas con la misión de la entidad
	Teleconferencias
	Capacitación
Comunicaciones: entrada y salida de datos	Descargas de documentos, archivos e información
	Consulta de información, etc. Indagar
Dependencia	Canal de datos de Internet ETB, Contrato 450/13 Firewall de acceso Perimetral DNS Interno y Externo Red LAN
DIRECTORIO ACTIVO	
Consideración	**Observación**
Nivel de importancia de la aplicación en la entidad	Medio
Impacto operativo, financiero o contable	3
Oportunidad de servicio	Software libre mantenido con contrato de soporte a LINUX
Programas críticos	Samba 4
	DNS
	Indagar
Usos críticos	Acceso de los usuarios a los Computadores de la red
	Políticas de directivas de grupo
	Compartición CONTROLADA de archivos LAN

	Papel tapiz
	Instalación de programas
Comunicaciones: entrada y salida de datos	N/A
Dependencia	Red LAN Servidor PERSOBOGOTA1 y todos sus servicios,

Fuente: Las autoras

4.2.3.4.8 Bases de Datos

Cuadro 24. Prioridad A - Base de Datos

Consideración	Observación
Nivel de importancia de la aplicación en la entidad	Alto
Impacto operativo, financiero o contable	4
Oportunidad de servicio	El motor de base de datos es muy estable y maneja seguridades de acuerdo a su afinamiento y administración
Productos críticos	ASM
	Enterprise manager
	LISTENER
	SQL/PLUS
	Indagar
Usos críticos	Instancia ORCL
	Instancia de WEBOIDO (Sistema Sinproc)
	Instancia de Siafi2 (Correspondencia)
	Instancia de Sicapita (siprueba)
	Instancia INTRANET
Comunicaciones: entrada y salida de datos	Información misional
	Información critica
Dependencia	Red LAN, DNS interno y externo Canal de datos de Internet ETB Firewall de acceso perimetral Servidor BDPERSO

Fuente: Las autoras

4.2.3.4.9 Antivirus

Cuadro 25. Prioridad A – Antivirus

Consideración	Observación
Nivel de importancia de la aplicación en la entidad	Alto
Impacto operativo, financiero o contable	3
Oportunidad de servicio	Todos los días hay nuevas amenazas, el antivirus es una herramienta que mediante consola automatiza toda actualización y no necesita instalarse si desplegar un agente liviano

Cuadro 25. (Continuación)

Consideración	Observación
Productos críticos	Consola ePO
	Agente McAfee
	Motor 8.8 última versión ePA
	SQL/PLUS
	DLP (para dispositivos)
	Indagar
Usos críticos	Escaneo automático
	Impide la instalación de programas
	Limpia y elimina virus
	Impide ingreso de código malicioso
Comunicaciones: entrada y salida de datos	N/A
Dependencia	Red LAN Directorio Activo, Servidor Persobogota1 Servidor CONSOLAEPO,

Fuente: Las autoras

Prioridades: La estimación de los daños en los bienes y su impacto, establece la prioridad en relación al tiempo estimado y los recursos necesarios para la recuperación de los servicios afectados con el incidente.

Por lo tanto los activos valorados como prioridad A o más alta, serán los tenidos en cuenta en el proceso de restablecimiento ante un evento.

4.2.3.4.10 Fuentes de daño

- Accesos no autorizados
- Código malicioso (Virus, sabotaje).

- Mala operación o malas intenciones.
- Desastres Naturales
- Fallas en la infraestructura de soporte (UPS´s, Sistema de aire acondicionado)
- Fallas de la red de energía eléctrica pública por diferentes razones ajenas al manejo por arte de la entidad.
- Fallas de las comunicaciones.
- Abandono de sus puestos de trabajo.
- Otros imponderables.
- Fallas de Hardware

4.2.3.5 Fase III: Plan de respuesta y recuperación

4.2.3.5.1 Medidas preventivas

Control de Accesos: El control de acceso reside en la autorización, autenticación, autorización de acceso y auditoría, donde se definen medidas efectivas para controlar el ingreso a los activos computacionales:

- Acceso físico de personas no autorizadas.
- Acceso a la Red de PC's y Servidores.
- Acceso restringido a las librerías, programas, y datos.

Respaldos: Resguardo adecuado de los dispositivos críticos. Las fallas de los equipos de procesamiento de información pueden minimizarse mediante el uso de otros equipos, a los cuales también se les debe controlar periódicamente su buen funcionamiento, entre los cuales se cuenta:

- UPS de respaldo de actual Centro de Computo
- Centro de datos alterno

Seguridad Física del Personal: Tomando las medidas adecuadas que permitan mejorar los niveles de seguridad, capacitando apropiadamente al personal, soportando personal de respaldo en funciones o reemplazos en caso de desastres, emergencias o períodos de ausencia ya sea por vacaciones, permisos, calamidades o enfermedad.

Seguridad de la Información: La información y programas de los Sistemas de Información que se encuentran en el Servidor, o de otras estaciones de trabajo críticas deben protegerse mediante claves de acceso y a través de un plan de respaldo adecuado.

Plan de mitigación y respaldo: El Plan de Respaldo trata de cómo se llevan a cabo las acciones críticas entre la pérdida de un servicio o recurso, y su recuperación y/o restablecimiento. Todos nuevos diseños de Sistemas, o proyecto realizado deben tener un plan de respaldo. Se deben tener presentes las bitácoras como documentación de eventos que sirven de apoyo para restablecer un servicio con ocurrencia repetida.

Respaldo de datos Vitales: Identificar las áreas para realizar respaldos:

- Sistemas de Información.
- Configuraciones e instalaciones
- Sistemas de Red.
- Sistemas de backup
- Nube

4.2.3.5.2 Reacción Inicial

El responsable de la seguridad informática quien declara la emergencia debe:

- Determinar qué clase de siniestro o incidente se ha presentado.
- Dar aviso al administrador de edificio en caso necesario.
- Notificar a los miembros del equipo de recuperación que se consideren necesarios, de acuerdo con el tipo de suceso presentado.
- Notificar a los miembros del Comité de Seguridad sobre el estado de la emergencia.
- Mantener actualizados a los funcionarios sobre la evolución de la emergencia.
- Nombrar otros miembros del equipo cuando así lo exijan las circunstancias.
- Definir los servicios que se deban trasladar de la nube publica al Data Center de la entidad o viceversa, en caso de que el siniestro así lo requiera.
- Analizar las alternativas de procesamiento de acuerdo con la evaluación del daño.
- Establecer los controles que considere necesarios para llevar a cabo las actividades del plan, en forma confiable.
- Determinar, con los otros miembros y con el proveedor del equipo, la magnitud del daño generado por el siniestro y establecer si se requiere poner en marcha el Plan.
- Reunir al Comité de Seguridad para informarle sobre el estado de emergencia y solicitar autorización para la puesta en marcha del Plan.
- Poner en marcha el Plan.

4.2.3.5.3 Plan para traslado al respaldo

- Efectuar una reunión inicial del equipo humano de recuperación para distribuir las tareas y responsabilidades asignadas de acuerdo al Plan de recuperación.
- Coordinar los recursos de comunicación para la activación de los procesos de restauración, grabación y puesta en marcha en la Nube pública.
- Obtener los medios de los Backups en su versión más actualizada en caso de pérdida de información.
- Mantener informado al Comité de Seguridad por escrito.
- Nombrar otros miembros del equipo cuando así lo exijan las circunstancias.
- Ordenar, junto con los otros miembros del equipo, el traslado a los Sistemas Alternos de los recursos adicionales que se requieran.

4.2.3.5.4 Tareas en sitio alterno de respaldo

- Verificar que se estén efectuando adecuadamente los procedimientos de recuperación.
- Coordinar el flujo de los documentos e información entre la Personería y los sistemas alternos.
- Coordinar que se provean los recursos para la ejecución normal de las labores en la Nube Pública o viceversa según la contingencia.
- Verificar los informes de funcionamiento de las aplicaciones críticas, con el fin de asegurar su adecuada operación.
- Autorizar la operación de las aplicaciones críticas.
- Revisar los informes obtenidos en la ejecución de las aplicaciones críticas.
- Verificar y analizar que la información producida sea confiable, con base en los controles definidos.
- Mantener constantemente informado al Comité de Seguridad sobre la evolución del plan.

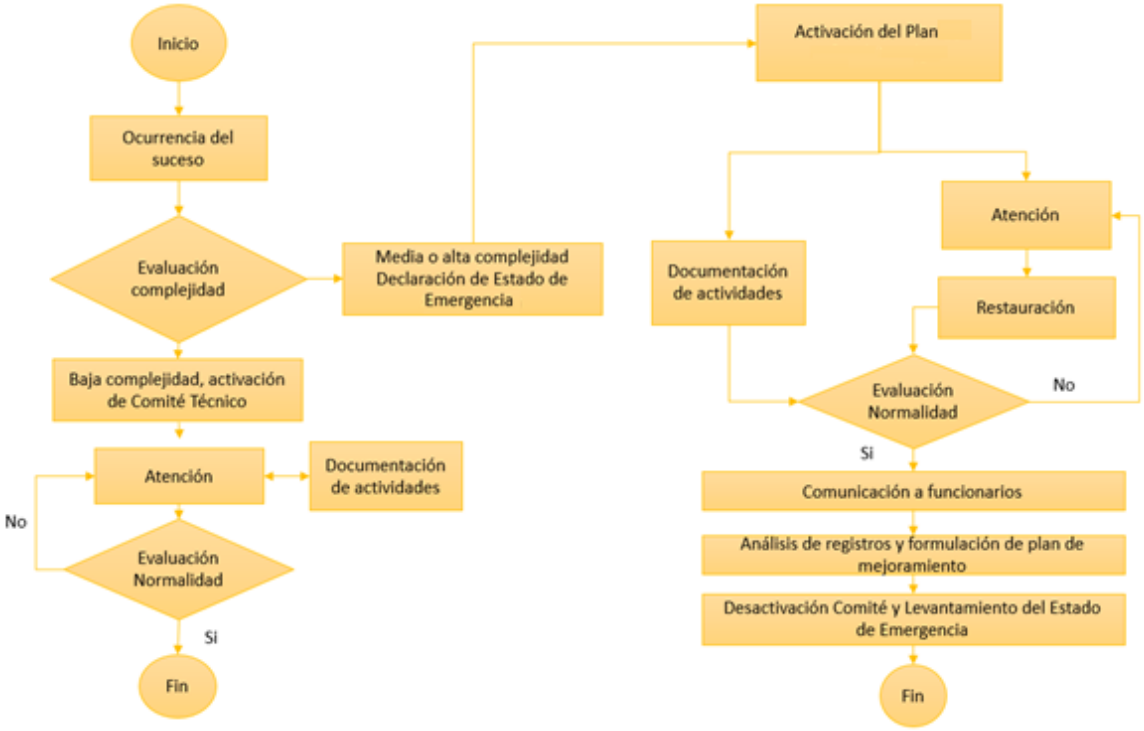
4.2.3.5.5 Retorno a la normal operación

- Coordinar el regreso a una situación normal de operación.
- Iniciar las tareas conducentes a restablecer la normalidad de la operación en el menor tiempo posible.
- Coordinar la adecuada instalación del hardware.
- Coordinar la adecuada instalación del software aplicativo, operativo y utilitario.

- Coordinar la instalación de las comunicaciones.
- Verificar que la operación de las aplicaciones críticas se realice en forma satisfactoria mediante pruebas iniciales y análisis de controles.
- Coordinar el traslado de las operaciones al Centro de Computa de la entidad Comité Técnico Operativo de la Personería.
- Autorizar la operación de las aplicaciones.
- Revisar los informes obtenidos de la ejecución de las aplicaciones.
- Verificar y analizar que la información producida sea confiable, con base en los controles definidos previamente.
- Mantener constantemente informado de la situación al Comité de Seguridad
- Liberar al Sistemas Alternos de los recursos innecesarios que se hayan requerido durante la contingencia.
- Dar por concluida la situación de emergencia, en compañía de los otros miembros del equipo.
- Informar al Comité Directivo sobre el restablecimiento normal de las operaciones.

El siguiente flujo muestra en detalle las fases y etapas por las que la Personería atravesará una vez producido el evento que conlleve a aplicar el Plan de Contingencia.

Figura 12. Flujo para la Activación Plan de Continuidad



Fuente: Las autoras

4.2.3.5.6 Plan de recuperación

Parte de la premisa de que ha ocurrido un evento de gran magnitud o un desastre originado por daño, error o incidente no controlable, pero que puede dejar operativos los sistemas temporalmente o reemplazarlos y vueltos a la normalidad durante el transcurso de 5 días como mínimo.

Contempla las gestiones necesarias durante la materialización de un incidente no controlable. Su finalidad es operar temporalmente como plan de continuidad de negocio y restaurar los procesos a la normalidad a partir de procedimientos definidos para tal fin. El objetivo es restablecer las operaciones de los recursos en el menor tiempo posible.

El nivel de este evento es considerado crítico cuando según la matriz se ve afectada la integridad de la entidad y se puede perder la gestión que conlleva a la pérdida de credibilidad y confianza en la misión de la entidad. Los riesgos secundarios tienen una alta severidad y derivados de un riesgo residual con alta severidad.

Cada uno de estos procesos debe llevarse de la manera más detallada posible, ya que las prioridades de continuidad se consigan como resultado. Se permite el uso de sistemas manuales mientras es gestionada.

Se pretende restablecer en el menor tiempo posible el nivel de operación normal del centro de datos, basándose en los planes de emergencia y de respaldo a los niveles del Comité Técnico Operativos y de los demás niveles.

La responsabilidad sobre el Plan de Recuperación es de la Administración, la cual debe considerar la combinación de todo su personal, equipos, datos, sistemas, comunicaciones y suministros.

El plan de Recuperación contempla los siguientes objetivos:

- Determinar las políticas y procedimientos para respaldar las aplicaciones y los datos.
- Planificar la reactivación dentro de las 12 horas de producido un desastre, el sistema de procesamiento y las funciones asociadas.
- Supervisar los sistemas y aplicaciones.
- Establecer las acciones a realizar para garantizar una oportuna respuesta frente a un desastre.

4.2.3.5.7 Activación del Plan

Queda a juicio del Director de emergencias determinar la activación del Plan, y además indicar el lugar alternativo de ejecución del Respaldo y/o operación de emergencia, basándose en las recomendaciones indicadas por éste.

Los Directores de cada área determinarán la duración estimada de la interrupción del servicio, siendo un factor clave que podrá sugerir continuar el procesamiento en el lugar afectado o proceder al traslado del procesamiento a un lugar alternativo.

Se aplicará el plan siempre que se prevea una pérdida de servicio por un período mayor de 48 horas, en los casos que no sea un fin de mes, y un período mayor a 24 horas durante los fines de mes (durante los cierres de operaciones).

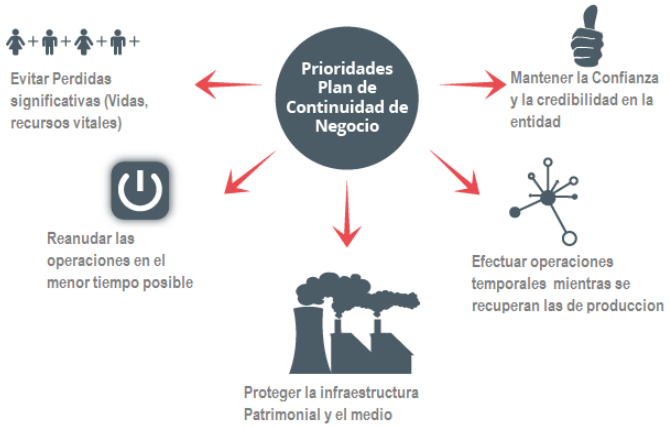
Parte de la pregunta ¿Qué eventos activan la Contingencia? A fin de establecer los mecanismos de mitigación más importantes en las incidencias más críticas de alto impacto.

Contempla las medidas de contraataque necesarias durante la materialización de una amenaza, o inmediatamente alertada. Su finalidad es mitigar los efectos adversos de la posible y probable amenaza.

Tiene como objetivo mantener operativo los equipos para el correcto funcionamiento de la red y procesos más críticos en la Personería de Bogotá.

Cada documento, debe guiar el paso a paso de reinstalación y configuración del servicio afectado y puede ser retroalimentado por cada uno de los ingenieros que participen en el proceso de restauración del servicio, de acuerdo con la responsabilidad de gestión de mitigación

Figura 13. Prioridades Plan de Continuidad de Negocio



Fuente:
https://www.incibe.es/empresas/que_te_interesa/Plan_de_contingencia_y_continuidad_del_negocio

Eventos a tener en cuenta como señales de prevención

- Alarma del Centro de Cómputo.
- Alarma del (los) servidor(es).
- Alarmas del (los) equipo(s) de comunicación.
- Reporte de Falla de Aplicaciones (falta de acceso, lentitud, perdida de información, latencias, errores de código).
- Reporte de Falla de Servicios (falta de acceso, lentitud, perdida de gestión, latencias, errores de ejecución).
- Reportes de Pérdida de Conexión a La Base de Datos
- Reporte de inasistencia del personal: administrador de la Red, administrador de las Bases de Datos, administrador de la Red, administrador de Soporte Técnico.
- Mensajes de error durante la ejecución de programas.
- Falla general en las estaciones de trabajo.
- Falla de comunicación de estaciones de trabajo
- Fallo de comunicación telefónica.
- Anuncio de virus informático.

4.2.3.5.8 ¿Qué hacer cuando ocurre una alarma?

La gestión de mitigación contempla los siguientes procedimientos:

Notificación de la Incidencia mediante correo electrónico o telefónicamente al área de soporte (e-mail admin@personeriabogota.gov.co, y/o ext. 5316).
Aviso de notificación al Director de Tecnologías.
Transferencia de caso al grupo Técnico operativo que corresponda, (el ingeniero designado por el Director de Tecnologías encargado de cada una de las áreas de DTIC) para gestionar mitigación.
Solicitud de uno o todos de los siguientes documento(s) necesario(s) al documentador del Plan según el caso, y solicitud de las contraseñas que corresponda al Director de Tecnologías, los cuales se relacionan a continuación:

- Mapa de dependencia de servicios. Este apartado permite realizar un diagnóstico más preciso de los incidentes registrados, mediante metodología de descarte, para gestionar la corrección del incidente.
- Gestión de Copias de Respaldo Con la administración de las copias se facilita el registro de los backups para su localización, ubicación de los medios (cintas, discos, cds), proceso de copia, tipos de copias, archivos importantes copiados, métodos de copia (scripts, comandos, archivo).
- Documento Procedimiento para copias de respaldo Código:DTIC2015001
- Información de Backups
- Formato de control de copias de respaldo
- Administración de servidores: Este protocolo permite el regreso de los servicios a la normalidad en caso de pérdida de disponibilidad; incluye el procedimiento para restaurar las aplicaciones y servicios descritos en el acápite de identificación de procesos críticos.
- Documento Procedimiento para apagado y encendido de servidores Código:DTIC2015005
- Documento Procedimiento Activación de servidores de respaldo Código:DTIC2015006
- Documento Scripts para migrar automáticamente bases de datos contingentes
- Documento Administración de servidores Código:DTIC2015007
- Documento Instalación y configuración de servidores Código:DTIC2015007
- Equipos con Alta disponibilidad

Identificación de los equipos con alta disponibilidad con que se cuenta en el momento, relacionados con su correspondiente respaldo (potencia regulada, equipos de comunicaciones y seguridad perimetral).

- Documento Canal de datos alterno de 50 MB Código:DTIC2015008
- Documento Alta Disponibilidad Equipo de seguridad perimetral para acceso a internet Código: DTIC 2015009

- Documento Procedimiento para el montaje de switches de respaldo Código: DTIC201510.
- Documento Procesos en la Nube Código:DTIC201511

Aplicación del procedimiento relacionado según el caso por parte del Ingeniero de cada área o en su delegación al Ingeniero Junior.
Registro en la Bitácora de eventos

4.2.3.5.9 Elementos necesarios para recuperación de negocio

Formatos de captura de procesos: Se trata de un Formulario para Tramite Usuario, elaborado en hoja de cálculo, el cual sirve para la captura de los procesos disciplinarios y es necesario para la atención de requerimiento ciudadano, PQRs, trámite respuesta, veedurías, ministerios públicos, etc. y que puede ser migrado fácilmente en el momento de poner en producción el sistema SINPROC.

Servicio cloud: Se debe tener en cuenta que entró en operación el servicio de la Nube que permite tener 99.9% de disponibilidad de los servicios más críticos de la entidad y que contempla la replicación de estos servicios de manera geográficamente distante de manera automática, con copia de respaldo incluida y en caso de que alguno de los servicios falle en esta plataforma se utilizaría los copia de los servers en el Data Center de la entidad, donde cada uno de los servidores de alta criticidad está en producción y los del Centro de Computo tienen copia. En este caso se puede aplicar contingencias de manera trasversal

Copias de respaldo (backups): Importante recurso para restauración inmediata y que se activa como la contingencia más efectiva para la recuperación de los datos, tan pronto ocurrido el siniestro.

Switches de respaldo: Se trata de un stock de dispositivos de comunicación que se encuentran en bodega (calle 21 No. 6-22) sótano y que se pueden disponer en el momento de pérdida de comunicación del CORE (equipo principal de red que controla los dispositivos de comunicaciones).

En caso algún daño físico de uno de los switches de piso, también pueden servir de reemplazo temporal mientras se corrige la operación de alguno de los de producción.

Infraestructura de respaldo: Se trata de un stock de UPS’s que están en el Centro de Computo principal y que se puede disponer en el momento de daños de interrupción de la UPS que alimenta el parque computacional de la entidad.

También se puede poner a disposición el sistema de aire acondicionado del Centro de Cómputo, el cual se encuentra apagado mientras esta en operación el principal.

4.2.3.5.10 Recursos afectados

Centro de datos redes y comunicaciones

- Apagado total del Centro de datos
- Pérdida de operaciones de los servicios en la Nube
- Pérdida de operaciones de los servicios del Centro de datos
- Daños físicos de Infraestructura

Descripción del problema: Se encuentra que es imposible el uso de Centro de Cómputo en su totalidad, ya que hubo un incidente catalogado como no controlable, fallo de energía o una falla humana de operación catastrófica para los sistemas.

Tiempo de Tolerancia: 5 días - Capacidad en tiempo de soportar sin perjuicios para el restablecimiento de los servicios más críticos, pasada la recuperación, se esperan 20 días para recuperar totalmente la operación de los sistemas en la nube pública.

Procedimiento a seguir:

Dentro de las 6 horas siguientes al desastre se debe:

- Notificar a los usuarios la interrupción del servicio.
- Notificar al Comité de Seguridad Informática, al Director de Tecnologías y al ingeniero designado por el Director de Tecnologías encargado de las áreas.
- Activar el procesamiento manual de las aplicaciones (si es necesario), cuya responsabilidad es del Comité Técnico de Operación.
- Efectuar una evaluación de daños e identificar equipos reusables para transferirlo al Centro de datos temporal.
- Notificar al Proveedor las configuraciones de hardware y alistar los requerimientos.
- Notificar a todos los funcionarios de la Dirección de Tecnologías, que están involucrados en el Plan.
- Seleccionar y catalogar las oficinas de servicio para el procesamiento de los reportes de respaldo.
- Inicializar las preparaciones ambientales en el Centro de Cómputo temporal. (voz, datos red eléctrica).
- Ordenar los servicios para comunicación de datos en la nube pública, si es necesario.

Dentro de las 24 horas siguientes al desastre debe:

- Contactar con el proveedor y ordenar el soporte tanto de hardware como de software
- Iniciar y coordinar los procedimientos de preparación del lugar para el Centro de Cómputo Temporal.

- Iniciar el ensamblaje de la documentación y medios magnéticos en el lugar de almacenamiento externo (Cinto-teca de la Dirección de Tecnologías).
- Confirmar el soporte dado por el proveedor.
- Complementar el procesamiento de los reportes seleccionados en el Centro de Cómputo Temporal.

Dentro de los 2 días siguientes al desastre debe:

- Catalogar el despacho de suministros
- Trasladar el personal necesario y/o requerimientos al Centro de Cómputo Temporal
- Completar el ensamblaje de la documentación y los medios magnéticos en el Centro de Cómputo Temporal, coordinando la prestación de los servicios desde el Centro de Cómputo Temporal.

Dentro de los 3 días siguientes al desastre:

- El Centro de Cómputo Temporal debe estar totalmente preparado para operar
- Llevar el inventario de los medios magnéticos, los listados y otra documentación en el Centro de Cómputo Temporal.
- Recibir en el Centro de Cómputo Temporal suficientes suministros, muebles y equipo relacionado.
- Determinar el punto inicial de aplicaciones críticas.
- Establecer un catálogo de procesamiento de las aplicaciones críticas.
- Evaluar las líneas de comunicación de datos catalogados para una restauración inicial.

Dentro de los 4 días siguientes al desastre debe:

- Completar la preparación ambiental del Centro de Cómputo Temporal
- Recibir la documentación y el medio magnético de los lugares de almacenamiento en el Centro de Cómputo Temporal.
- Asegurar el ambiente físico en el Centro de Cómputo Temporal y establecer la seguridad de los datos.
- Restablecer los backups de datos de producción de las cintas de backups.
- Evaluar los sistemas en línea, para verificar la operación y validez de los datos restaurados.
- Evaluar los sistemas operacionales
- Notificar a los usuarios el estado de la recuperación y validar operaciones en las estaciones de trabajo.

Dentro de los cinco días siguientes al desastre:

- Asegurar la operación total de los sistemas críticos.
- Migrar datos de los sistemas manuales al sistema en producción.
- Continuar la implantación por fases de la red de comunicación de datos

Dentro de los 20 días siguientes al desastre:

- Restauración completa de la red de comunicación de datos y de las operaciones.

Amenazas asociadas:

Cuadro 26. Amenazas asociadas (Centro de datos redes y comunicaciones)

Amenazas	Riesgo	Recomendación
Desastre físico	B	En el caso de incidente no controlable (ya descrito en identificación de riesgos) en el Centro de Cómputo, deben ejecutarse inmediatamente los procedimientos de emergencia implementados por el grupo de Salud Ocupacional previa notificación a uno de sus integrantes.
Mala operación (falla humana)	M	Determinar el punto de quiebre mediante diagnóstico, notificar a la Dirección del Plan, gestionar restauración y documentar
Daño del fluido eléctrico	M	Solicitar la activación de la UPS alterna para reiniciar los servicios
Daño del aire acondicionado	B	En caso de evidencia de daño, se activaría el interruptor de la condensadora que se encuentra en la parta posterior del Centro de Cómputo, marcado como CONDENSADORA, en el segundo tablero de izquierda a derecha.

Fuente: Las autoras

Pérdida de operaciones de los servicios en la Nube Pública

Descripción del problema: Uno o varios servicios se encuentras inoperantes con caídas de las comunicaciones o daño total de los equipos virtualizados, ya que hubo un incidente catalogado como no controlable, fallo de energía o una falla de operación por error humano o caída del canal de internet.

Tiempo de Tolerancia: 5 días - Capacidad en tiempo de soportar sin perjuicios, algún imprevisto

Procedimiento a seguir:

- Solicitar al documentador técnico acceso al archivo para la activación de servidores de contingencia.
- Solicitar al administrador de bases de datos backups de la información
- Solicitar la guía de instalación de servidores y aplicaciones en caso de ser necesario.

- Verificar que la causa del problema y restaure la última actualización del aplicativo; si los datos han sufrido daños restaure desde el último Backup

Amenazas asociadas:

Cuadro 27. Pérdida de operaciones de los servicios en la Nube Pública

Amenazas	Riesgo	Recomendación
Borrado o modificación de alguno de sus componentes	M	Restauración de copias de respaldo (backups) Identificación del componente faltante
Aparición de virus informático	B	Mantener software antivirus actualizado. Mantener software Guardián y vacunar todo tipo de información que penetre al servidor
Interrupción del fluido eléctrico	A	Mantener en buen estado el sistema de UPS y contrato de mantenimiento al día
Sabotaje	M	Creación de políticas de control para el acceso al Centro de Computo y en especial a los servidores y/o equipos de cómputo

Fuente: Las autoras

Daños físicos de Infraestructura

Daño físico Servidores en el Centro de Cómputo de la entidad.

Descripción del problema: El servidor no puede responder a los requerimientos de los clientes. Los recursos de red no pueden ser accedidos o el servidor no responde y no se deja acceder desde consola.

Tiempo De Tolerancia: 6 horas.

Procedimiento a seguir:

- Llamada de servicio con carácter urgente y comunicar al encargado del Centro de datos.
- Esperar el diagnostico; si excede el tiempo de tolerancia para su recuperación, aplicar procedimiento de contingencia en la nube o el servidor alterno.
- Restaurar el soporte del disco(s) en espacio temporal y llamar al servicio de soporte con carácter urgente.
- Llamada de servicio con carácter urgente y comunicar al encargado del Centro de datos.
- Llamar al Proveedor.

- Llamar al servicio de soporte con carácter urgente.

Amenazas asociadas
Daño en alguno de los equipos (disco, memoria, procesador, main board) que afecte la función de multitarea, bloqueos continuos y caídas del sistema. No se deja acceder y por tanto no reinicia el sistema.

Cuadro 28. Daños físicos de Infraestructura

Amenazas	Riesgo	Recomendación
Se queme el disco duro	B	Mantener regulada la energía eléctrica. En caso de incendio extinguir, en primer lugar, el fuego de la CPU (En la CPU se encuentra toda la información del servidor).Mantener extintores.
Posibilidad de que se moje	B	No debe estar cerca a los ductos de agua. No debe estar cerca de la ventana Mantener cubierto el sistema con forros plásticos
El disco duro se des configure	B	Realizar mantenimientos preventivos al servidor,. Mantener controles para el acceso al servidor (tanto físico como lógico)
Desconfiguración del Setup	B	Mantener las características de setup disponibles para configurarlo de nuevo. Realizar mantenimiento correctivo
Aparición de virus informático	B	Mantener software antivirus actualizado. Mantener software Guardián y vacunar todo tipo de información que penetre al servidor
Sabotaje	M	Creación de políticas de control para el acceso al Centro de Computo y en especial a los servidores y/o equipos de cómputo
Posibilidad de que se queme la main board	B	Mantener regulada la energía eléctrica. En caso de incendio extinguir, en primer lugar, el fuego de la CPU (En la CPU se encuentra toda la información del servidor). Mantener condiciones de temperatura controlada

Cuadro 28. (Continuación)

Amenazas	Riesgo	Recomendación
Posibilidad de que se moje la main Board	B	No debe estar cerca a los ductos de agua. No debe estar cerca a la ventana
La main Board se des configura	B	Realizar mantenimientos preventivos al servidor. Mantener controles para el acceso al servidor (tanto físico como lógico)
Desconfiguración del Setup	B	Mantener las características de setup disponibles para configurarlo de nuevo.

		Realizar mantenimiento correctivo. Tener una hoja de vida del sistema de hardware

Fuente: Las autoras

Conexión a Red.

Descripción del problema: El dispositivo de comunicaciones no puede responder a los requerimientos de los clientes. Los servicios no pueden ser accedidos, no responden y no se dejan acceder desde consola. Se pierde comunicación con las estaciones de trabajo. Falla en la RED de acceso soportada por la ETB (Canales de datos y ADSL), se pierde el enlace de la Personería con las Personerías locales.
Tiempo de Tolerancia: 6 horas.

Procedimiento a seguir:

- Se deben definir los procedimientos para que las estaciones trabajen en la modalidad fuera de línea (off line).
- Atender el mantenimiento correctivo con el área de redes y comunicaciones.
- Revisar los procedimientos con que cuente la ETB.
- Determinación y notificación del daño.
- Registro en la Bitácora de servicios.

Cuadro 29. Amenazas asociadas - Conexión a Red

Amenazas	Riesgos	Recomendación
Desconfiguración de alguno de los equipos de Red, desde los RACKS	M	Restringir el acceso a la zona en donde se encuentran los RACKS. Los RACKS deben permanecer libres de cualquier objeto ajeno a ellos.
Sabotaje	M	Creación de políticas de control para el acceso a los Centros de Cableado, en especial al del Cómputo.

Fuente: Las autoras

Sistema operativo

Descripción del problema: Falla del equipo al intentar arrancarlo y/o al intentar entrar a los aplicativos. Se encuentra imposible inicializar el sistema operacional instalado o sale error o irreparable (PANIC por el kernel o Pantalla Azul).

Tiempo De Tolerancia: 6 horas.

Procedimiento a seguir:

- Diagnosticar y encontrar punto de quiebre.

- Notificar al encargado del Centro de Cómputo para la correspondiente activación de la contingencia, quien identificará el servicio afectado y:
  - ✓ Encenderá el servidor de respaldo correspondiente.
  - ✓ Restaurará la información más reciente mediante procedimiento.
- Reinstalación de sistema y servicio
  - ✓ Solicitará al documentador técnico la guía de instalación de servicios y servidores.
  - ✓ Solicitará al El ingeniero designado por el Director de Tecnologías encargado de Soporte los medios de instalación.
  - ✓ Instalará de acuerdo con la guía.
  - ✓ Sacará de la copia más actualizada posible para la restauración.
  - ✓ Registrará en la bitácora de servicios.

Amenazas asociadas

Cuadro 30. Amenazas Asociadas – Sistema Operativo

Amenazas	**Riesgo**	**Recomendación**
Borrado de Sistema Operativo o alguno de sus componentes	M	Disponer de servidores de contingencia.
Aparición de virus informático	B	Mantener software antivirus actualizado. Mantener software Guardián y vacunar todo tipo de información que penetre al servidor. No permitir el ingreso de archivos de dudosa procedencia.
Sabotaje	M	Creación de políticas de control para el acceso al Centro de Computo y en especial a los servidores y/o equipos de cómputo

Fuente: Las autoras

Bases de datos

Descripción del problema: Falla del motor de bases de datos descrito así:

- Un registro de transacciones o de la base de datos que los sistemas de información usan se ha quedado sin espacio en disco.
- La base de datos de los sistemas de información entra en un estado de incoherencia o se daña.
- El servicio de SQL Server u Oracle Databases Enterprise no se está ejecutando o no está configurado correctamente.

Tiempo De Tolerancia: 6 horas.

Procedimiento a seguir:

- Comprobar que se esté ejecutando el servicio de database asociado, con las herramientas administrativas.
- Consultar los datos desde las herramientas de desarrollo.
- Diagnosticar y encontrar punto de quiebre.
- Notificar al administrador de las bases de datos para la correspondiente activación de la contingencia, quien identificará el servicio afectado y:
  - ✓ Solicitará el encendido del servidor de respaldo correspondiente.
  - ✓ Restaurará la información más reciente mediante procedimiento.
- Reinstalación del servicio
  - ✓ Solicitará al documentador técnico la guía de instalación de servicios y servidores.
  - ✓ Solicitará al El ingeniero designado por el Director de Tecnologías encargado de Soporte los medios de instalación.
  - ✓ Instalará de acuerdo con la guía.
  - ✓ Sacará de la cintoteca el backup más actualizado posible para la restauración más reciente.

Amenazas asociadas

Cuadro 31. Amenazas Asociadas – Base de Datos

Amenazas	Riesgo	Recomendación
Borrado Información por ejecución de programas y/o sentencias equivocas	A	Las bases de datos están sujetas a las políticas de control de acceso a la información y solo deben ser accedidas por el encargado de las Bases de datos en caso de requerirse cambios, eliminaciones, modificaciones o consultas especializadas. En caso de tener que ser reemplazado, debe de hacerlo alguien con idoneidad (capacitación) para ello y que se encuentre debidamente autorizado. Políticas de seguridad contraseñas

Cuadro 31. (Continuación)

Amenazas	Riesgo	Recomendación
Indisposición o caída abruptas de las aplicaciones y/o servidores de bases de datos y aplicaciones	B	Aplicar políticas y procedimientos de copias de seguridad: Documento definido en el plan de ejecución
Sabotaje	M	Creación de políticas de control para el acceso a las aplicaciones misionales y criticas (Políticas de contraseñas definidas en las Políticas de seguridad Informática

Fuente: Las autoras

4.2.3.5.11 Recuperación y Respaldo

Son los procedimientos que se utilizan en las tareas para recobrar la información lo más actualizada posible, con el único propósito de restablecer la normalidad de esta área en la organización.

Establecer con claridad, los procesos a seguir para mantener respaldada la información de la entidad, clasificada como valiosa o importante.

Determinar, en el menor tiempo posible, cuál, dónde, cómo y qué información se debe recuperar en cada contingencia de acuerdo con el nivel de riesgo.

Determinación de la importancia, periodicidad y/o rotación de los archivos y dispositivos de almacenamiento temporal.

Determinación de dispositivos de respaldo adecuados para su almacenamiento temporal.

Determinación del lugar y el establecimiento de convenios con empresas especializadas en almacenamiento externo.

Determinación del lugar y el establecimiento de convenios con empresas especializadas en prestar el servicio de respaldo de equipos de cómputo.

Secuencia de eventos de recuperación

- Clasificar cada una de las secuencias dadas en eventos no deseables, con el fin de lograr la normalidad de las actividades en un tiempo adecuado.
- Determinar el proceso de recuperación y reinicio de operaciones.
- Establecer las pautas que garanticen la eliminación de errores e inconsistencias en el instante de la restauración de copias de seguridad.

Estatus para la recuperación

- Establecer los elementos para la copia de respaldo de la información, definiendo claramente quién, cómo y cuándo se hace este procedimiento. Además, teniendo en cuenta aspectos técnicos como dispositivos, almacenamiento, rotación y seguridad de la información de respaldo.

- Entrar en acción cuando ocurre una contingencia. Para ello se deben determinar la gravedad de la situación, las acciones a ejecutar y la documentación del incidente (dónde, cómo, cuándo, quiénes, así como las

acciones tomadas para resolver la contingencia en cuanto al tiempo de solución del percance).

Acciones

- Evaluación preliminar del evento y su impacto.
- Reacción de grupos activos de recuperación de contingencias.
- Informe técnico elaborado de acuerdo con el Plan de Contingencias.

Acción I: Evaluación preliminar del evento y su impacto

- Procedimientos:

  - ✓ Notificación de la eventualidad. Este aspecto implica la oportuna y confiable comunicación de los usuarios con los administradores de los sistemas. Se debe dar a entender al usuario la importancia de reportar las eventualidades y no tratar de solucionar el problema sin estar capacitado. Puede ser contraproducente, en la medida que por acciones equivocadas, puede complicar la situación.
  - ✓ Recopilar la información del evento presentado. Se deben tener en cuenta aspectos como hora de la eventualidad, estado de la aplicación, cifras de control, Logs del sistema y registro de otros datos relevantes.
  - ✓ Redactar un informe técnico del estado del problema.

- Tiempo estimado: Lo más rápido posible de acuerdo con la situación presentada. Intervalo de 15 minutos a 6 horas.

- Responsables: El ingeniero designado por el Director de Tecnologías encargado es, equipo de Ingenieros Junior y de soporte de las aplicaciones.

Acción II: Reacción del grupo directivo

- Tiempo Estimado: Entre una (1) y seis (6) horas.

- Responsables: El ingeniero designado por el Director de Tecnologías encargado es y Equipo de contingencias determinado en el plan.

  - ✓ Ubicación y solicitud de las copias de seguridad, de acuerdo con la última actualización reportada en el informe técnico.
  - ✓ Solicitar a los usuarios abstenerse de utilizar el sistema durante el tiempo que dure la eventualidad.
  - ✓ Realizar el proceso de restauración de los archivos y actualizar la configuración, de ser necesario.

- ✓ Evaluar la necesidad de actualizar manualmente los registros que, por desfase de tiempo, no hayan quedado en el sistema.
- ✓ Aplicar los procesos de verificación del sistema de retorno, para la operación correcta de las aplicaciones.
- ✓ Indicar a los usuarios que pueden reiniciar sus actividades

Acción III: Informe técnico

- Tiempo de duración: Tres (3) días.

- Responsables: Comité de recuperación, personal capacitado que participe durante la contingencia.

  - ✓ Explicación del estado de la situación actual del sistema.
  - ✓ Áreas afectadas por la eventualidad.
  - ✓ Metodología y aspectos aplicados en la determinación de la evaluación preliminar.
  - ✓ Personal contactado (interno o externo) durante el tiempo de ejecución del plan.
  - ✓ Procedimientos aplicados en la recuperación.
  - ✓ Estado final y explicación del procedimiento garantizando la fiabilidad de la recuperación.
  - ✓ Incluir personal del grupo de contingencias y recuperación que participaron.
  - ✓ Dejar constancia ante el Comité de Seguridad del Plan de Contingencias y dependencias afectadas.
  - ✓ Tiempo de duración de la eventualidad.
  - ✓ Consignación de esta información para futuras fallas.

En general, el Plan de Contingencias saldrá adelante, siempre y cuando cuente la colaboración de todos, respetando y acatando las recomendaciones hechas y los procesos a seguir.

4.2.3.6 Fase IV: Plan de revisión procedimental, pruebas y mantenimiento

Para la puesta en marcha y el funcionamiento de los proyectos, es imprescindible la creación de mecanismos de divulgación de los procesos a nivel de la dirección del comité y a cada integrante de los diferentes comités de continuidad y recuperación, verificando que los documentos y procedimientos, objeto de este trabajo, estén completos, cumplan con los estándares y sean los adecuados para el desarrollo del plan.

En este punto podemos suponer que se tiene toda la infraestructura necesaria para la ejecución del plan, pero si no hay preparación de los procedimientos, el equipo directivo y operativo estará abocado a fracasar.

Una vez establecidas responsabilidades y tareas, el documentador técnico es el encargado de facilitar los archivos requeridos y los procedimientos necesarios para la activación del Plan.

Objetivos

- Establecer cuál es el control que se tiene para la guarda y custodia de los procedimientos y documentos requeridos.
- Establecer cuál es la ubicación de estos archivos, con el fin de identificar los pasos a seguir en caso de la aplicación de algunas de las fases del Plan de Contingencias por la presentación de algún incidente.
- Garantizar el cubrimiento de toda la infraestructura en esta documentación técnica.
- Complementar y oficializar la documentación del plan de contingencias

Procedimiento

Nombrar los responsables para la verificación.
Solicitar la documentación.
Revisar cada uno de los documentos relacionados en el Plan de Contingencias.
Clasificar, regular y reglamentar los contenidos, remitiendo información a la oficina de control interno para su correspondiente proceso.

4.2.3.6.1 Plan de Capacitación

Se deben crear mecanismos para la publicación y ejecución del Plan de Contingencias y la divulgación de todos los procesos asignados a cada integrante de los comités de recuperación.

En este sentido si no hay preparación del equipo directivo y operativo no sirve de nada el establecimiento del Plan.

Objetivos

- Establecer cuál es el personal que debe conocer los procedimientos, con el fin de capacitarlos sobre cada una de las fases del Plan de continuidad
- Garantizar el pleno cubrimiento de todas las fases de Plan de continuidad por parte de las personas involucradas.
- Establecer responsables de la inducción y re-inducción para la continuidad del plan de capacitación.
- Elaborar por cada fase procedimientos de entrenamiento simulado.

- Generar factores de evaluación que cualifiquen el nivel de entrenamiento.
- Determinar el contenido a tratar para cada líder.
- Dotar de herramientas de capacitación a cada líder.

Procedimiento

- Nombrar y hacer responsable de cada fase a un líder.
- Dotar de elementos para la capacitación y el entrenamiento a cada uno de los líderes involucrados.
- Obtener un esquema general, el cual conduzca a determinar cada una de las actividades a tratar en la capacitación.
- Elaborar por cada fase procedimientos de entrenamiento simulado.
- Generar factores de evaluación que cualifiquen el nivel de entrenamiento.

4.2.3.6.2 Manual de procedimientos

Su cuidado, conservación y actualización es responsabilidad del Comité de Seguridad

Las normas y procedimientos del manual son de obligatorio cumplimiento, siempre y cuando se quiera que todo salga bien; el manual es de carácter confidencial, ya que este documento presenta las debilidades y fortalezas de la Personería.

Es responsabilidad del Jefe de la Dirección de Sistemas, como parte del Comité de Seguridad, hacer conocer el contenido del manual al personal que desempeña las funciones relativas a las normas y procedimientos en él descritos.

Cada manual debe tener un número de identificación que permita controlar la dependencia a la cual es asignado éste, así como la cantidad existente de ellos.

El contenido de los manuales será permanentemente actualizado por el ingeniero designado por el Director de Tecnologías encargado de la documentación técnica, que pertenece al Comité técnico operativo, mediante el sistema de hojas intercambiables, las cuales serán enviadas con una hoja remisoria, que deben ser devueltas al Comité de Seguridad, junto con las hojas cambiadas, teniendo en cuenta los cambios realizados y los que el comité técnico operativo y Directivo crean necesarios, este se debe actualizar en un período no mayor a 6 meses.

4.2.3.6.3 Procedimiento operativo y administrativo

Objetivos

- Establecer pautas operativas y administrativas que conduzcan a definir políticas de atención.
- Fortalecer el ámbito cultural del procedimiento de capacitación del Plan de Contingencias.

Procedimientos

- Establecer fechas, tiempo de duración y objetivos del plan de recuperación, al igual que los elementos de evaluación.
- Involucrar directamente a la alta gerencia para que se dote de los recursos necesarios y cada proceso de capacitación.

4.2.3.6.4 Planes de emergencia

Objetivos

- Proveer de elementos o pautas que normalicen la reacción ante la posibilidad de materialización de eventualidades.
- Fortalecer el personal operativo y directivo con los elementos de decisión propios de la situación de emergencia.

Procedimientos

- Establecer fechas en las cuales se deben realizar simulacros que evidencien la capacidad de reacción en cada caso de emergencia.
- Establecer políticas de evaluación y ajuste del plan.

4.2.3.6.5 Procedimiento operativo y administrativo

Objetivos

- Establecer pautas operativas y administrativas que conduzcan a definir políticas de atención.
- Fortalecer el ámbito cultural del procedimiento de capacitación del Plan de Contingencias.

Procedimientos

- Establecer fechas, tiempo de duración y objetivos del plan de recuperación, al igual que los elementos de evaluación.
- Involucrar directamente a la alta gerencia para que se dote de los recursos necesarios y cada proceso de capacitación.

4.2.3.6.6 Procedimiento de respaldo y recuperación

Objetivos

- Fortalecer los mecanismos de respaldo para casos de contingencia.
- Evaluar los procedimientos de respaldo y recuperación, para efectuar los respectivos ajustes.

Procedimientos

- Verificar el normal funcionamiento de los mecanismos de respaldo.
- Fijar la rotación y cuidado de los dispositivos de respaldo.
- Identificar los posibles convenios.
- Realizar los simulacros de recuperación, evaluando el estudio y actualización de las copias de seguridad.

4.2.3.6.7 Plan de Pruebas

El desarrollo de un plan experimental de pruebas en el cual se incluye la simulación de los diferentes siniestros para comprobar que el plan diseñado es eficaz o, en caso contrario, se le deben efectuar ajustes para su funcionalidad.

El mayor énfasis será ejercido sobre las pruebas o simulacros, y sobre los eventos posteriores a la emergencia relacionados con el reinicio de las operaciones normales de la entidad.

En este ejercicios se deben tener en cuenta los siguientes aspectos:

- Validar la habilidad de los funcionarios y la consistencia de los procedimientos en eventos de recuperación de siniestros.
- Probar la factibilidad y compatibilidad de las instalaciones de respaldo y de los procedimientos relacionados.
- Identificar y corregir fallas en el plan.
- Divulgar y retroalimentar el entrenamiento en los procedimientos y guías de recuperación
- Comprometerse con plan y la seguridad para su efectiva aplicación en caso de presentarse emergencias.
- Estar preparado para corregir aspectos de pólizas y seguros y reducir al máximo los costos en compras de nuevos equipos.

La metodología para pruebas, consiste en la realización de simulacros y ensayos en los eventos donde se puede presentar la contingencia, en los cuales se evidencia el grado y prioridad de cada proceso para establecer los ajustes y mejoras a que haya lugar.

Objetivos

- Validar la habilidad de los funcionarios y la consistencia de los procedimientos en eventos de recuperación en caso de desastres.
- Probar la factibilidad de las instalaciones de respaldo y de los procedimientos relacionados.
- Identificar, supervisar y corregir fallas en el plan.

- Facilitar la divulgación y el entrenamiento en los procedimientos y guías de recuperación.
- Establecer un compromiso con la alta Gerencia de la entidad para que a través de él, se ejerza la aplicación del plan y se fomente la cultura de la seguridad y prevención en la administración.
- Estar preparado para evaluar las necesidades de seguridad y reducir al máximo los costos en primas de aseguramiento.
- Motivar a los funcionarios involucrados en el diseño y desarrollo del plan a mantener actualizados los procedimientos.

Normas

La oficina de Control Interno, evaluará la fijación de responsabilidades de las pruebas del plan, como se sugiere:

- Personal de Administración: Grado de participación y compromiso, niveles de jerarquía de aprobación, asignación de recursos constantes y temporales.
- Personal de la Dirección de Tecnologías: programación, operación y soporte técnico.
- Grupo de usuarios por área operativa.
- Personal externo: Proveedores, asesores, compañías de mantenimiento y/o garantía, grupos de apoyo internos o externos, centro de recuperación contratados o comprometidos.

Procedimientos

- Como mínimo se debe garantizar que los segmentos de respaldo para instalaciones, datos y documentación, sean probados.
- Una falla en la recuperación en estas tres áreas esenciales puede significar una demora más allá de un período tolerable.
- Las áreas de tecnología o telemática, apoyadas en la oficina de Control interno, identificarán y documentarán los diferentes niveles de prueba del plan. Esos pueden ser: por segmento, por áreas relacionadas o a gran escala.

4.2.3.6.8 Pasos para conducir la prueba

El Comité técnico operativo del plan indicará a los entes de Control Interno, el esquema de las pruebas teniendo en cuenta:

- Selección del objeto de la prueba, para identificar los aspectos o capítulos del plan que está siendo evaluados.
- Descripción de los objetivos de la prueba y mecanismos de medición del alcance del éxito de los objetivos.
- Reunión con los entes directivos y operativos para explicar la prueba y sus objetivos y obtener como resultado su acuerdo y soporte.

- Comunicación formal de una prueba anunciada, los factores críticos a considerar y el tiempo estimado de la prueba.
- Consolidar los resultados de la prueba al final de esta.
- Evaluación de resultados: progresos, inconvenientes y logros.
- Determinación de las implicaciones de los resultados de la prueba. Se debe analizar si el resultado de un caso simple (segmento), puede tomarse como referencia para la realización satisfactoria de todos los capítulos del plan a gran escala.
- Generación de recomendaciones para cambios o ajustes.
- Definición del tiempo límite para respuesta y gestión.
- Notificación de los resultados de las pruebas al Comité de Seguridad
- Cambios en documentación o manuales, si es aplicable.

4.2.3.6.9 Áreas específicas del plan que debe ser aprobados

Las áreas de tecnología, con el apoyo del Control Interno, conocerán y recomendarán las partes específicas del plan que deben ser probadas, enfatizando en las siguientes:

- Recuperación del sistema operativo en el Equipo Central y en cada una de las estaciones necesarias en el plan de pruebas, utilizando archivos y documentación almacenada en el sitio externo.
- Habilidad para procesar en modo degradado o limitado. Como consecuencia del estado de disponibilidad de los recursos físicos para su utilización.
- Recarga de los discos del sistema y de los procedimientos de cargue y arranque utilizando archivos y documentación almacenada en el sitio externo.
- En sitios de procesamiento alterno, solución de diferencias en la configuración de equipos.
- Disponibilidad de equipos periféricos de procesamiento
- Disponibilidad de equipos de soporte; aire acondicionado, unidades de potencia no interrumpida de corriente eléctrica.
- Disponibilidad de soporte logístico, provisiones y suministros, transporte y comunicaciones.
- Evacuación del equipo central desde el Centro de Computo Operativo de la entidad, en respuesta a eventos tales como, incendio, inundación o sabotaje.
- Habilidad de la administración y del Comité Asesor de Sistemas para determinar su prioridad cuando se procesan recursos computacionales limitados.
- Capacidad para recuperar y procesar en forma satisfactoria sin personal clave, asumiendo la pérdida de personal de turnos primarios.
- Destreza para adaptar el plan a desastres menores.

- Efectividad de alternativas manuales para aquellos sistemas que confían en esa opción.
- Habilidad de entrada de datos para alimentar sistemas críticos utilizando las instalaciones del área de soporte externo.
- Habilidad de los usuarios para continuar con las operaciones normales de la entidad para los sistemas identificados como no críticos.
- Ingenio para establecer contacto, en un período definido por emergencia y de manera organizada, con el personal clave o sus funcionarios alternos.
- Nivel de cumplimiento de los estándares normativos aprobados por la entidad.
- Identificación de los recursos utilizados durante la emergencia que son cubierto por la póliza de seguros.
- Disponibilidad de formas y cantidad mínima de papelería.
- Adherencia nula, parcial o total a medidas de seguridad durante el período de emergencia.
- Habilidad para ejecutar tareas de evaluación y tratamiento de primeros auxilios.
- Mecanismos para recuperación de información perdida en caso de sistemas en línea.
- Análisis de tiempos y procedimientos durante la prueba

4.2.3.6.10 Plan de prevención

Parte de la pregunta ¿Qué condiciones permiten evitar que ocurra un incidente de alto impacto?; a fin de responder preventivamente a los efectos negativos que estos causen. Su finalidad es prevenir los efectos adversos de la posible y probable amenaza.

Su objetivo es mantener operativos los procesos para el correcto funcionamiento de los servicios más críticos en la Personería de Bogotá.

El nivel de este evento es considerado evitable cuando de acuerdo al análisis de riesgo así se considere. Aquí se tiene en cuenta el nivel de criticidad sin asumir su probabilidad; en este caso se aplicará la acción de prevención de acuerdo con las mencionadas condiciones de prevención de riesgo.

Cada uno de los protocolos nos guiará a la aplicación de la gestión correspondiente y en ocasiones se requiere de la clave de acceso a las maquinas, en cuyo caso existe un documento base de todas las contraseñas llamado Información de seguridad, que se maneja a nivel de protocolo de seguridad informática, y está en poder del Director de Tecnologías.

4.2.3.6.11 Condiciones de prevención de riesgo

Tomar las siguientes acciones preventivas que están implementadas por la Dirección de Tecnologías, para adelantar la prevención de riesgos, con los documentos que se mencionan y se anexan para tal fin:

- Gestión de Protocolos y Guías
- Des-habilitación de los puertos de comunicación y habilitación de los puertos seguros (administración de servidores y servicios)
- Filtrado y control de contenidos
- Contar con equipos de respaldo ante posibles fallas de los equipos de producción, para su reemplazo provisional hasta su desinfección y habilitación.
- Gestión de backups referidos a aplicaciones, configuraciones y datos.
- Contar con garantía, bolsa de repuestos y/o Bolsas de soporte y mantenimiento preventivo con el respectivo protocolo de soporte, para la infraestructura.
- Contar con servicios de soporte vigentes para la infraestructura.
- Gestión de Monitoreo de servidores, servicios y dispositivos de comunicación según protocolo.

4.2.3.6.12 Medidas de contraataque

Las siguientes son las diferentes medidas a tener en cuenta en el caso de tener que activarse el plan de continuidad:

- Documento Estado General de la Infraestructura; Código:DTIC2015000 Documento clave para identificar, cuantificar y determinar la configuración de todos los recursos con los que cuenta la entidad en materia de infraestructura y su estado actual, necesario para: tener claro cómo deberían estar configurados todos los equipos, las redes, las conexiones y sus respectivos servicios, para prevenir el riesgo de Ausencia o inasistencia del personal calificado y para que cualquier persona con conocimientos tecnológicos pueda administrar en caso de requerirse con urgencia.
- Documento Procedimiento para copias de respaldo; Código:DTIC2015001 Identifica el proceso de copias de respaldo, necesario para asegurar la información de las bases de datos, configuraciones, servicios y aplicaciones, y su aplicación en el plan de ejecución.
- Documento Políticas de Seguridad Informática Código: DTIC2015002 En estas políticas se encuentra lo necesario para identificar los diferentes lineamientos de los servicios, seguridad de la información, copias de respaldo, controles de acceso, y su aplicación en el plan de prevención contra ataques y vulnerabilidades.
- Documento Protocolo de Redes y Comunicaciones, Código: 11-PC-01 Muestra el estado actual de la infraestructura relacionada con las comunicaciones internas y externas y su procedimiento de atención al

usuario final, para aplicar la contramedida de prevención de des-configuración y/o daño de las redes.

- Documento Protocolo de Soporte Técnico, Código: 11-PC-02 Se relacionan los inventarios de bienes informáticos, el procedimiento de instalación de estaciones, atención al usuario, instalación de antivirus, entre las más importantes gestiones de usuario final, necesario para contrarrestar cualquier incidente que ocurra con la gestión que desarrollan los usuarios.
- Documento Configuración de Seguridad Perimetral Código: DTIC2015003 con alta disponibilidad. Identifica el estado actual de la seguridad perimetral en cuanto a alta disponibilidad del equipo perimetral, las reglas de control de acceso, la prevención de ataques de software malicioso, la configuración de las VPN para acceso seguro a la red interna, las reglas NAT para acceso a los servidores de manera segura.
- Ficha Técnica Servidores de Respaldo y Contingencia Identifica los servidores con los que se cuenta para la restauración de los procesos más críticos como aplicaciones misionales y críticas, página web, bases de datos, y el estado de la virtualización, lo que permite tener claro que hacer en caso de necesitar activar esta contingencia.
- Informe Conexión de equipos del Centro de Computo con Fuente de Poder Redundante Código: DTIC2015004 Muestra cómo están conectados en el momento los servidores y equipos del Centro de Cómputo con fuente de poder redundante, necesario para mitigar cualquier caída de la red regulada de este espacio de la Dirección de Tecnologías.
- Contratos: Lo siguientes contratos son importantes para asegurar el soporte técnico para evitar daños por operación constante de los equipos y servicios más críticos.
- Convenio ETB
- Mantenimiento preventivo y Correctivo de UPS
- Mantenimiento y actualización de Linux
- Garantía de Aire acondicionado
- Monitoreo: Con este monitoreo se está revisando constantemente la operación normal de la red, los servidores y las aplicaciones y cuando se muestra un estado de alerta es cuando se aplicaría la contingencia de ejecución. También permite analizar que está operando mal.
- Gestión de Switches syslog Herramientas IMC Documento de Gestión
- Gestión de Browser session TOAD
- Bitácora de eventos servicios y equipos-1
- Allí se registran los incidentes más importantes y permite volver a aplicar la gestión en caso de reincidencia de los problemas presentados o los más comunes y como fueron corregidos.
- Relación de Pólizas Dirección Administrativa y Financiera
- Estas pólizas demuestran la protección de bienes informáticos en caso de robo, pérdida o daño.
- Mapa de Gestión de Riesgos por Proceso Código: 14 - RE- 06

- Este documento demuestra que la entidad está preparada para cualquier eventualidad crítica en materia de conmoción interna por causa de un siniestro.

4.2.3.7 Recomendaciones

Las Condiciones generales que se deben dar para que el plan de continuidad tenga éxito y el manual sea práctico son:

- Conciencia de los directivos y funcionarios de la Personería sobre la necesidad del Plan.
- Verificación periódica de las copias de respaldo.
- Realizar los simulacros periódicos del plan, en toda la Personería.
- Mantenimiento o actualización de la documentación de las aplicaciones críticas.
- Que los miembros del equipo humano de recuperación o contingencia conozcan sus funciones y responsabilidades.
- Mantenimiento de copias de las copias de respaldo en lugares exteriores a la entidad.
- Que se haya definido donde mantener o guardar los equipos de soporte.
- Que se tengan suficientes existencias de medios magnéticos, formas continuas, tinta para impresoras y demás suministros.
- Que las hojas de vida de los equipos de soporte se encuentren actualizadas.
- Que el manual del Plan este actualizado.
- Verificación y actualización del Plan cada seis meses.
- Que las gestiones dadas en el análisis de riesgos, se hayan tenido en cuenta.
- Que se cuente con todos los equipos requeridos para la contingencia.

Será muy importante aprovechar los resultados de este Plan, con miras a generar una cultura de control y seguridad, permitiendo que cada funcionario sea consciente de las amenazas a que está expuesta la Dirección de Tecnologías, y la forma como puede contribuir al disminuir el riesgo de que estas puedan ocurrir.

Se considera que la toma de decisión a cerca de la alternativa de respaldo no es muy difícil y además se deja una buena base para dicho desarrollo, a la vez definido: los comités, sus funciones, los documentos, el plan de capacitación, las actividades, los procedimientos, y una metodología para las pruebas.

4.2.4. Implementación

Para la implementación, se debe realizar la implementación de los controles, de acuerdo a lo señalado en los objetivos de control, a cada uno de los controles se le debe realizar seguimiento, definiendo los responsables de su realización.

Es también importante realizar un plan de entrenamiento y concientización del personal, tanto a funcionarios, contratista y terceros, con esto se pretende:

- Crear sentido de pertenencia y evitar rechazo a los nuevos controles que se deban implementar.
- Dar a conocer la importancia de tener un nivel de seguridad propicio
- Generar un compromiso en todos los funcionarios, evitando fallas por desconocimiento.
- Retroalimentación por parte de los funcionarios.

Es fundamental la implementación del plan de continuidad, realizando pruebas del mismo y tomando las acciones correctivas que se deban asumir.

Para la implementación del SGSI se requiere contar con recursos humanos, económicos y tecnológicos, de acuerdo con los análisis y controles previstos.

4.2.5.Documentación

Los documentos que se realizan para formalizar el SGSI se pueden catalogar en los siguientes tipos:

Política de seguridad: Es la guía donde se implanta las necesidades y obligaciones de protección en la entidad. La Política de seguridad de la Personería se presenta en el numeral 12.1.2. Una política de seguridad puede apoyarse de otros documentos tales como las normas, políticas de uso, procedimientos y/o instrucciones.

Las normas de seguridad: Precisan qué hay que proteger, en qué condiciones bajo unas circunstancias específicas. Debe ser clara, breve y sin dar lugar a dobles interpretaciones.

Los procedimientos de seguridad: Establecen las acciones a realizar, como una serie de pasos para la realización de un proceso relacionado con la seguridad y las personas o grupos responsables de su ejecución. Debe ser claro, fácil de interpretar y concreto en su ejecución. Puede apoyarse en otros documentos.

Las instrucciones técnicas de seguridad: Determinan las tareas requeridas para terminar una actividad o proceso de un procedimiento, documenta los aspectos técnicos precisos para que la persona que ejecute la instrucción no tenga que tomar decisiones en el desarrollo de la misma.

Las políticas de uso: Son documentos enfocados en los usuarios finales, con la intención de definir una regulación clara sobre la utilización de los recursos, servicios o tecnología.

La documentación es importante para tener los criterios claros, y debe ser conocida por todos los empleados de la entidad. Se debe establecer un procedimiento donde se definan la gestión adecuada en cuanto a documentación en cuanto a los siguientes ítems:

- Aprobación
- Actualización
- Identificación de cambios (versionamiento)
- Verificación de que este publicada y disponible la última versión aprobada
- Prevenir la utilización de documentos obsoletos

La siguiente lista detalla la cantidad mínima de documentos y registros requeridos por la Revisión 2013 de la norma ISO/IEC 27001-2013

Cuadro 14. Documentos Requeridos Norma ISO 27001- 2013

Documentos	Capítulo de ISO 27001:2013	Observaciones
Alcance del SGSI	4.3	Se encuentra en el capítulo 12 ítem 12.1.1 del presente documento
Políticas y objetivos de seguridad de la información	5.2, 6.2	Ver ítem 12.1.2
Metodología de evaluación y tratamiento de riesgos	6.1.2	Ubicado capítulo 12 ítem 12.1.3
Declaración de aplicabilidad	6.1.3 d	Ver ítem 12.2.2
Plan de tratamiento del riesgo	6.1.3 e, 6.2	Ver ítem 12.2.1
Informe de evaluación de riesgos	8.2	Ubicado ítem 12.1.10
Definición de funciones y responsabilidades de seguridad	A.7.1.2, A.13.2.4	Ver ítem12.2.3

Cuadro 32 (Continuación)

Documentos	Capítulo de ISO 27001:2013	Observaciones
Inventario de activos	A.8.1.1	12.1.4
Política de control de acceso	A.9.1.1	Anexo 12.1.2
Procedimientos operativos para gestión de TI	A.12.1.1	Documentación interna de la Dirección en elaboración

Política de seguridad para proveedores	A.15.1.1	Ítem 12.1.2
Procedimiento para gestión de incidentes	A.16.1.5	Anexo C
Procedimientos de la continuidad del negocio	A.17.1.2	Anexo C
Requisitos legales, normativos y contractuales	A.18.1.1	7.2
Resultados de supervisión y medición	9.1	Futura fase de Implementación
Programa de auditoría interna	9.2	Se anexa plan de auditoría
Resultados de las auditorías internas	9.2	Siguiente fase Implementación
Resultados de la revisión por parte de la dirección	9.3	Siguiente fase Implementación
Resultados de acciones correctivas	10.1	Siguiente fase Implementación

Fuente.
http://cdn2.iso27001standard.com/Checklist_of_Mandatory_Documentation_Required_by_ISO_27001_2013_ES.pdf

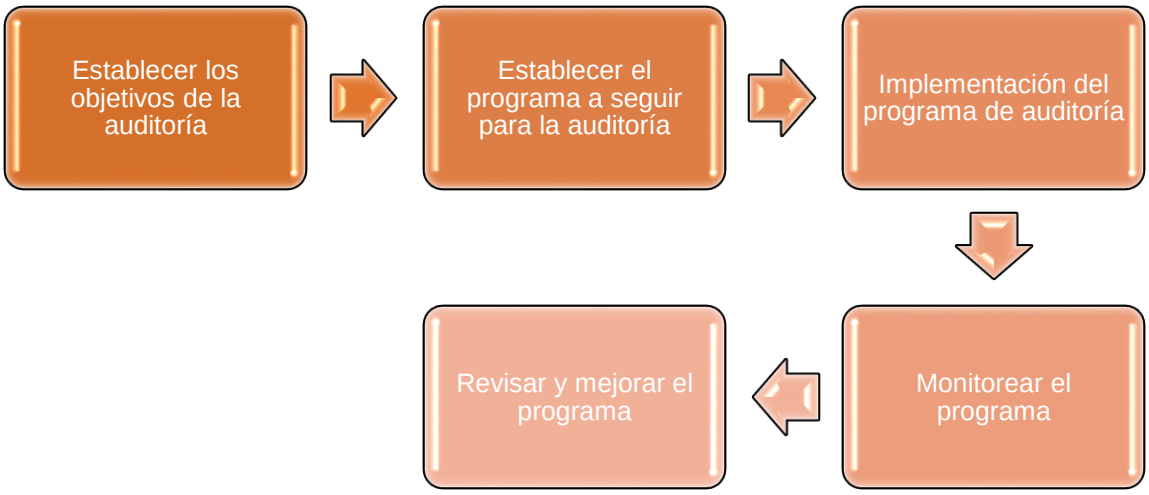
4.3.ETAPA 3 SEGUIMIENTO

4.3.1.Procedimientos de monitorización y revisión

Los proceso de monitoreo contribuyen a encontrar errores y determinar las acciones de mejora que se deban implementar para evitar las fallas detectadas.

Uno de los procedimientos que se ejecutan para la revisión del SGSI, es la auditoria interna, la norma 27001:2013 direcciona la ejecución a la norma ISO 19011:2011, en la cual se observan los pasos para realizar un plan de auditoría:

Figura 9. Pasos para realizar auditoría



Fuente. Las autoras. Basada en ISO 19011:2011

La ejecución de una auditoría implica la definición de:

- Establecer los objetivos de la auditoría
- Establecer roles y responsabilidades de los gestores de la auditoría
- Delimitar la competencia básica del gestor de auditoría
- Establecer alcance
- Identificación de riesgos del plan de auditoría
- Establecer procedimientos
- Identificar los recursos
- Implementar el programa

La implementación del programa de auditoría se produce mediante la secuencia de las siguientes etapas:

Cuadro 15. Etapas de un proceso de auditoría

ETAPA	ACTIVIDADES
Inicio de la auditoría	Definir viabilidad de la auditoría a directivos
Preparación de las actividades para el desarrollo de la auditoría	Revisión de documentación Preparación del Plan Asignación del trabajo al equipo de auditoría Preparación de los documentos de trabajo

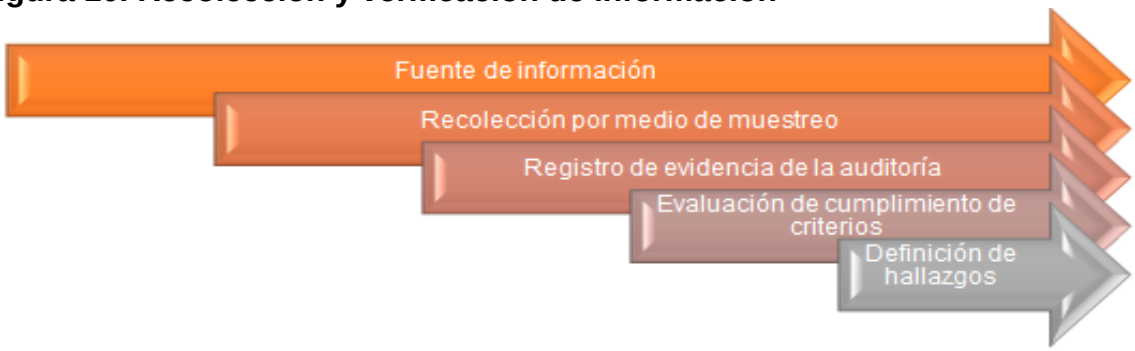
Cuadro 33 (Continuación)

ETAPA	ACTIVIDADES
Realización de las actividades de la auditoría	Reunión de apertura Revisión documental Comunicación del estado de forma permanente Asignación de roles y responsabilidades Recolección y verificación de información Generación de hallazgos Preparación de conclusiones Reunión de cierre
Preparación y distribución del reporte	Preparación del reporte de auditoría Distribución del reporte de auditoría por competencia
Seguimiento	Se realiza una nueva auditoría de seguimiento concentrando la atención en aquellos aspectos que fueron objeto de hallazgos

Fuente. Las autoras. Basada en ISO 27007

El proceso de recolección y de verificación de información contempla lo siguiente:

Figura 10. Recolección y verificación de información



Fuente: Las Autoras

Las normas y procedimientos fundamentales presentes en una auditoría es la planificación y supervisión, por lo cual todo debe ser cuidadosamente planificado y supervisado. En la figura se observa un formato propuesto para la programación de las auditorias.

Figura 11. Formato programas de auditoría

Personería de Bogotá, D. C. Al servicio de la ciudad	PROGRAMA ANUAL DE AUDITORÍAS INTEGRALES	Código: 14-RE-05
		Versión: 01 Página: 01
		Vigente Desde:

Objetivo:													
Alcance:													
Criterios:													
Recursos:													
Vigencia:													
PROCESOS	*GENERALES*								*SEGUIMIENTO*				**Responsable:**
	Enero	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	
Proceso 1													
Proceso 2													
Proceso 3													

Fuente: Oficina de Control Interno Personería de Bogotá

El procedimiento del programa de auditoría debe tratar los siguientes ítems

- Planificación y elaboración de un calendario de auditorías
- Aseguramiento de la capacidad de los auditores y del líder del equipo.
- Selección del equipo de auditores y asignación de funciones y responsabilidades.
- La realización de las auditorías.
- Realización del seguimiento de la auditoría
- Conservación de los registros del programa de auditoría.
- Seguimiento del desempeño y eficacia del programa de auditoría.
- Comunicación de los logros del programa de auditoría a la alta dirección.

La lista de verificación es una guía que presta apoyo en la planificación y ejecución de la auditoría, pero que en ningún caso debe restringir la extensión de las actividades del ejercicio, que pueden cambiarse como resultado de la información recopilada durante la visita en sitio. Ayuda a la gestión del tiempo, a recopilar evidencias en orden lógico, facilitar el cubrimiento de cada actividad. Esta se presenta en el Anexo D se presenta la lista de chequeo de auditoria.

4.3.2.Instrumentos para registro de acciones y eventos

Es importante que el auditor realice una lista de verificación, que le ayude a realizar un adecuado trabajo, en el Anexo C se presenta un formato que sirve de herramienta para realizar las observaciones encontradas durante una auditoria, en cuanto al cumplimiento de la norma ISO 27002 2013.

En el Anexo E se da el formato para registro de visita de auditoria.

4.4.ETAPA 4 MANTENIMIENTO Y MEJORA

Se sugieren como actividades de mantenimiento y mejora las siguientes:

- Elaboración de un autodiagnóstico institucional de cumplimiento de compromisos, al inicio de cada vigencia, teniendo en cuenta los objetivos propuestos por la norma NTC-ISO27001:2013
- Verificación de cumplimiento de las actividades acordadas en la planificación del SGSI
- Realizar test de intrusión sobre los diferentes sistemas de información y esquemas de bases de datos
- Levantamiento de registros y documentación permanentemente para cada actividad realizada
- Elaboración detallada de toda la documentación mínima requerida en cumplimiento de la NTC-ISO27001:2013 en pro de un proceso de acreditación
- Programar tareas periódicas de auditoría
- Suministrar la capacitación requerida al personal que lidera el SGSI de la entidad
- Reuniones bimestrales para el análisis de la información levantada durante los procesos de auditoría en las cuales participen todos los miembros de la organización de plan de contingencias y el comité de seguridad informática
- Actualización permanente de mapa de red y esquema básico de la infraestructura computacional con que cuenta la entidad
- Realización de simulacros y pruebas simulando la ocurrencia de siniestros, para levantar información suficiente, que permita una completa formulación de procedimientos operativos normalizados que complementen el plan de contingencias
- Completar el levantamiento de activos de información para toda la entidad y formulación de un SGSI aplicable a todas las áreas
- Formación y sensibilización a los empleados según competencia, que posibiliten la implantación de medidas de seguridad acordes con las necesidades institucionales
- Contratación de consultorías externas para revisión de cumplimiento y selección de los nuevos controles a que haya lugar

- Implementar procedimientos de criptografía para asegurar la información sensible de la entidad y proteger información personal
- Diferenciar los ambientes de desarrollo, pruebas y producción para cada uno de los sistemas de información implementados

5. CONCLUSIONES

La seguridad informática es un campo bastante amplio y en constante cambio y evolución, sobre el cual, no se ha dicho la última palabra; por lo anterior, el ambicionar la implementación de un SGSI para toda la entidad requiere de bastante dedicación y esfuerzo. Las Condiciones generales que se deben dar para que el plan de contingencias tenga éxito y el manual sea práctico son:

- Conciencia de los directivos y funcionarios de la Personería sobre la necesidad del Plan.
- Verificación periódica de los Backups.
- Realizar los simulacros periódicos del plan, en toda la Personería.
- Mantenimiento o actualización de la documentación de las aplicaciones críticas.
- Que los miembros del equipo humano de recuperación o contingencia conozcan sus funciones y responsabilidades.
- Mantenimiento de copias de los backups en lugares exteriores a la entidad.
- Que se haya definido donde mantener o guardar los equipos de soporte.
- Que se tengan suficientes existencias de medios magnéticos, formas continuas, tinta para impresoras y demás suministros.
- Que las hojas de vida de los equipos de soporte se encuentren actualizadas.
- Que el manual del Plan este actualizado.
- Verificación y actualización del Plan cada seis meses.
- Que las gestiones dadas en el análisis de riesgos, se hayan tenido en cuenta.
- Que se cuente con todos los equipos requeridos para la contingencia.

Se considera que la toma de decisión a cerca de la alternativa de respaldo no es muy difícil y además se deja una buena base para dicho desarrollo. Al mismo tiempo, se dejan definidos: los comités, sus funciones, los documentos, el plan de capacitación, las actividades, los procedimientos, y una metodología para las pruebas.

En la presente propuesta, se realizó un levantamiento de activos con que cuenta la entidad en su centro de cómputo, un reconocimiento de las amenazas, plan de tratamiento de riesgos y definición de los responsables de las tareas entre otros, sin embargo constituye solamente la piedra angular para la construcción del SGSI institucional.

Será muy importante aprovechar los resultados de este Plan, con miras a generar una cultura de control y seguridad, permitiendo que cada funcionario sea consciente de las amenazas a que está expuesta la Dirección de Tecnologías, y la forma como puede contribuir al disminuir el riesgo de que estas puedan ocurrir.

BIBLIOGRAFÍA

ALCALDÍA DE BOGOTÁ. Acuerdo 514 de 2012, diciembre 18. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=50952

--------. Diario Oficial - Ley 527 de 1999. (21 de 08 de 1999). Secretaría General. Recuperado el 11 de 05 de 2015. Disponible en: http://Www.Alcaldiabogota.Gov.Co/sisjur/normas/Norma1.jsp?i=4276

ALEGSA. Definición de Log de accesos, 01 de 01 de 2015. Recuperado el 11 de 05 de 2015, Disponible en: http://www.alegsa.com.ar/Dic/log%20de%20accesos.php

--------. Definición de Servidor, 01 de 01 de 2015. Recuperado el 11 de 05 de 2015. Disponible en: http://www.alegsa.com.ar/Dic/servidor.php

--------. Definición de Usuario, 01 de 01 de 2015. Recuperado el 11 de 05 de 2015, Disponible en: http://www.alegsa.com.ar/Dic/usuario.php

ALFARO, Liliana y ORELLANA, Yanira. Tesis- Diseño de un sistema de medidas de seguridad de aplicación integral, que evite que los ataques informáticos traspasen las paredes de fuego, para lograr la seguridad informática de las grandes empresas comerciales que poseen páginas web ubicadas en el área metropolitana de San Salvador. (2005). Disponible en: http://wwwisis.ufg.edu.sv/wwwisis/documentos/TE/658.023-A382d/

CHEMA, Alonso. Conferencia Thinking about security Disponible en: https://www.youtube.com/watch?v=QccQjXhgub0

Estándar Internacional ISO/IEC 17799. (15 de 06 de 2005). Wordpress.com. Recuperado el 11 de 02 de 2015, de https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27001. (22 de 03 de 2006). Recuperado el 11 de 05 de 2015, de Tecnología de la Información, técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Disponible en: http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

--------. Norma Técnica Colombiana NTC 3270 (15 de 06 de 2004). Disponible en: http://tienda.icontec.org/brief/NTC3270.pdf

IFAI, Transparencia y Privacidad. Guía para implementar un Sistema de seguridad de datos personales. Disponible en:

http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_implementacion_SGSDP_nuevo_aviso.pdf

ISO27000. Sistema de Gestión de la Seguridad de la Información. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

MAGAZCITUM. (n.d.). Retrieved April 16, 2015, Disponible en: http://www.magazcitum.com.mx/?p=2193

MAGERIT V3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VWU20s9_Oko

MINISTERIO DE COMUNICACIONES (2008) Modelo de Seguridad de la Información – Sistema SANSI – SGSI. Disponible en: http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf

MINTIC. Ecosistema Digital. (s.f.). Vive Digital Colombia. Recuperado el 11 de 05 de 2015, de Ejes del Ecosistema: http://www.mintic.gov.co/portal/vivedigital/612/w3-channel.html

--------. Definiciones o Glosario -. (5 de diciembre de 2014). Arquitectura TI Colombia - Marco de Referencia. Recuperado el 11 de 05 de 2015. Disponible en: http://www.mintic.gov.co/marcodereferencia/624/w3-article-7377.html

PERSONERÍA DE BOGOTÁ. Misión, visión y objetivos. Disponible en: http://personeriabogota.gov.co/la-entidad/mision-vision-y-objetivos.

--------. (22 de 01 de 2015). Políticas de Privacidad y Condiciones de uso. Recuperado el 11 de 05 de 2015, de http://www.personeriabogota.gov.co/politicas-de-privacidad-y-condiciones-de-uso

PEREZ, E. (16 de 04 de 2011). Activos, Ataques, Amenazas y vulnerabilidades. Recuperado el 2011, de http://es.slideshare.net/jonbonachon/activos-ataques-amenazas-y-vulnerabilidades-de-informacin

UNAD. Capítulo 2: Investigación En Seguridad Informática. Disponible en: http://66.165.175.235/campus18_20142/file.php/596/entorno_de_conocimiento/Investigacion_en_seguridad_informatica.pdf

ANEXOS

Anexo A – Codificación de grupos

Nombre	Descripción	Nombre	Descripción
OCI	Oficina de Control Interno	prensa	Oficina Asesora de Divulgación y Prensa
PerAuxiliar	Personería Auxiliar	SecGeneral	Secretaria General
Juridica	Oficina Asesora de Jurídica	SegundaIns	Personería Delegada para la Segunda Instancia
TalentoHum	Dirección de Talento Humano	Administrativa	Dirección Administrativa y Financiera
DIRECCION DE TECNOLOGIAS	Dirección de Tecnologías de Información y Comunicación	Planeación	Dirección de Planeación
gestiontalento	Subdirección de Gestión del Talento Humano	Destalento	Subdirección de Desarrollo del Talento Humano
conciliacion	Dirección Centro de Conciliación	PenalesI	Personería Delegada para Asuntos Penales I
policivos	Personería Delegada para Asuntos Policivos	PenalesII	Personería Delegada para Asuntos Penales II
Del-Juridica	Personería Delegada para la Asistencia Jurídica al Ciudadano	Del-humanos	Personería Delegada para la Defensa de los Derechos Humanos
Protec-consumidor	Personería Delegada para la Defensa y Protección de los Derechos Colectivos y del Consumidor	Victimas	Personería Delegada para la Protección de Victimas
Infancia	Personería Delegada para la Protección de Infancia, Adolescencia,	Coorminpub	Personería Delegada para la coordinación del Ministerio Público y derechos humanos

Nombre	Descripción	Nombre	Descripción
	Adulto Mayor, Mujer, Familia y Personas en Situación de Discapacidad		
Coor-veedurias	Personería Delegada para la Coordinación de Veedurías	Coor-disciplinarios	Personería Delegada para la coordinación de asuntos disciplinarios
Coor-locales	Personeria Delegada para la Coordinación de Personerías Locales	Movilidad	Personería Delegada para la movilidad y la planeación urbana
Ambiente	Personeria Delegada para la Protección Del Ambiente, Asuntos Agrarios y Rurales	Social	Personería Delegada para el sector social
Gobierno	Personeria Delegada para Asuntos De Gobierno y Gestión Pública.	Educacion	Personería Delegada para asuntos de Educación, cultura, recreación y deporte
Hábitat	Personeria Delegada para el Hábitat y Servicios Públicos	Finanzas	Personería Delegada para Finanzas y desarrollo económico
Investigaciones	Dirección de Investigaciones Especiales Y Apoyo Técnico		
disciplinariosII	Personeria Delegada para Asuntos Disciplinarios II	disciplinariosIII	Personería Delegada para Asuntos Disciplinarios III
disciplinariosI	Personeria Delegada para asuntos Disciplinarios I	disciplinariosIV	Personería Delegada para Asuntos Disciplinarios IV

Nombre	Descripción	Nombre	Descripción
Usaquen	P. Local Usaquén	Chapinero	P. Local chapinero
Santafe	P. Local Santafé	Sancristobal	P. Local San Cristóbal
Usme	P. Local Usme	Tunjuelito	P. Local Tunjuelito
Bosa	P. Local Bosa	Kennedy	P. Local Kennedy
Fontibon	P. Local Fontibón	Engativa	P. Local Engativá
Suba	P. Local Suba	Barriosunidos	P. Local Barrios Unidos
Teusaquillo	P. Local Teusaquillo	Mártires	P. Local Los Mártires
Antnarino	P. Local Antonio Nariño	Ptearanda	P. Local Puente Aranda
Candelaria	P. Local La Calendaría	Rafael Uribe	P. Local Rafael Uribe
CiudadBolívar	P. Local Ciudad Bolívar	Sumapaz	P. Local Sumapaz

Anexo B. Amenazas Metodología Magerit

Las siguientes son las amenazas que relaciona la metodología Magerit – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información en el Libro II Catalogo de elementos, capítulo 5.

[código] descripción sucinta de lo que puede pasar	
Tipos de activos: • que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** 1. de seguridad que se pueden ver afecta das por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

5.1. [N] Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

Origen:

Natural (accidental)

5.1.1. [N.1] Fuego

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: Incendios: posibilidad de que el fuego acabe con recursos del sistema. **Ver:** EBIOS: 01- INCENDIO	

5.1.2. [N.2] Daños por agua

[N.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: Inundaciones: posibilidad de que el agua acabe con recursos del sistema. **Ver:** EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA	

5.1.3. [N.*] Desastres naturales

[N.*] Desastres naturales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ... Se excluyen desastres específicos tales como incendios (ver [N.1]) e inundaciones (ver [N.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. **Ver:** EBIOS: 03 – CONTAMINACIÓN 04 - SINIESTRO MAYOR 06 - FENÓMENO CLIMÁTICO 07 - FENÓMENO SÍSMICO 08 - FENÓMENO DE ORIGEN VOLCÁNICO 09 - FENÓMENO METEOROLÓGICO 10 - INUNDACIÓN	

5.2. [I] De origen industrial

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

5.2.1. [I.1] Fuego

[I.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: Incendio: posibilidad de que el fuego acabe con los recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 01- INCENDIO	

5.2.2. [I.2] Daños por agua

[I.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA	

5.2.3. [I.*] Desastres industriales

[I.*] Desastres industriales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: Otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ... Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 04 - SINIESTRO MAYOR	

5.2.4. [I.3] Contaminación mecánica

[I.3] Contaminación mecánica	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información	**Dimensiones:** 1. [D] disponibilidad
Descripción: vibraciones, polvo, suciedad, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 03 – CONTAMINACIÓN	

5.2.5. [I.4] Contaminación electromagnética

[I.4] Contaminación electromagnética	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información	**Dimensiones:** 1. [D] disponibilidad
Descripción: interferencias de radio, campos magnéticos, luz ultravioleta, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 14 - EMISIONES ELECTROMAGNÉTICAS 15- RADIACIONES TÉRMICAS 16 - IMPULSOS ELECTROMAGNÉTICOS	

5.2.6. [I.5] Avería de origen físico o lógico

[I.5] Avería de origen físico o lógico	
Tipos de activos: • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [Media] soportes de información	**Dimensiones:** 1. [D] disponibilidad

Descripción:

Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

Origen:

Entorno (accidental)
Humano (accidental o deliberado)

Ver:

EBIOS:
28 - AVERÍA DEL HARDWARE
29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE

5.2.7. [I.6] Corte del suministro eléctrico

[I.6] Corte del suministro eléctrico	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: cese de la alimentación de potencia **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA	

5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad

[I.7] Condiciones inadecuadas de temperatura y/o humedad	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad

Descripción:
Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ...
Origen:
Entorno (accidental)
Humano (accidental o deliberado)
Ver:
EBIOS: 11- FALLAS EN LA CLIMATIZACIÓN

5.2.9. [I.8] Fallo de servicios de comunicaciones

[I.8] Fallo de servicios de comunicaciones	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad

Descripción:
Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.
Origen:
Entorno (accidental)
Humano (accidental o deliberado)
Ver:
EBIOS: 13 - PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN

5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales

[I.9] Interrupción de otros servicios y suministros esenciales	
Tipos de activos: • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad

Descripción:
otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, ...
Origen:
Entorno (accidental)
Humano (accidental o deliberado)
Ver:
EBIOS: no disponible

5.2.11. [I.10] Degradación de los soportes de almacenamiento de la información

[I.10] Degradación de los soportes de almacenamiento de la información	
Tipos de activos: • [Media] soportes de información	**Dimensiones:** 1. [D] disponibilidad

Descripción:
como consecuencia del paso del tiempo
Origen:
Entorno (accidental)
Humano (accidental o deliberado)
Ver:
EBIOS:
28 - AVERÍA DEL HARDWARE
29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE

5.2.12. [I.11] Emanaciones electromagnéticas

[I.11] Emanaciones electromagnéticas	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] media • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [C] confidencialidad

Descripción:
Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque.

Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.

Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés *Transient Electromagnetic Pulse Standard).* Abusando del significado primigenio, es frecuen- te oír hablar de que un equipo disfruta de *TEMPEST protection,* queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara.

No se contempla en esta amenaza la emisión por necesidades del medio de comunicación:
redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.
Origen:
Entorno (accidental)
Humano (accidental o deliberado)
Ver:
EBIOS: 17 - INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS

5.3. [E] Errores y fallos no intencionados

Fallos no intencionales causados por las personas.

La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

Origen:
Humano (accidental)

5.3.1. [E.1] Errores de los usuarios

[E.1] Errores de los usuarios	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [Media] soportes de información	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc. **Ver:** EBIOS: 38 - ERROR DE USO	

5.3.2. [E.2] Errores del administrador

[E.2] Errores del administrador	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: equivocaciones de personas con responsabilidades de instalación y operación **Ver:** EBIOS: 38 - ERROR DE USO	

5.3.3. [E.3] Errores de monitorización *(log)*

[E.3] Errores de monitorización *(log)*	
Tipos de activos: • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad (trazabilidad)
Descripción: Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ... **Ver:** EBIOS: no disponible	

5.3.4. [E.4] Errores de configuración

[E.4] Errores de configuración	
Tipos de activos: • [D.conf] datos de configuración	**Dimensiones:** 1. [I] integridad
Descripción: Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del ad ministrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. **Ver:** EBIOS: no disponible	

5.3.5. [E.7] Deficiencias en la organización

Obsoleta.

[E.7] Deficiencias en la organización	
Tipos de activos: • [P] personal	**Dimensiones:** 1. [D] disponibilidad
Descripción: cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc. **Ver:** EBIOS: no disponible	

5.3.6. [E.8] Difusión de software dañino

[E.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: Propagación inocente de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc. **Ver:** EBIOS: no disponible	

5.3.7. [E.9] Errores de [re-]encaminamiento

[E.9] Errores de [re-]encaminamiento	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: Envío de información a través de un sistema o una red usando, accidentalmente, una ruta in correcta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera. **Ver:** EBIOS: no disponible	

5.3.8. [E.10] Errores de secuencia

[E.10] Errores de secuencia	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración accidental del orden de los mensajes transmitidos. **Ver:** EBIOS: no disponible	

5.3.9. [E.14] Escapes de información

Obsoleta: use E.19.

[E.14] Escapes de información	
Tipos de activos: •	**Dimensiones:** 1. [C] confidencialidad
Descripción: la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	

5.3.10. [E.15] Alteración accidental de la información

[E.15] Alteración accidental de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [I] integridad
Descripción: Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. **Ver:** EBIOS: no disponible	

5.3.11. [E.18] Destrucción de información

[E.18] Destrucción de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. **Ver:** EBIOS: no disponible	

5.3.12. [E.19] Fugas de información

[E.19] Fugas de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones • [P] personal (revelación)	**Dimensiones:** 1. [C] confidencialidad
Descripción: Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc. **Ver:** EBIOS: no disponible	

5.3.13. [E.20] Vulnerabilidades de los programas (software)

[E.20] Vulnerabilidades de los programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad 3. [C] confidencialidad
Descripción: Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. **Ver:** EBIOS: no disponible	

5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)

[E.21] Errores de mantenimiento / actualización de programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad
Descripción: Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. **Ver:** EBIOS: 31 - FALLA DE FUNCIONAMIENTO DEL SOFTWARE 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes electrónicos	**Dimensiones:** 1. [D] disponibilidad
Descripción: Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. **Ver:** EBIOS: 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

5.3.16. [E.24] Caída del sistema por agotamiento de recursos

[E.24] Caída del sistema por agotamiento de recursos	
Tipos de activos: • [S] servicios • [HW] equipos informáticos (hardware)	**Dimensiones:** 1. [D] disponibilidad
Descripción: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. **Ver:** EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO	

5.3.17. [E.25] Pérdida de equipos

[E.25] Robo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información	**Dimensiones:** 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	

5.3.18. [E.28] Indisponibilidad del personal

[E.28] Indisponibilidad del personal	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [D] disponibilidad
Descripción: Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica **Ver:** EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL	

5.4. [A] Ataques intencionados

Fallos deliberados causados por las personas.

La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas ve ces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

Origen
Humano (deliberado)

5.4.1. [A.3] Manipulación de los registros de actividad (log)

[A.4] Manipulación de los registros de actividad (log)	
Tipos de activos: • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad (trazabilidad)
Descripción: **Ver:** EBIOS: no disponible	

5.4.2. [A.4] Manipulación de la configuración

[A.4] Manipulación de la configuración	
Tipos de activos: • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [A] disponibilidad
Descripción: Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del ad ministrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. **Ver:** EBIOS: no	

5.4.3. [A.5] Suplantación de la identidad del usuario

[A.5] Suplantación de la identidad del usuario	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [A] autenticidad 3. [I] integridad
Descripción: Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. **Ver:** EBIOS: 40 - USURPACIÓN DE DERECHO	

5.4.4. [A.6] Abuso de privilegios de acceso

[A.6] Abuso de privilegios de acceso	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas. **Ver:** EBIOS: 39 - ABUSO DE DERECHO	

5.4.5. [A.7] Uso no previsto

[A.7] Uso no previsto	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [C] confidencialidad 3. [I] integridad
Descripción: Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc. **Ver:** EBIOS: no disponible	

5.4.6. [A.8] Difusión de software dañino

[A.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: Propagación intencionada de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc. **Ver:** EBIOS: no disponible	

5.4.7. [A.9] [Re-]encaminamiento de mensajes

[A.9] [Re-]encaminamiento de mensajes	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad

Descripción:

Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.

Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado.

Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.

Ver:

EBIOS: no disponible

5.4.8. [A.10] Alteración de secuencia

[A.10] Alteración de secuencia	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [I] integridad
Descripción: Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados. **Ver:** EBIOS: 36 - ALTERACIÓN DE DATOS	

5.4.9. [A.11] Acceso no autorizado

[A.11] Acceso no autorizado	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dim1nsiones:** 1. [C] confidencialidad 2. [I] integridad
Descripción: El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. **Ver:** EBIOS: 33 - USO ILÍCITO DEL HARDWARE	

5.4.10. [A.12] Análisis de tráfico

[A.12] Análisis de tráfico	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad

Descripción:
El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.

A veces se denomina monitorización de tráfico.

Ver:
EBIOS: no disponible

5.4.11. [A.13] Repudio

[A.13] Repudio	
Tipos de activos: • [S] servicios • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad (trazabilidad)

Descripción:
Negación a posteriori de actuaciones o compromisos adquiridos en el pasado.

Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación.
Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.

Ver:
EBIOS: 41 - NEGACIÓN DE ACCIONES

5.4.12. [A.14] Interceptación de información (escucha)

[A.14] Interceptación de información (escucha)	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad

Descripción:
El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.

Ver:
EBIOS: 19 - ESCUCHA PASIVA

5.4.13. [A.15] Modificación deliberada de la información

[A.15] Modificación deliberada de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [I] integridad
Descripción: Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. **Ver:** EBIOS: no disponible	

5.4.14. [A.18] Destrucción de información

[A.18] Destrucción de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. **Ver:** EBIOS: no disponible	

5.4.15. [A.19] Divulgación de información

[A.19] Revelación de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: Revelación de información. **Ver:** EBIOS: 23 – DIVULGACIÓN 27 – GEOLOCALIZACIÓN 34 - COPIA ILEGAL DE SOFTWARE	

5.4.16. [A.22] Manipulación de programas

[A.22] Manipulación de programas	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. **Ver:** EBIOS: 26 - ALTERACIÓN DE PROGRAMAS	

5.4.17. [A.23] Manipulación de los equipos

[A.22] Manipulación de los equipos	
Tipos de activos: • [HW] equipos • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [C] confidencialidad 2. [D] disponibilidad
Descripción: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. **Ver:** EBIOS: 25 - SABOTAJE DEL HARDWARE	

[A.26] Ataque destructivo	
Tipos de activos: • [HW] equipos informáticos (hardware)	**Dimensiones:** 1. [D] disponibilidad

Anexo C. Verificación de cumplimiento ISO 27002:2013

CARACTERIZACIÓN DE LA EMPRESA AUDITADA		DATOS PROCESO AUDITORÍA	
RAZÓN SOCIAL:		PROCESO N°:	
DEPENDENCIA/SEDE:		NORMA BASE:	NTC 27002:2013
DATOS ENTREVISTADO:		AUDITOR:	
DATOS DE CONTACTO:		FECHA INICIAL:	

ITEM	ASPECTO A AUDITAR	CUMPLIMIENTO	FUENTE	EVIDENCIA	OBSERVACIÓN
	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION				
A5.1.1	Políticas para la seguridad de la información				
A5.1.2	Revisión de las políticas para la seguridad de la información.				
	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION				
A6.1.1	Roles y responsabilidades para la seguridad de la información				
A6.1.2	Separación de deberes				
A6.1.3	Contacto con las autoridades				
A6.1.4	Contacto con grupos de interés especial				
A6.1.5	Seguridad de la información en la gestión de proyectos.				
A6.2.1	Política para dispositivos móviles				
A6.2.2	Teletrabajo				
	SEGURIDAD DE LOS RECURSOS HUMANOS				
A7.1.1	Selección				
A7.1.2	Términos y condiciones del empleo				
A7.2.1	Responsabilidades de la dirección				
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.				
A7.2.3	Proceso disciplinario				
A7.3.1	Terminación o cambio de responsabilidades de empleo				
	GESTION DE ACTIVOS				
A8.1.1	Inventario de activos				
A8.1.2	Propiedad de los activos				
A8.1.3	Uso aceptable de los activos				
A8.1.4	Devolución de activos				

A8.2.1	Clasificación de la información				
A8.2.2	Etiquetado de la información				
A8.2.3	Manejo de activos				
A8.3.1	Gestión de medio removibles				
A8.3.2	Disposición de los medios				
A8.3.3	Transferencia de medios físicos				
	CONTROL DE ACCESO				
A9.1.1	Política de control de acceso				
A9.1.2	Acceso a redes y a servicios en red				
A9.2.1	Registro y cancelación del registro de usuarios				
A9.2.2	Suministro de acceso de usuarios				
A9.2.3	Gestión de derechos de acceso privilegiado				
A9.2.4	Gestión de información de autenticación secreta de usuarios				
A9.2.5	Revisión de los derechos de acceso de usuarios				
A9.2.6	Retiro o ajuste de los derechos de acceso				
A9.3.1	Uso de información de autenticación secreta				
A9.4.1	Restricción de acceso a la información				
A9.4.2	Procedimiento de ingreso seguro				
A9.4.3	Sistema de gestión de contraseñas				
A9.4.4	Uso de programas utilitarios privilegiados				
A9.4.5	Control de acceso a códigos fuente de programas				
	CRIPTOGRAFIA				
A10.1.1	Política sobre el uso de controles criptográficos				
A10.1.2	Gestión de llaves				
	SEGURIDAD FISICA Y DEL ENTORNO				
A11.1.1	Perímetro de seguridad física				
A11.1.2	Controles de acceso físicos				
A11.1.3	Seguridad de oficinas, recintos e instalaciones.				
A11.1.4	Protección contra amenazas externas y ambientales.				

A11.1.5	Trabajo en áreas seguras.				
A11.1.6	Áreas de carga, despacho y acceso público				
A11.2.1	Ubicación y protección de los equipos				
A11.2.2	Servicios de suministro				
A11.2.3	Seguridad en el cableado.				
A11.2.4	Mantenimiento de los equipos.				
A11.2.5	Retiro de activos				
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones				
A11.2.7	Disposición segura o reutilización de equipos				
A11.2.8	Equipos de usuario desatendido				
A11.2.9	Política de escritorio limpio y pantalla limpia				
	SEGURIDAD DE LAS OPERACIONES				
A12.1.1	Procedimientos de operación documentados				
A12.1.2	Gestión de cambios				
A12.1.3	Gestión de capacidad				
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación				
A12.2.1	Controles contra códigos maliciosos				
A12.3.1	Respaldo de la información				
A12.4.1	Registro de eventos				
A12.4.2	Protección de la información de registro				
A12.4.3	Registros del administrador y del operador				

A12.4.4	Sincronización de relojes				
A12.5.1	Instalación de software en sistemas operativos				
A12.6.1	Gestión de las vulnerabilidades técnicas				
A12.6.2	Restricciones sobre la instalación de software				
A12.7.1	Controles de auditorías de sistemas de información				
	SEGURIDAD DE LAS COMUNICACIONES				
A13.1.1	Controles de redes				
A13.1.2	Seguridad de los servicios de red				
A13.1.3	Separación en las redes				
A13.2.1	Políticas y procedimientos de transferencia de información				
A13.2.2	Acuerdos sobre transferencia de información				
A13.2.3	Mensajería Electronica				
A13.2.4	Acuerdos de confidencialidad o de no divulgación				
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información				
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas				
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.				
A.14.2.1	Política de desarrollo seguro				
A.14.2.2	Procedimientos de control de cambios en sistemas				
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación				
A.14.2.4	Restricciones en los cambios a los paquetes de software				

A.14.2.5	Principio de Construcción de los Sistemas Seguros.				
A.14.2.6	Ambiente de desarrollo seguro				
A.14.2.7	Desarrollo contratado externamente				
A.14.2.8	Pruebas de seguridad de sistemas				
A.14.2.9	Prueba de aceptación de sistemas				
A.14.3.1	Protección de datos de prueba				
	RELACIONES CON LOS PROVEEDORES				
A15.1.1	Política de seguridad de la información para las relaciones con proveedores				
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores				
A15.1.3	Cadena de suministro de tecnología de información y comunicación				
A15.2.1	Seguimiento y revisión de los servicios de los proveedores				
A15.2.2	Gestión del cambio en los servicios de los proveedores				
	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION				
A16.1.1	Responsabilidades y procedimientos				
A16.1.2	Reporte de eventos de seguridad de la información				
A16.1.3	Reporte de debilidades de seguridad de la información				
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos				
A16.1.5	Respuesta a incidentes de seguridad de la información				
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información				
A16.1.7	Recolección de evidencia				
	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO				
A17.1.1	Planificación de la continuidad de la seguridad de la información				
A17.1.2	Implementación de la continuidad de la seguridad de la información				

A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información				
A17.2.1	Disponibilidad de instalaciones de procesamiento de información				
	CUMPLIMIENTO				
A18.1.1	Identificación de la legislación aplicable.				
A18.1.2	Derechos propiedad intelectual (DPI)				
A18.1.3	Protección de registros				
A18.1.4	Privacidad y protección de información de datos personales				
A18.1.5	Reglamentación de controles criptográficos.				
A18.2.1	Revisión independiente de la seguridad de la información				
A18.2.2	Cumplimiento con las políticas y normas de seguridad				
A18.2.3	Revisión del cumplimiento técnico				

Anexo D. Lista de chequeo de auditoría interna

LISTA DE CHEQUEO DE AUDITORÍA INTERNA				Página 52 de 10		
				Código: AU1		
				Versión: 1		
PROCESO						
FECHA		**HORA**		**LUGAR**		
AUDITOR LIDER						
AUDITOR AUXILIAR						
AUDITADO						
PROCESO/PROCEDIMIENTO/ACTIVIDAD/REQUISITO A AUDITAR				**HALLAZGO**		**EVIDENCIAS**
				C	**NC**	
Políticas de seguridad						
	¿Existe una Política de Seguridad de la Información la empresa?					
	¿Es claro en la política lo que es y no es permisible?					
	¿Defina que es una política de seguridad y que identifica como información?					
	¿La política de seguridad apoya los objetivos o la mis de la empresa?					
	¿Cómo se comunica la política de seguridad en organización?					
	¿Es claro en las políticas las consecuencias incumplimiento de las mismas?					
	¿La política de seguridad es revisada regularment actualizada de acuerdo a las necesidades de la empresa?					
Organización Interna						
	¿Se tiene claramente identificados las responsabilida de gestión y de los empleados?					
	¿La alta dirección apoya el programa de seguridad d información?					
	¿Están claramente definidas las áreas responsabilidad de la empresa?					
	¿Cómo se evalúan las acciones tomadas para garanti que las personas de la empresa tienen las competenc necesarias?					
	¿Se tienen definidos niveles jerárquicos de autorid manejando los contactos con las autoridades pertinentes?					
	¿Existe un procedimiento formal para la asignación usuarios y roles?					
	¿El grupo de seguridad tiene la autoridad para preser cambios en la política de seguridad necesarios en toda empresa?					

Empleados antes y ejecución del empleo				
	¿Existen procedimientos o mecanismos adecuados p la selección de personal, y la verificación de anteceden para los candidatos? Explíquelos			
	¿El personal contratistas está sujeto a acuerdos confidencialidad?			
	¿La alta dirección apoya el programa de seguridad de información?			
	¿Los empleados y directivos son conscientes de s responsabilidades en materia de protección de los recurs de información?			
	¿Qué capacitaciones se realizan a los funcionarios de empresa?			
	¿Los empleados conocen los objetivos de negocio dirección?			
	¿Los empleados reciben formación específ relacionada con la seguridad de sus responsabilidades?			
	¿Los empleados capaces de desempeñar sus funcion de manera eficiente y eficaz al seguir los procedimientos seguridad?			
	¿Los administradores de red y del sistema tienen experiencia adecuada para aplicar las normas de seguridad			
	¿Existe una conciencia de seguridad regular y progra de entrenamiento en su lugar?			
	¿Existen procesos disciplinarios, claros y conformes a la normatividad vigente?			
Terminación y cambio de empleo				
	¿Existe algún procedimiento para la entrega inventario al retirarse un empleado?			
	¿Existen cuentas activas de usuarios que no tien vínculo con la empresa?			
	¿Las cuentas de usuario temporales manejan fechas caducidad?			
	¿Existe algún procedimiento formal para la terminac del contrato laboral o cambio de puesto de un empleado?			
Responsabilidad por los Activos				
	¿Hay un inventario en la compañía de Sistem Hardware y Datos?			
	¿Se tiene identificado los activos críticos de la empres			
	¿Se sabe quiénes son los propietarios de los elemen del inventario?			
	¿Cuáles son las normas que aplican para el u aceptable de los activos?			
	¿Existe un proceso implementado para el mane marcación y etiquetado de los activos?			
	¿Se tiene implementado procesos para el uso acepta de los activos?			
	¿Cómo se manejan los medios que deben desechados?			
	¿Qué procedimiento se utiliza para el transporte de medios fuera de la entidad?			
	¿Cómo se da a los empleados acceso al sistema?			

	¿Se distingue entre: riesgos para el negocio, riesg para el servicio prestado a los clientes y riesgo de parálisis la gestión de la Empresa?			
	Dispositivos móviles y Teletrabajo			
	¿Existe un procedimiento de acceso remoto a empresa?			
	¿Se tiene control de los dispositivos móviles?			
	Control de Acceso Usuarios			
	¿Existen políticas y procedimientos de control acceso?			
	¿Están los servidores críticos protegidos con contro de acceso adecuados?			
	¿Cómo un usuario obtiene permiso de ingresar a servidores, servicios y/o aplicativos?			
	¿Se tienen políticas de manejo de contraseñas?			
	¿Las contraseñas y cuentas de usuario se comparter			
	¿Existen dispositivos especiales para el control acceso?			
	¿Existen protocolos definidos para ir al otro lado firewall?			
	¿Se ha llevado a cabo un análisis de riesgos p determinar si las reglas establecidas en el firewall permi mantener un nivel aceptable de riesgo?			
	Gestión del Acceso de Usuarios			
	¿Los usuarios de los recursos de red están facultad para cambiar la contraseña predeterminada inicial?			
	¿Existe un procedimiento formal para creaci modificación y eliminación de cuentas de usuario?			
	¿Cómo se garantiza que los empleados tengan permisos adecuados según su rol?			
	¿Existe un administrador de sistemas que controle a usuarios?			
	¿Existen políticas para el manejo de cuentas de usuar			
	¿Los usuarios de los recursos de red están facultad para cambiar la contraseña predeterminada inicial?			
	¿Las políticas y procedimientos son continuame evaluados contra las necesidades del negocio de la empre actual?			
	Responsabilidad de los Usuarios			
	¿ Los usuarios tienen conocimiento de sus obligacion con la seguridad y normas de uso de contraseñas?			
	Control de Acceso a Sistemas y Aplicaciones			
	¿Es el acceso a la información sensible / confidencial monitoreado?			
	¿Existe un administrador de bases de datos que gestio las instancias de las mismas y de las aplicaciones?			
	¿Existe un acceso restringido a las instancias d contienen el Repositorio de BD y el de las aplicaciones?			
	¿Es autocambiable la clave de acceso a Servidores, y aplicaciones?			
	¿Se obliga, cada cierto tiempo, a cambiar la contrase automáticamente?			

	¿Existen listados de intentos de accesos satisfactorios?			
	¿Está disponible el código fuente?			
	¿Está restringido el acceso al entorno de desarrollo?			
	¿Existe un acceso restringido a la sala del Data Cent			
Controles Criptográficos				
	¿Se usaron programas automatizados de cifrado archivos?			
	¿Se efectuó un ataque al archivo de contraseñas?			
Áreas Seguras				
	¿Existe demarcación de las áreas restringidas?			
	¿Se controla el acceso a los edificios?			
	¿Existe un registro de auditoría para identificar individuo y el tiempo de acceso para acceder horas estándar?			
	¿Existen mecanismos de seguridad física en las sa del Data Center??			
	¿Se cuenta con equipos para el control de la temperat y humedad, sistemas de extinción de incendios, dispositi de suministro eléctrico ininterrumpido?			
	¿Existen puntos de acceso, tales como las zonas entrega y de carga están?			
	¿Están los sistemas y el hardware adecuadame protegidos contra el robo?			
Equipos				
	¿Existe procedimientos para sacar equipos, informac o software fuera de la empresa?			
	¿Cuando un usuario se ausenta deja el equ desbloqueado?			
	¿Existe política de escritorio limpio de papeles y sopor de almacenamiento extraíbles?			
	¿Los equipos cuentan programación de mantenier preventivos?			
Procedimientos Operacionales y Responsabilidades				
	¿Existe una política de clasificación de informac razonable y útil?			
	¿Los procedimientos de operación deberán s documentados, mantenidos y puestos a disposición de toc los usuarios que los necesitan?			
	¿Se siguió la política de clasificación de la informació			
	¿Existen políticas para el desarrollo de aplicaciones?			
	¿Cómo seleccionan los datos para las pruebas aplicativos?			
	¿Qué pruebas se realizan para verificar que el méto de control es el más apropiado?			
	¿Existe un manual del empleado de seguridad información?			
	¿Se debe planifica la capacidad futura de infraestructura?			
Protección contra Códigos Maliciosos				
	¿Se tiene instalados aplicativos que protejan los equip de códigos maliciosos o antivirus?			

	¿Existen procedimientos para el manejo de equi infectados?			
	¿Existen zonas de seguridad para el tratamiento equipos peligrosos para la red?			
	Copias de respaldo			
	¿Existen procedimiento de copias de respaldo?			
	¿Se realiza verificación de las copias de respaldo?			
	¿Se lleva un registro o bitácora de las copias de respa realizadas?			
	¿Se hacen copias de seguridad diariamente?			
	¿Se almacenan las copias de seguridad en dispositi externos?			
	¿Se ubican los dispositivos externos en loca diferentes al edificio en el que se encuentran las redes y servidores?			
	Registro y Seguimiento			
	¿Cómo se maneja los log de los servidores?			
	¿Con que periodicidad se refrescan los registros eventos?			
	¿Quiénes tienen acceso a los log del sistema?			
	¿Se cuenta un sistema de sincronización de hora de equipos, base de datos y servidores?			
	Control de Software Operacional			
	¿Existen controles para la instalación de software sistemas operativos?			
	¿Ha tenido en cuenta las distintas versiones de elementos Software?			
	¿Se han hecho estudios coste/beneficio sobre si camb los sistemas del departamento o mejorarlos?			
	Gestión de la Vulnerabilidad Técnica			
	¿Se han hecho estudios que revelan cuál es la man más sencilla y menos costosa de cambiar y mejorar sistema?			
	¿Existen políticas para la instalación de software parte de los usuarios?			
	Consideraciones sobre Auditorías de sistemas de Información			
	¿Cómo han contribuido las auditorías internas a evolución del sistema?			
	¿Qué aporte han tenido las acciones correctivas preventivas en la mejora de la empresa?			
	Gestión de la Seguridad de las Redes			
	¿Administradores utilizan herramientas adecuadas p realizar su trabajo?			
	¿Hay un diagrama de la red actual disponible?			
	¿Las listas son de control de acceso (ACL) mantienen forma regular?			
	¿Es la infraestructura de red auditada de forma regul			
	¿Se ha implementado una zona desmilitarizada (DMZ red perimetral (un segmento de red entre el router que conecta a Internet y el servidor de seguridad)?			
	¿Se maneja una política de seguridad en cuanto al u de la tecnología inalámbrica?			

	¿Se posee un inventario actualizado de todos dispositivos inalámbricos de la red?			
	¿Se verificó que todos los clientes inalámbricos tuvies un antivirus instalado?			
	¿Los datos que van a la DMZ o red perimetral encuentran cifrados?			
	Transferencia de Información			
	¿Existen procedimientos de transferencia información?			
	¿Se utilizan mecanismos de protección para mensajería electrónica?			
	¿Existen acuerdos de confidencialidad para trasferencia de información?			
	Requisitos de seguridad de los Sistemas de Información			
	¿Se tienen especificados los controles de seguric requeridos para nuevos sistemas de información?			
	¿Se utiliza encriptación para las trasferenc electrónicas?			
	¿Existen mecanismo de control y seguridad para ingre a las redes privadas?			
	Seguridad en los procesos de desarrollo y soporte			
	¿Se ha implementado una metodología de desarrollo aplicaciones?			
	¿Se monitorea el uso de los recursos?			
	¿Las pruebas de parches o actualizaciones se realiz en ambientes aislados?			
	¿Existe procedimientos establecidos para la realizac de cambios en la entidad?			
	¿Existe un formulario de petición de cambio modificación?			
	¿Es necesaria la autorización para realizar un cambic			
	¿Se realiza la modificación sobre una copia del sitio?			
	¿Existe algún fichero log que almacene todos cambios realizados?			
	¿Se comunica al solicitante del cambio que se ha lleva a cabo la modificación?			
	¿Existe documentación escrita sobre el cam (formulario de petición, script del cambio realiza aprobación del solicitante)?			
	¿Se realizan pruebas sobre el cambio para compro que la aplicación funciona correctamente?			
	¿Cuándo se cambian los sistemas operativ aplicaciones críticas de negocio son revisadas y probadas			
	¿Existen ambientes separados para los ambientes desarrollo y producción?			
	¿Ha verificado en general los productos adquirid recientemente? (contratos de utilización, códigos fuente,...			
	¿Son claros los criterios de aceptación para los nuev sistemas de información?			
	¿Se realizan pruebas de seguridad de sistemas?			

	Datos de Prueba			
	¿Cómo se selecciona los datos suministrados para pruebas?			
	¿Qué mecanismos de protección se emplean para datos de pruebas?			
	Seguridad de la Información en las Relaciones con los Proveedores			
	¿Se lleva un registro de los servicios proporcionados proveedores?			
	¿Se maneja el procedimiento de gestión de cambios los servicios con los proveedores?			
	Gestión de los incidentes y las Mejoras en la Seguridad de la Información			
	¿Se ha establecido un Equipo de Respuesta Incidentes?			
	¿Los empleados han sido entrenados en cuanto a respuesta a incidentes?			
	¿Después de un incidente son las políticas procedimientos revisados, para determinar que modificaciones deben implementarse?			
	¿Los informes de incidentes se emiten a la gest adecuada?			
	Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio			
	¿Se ha llevado a cabo un Análisis de Impacto al Nego en todos los sistemas, aplicaciones y plataformas?			
	¿Existe un plan documentado centro de datos recuperación de desastre en su lugar?			
	¿Los sistemas, aplicaciones y copias de seguridad datos son enviados a un lugar seguro fuera de la empresa manera regular?			
	¿Se tienen claros los acuerdos de nivel de servicio, todos los usuarios y los proveedores de servicios?			
	¿Se ha probado el plan de contingencia?			
	Redundancias			
	¿Se tienen implementados instalaciones redundan de procesamiento de información para cumplir con el requi de disponibilidad?			
	Cumplimiento de los Requisitos Legales y Contractuales			
	¿Se tiene conocimiento de las leyes que se aplican p los delitos informáticos?			
	¿La organización tiene normas claras para el manejo la normatividad legal vigente?			
	¿Se preserva y respecta el derecho de autor?			
	¿Cómo se contrala el software instalado en los equip			
	¿Se tiene un inventario del software legal propiedad la empresa y en que equipos se encuentra instalado?			
	¿Cómo se protege los datos confidenciales de funcionarios, clientes y aplicativos?			
	Revisiones de Seguridad de la Información			
	¿Está la información confidencial debidame asegurados?			
	¿Se ha probado el servidor de seguridad para determi si la penetración exterior es posible?			

	¿Existen procedimientos establecidos para aplicar política de seguridad de la información?			
	¿Existen procedimientos establecidos para eliminación adecuada de la información confidencial?			
	¿Se monitorea periódicamente el cumplimiento de políticas y procedimientos implementados?			
OBSERVACIONES:				

Anexo E: Formato para registro de visita de auditoria

CARACTERIZACIÓN DE LA ENTIDAD

NIT: _____

RAZÓN SOCIAL EMPRESA:

DEPENDENCIA/SEDE:

DATOS ENTREVISTADO:

DATOS DE CONTACTO:

DATOS PROCESO AUDITORÍA

PROCESO N°:

NORMA BASE:

METODOLOGIA

FECHA INICIAL: DD/MM/YYYY

FECHA FINAL: DD/MM/YYYY

Clausula ISO	Sección e ITEM analizado	¿Aplica pregunta? S/N	Cumplimiento			Hallazgos	Requiere plan de mejoramiento	
			Alcanzado	Pendiente	No aplica		Si	No
	Sección A -Seguridad de la Información							
	1. Revisión de la Inteligencia Competitiva							
	2. Revisión de Privacidad							
	3. Recolección de Documentos							
	Sección B – Seguridad de los Procesos							
	1. Testeo de Solicitud							
	2. Testeo de Sugerencia Dirigida							
	3. Testeo de las Personas Confiables							
	Sección C – Seguridad en las tecnologías de Internet							
	1. Logística y Controles							
	2. Exploración de Red							
	3. Identificación de los Servicios del Sistema							

	4. Búsqueda de Información Competitiva							
	5. Revisión de Privacidad							
	6. Obtención de Documentos							
	7. Búsqueda y Verificación de Vulnerabilidades							
	8. Testeo de Aplicaciones de Internet							
	9. Enrutamiento							
	10. Testeo de Sistemas Confiados							
	11. Testeo de Control de Acceso							
	12. Testeo de Sistema de Detección de Intrusos							
	13. Testeo de Medidas de Contingencia							
	14. Descifrado de Contraseñas							
	15. Testeo de Denegación de Servicios							
	16. Evaluación de Políticas de Seguridad							
	Sección D – Seguridad en las Comunicaciones							
	1. Testeo de PBX							
	2. Testeo del Correo de Voz							
	3. Revisión del FAX							
	4. Testeo del Modem							
	Sección E – Seguridad Inalámbrica							
	1. Verificación de Radiación Electromagnética (EMR)							
	2. Verificación de Redes Inalámbricas [802.11]							
	3. Verificación de Redes Bluetooth							
	4. Verificación de Dispositivos de Entrada Inalámbricos							
	5. Verificación de Dispositivos de Mano Inalámbricos							
	6. Verificación de Comunicaciones sin Cable							
	7. Verificación de Dispositivos de Vigilancia Inalámbricos							
	8. Verificación de Dispositivos de Transacción Inalámbricos							
	9. Verficación de RFID							

	10. Verificación de Sistemas Infrarrojos							
	11. Revisión de Privacidad							
	Sección F – Seguridad Física							
	1. Revisión de Perímetro							
	2. Revisión de monitoreo							
	3. Evaluación de Controles de Acceso							
	4. Revisión de Respuesta de Alarmas							
	5. Revisión de Ubicación							
	6. Revisión de Entorno							

MIEMBRO EQUIPO AUDITOR:

OBSERVACIONES COORDINADOR EQUIPO: