



# DIAGNÓSTICO DE SEGURIDAD DE LA INFORMACIÓN

## MUNICIPIO DE APARTADÓ

Eliecer Arteaga Vargas

**Alcalde Municipal**

Marta Cecilia Rivera Higueta

**Subsecretaria Gestión Tics y Documental**

Alejandro A. Almario Rincón

**Profesional Universitario**

**Marzo - 2018**





DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



## TABLA DE CONTENIDO

<b>1. INTRODUCCIÓN.....</b>	<b>7</b>
<b>2. OBJETIVO.....</b>	<b>7</b>
<b>3. ALCANCE .....</b>	<b>8</b>
<b>4. DEFINICIONES .....</b>	<b>8</b>
<b>5. DIAGNÓSTICO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LOS DOMINIOS DE ISO 27001 E ISO 27002.....</b>	<b>20</b>
5.1. <b>POLÍTICAS DE SEGURIDAD – ADMINISTRATIVA. ....</b>	<b>20</b>
<b>6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION – ADMINISTRATIVA. ....</b>	<b>20</b>
<b>7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS – ADMINISTRATIVA. ...</b>	<b>23</b>
7.1. <i>Antes de Asumir el empleo: .....</i>	<i>23</i>
7.1.1. <i>Selección e investigación de antecedentes: .....</i>	<i>23</i>
7.2. <i>Durante la Ejecución del Empleo:.....</i>	<i>23</i>
7.2.1. <i>Responsabilidades de la Dirección: .....</i>	<i>23</i>
7.2.2. <i>Toma de Conciencia, Educación y Formación en la Seguridad de la Información: 24</i>	
7.2.3. <i>Proceso Disciplinario: .....</i>	<i>24</i>
7.3. <i>Terminación de Contrato o Traslado de Funcionario: .....</i>	<i>24</i>
<b>8. GESTIÓN DE ACTIVOS – ADMINISTRATIVA.....</b>	<b>25</b>
8.1. <i>Responsabilidad de los Activos: .....</i>	<i>25</i>
8.1.1. <i>Responsabilidad de los Activos: .....</i>	<i>25</i>
8.2. <i>Clasificación de información: .....</i>	<i>25</i>
<b>9. CONTROL DE ACCESO –TECNICA.....</b>	<b>26</b>
9.1. <i>Requisitos del Negocio para Control de Acceso: .....</i>	<i>26</i>
9.1.1. <i>Política de Control de Acceso: .....</i>	<i>26</i>
9.1.2. <i>Acceso a Redes y a Servicios en Red: .....</i>	<i>27</i>
9.2. <i>Gestión de Acceso de Usuarios:.....</i>	<i>27</i>
9.2.1. <i>Registro y Cancelación del Registro de Usuarios:.....</i>	<i>27</i>
9.2.2. <i>Suministro de Acceso de Usuarios:.....</i>	<i>28</i>
9.2.3. <i>Gestión de Derechos de Acceso Privilegiado:.....</i>	<i>28</i>



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



9.2.4.	Gestión de Información de Autenticación Secreta de Usuarios:.....	29
9.2.5.	Revisión de los Derechos de Acceso de Usuarios: .....	29
9.2.6.	Retiro o Ajuste de los Derechos de Acceso:.....	30
9.3.	Responsabilidades de los Usuarios: .....	30
9.3.1.	Uso de Información de Autenticación Secreta:.....	30
9.4.	Control de Acceso a Sistemas y Aplicaciones:.....	31
9.4.1.	Restricción de Acceso a la Información:.....	31
9.4.2.	Procedimiento de Ingreso Seguro: .....	31
9.4.3.	Sistema de Gestión de Contraseñas:.....	32
9.4.4.	Uso de Programas Utilitarios:.....	33
9.4.5.	Control de Acceso a Códigos Fuente de Programas: .....	33
<b>10.</b>	<b>CRIPTOGRAFÍA –TECNICA.</b> .....	<b>34</b>
10.1.	Controles Criptográficos:.....	34
10.1.1.	Política Sobre el Uso de Controles Criptográficos: .....	34
10.1.2.	Gestión de Llaves: .....	34
<b>11.</b>	<b>SEGURIDAD FÍSICA Y DEL ENTORNO –TECNICA.</b> .....	<b>35</b>
11.1.	Áreas Seguras: .....	35
11.1.1.	Perímetro de Seguridad Física:.....	35
11.1.2.	Controles Físicos de Entrada: .....	36
11.1.3.	Seguridad de Oficinas, Recintos e Instalaciones:.....	36
11.1.4.	Protección Contra amenazas externas y ambientales: .....	36
11.1.5.	Trabajo en Áreas Seguras: .....	37
11.1.6.	Áreas de Despacho y Carga:.....	37
11.2.	Equipos: .....	37
11.2.1.	Ubicación y Protección de los Equipos:.....	37
11.2.2.	Servicios de Suministro: .....	38
11.2.3.	Seguridad del Cableado:.....	40
11.2.4.	Mantenimiento de Equipos: .....	49
11.2.5.	Retiro de Activos:.....	50
11.2.6.	Seguridad de Equipos y Activos Fuera de las Instalaciones:.....	50
11.2.7.	Disposición Segura o Reutilización de Equipos: .....	50
11.2.8.	Equipos de Usuarios Desatendidos: .....	50



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



11.2.9.	Política de Escritorio Limpio y Pantalla Limpia: .....	51
<b>12.</b>	<b>SEGURIDAD DE LAS OPERACIONES –TECNICA.</b> .....	51
12.1.	Procedimientos Operacionales y Responsabilidades: .....	51
12.1.1.	Procedimientos de Operación Documentados: .....	51
12.1.2.	Gestión de Cambios:.....	52
12.1.3.	Gestión de Capacidad: .....	52
12.1.4.	Separación de los Ambientes de Desarrollo, Pruebas y Operación: .....	52
12.2.	Protección Contra Códigos Maliciosos: .....	53
12.2.1.	Controles Contra Códigos Maliciosos: .....	53
12.3.	Copias de Respaldo:.....	54
12.3.1.	Respaldo de la Información: .....	54
12.4.	Registro y Seguimiento: .....	55
12.4.1.	Registro de Eventos:.....	55
12.4.2.	Protección de la Información de Registro:.....	56
12.4.3.	Registros del Administrador y del Operador: .....	56
12.4.4.	Sincronización de Relojes:.....	56
12.5.	Control de Software Operacional:.....	56
12.5.1.	Instalación de Software en Sistemas Operativos:.....	56
12.6.	Gestión de la Vulnerabilidad Técnica:.....	57
12.6.1.	Gestión de las Vulnerabilidades Técnicas:.....	57
12.6.2.	Restricciones Sobre la Instalación de Software: .....	58
12.7.	Consideraciones Sobre Auditorías de Sistemas de Información:.....	58
12.7.1.	Controles Sobre Auditorías de Sistemas de Información: .....	58
<b>13.</b>	<b>SEGURIDAD DE LAS COMUNICACIONES –TECNICA.</b> .....	58
13.1.	Gestión de la Seguridad de las Redes: .....	58
13.1.1.	Controles de Redes: .....	59
13.1.2.	Seguridad de los Servicios de Red:.....	59
13.1.3.	Separación en las Redes: .....	60
13.2.	Transferencia de Información:.....	60
13.2.1.	Políticas y Procedimientos de Transferencia de Información: .....	60
13.2.2.	Acuerdos Sobre Transferencia de Información: .....	60
13.2.3.	Mensajería Electrónica: .....	61



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



13.2.4.	Acuerdos de Confidencialidad o de no Divulgación:.....	61
<b>14.</b>	<b>ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN –TECNICA.</b> .....	<b>62</b>
14.1.	Requisitos de Seguridad de los Sistemas de Información: .....	62
14.1.1.	Análisis y Especificación de Requisitos de Seguridad de la Información: .....	62
14.1.2.	Seguridad de Servicios de las Aplicaciones en Redes Públicas: .....	62
14.1.3.	Protección de Transacciones de los Servicios de las Aplicaciones: .....	62
14.2.	Seguridad en los Procesos de Desarrollo y de Soporte: .....	63
14.2.1.	Política de Desarrollo Seguro:.....	63
14.2.2.	Procedimientos de Control de Cambios en Sistemas: .....	63
14.2.3.	Revisión Técnica de las Aplicaciones Después de Cambios en la Plataforma de Operación:.....	63
14.2.4.	Restricciones en los Cambios a los Paquetes de Software: .....	64
14.2.5.	Principios de Construcción de Sistemas Seguros:.....	64
14.2.6.	Ambiente de Desarrollo Seguro: .....	64
14.2.7.	Desarrollo Contratado Externamente:.....	64
14.2.8.	Pruebas de Seguridad de Sistemas:.....	65
14.3.	Datos de Prueba:.....	65
14.3.1.	Protección de Datos de Prueba: .....	65
<b>15.</b>	<b>RELACIÓN CON PROVEEDORES – ADMINISTRATIVA.</b> .....	<b>65</b>
15.1.	Seguridad de la Información en las Relaciones con los Proveedores:.....	65
15.2.	Gestión en la Prestación de Servicios de Proveedores: .....	66
<b>16.</b>	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN –TECNICA.</b>	<b>66</b>
16.1.	Gestión de Incidentes y Mejoras en la Seguridad de la Información: .....	66
16.1.1.	Responsabilidades y Procedimientos: .....	66
16.1.2.	Reporte de Eventos de Seguridad de la Información: .....	67
16.1.3.	Reporte de Debilidades de Seguridad de la Información: .....	67
16.1.4.	Evaluación de Eventos de Seguridad de la Información y Decisiones Sobre Ellos:	67
16.1.5.	Respuesta a Incidentes de Seguridad de la Información: .....	68
16.1.6.	Aprendizaje Obtenido de los Incidentes de Seguridad de la Información: .....	68
16.1.7.	Recolección de Evidencia: .....	68



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



<b>17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO – ADMINISTRATIVA.</b>	69
17.1. Continuidad de la Seguridad de la Información:	69
17.1.1. Planificación de la Continuidad de la Seguridad de la Información:	69
17.1.2. Implementación de la Continuidad de la Seguridad de la Información:	69
17.1.3. Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información:	70
17.2. Redundancias:	70
17.2.1. Disponibilidad de Instalaciones de Procesamiento de Información:	70
<b>18. CUMPLIMIENTO – ADMINISTRATIVA.</b>	71
18.1. Cumplimiento de Requisitos Legales y Contractuales:	71
18.1.1. Identificación de la Legislación Aplicable y de los Requisitos Contractuales:	71
18.1.2. Derechos de Propiedad Intelectual:	71
18.1.3. Protección de Registros:	71
18.1.4. Protección de los Datos y Privacidad de la Información Relacionada con los Datos Personales:	72
18.2. Revisiones de Seguridad de la Información:	72
18.2.1. Revisión Independiente de la Seguridad de la Información:	72
18.2.2. Cumplimiento con las Políticas y Normas de Seguridad:	72
18.2.3. Revisión de Cumplimiento Técnico:	73



## 1. INTRODUCCIÓN

La seguridad de la información, es uno de los componentes más importantes de toda empresa, para brindar confianza a los clientes y brindar la seguridad necesaria a los procesos que lo requieren. Los pilares más importantes de la seguridad son la de integridad, disponibilidad y confidencialidad.

En los tiempos actuales en la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial y que no, la información que se tienen, aunque no se crea puede tener un alto valor y simplemente por ley esta se debe resguardada.

Por estas razones es necesaria la implementación de controles a los riesgos basados en estándares, que nos permitan controlar la información para que sea resguardada, porque la tecnología ha traído consigo nuevos retos en materia de seguridad, pero para realizar la implementación de estos estándares, los primeros que debe reconocer una empresa son sus vulnerabilidades, los riesgos frente a una amenaza y determinar el impacto que ocasionar esta.

La Alcaldía de Apartadó es una entidad perteneciente al sector público que tiene como misión la de prestar servicios públicos que determine la ley, construir las obras que demande el progreso local, ordenar el desarrollo de su territorio, promover la participación comunitaria, el mejoramiento social y cultural de sus habitantes y cumplir las demás funciones que le asignen la Constitución y las leyes. Para el cumplimiento de estas funciones designadas la entidad cuenta con una infraestructura tecnológica, donde se ha diseñado e implementado todo un sistema tecnológico que incluye un Datacenter, bajo una plataforma Microsoft y una topología de red propia, LAN para su sede. Esta infraestructura cuenta con una serie de mecanismos de seguridad que permiten proteger en cierta medida a la entidad misma de algunos ataques y de incidentes de seguridad menores, pero está aún no posee los suficientes mecanismos de defensa para poder establecer las bases sólidas de la seguridad necesarias para minimizar el impacto de una posible amenaza.

## 2. OBJETIVO

Realizar un diagnóstico para analizar el nivel de seguridad de la información existente en la Alcaldía de Apartadó. Con el fin proteger recursos valiosos de la organización, tales como la información y los que contienen y administran esta, como lo son el hardware y el software.



### 3. ALCANCE

Este diagnóstico está enfocado en la seguridad de información, y comprende todo lo relacionado con la seguridad desde la física, hasta la lógica, basados en la ley y en estándares como la ISO 27001, ISO 27002 y metodologías de análisis y gestión de riesgo como Magerit versión 3.

### 4. DEFINICIONES

- 4.1. **Acción Correctiva:** Conjunto de acciones tomadas para eliminar la(s) causa(s) de no una conformidad detectada u otra situación no deseable.
- 4.2. **Acción Preventiva:** Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad potencial u otra situación potencial no deseable.
- 4.3. **Aceptación del Riesgo:** Después de revisar las consecuencias que puede acarrear el riesgo, se toma la decisión de afrontarlo.
- 4.4. **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.
- 4.5. **Administración de Riesgos:** Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo. Las estrategias incluyen transferir el riesgo a otra parte, evitar el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.
- 4.6. **Administración de incidentes de seguridad:** Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del





DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



desempeño de todos los activos y recursos gerenciales que tiene la entidad. Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

- ✓ Detectar cualquier alteración en los servicios TI.
- ✓ Registrar y clasificar estas alteraciones.
- ✓ Asignar el personal encargado de restaurar el servicio.

- 4.7. Alcance:** Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información - SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.
- 4.8. Alerta:** Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.
- 4.9. Amenaza:** Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
- 4.10. Análisis de riesgos:** Según [ISO/IEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo.
- 4.11. Auditabilidad:** Los activos de información deben tener controles que permitan su revisión. Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.
- 4.12. Auditor:** Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.
- 4.13. Auditoria:** Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



- 4.14. Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
- 4.15. Autenticidad:** Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.
- 4.16. Base de datos de gestión de configuraciones (CMDB, Configuration Management Database):** Es una base de datos que contiene toda la información pertinente acerca de los componentes del sistema de información utilizado en una organización de servicios de TI y las relaciones entre esos componentes. Una CMDB ofrece una vista organizada de los datos y una forma de examinar los datos desde cualquier perspectiva que desee. En este contexto, los componentes de un sistema de información se conocen como elementos de configuración (CI). Un CI puede ser cualquier elemento imaginable de TI, incluyendo software, hardware, documentación y personal, así como cualquier combinación de ellos. Los procesos de gestión de la configuración tratan de especificar, controlar y realizar seguimiento de elementos de configuración y los cambios introducidos en ellos de manera integral y sistemática.
- 4.17. BS7799:** Estándar británico de seguridad de la información, publicado por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera es un conjunto de buenas prácticas para la gestión de la seguridad de la información –no es certificable- y la parte segunda especifica el sistema de gestión de seguridad de la información –es certificable- Asimismo la parte primera es el origen de ISO 17799 e ISO 27002 Y la parte segunda de ISO 27001. Como tal el estándar, ha sido derogado ya, por la aparición de estos últimos.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



- 4.18. Características de la Información:** las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.
- 4.19. Checklist o lista de Chequeo:** Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo, Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.
- 4.20. CobiT - Control Objectives for Information and related Technology – (Objetivos de Control para la información y Tecnologías Relacionadas):** Publicados y mantenidos por ISACA, sus siglas en inglés (Information System Audit And Control Association) – Asociación de Auditoría y Control de Sistemas de Información Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.
- 4.21. Compromiso de la Dirección:** Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - Sistema de Gestión de la Seguridad de la Información.
- 4.22. Computo forense:** El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.
- 4.23. Confiabilidad:** Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

- 4.24. Confidencialidad:** Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC13335-1:2004]: "característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.
- 4.25. Control:** Son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).
- 4.26. Control correctivo:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.
- 4.27. Control detectivo:** Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
- 4.28. Control disuasorio:** Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos disuasorios.
- 4.29. Control preventivo:** Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.
- 4.30. Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.
- 4.31. Denegación de servicios:** Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes. Un aspecto a resaltar es el gran daño a la imagen y reputación de las entidades que estas acciones dejan en el ambiente público.

- 4.32. Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.
- 4.33. Directiva:** Según [ISO/IEC 13335-1: 2004]: una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.
- 4.34. Disponibilidad:** Según [ISO/IEC 13335-1: 2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.
- 4.35. Evaluación de riesgos:** Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.
- 4.36. Evento:** Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.
- 4.37. Evidencia objetiva:** Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.
- 4.38. Gestión de claves:** Controles referidos a la gestión de claves criptográficas.
- 4.39. Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

- 4.40. Gusano (Worm):** Es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo de ancho de banda y su gran facilidad para mutar.
- 4.41. Impacto:** Resultado de un incidente de seguridad de la información.
- 4.42. Incidente:** Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- 4.43. Información:** La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.
- 4.44. Ingeniería Social:** Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la entidad o faciliten información con clasificación confidencial o superior. En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad de medios para llevar a cabo esta actividad, un uso común es a través de correos electrónicos o llamadas al lugar de trabajo o residencia, de ahí la



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



importancia de tener una buena cultura digital respecto a que información suministramos.

- 4.45. Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.
- 4.46. Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
- 4.47. IPS:** Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.
- 4.48. ISO:** Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.
- 4.49. ISO 17799:** Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS 7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de julio de 2007. No es certificable.
- 4.50. ISO 19011:** "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.
- 4.51. ISO 27001:** Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.
- 4.52. ISO 27002:** Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio





DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



oficial de nomenclatura de ISO 17799:20005 a ISO 27002:20005 el 1 de julio de 2007.

- 4.53. ISO 9000:** Normas de gestión y garantía de calidad definidas por la ISO.
- 4.54. ISO/IEC TR 13335-3:** "Information technology. Guidelines for the management of IT Security .Techniques for the management of IT Security." Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.
- 4.55. ISO/IEC TR 18044:** "Information technology. Security techniques. Information security incident management". Guía de utilidad para la gestión de incidentes de seguridad de la información.
- 4.56. ITIL IT Infrastructure Library:** Un marco de gestión de los servicios de tecnologías de la información.
- 4.57. Keyloggers:** Son software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario; es común relacionar este termino con malware del tipo daemon (demonio), es decir, actúa como un proceso informático que no interactúa con el usuario, ya que se ejecuta en segundo plano. Usualmente puede ser un tipo de software o un dispositivo hardware que se encarga de registrar las pulsaciones que se hacen con el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.
- 4.58. Legalidad:** El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.
- 4.59. Magerit:** Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica. Actualizada en 2012 en su versión 3





DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



- 4.60. No conformidad:** Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.
- 4.61. No conformidad grave o mayor:** Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.
- 4.62. No repudio:** Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.
- 4.63. PDCA Plan-Do-Check-Act:** Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).
- 4.64. Phishing:** Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.
- 4.65. Plan de continuidad del negocio (Business Continuity Plan):** Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que ponga en peligro el funcionamiento de este.
- 4.66. Plan de tratamiento de riesgos (Risk treatment plan):** Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



- 4.67. Política de seguridad:** Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:20005]: intención y dirección general expresada formalmente por la Dirección.
- 4.68. Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.
- 4.69. Riesgo Residual:** Según [ISO/IEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.
- 4.70. Salvaguarda:** Véase: Control.
- 4.71. Segregación de tareas:** Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.
- 4.72. Seguridad de la información:** Según [ISO/IEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.
- 4.73. SGSI Sistema de Gestión de la Seguridad de la Información:** Según [ISO/IEC 27001: 20005]: es un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)
- 4.74. Spamming:** Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



- 4.75. **Sniffers:** Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.
- 4.76. **Spoofing:** Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.
- 4.77. **Tratamiento de riesgos:** Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.
- 4.78. **Troyano:** Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.
- 4.79. **Valoración de riesgos:** Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.
- 4.80. **Virus:** Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tarda tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.
- 4.81. **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.



## **5. DIAGNÓSTICO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LOS DOMINIOS DE ISO 27001 E ISO 27002**

El diagnóstico que se va a realizar va a estar basado en las Normas internacionales ISO 27001 e ISO 27002, los cuales no se van a abarcar en un 100% solo los aspectos más relevantes de estas.

### **5.1. POLÍTICAS DE SEGURIDAD – ADMINISTRATIVA.**

Se verifican las Políticas de seguridad de la Información aprobadas según decreto 163 del 15 de agosto de 2013 en el cual se definen los objetivos, el alcance y se encuentra alineada con la estrategia y objetivos de la entidad, pero esta no ha sido revisada, ni actualizada, no hay evidencias de la socialización al interior de la entidad, ni la implementación de esta.

Hay un Manual de Políticas de Seguridad de la Información Actualizado el cual no está aprobado, este contiene la política General de Seguridad y Privacidad de la Información, define que es seguridad de la información, con los conceptos asociados a esta, La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos. Este documento es un compendio de todas las políticas que tienen que ver con la seguridad de la información en todas las áreas y niveles.

No hay responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas.

**CUMPLE PARCIALMENTE:** Aunque se tiene el Manual de Políticas de Seguridad de la Información actualizado, este aún no está aprobado y por lo tanto no hay implementación de las políticas al interior de la entidad.

Se obtiene una calificación sobre esta actividad de: **20**.

## **6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN – ADMINISTRATIVA.**

- a) No han sido establecidos roles y responsabilidades frente a la ciberseguridad, de estos no hay evidencia, sino de pequeñas responsabilidades establecidas dentro de este rol, además no están claros los roles y responsabilidades para la detección de incidentes.



**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARÍA GENERAL**



- b) No hay un comité de gestión institucional, se revisan algunos temas de seguridad, aprobado por la alta Dirección.
- c) No hay implementado un SGSI.
- d) No hay procedimientos establecidos que especifiquen cuándo, cuáles y a través de que se deberían contactar a las autoridades. Se han reportado algunos eventos o incidentes de Seguridad de la Información de forma aislada.
- e) La entidad no integra la seguridad de la información en el ciclo de vida de los proyectos, por lo tanto, no asegura que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto.
- f) Aunque existen políticas y controles para el uso, de dispositivo móviles estas no son muy fuertes para proteger la información almacenada o procesada en estos dispositivos y el acceso a servicios de TI desde los mismos.
- g) Existe una política de dispositivos móviles la cual no está implementada esta no permite el uso de dispositivos móviles de propiedad personal, la política y las medidas de seguridad relacionadas no se han tenido en cuenta las siguientes políticas:
  - ✓ La separación entre el uso privado y de la Entidad de los dispositivos, incluido el uso del software para apoyar esta separación y proteger los datos del negocio en un dispositivo privado;
  - ✓ Brindar acceso a la información de la Entidad solo cuando los usuarios hayan firmado un acuerdo de usuario final, en el que se reconocen sus deberes (protección física, actualización del software, etc.), desistir de la propiedad de los datos de la Entidad, permitir el borrado remoto de datos por parte de la organización en caso de robo o pérdida del dispositivo, o cuando ya no se posee autorización para usar el servicio.
- h) Existen algunos controles muy básicos que no evitan en un 100% que una persona pueda acceder, modificar o usar activos sin autorización ni detección. No hay mejores prácticas implementadas donde por ejemplo separar eventos de su autorización (solo en algunos casos).



**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARÍA GENERAL**



**PRÁCTICAS QUE SE SUGIEREN:**

1. Solicitar apoyo suficiente de la alta dirección para el SGSI, esto se ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o incidentes.
2. Definir claramente los roles y responsabilidades, asignados a personal con las competencias requeridas para este fin.
3. Identificar los responsables y responsabilidades para la protección de los activos.
4. Definir las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales.
5. Definir y documentar los niveles de autorización.
6. Se debe contar con un presupuesto formalmente asignado a las actividades del SGSI (por ejemplo, campañas de sensibilización en seguridad de la información).
7. Los objetivos de la seguridad de la información se deben incluir en los objetivos del proyecto.
8. La valoración de los riesgos de seguridad de la información se debe llevar a cabo en una etapa temprana del proyecto, para identificar los controles necesarios.
9. La seguridad de la información debe ser parte de todas las fases de la metodología del proyecto aplicada.
10. Debe haber un registro de los dispositivos móviles.
11. Debe haber requisitos básicos para la protección física.
12. Restricciones para la instalación de software.
13. Los requisitos para las versiones de software de dispositivos móviles y para aplicar parches.
14. Restricción de la conexión a servicios de información.
15. Controles de acceso.
16. Manejo de técnicas criptográficas.
17. Protección contra software malicioso.
18. Deshabilitación remota, borrado o cierre.
19. Administración de Copias de respaldo.
20. Uso de servicios y aplicaciones web.
21. Al diseñar los controles se debería considerar la posibilidad de confabulación. Hay que tener en cuenta la separación de deberes y/o controles compensatorios como revisión periódica de los rastros de auditoría y la supervisión de cargos superiores.



## **7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS – ADMINISTRATIVA.**

### **7.1. Antes de Asumir el empleo:**

#### **7.1.1. Selección e investigación de antecedentes:**

Las verificaciones de los antecedentes de todos los candidatos a un empleo, se lleva a cabo en etapas no previas, esta se hace después de la contratación, pero acuerdo con las leyes, no hay evidencia de la verificación de las referencias. En el caso de los contratistas estos no se manejan por la Subsecretaría de talento humano si no por medio de cada secretaria que contrata y la oficina jurídica.

Se realiza auditoria tipo preguntas a funcionario que apoya el proceso de vinculación y se detentaron algunas situaciones para analizar:

- ✓ No se verifican las referencias, ni las certificaciones laborales.
- ✓ Se verifican certificaciones académicas posterior a la contratación.
- ✓ Se verifican los antecedentes penales por medio de herramientas dispuestas para esto.
- ✓ No se realiza un proceso de selección para contratistas.
- ✓ La información de los candidatos que se consideran para cargos dentro de la organización, no se recolectan y manejan apropiadamente de acuerdo con la ley de protección de datos personales.

### **7.2. Durante la Ejecución del Empleo:**

#### **7.2.1. Responsabilidades de la Dirección:**

La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización, pero aún no hay implementados procedimientos ni políticas relativas a la seguridad, salvo algunos procedimientos.

Los contratistas y empleados no están coordinados y alineados con los roles y responsabilidades de seguridad de la información, como los definen las NIST.

- ✓ Los funcionarios no están debidamente informados sobre sus roles y responsabilidades de seguridad de la información, antes de que se les





DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



otorgue el acceso a información o sistemas de información confidenciales.

- ✓ Los funcionarios no tienen un nivel de toma de conciencia sobre seguridad de la información pertinente a sus roles y responsabilidades dentro de la organización.
- ✓ No hay capacitaciones continuas en el tema de seguridad de la información para los empleados o contratistas.
- ✓ Los funcionarios no cuentan con un canal para reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad de la información (“denuncias internas”).

*7.2.2. Toma de Conciencia, Educación y Formación en la Seguridad de la Información:*

Los empleados de la Entidad y los contratistas (donde sea pertinente), no reciben la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas de seguridad de la información y procedimientos pertinentes para su cargo enfocados en esta.

No se evidencia la toma de conciencia en seguridad de la información en funcionarios y contratistas, alineado con las responsabilidades, políticas y procedimientos existentes en la Entidad.

*7.2.3. Proceso Disciplinario:*

Se cuenta con una oficina de control interno disciplinario, la cual lleva los procesos de acuerdo a la norma, pero aún no hay implicados por violación a los principios y políticas de la Seguridad de la Información.

*7.3. Terminación de Contrato o Traslado de Funcionario:*

No hay acuerdos de confidencialidad, que persistan por un tiempo después de terminada la relación laboral o contrato.





## **8. GESTIÓN DE ACTIVOS – ADMINISTRATIVA.**

### **8.1. Responsabilidad de los Activos:**

No hay definida una identificación de los activos organizacionales adecuada y no hay una definición las responsabilidades de protección apropiadas para cada uno de los activos.

#### **8.1.1. Responsabilidad de los Activos:**

En la alcaldía de Apartadó solo se tiene el inventario de bienes muebles e inmuebles, aunque se lleva en una aplicativo antiguo, que dificulta la administración de estos.

No se han identificado los activos asociados con la información y las instalaciones de procesamiento de información, por lo tanto, no hay un inventario de estos activos específicamente.

De acuerdo a NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos.

No se han identificado, documentado e implementado reglas para el uso aceptable de la información y de activos asociados con información e instalaciones de procesamiento de información.

### **8.2. Clasificación de información:**

No se asegura que la información recibe un nivel apropiado de protección, de acuerdo con su importancia porque la entidad la protege toda de igual forma.

La administración de la información no es la más viable ya que está se encuentra administrada de manera manual y algunos en archivos de Excel no se tienen analizados temas de etiquetas ni metadatos de activos en formatos físicos y electrónicos.

Se evidencia:

- ✓ Pocas restricciones de acceso a los centros de datos y almacenamiento de la información.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



- ✓ Poca protección de copias de seguridad y el marcado para búsqueda es muy manual.
- ✓ Los centros de datos no cuentan con ningún sistema de conservación de la información.
- ✓ Poca protección a la información en uso, en tránsito o en almacenamiento definitivo.

## **9. CONTROL DE ACCESO –TECNICA.**

### **9.1. Requisitos del Negocio para Control de Acceso:**

Se posee pocas o nulas restricciones de seguridad en el acceso a información y a las instalaciones de procesamiento de esta.

#### **9.1.1. Política de Control de Acceso:**

Se encuentra establecida y documentada una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

Pero la política no está implementada y además carece del siguiente contenido de manera clara:

- ✓ Los requisitos de seguridad para las aplicaciones del negocio.
- ✓ Las políticas para la divulgación y autorización de la información, y los niveles de seguridad de la información y de clasificación de la información.
- ✓ La coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes.
- ✓ La legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios.
- ✓ La gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles.
- ✓ La separación de los roles de control de acceso, (solicitud de acceso, autorización de acceso, administración del acceso).
- ✓ Los requisitos para la autorización formal de las solicitudes de acceso.
- ✓ Los requisitos para la revisión periódica de los derechos de acceso.
- ✓ El retiro de los derechos de acceso.
- ✓ El ingreso de los registros de todos los eventos significativos concernientes al uso y gestión de identificación de los usuarios, e información de autenticación secreta, en el archivo permanente.



- ✓ Los roles de acceso privilegiado.

#### *9.1.2. Acceso a Redes y a Servicios en Red:*

En la configuración actual de la red se permite el acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente pero no algunas situaciones en lo cual no se ha cumplido en un 100% las cuales son:

Revisar relacionada con el uso de redes y de servicios de red y verificar que incluya:

- ✓ La política no incluye específicamente las redes y servicios de red a los que se permite el acceso.
- ✓ No existen procedimientos de autorización para determinar a quién se permite el acceso a qué redes y a que servicios de red.
- ✓ La protección al acceso a las conexiones de red y a los servicios de red físicos no tienen ninguna seguridad y es muy fácil acceder a estos.
- ✓ Las redes inalámbricas, en algunos casos presentan falencias en la configuración de estas, como por ejemplo claves WEP o WPA.
- ✓ No hay un seguimiento al uso de servicios de red o a la información utilizada.

#### *9.2. Gestión de Acceso de Usuarios:*

Se asegura el acceso de los usuarios autorizados, pero no hay políticas muy fuertes que permitan mitigar o evitar el acceso no autorizado a sistemas y servicios.

##### *9.2.1. Registro y Cancelación del Registro de Usuarios:*

No hay Implementado un proceso formal de registro y de cancelación de registro de usuarios.

En la gestión y la identificación de los usuarios se comenten varios errores los cuales son:

- ✓ No hay Identificaciones únicas para los usuarios esto se debe a que se evidencia el uso de un mismo usuario para varios empleados o usuarios genéricos como practicantes o contratistas, esto no permite que se pueda



**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARÍA GENERAL**



vincular un usuario a sus acciones y mantener la responsabilidad por ellas.

- ✓ No se deshabilitan o retiran inmediatamente las identificaciones de los usuarios que han dejado la entidad, todavía hay usuarios activos de empleados que han dejado la entidad desde hace varios años.

#### *9.2.2. Suministro de Acceso de Usuarios:*

No hay implementado un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todos los sistemas y servicios por lo cual no se cuenta con:

- ✓ Autorización del propietario del sistema de información o del servicio para el uso del sistema de información o servicio.
- ✓ Verificación que el nivel de acceso otorgado es apropiado a las políticas de acceso y es coherente con otros requisitos, tales como separación de deberes.
- ✓ Conservación de un registro central de los derechos de acceso suministrados a una identificación de usuario para acceder a sistemas de información y servicios.
- ✓ Adaptación de los derechos de acceso de usuarios que han cambiado de roles o de empleo, y retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han dejado la organización.
- ✓ Revisión periódicamente los derechos de acceso con los propietarios de los sistemas de información o servicios.

#### *9.2.3. Gestión de Derechos de Acceso Privilegiado:*

Se restringe, pero no se controlar la asignación y uso de derechos de acceso privilegiado, no existe un proceso de autorización formal de acuerdo con la política de control de acceso, por lo tanto, no cuenta con:

- ✓ Identificación los derechos de acceso privilegiado asociados con cada sistema o proceso, (sistema operativo, sistema de gestión de bases de datos, y cada aplicación) y los usuarios a los que es necesario asignar.
- ✓ Definición o establecimiento de los derechos de acceso privilegiado a usuarios con base en la necesidad de uso y caso por caso, alineada con la política de control de acceso.
- ✓ Conservación de un proceso de autorización y un registro de todos los privilegios asignados.



**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARÍA GENERAL**



- ✓ Definición de los requisitos para la expiración de los derechos de acceso privilegiado.

#### *9.2.4. Gestión de Información de Autenticación Secreta de Usuarios:*

La asignación de información de autenticación secreta no se controla por medio de un proceso formal, este proceso debería incluir:

- ✓ Establecimiento de la firma de una declaración para mantener confidencial la información de autenticación secreta personal, y mantener la información de autenticación secreta del grupo (cuando es compartida) únicamente dentro de los miembros del grupo; esta declaración firmada se puede incluir en los términos y condiciones del empleo.
- ✓ Establecimiento que todos los usuarios deben mantener su propia información de autenticación secreta, y se les suministra una autenticación secreta temporal segura, que se obligue a cambiar al usarla por primera vez (Esto se encuentra establecido en un alto porcentaje).
- ✓ Definición de la información de autenticación secreta temporal se debe suministrar a los usuarios de una manera segura.
- ✓ Definición de la información de autenticación secreta temporal es única para un individuo y no es fácil de adivinar.
- ✓ Que la información de autenticación secreta por defecto, del fabricante, se modifica después de la instalación de los sistemas o software.

#### *9.2.5. Revisión de los Derechos de Acceso de Usuarios:*

No se revisan los derechos de acceso de los usuarios. Estos deberían incluir:

- ✓ Revisión de los derechos de acceso de los usuarios periódicamente y después de cualquier cambio o terminación del empleo.
- ✓ Establecimiento de que los derechos de acceso de usuario se revisan y reasignan cuando pasan de un rol a otro dentro de la misma organización.
- ✓ Verificación de las asignaciones de privilegios periódicamente, para asegurar que no se hayan obtenido privilegios no autorizados.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



*9.2.6. Retiro o Ajuste de los Derechos de Acceso:*

Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información no se retiran al terminar su empleo, contrato o acuerdo, y no se ajustan cuando hay cambios.

*9.3. Responsabilidades de los Usuarios:*

No está establecido que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.

*9.3.1. Uso de Información de Autenticación Secreta:*

No hay una exigencia a los usuarios que cumplan con las prácticas de la entidad para el uso de información de autenticación secreta.

No existe proceso o procedimiento de notificación de autenticación secreta a los usuarios y por lo tanto no se tiene en cuenta lo siguiente:

- ✓ Mantener la confidencialidad de la información de autenticación secreta, asegurándose de que no sea divulgada a ninguna otra parte.
- ✓ En algunos casos se llevan registros en papel, en un archivo de software o en dispositivo portátil de la autenticación secreta, además este no se almacena de forma segura.
- ✓ Toma de conciencia frente al cambio de la información de autenticación secreta, cuando haya cualquier indicio de que se pueda comprometer la información.
- ✓ Toma de conciencia frente a la definición de contraseñas como información de autenticación secreta, las cuales deben tener como mínimo:
  - Longitud mínima suficiente.
  - ser fáciles de recordar.
  - Estar basadas en algo que otra persona no pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.);



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



- Que no sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios).
  - Que estén libres de caracteres completamente numéricos o alfabéticos idénticos consecutivos.
  - Si son temporales, cambiarlos la primera vez que se ingrese.
- 
- ✓ No compartir información de autenticación secreta del usuario individual.
  - ✓ No usar la misma información de autenticación secreta para propósitos de negocio y otros diferentes de estos.

#### *9.4. Control de Acceso a Sistemas y Aplicaciones:*

Hay algunas medidas que evitan el acceso no autorizado a sistemas y aplicaciones, pero estas son a consideración del desarrollador y/o encargados de la administración de la infraestructura de sistemas.

##### *9.4.1. Restricción de Acceso a la Información:*

El acceso a la información y a las funciones de los sistemas de las aplicaciones se restringe, pero no de acuerdo con la política de control de acceso definida o algún procedimiento, no hay documentación respecto a esta que incluya mínimamente:

- ✓ Suministro de menús para controlar el acceso a las funciones de sistemas de aplicaciones.
- ✓ Controlar a qué datos puede tener acceso un usuario particular.
- ✓ Controlar los derechos de acceso de los usuarios, (a leer, escribir, borrar y ejecutar).
- ✓ Controlar los derechos de acceso de otras aplicaciones.
- ✓ Limitar la información contenida en los elementos de salida.
- ✓ Proveer controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos.

##### *9.4.2. Procedimiento de Ingreso Seguro:*

La política de control de acceso no requiere, que el acceso a sistemas y aplicaciones se deban controlar mediante un proceso de ingreso seguro, pero



**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARÍA GENERAL**



sin embargo esta es una buena práctica que debería ser implementada por lo menos en parte la cual debe incluir en el procedimiento de ingreso:

- ✓ No visualizar los identificadores del sistema o de la aplicación sino hasta que el proceso de ingreso se haya completado exitosamente.
- ✓ Visualización una advertencia general acerca de que sólo los usuarios autorizados pueden acceder al computador o aplicación.
- ✓ Evitar los mensajes de ayuda durante el procedimiento de ingreso, que ayudarían a un usuario no autorizado.
- ✓ Validación de la información de ingreso solamente al completar todos los datos de entrada. ante una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta.
- ✓ Protección contra intentos de ingreso mediante fuerza bruta.
- ✓ Llevar un registro con los intentos exitosos y fallidos.
- ✓ Declaración de un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de ingreso.
- ✓ Visualización de la siguiente información al terminar un ingreso seguro:
  - Registro de la fecha y la hora del ingreso previo exitoso.
  - Registro de los detalles de cualquier intento de ingreso no exitoso desde el último ingreso exitoso.
- ✓ No transmisión de contraseñas en texto claro en la red.
- ✓ Terminación de sesiones inactivas después de un período de inactividad definido, especialmente en lugares de alto riesgo tales como áreas públicas o externas por fuera de la gestión de seguridad de la organización o en dispositivos móviles.
- ✓ Restricciones de los tiempos de conexión para brindar seguridad adicional para aplicaciones de alto riesgo y para reducir la ventana de oportunidad para acceso no autorizado.

#### **9.4.3. Sistema de Gestión de Contraseñas:**

Los sistemas de gestión de contraseñas de la entidad no aseguran la calidad de las contraseñas definidas, estos deberían de incluir:

- ✓ Cumplimiento del uso de identificaciones y contraseñas de usuarios individuales para mantener la rendición de cuentas.
- ✓ Permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluyan un procedimiento de confirmación para impedir los errores de entrada.
- ✓ Exigir que se escojan contraseñas de calidad.





**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARÍA GENERAL**



- ✓ Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez.
- ✓ Exigir que se cambien las contraseñas en forma regular, según sea necesario.
- ✓ Llevar un registro de las contraseñas usadas previamente, e impedir su reusó.
- ✓ No visualizar contraseñas en la pantalla cuando se está ingresando.
- ✓ Almacenar y transmitir las contraseñas en forma protegida.

**9.4.4. *Uso de Programas Utilitarios:***

No hay una restricción y controles estrictos con el uso de programas utilitarios. Las directrices a estos programas deben incluir:

- ✓ Separación de los programas utilitarios del software de aplicaciones.
- ✓ Limitación el uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados.
- ✓ Autorización el uso adhoc de programas utilitarios.
- ✓ Limitación de la disponibilidad de los programas utilitarios.
- ✓ Registro del uso de los programas utilitarios.
- ✓ Retirar o deshabilitar todos los programas utilitarios innecesarios.

**9.4.5. *Control de Acceso a Códigos Fuente de Programas:***

Se debe restringir el acceso a los códigos fuente de los programas. el procedimiento debe incluir:

- ✓ Definir que la actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los programadores sólo se deben hacer una vez que se haya recibido autorización apropiada.
- ✓ Establecer que los listados de programas se deben mantener en un entorno seguro.
- ✓ Conservar un registro de auditoría de todos los accesos a la librería de fuentes de programas.
- ✓ Mantener y copiar las bibliotecas de fuentes de programas a través de procedimientos estrictos de control de cambios.



## **10. CRIPTOGRAFÍA –TECNICA.**

Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización. Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles.

### **10.1. Controles Criptográficos:**

No se asegura el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

No existe ningún tipo de controles criptográficos que se encuentre documentado.

#### **10.1.1. Política Sobre el Uso de Controles Criptográficos:**

No hay una política sobre el uso de controles criptográficos para la protección de la información:

- ✓ No hay un establecimiento del enfoque de la dirección con relación al uso de controles criptográficos en toda la organización.
- ✓ No existe una valoración de riesgos, que identifique el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido.
- ✓ No se Gestionar las llaves ni certificados criptográficos y los métodos para la protección de llaves criptográficas y la recuperación de información encriptada.
  - No hay establecido roles y responsabilidades de la implementación de la política, ni la gestión de llaves, ni de certificados digitales.

#### **10.1.2. Gestión de llaves:**

No hay implementada una política sobre el uso, protección y tiempo de vida de las llaves criptográficas.



## **11. SEGURIDAD FÍSICA Y DEL ENTORNO –TECNICA.**

### **11.1. Áreas Seguras:**

La prevención al acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización, no es muy fuerte no se manejan fuertes protocolos de seguridad por parte de la entidad.

#### **11.1.1. Perímetro de Seguridad Física:**

No existen definidos perímetros de seguridad, por lo tanto, esta se maneja de igual forma para la protección de áreas que contengan información sensible o crítica, e instalaciones de manejo de información.

Dentro de las directrices relacionadas con los perímetros de seguridad física que no se encuentran implementadas tenemos las siguientes:

- ✓ No hay ninguna definición de los perímetros de seguridad, por lo tanto, no hay una fortaleza definida en cada uno de los perímetros definidos, la cual dependería de los resultados de la valoración de riesgos de los requisitos de seguridad de los activos de información.
- ✓ Las instalaciones de procesamiento de la información no son físicamente seguras; no está protegido adecuadamente contra acceso no autorizado, no existe ningún mecanismo de control solo cerradura sencilla.
- ✓ Existe un área de recepción con vigilancia para controlar el acceso físico al sitio o edificación; el acceso a los sitios y edificaciones no es muy seguro porque el público tiene acceso casi todo el edificio, la única protección en una cerradura.
- ✓ No hay barreras físicas para impedir el acceso físico no autorizado y la contaminación ambiental.
- ✓ No hay dispositivos de seguridad contra incendio puertas ni alarmas que permitan, monitorear un área, para establecer el nivel requerido de resistencia de acuerdo con normas regionales, nacionales e internacionales adecuadas.
- ✓ No hay instalado sistemas adecuados para detección de intrusos y/o alarmas de acuerdo con normas nacionales, regionales o internacionales, en las instalaciones donde se procesa información.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



**11.1.2. Controles Físicos de Entrada:**

Las áreas seguras están protegidas mediante controles de entrada no apropiados, esto para asegurar que solamente se permite el acceso a personal autorizado.

Se presentan los siguientes inconvenientes:

- ✓ No hay un registro de la fecha y hora de entrada y salida de los visitantes ni supervisión de estos, ni la emisión de instrucciones sobre los requisitos de seguridad del área.
- ✓ No hay establecido que el acceso a las áreas en las que se procesa o almacena información confidencial se debería restringir a los individuos autorizados solamente mediante la implementación de controles de acceso apropiados.
- ✓ No se puede realizar auditoría de todos los accesos, por no tener un registro donde se verifique los accesos.
- ✓ No hay posibilidades de realizar seguimiento a los visitantes de la Entidad por la apertura a la comunidad que posee esta.

**11.1.3. Seguridad de Oficinas, Recintos e Instalaciones:**

La seguridad física a oficinas, recintos e instalaciones, solo consta de una vigilancia a la entrada de la entidad.

Situaciones encontradas:

- ✓ Las instalaciones se encuentran ubicadas de cualquier manera, no se tiene en cuenta el procesamiento de la información.
- ✓ Fácil acceso del público a la mayoría de las oficinas.

**11.1.4. Protección Contra amenazas externas y ambientales:**

No existe una protección específica para la protección física contra desastres naturales, ataques maliciosos o accidentes.

No existe de Plan de Recuperación de Desastres (DRP).



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



**11.1.5. Trabajo en Áreas Seguras:**

No hay establecidas áreas de trabajo seguras.

**11.1.6. Áreas de Despacho y Carga:**

No existen, por lo tanto, no se controlan áreas de despacho ni de carga (el flujo de carga y descarga).

**11.2. Equipos:**

Dentro de la entidad no hay campañas y/o controles sobre la prevención de pérdida, daño, robo o compromiso de activos, y con esta situación la interrupción de las operaciones de la organización.

**11.2.1. Ubicación y Protección de los Equipos:**

Los equipos no se encuentran ubicados ni protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.

Dentro de estas tenemos:

- ✓ Los equipos no están ubicados de manera que se minimice el acceso innecesario a las áreas de trabajo por parte del público en general.
- ✓ No se ha definido que en las instalaciones de procesamiento de la información que manejan datos sensibles están ubicadas cuidadosamente para reducir el riesgo de que personas no autorizadas puedan ver la información durante su uso.
- ✓ Las instalaciones de almacenamiento no son seguras para evitar el acceso no autorizado.
- ✓ Los elementos que requieren protección especial no se salvaguardan de tal manera que permita aumentar el nivel de protección requerida, estos se salvaguardan como cualquier otro.
- ✓ Existen prácticamente controles nulos para minimizar el riesgo de amenazas físicas y ambientales como robo, incendio, explosivos, humo, agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones y vandalismo.
- ✓ No hay establecidas directrices acerca de comer, consumir líquidos y/o fumar en cercanías de las instalaciones de procesamiento de información.



**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARÍA GENERAL**



- ✓ No se realiza seguimiento a las condiciones ambientales tales como temperatura y humedad, por lo tanto no se pueden determinar las condiciones que puedan afectar adversamente las instalaciones de procesamiento de información.
- ✓ No hay ninguna protección especial a los equipos para procesamiento de información confidencial por lo tanto hay un riesgo de fuga de información.

**11.2.2. Servicios de Suministro:**

Un porcentaje muy pequeño de equipos se protege contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro eléctrico. Tampoco hay evidencia de una inspección y prueba regular al servicio eléctrico. No existen alarmas que permitan la detección de un mal funcionamiento.



Oficina de Sistemas





**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARÍA GENERAL**



Oficina de Sistemas



Oficina Gobierno



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



Oficina Planeación (Licencias)

Existen conexiones con riesgo las cuales no se encuentra debidamente instaladas ni protegidas. (Se toman algunas de ejemplo, porque la situación se repite en varias oficinas).

### 11.2.3. Seguridad del Cableado:

El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información, presenta muchos incumplimientos este no está protegido en su mayoría contra interceptación, interferencia o daño.

Se encuentran algunas situaciones:

- ✓ Los cables de potencia no se encuentran separados de los cables, presentando con esto posibles, fallas e interferencias de comunicaciones.
- ✓ No se encuentran definidos sistemas sensibles o críticos por lo tanto los controles adicionales que se deben considerar para estos no se tienen en cuenta, tampoco se ha realizado de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se conectan a los cables. No hay ninguna protección adicional de puntos de acceso físico a la red.





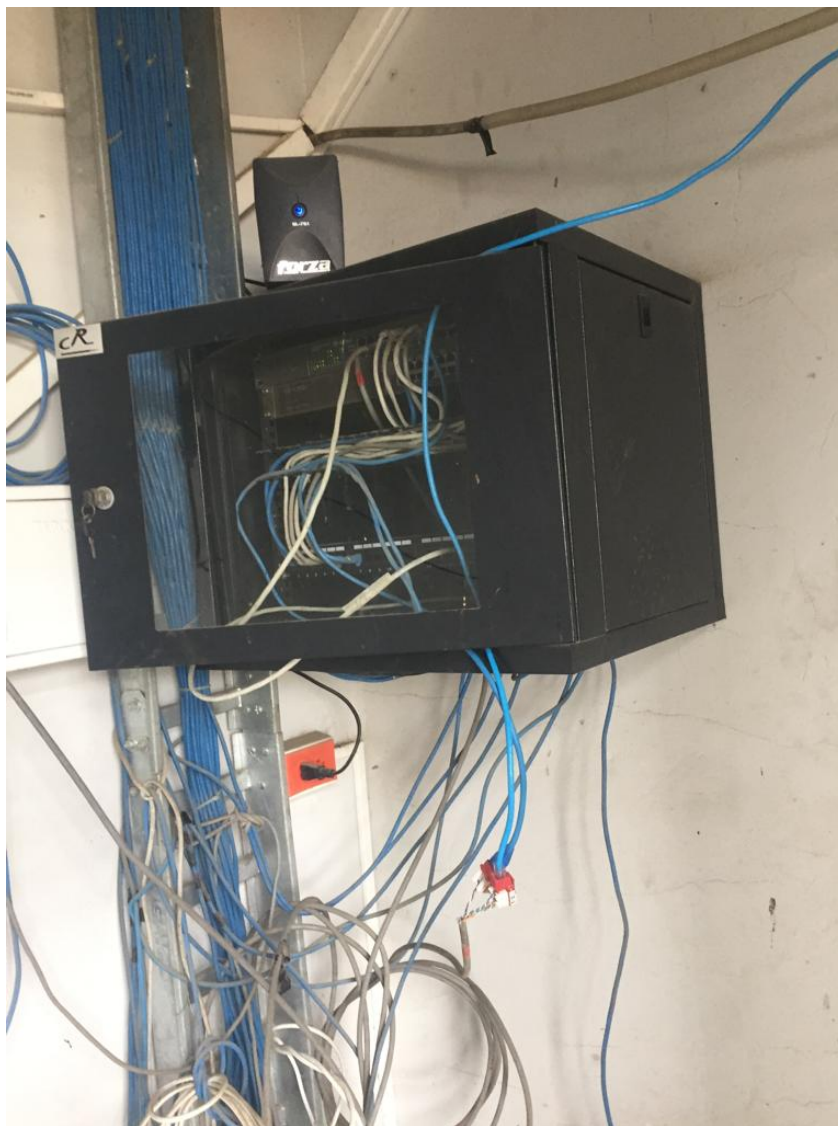
DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARIA GENERAL



Rack de Comunicaciones 1 piso Bloque A



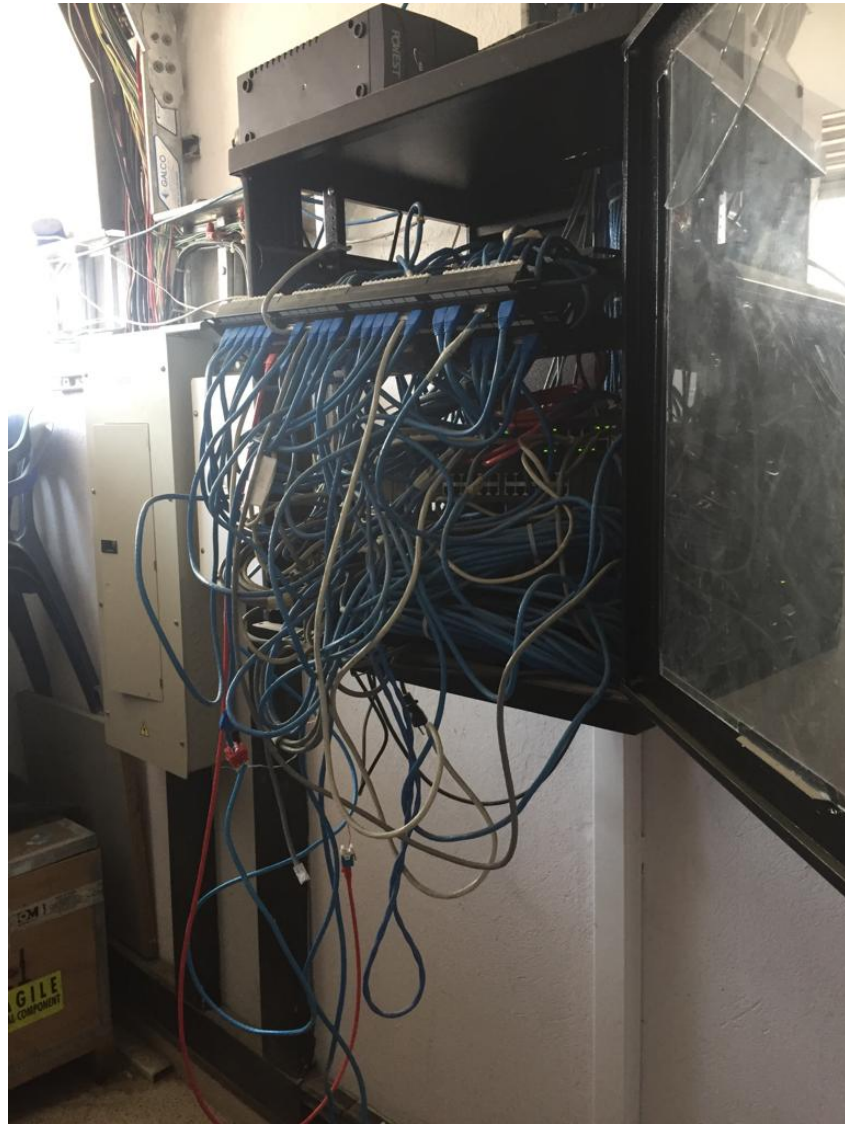
DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARIA GENERAL



RACK de Comunicaciones 2 Piso Bloque A



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL

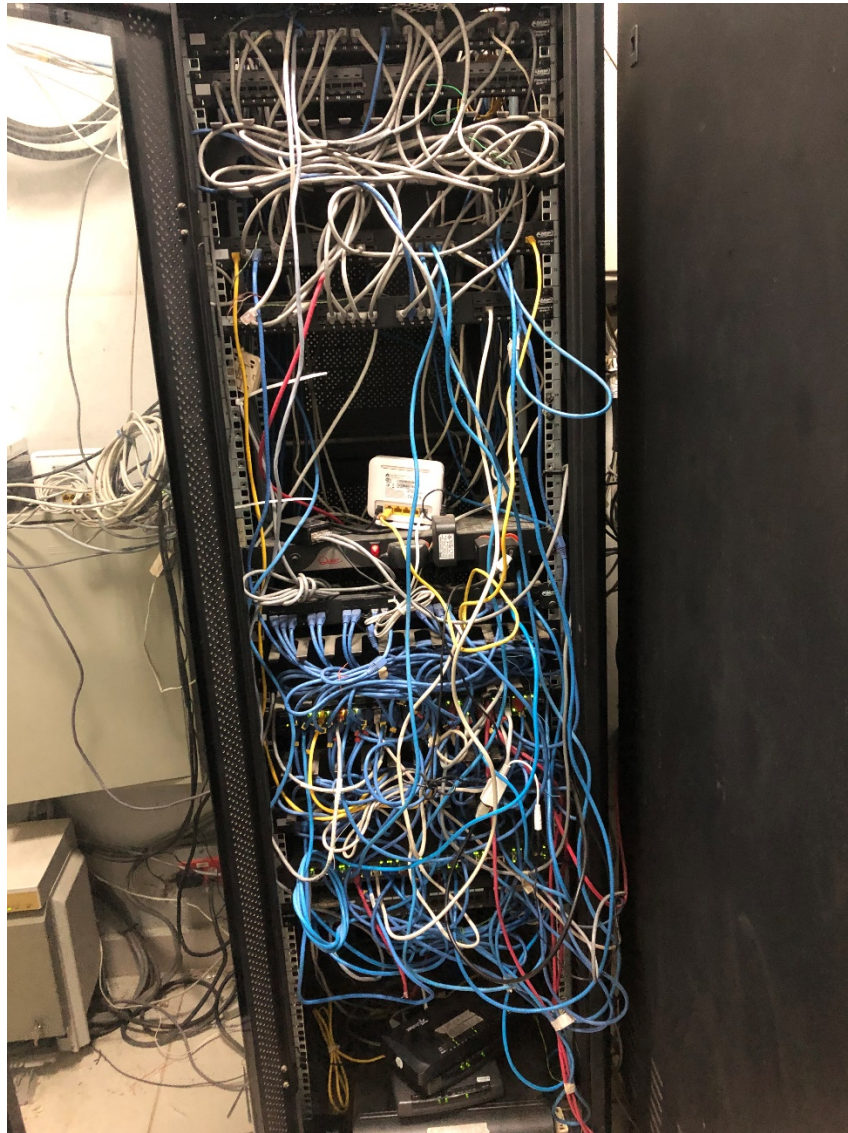


RACK de Comunicaciones 3 Piso bloque A





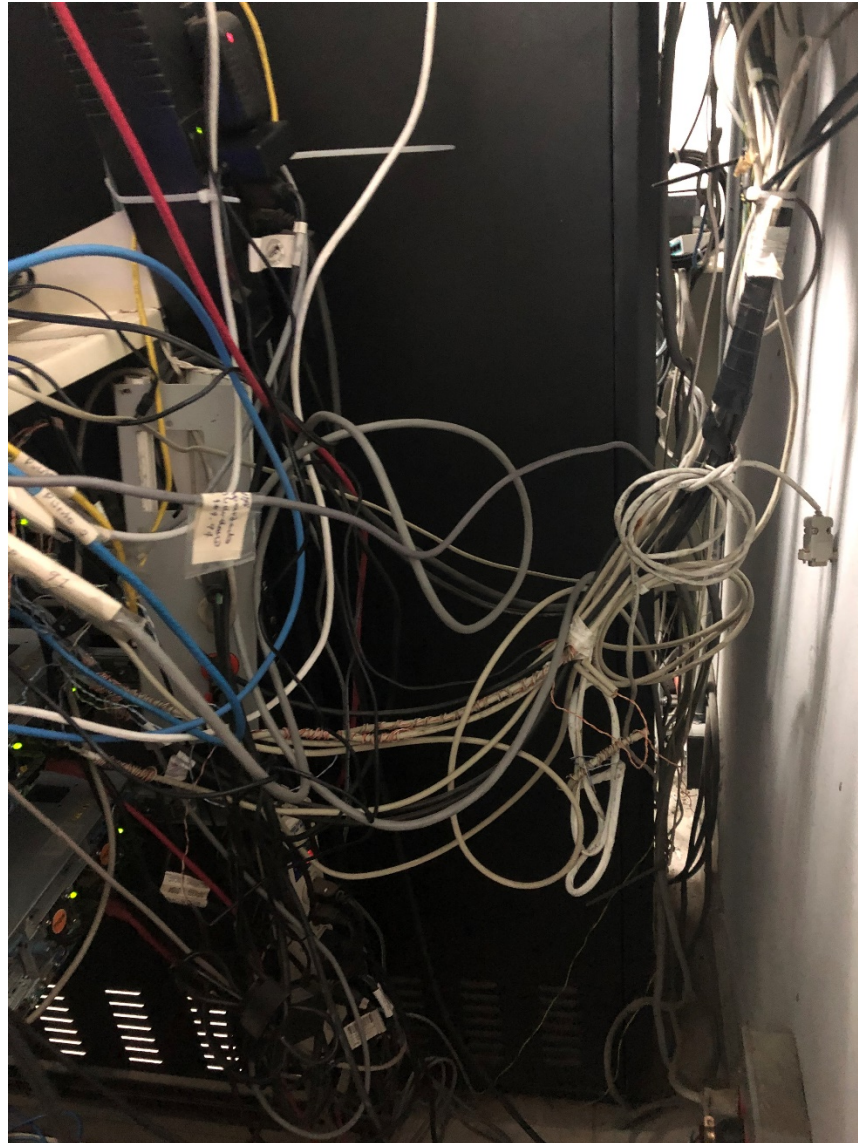
DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARIA GENERAL



RACK de Comunicaciones Principal 1 Piso Bloque B



**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARIA GENERAL**

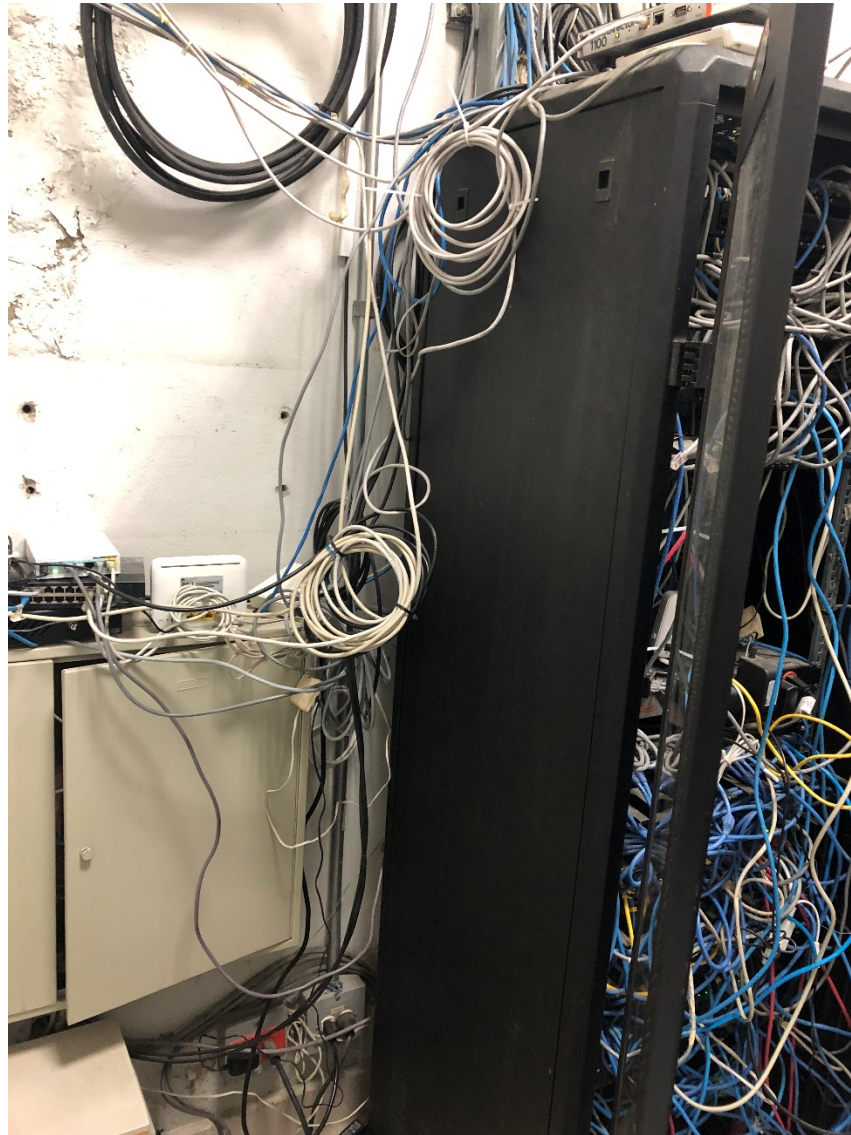


RACK de Comunicaciones Principal 1 Piso Bloque B





DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARIA GENERAL



RACK de Comunicaciones Principal 1 Piso Bloque B



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARIA GENERAL

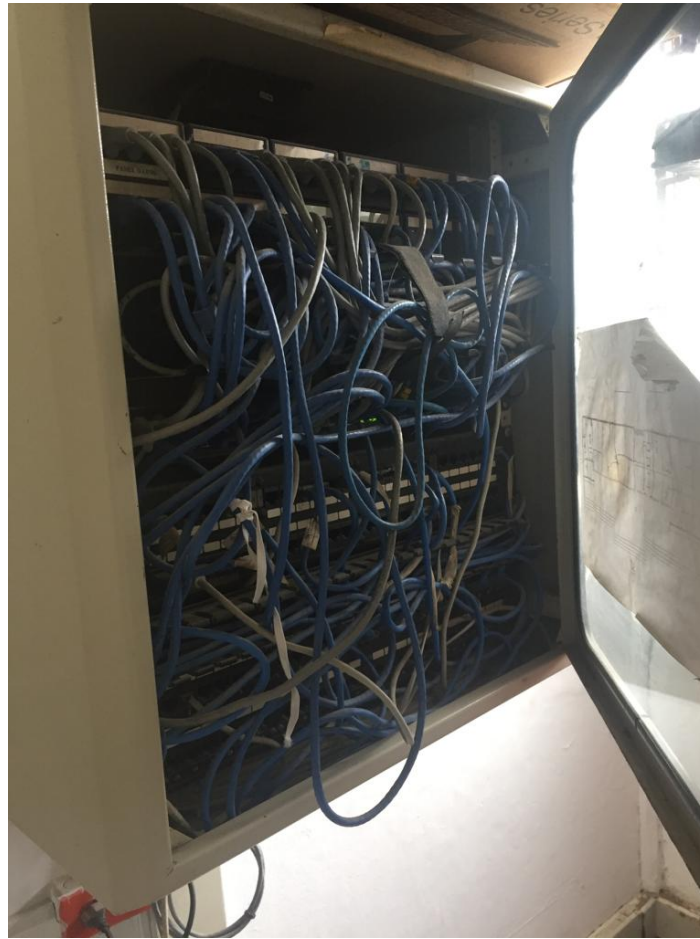


Rack de Comunicaciones 2 Piso Bloque B





**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARIA GENERAL**



Rack de Comunicaciones Bloque C

En todos los casos se nota falta de organización del cableado estructurado, generando un caos a la hora de la realización de mantenimientos preventivos o correctivos, no se encuentra una acción que a corto plazo solucione el problema.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



Oficina de Gobierno Swiches intermedios que degradan el servicio, generando inseguridad (Como este hay muchos más con este mismo inconveniente).

#### 11.2.4. *Mantenimiento de Equipos:*

No hay un plan de mantenimiento, el cual permita asegurar la realización de los mantenimientos de manera organizada. Se evidencia que se vienen realizando mantenimientos preventivos sin este.

Se detectan los siguientes inconvenientes:

- ✓ No hay intervalos especificados para el mantenimiento de los equipos, estos se realizan dependiendo de si hay o no presencia de personal practicante y presupuesto para la realización de este, esto afecta los intervalos los cuales son muy variados con lo cual hay más riesgos de fallas en los equipos.
- ✓ No está establecido ni comunicado que solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos.
- ✓ Llevar registros de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo.
- ✓ No se cumplen los procedimientos y las políticas implementadas en la entidad para la realización de los mantenimientos.
- ✓ Después de realizado el mantenimiento, no se realiza inspección para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



**11.2.5. Retiro de Activos:**

Los equipos, información o software se retiran de su sitio sin autorización previa, no hay comunicada una política o herramientas que controlen esta actividad.

**11.2.6. Seguridad de Equipos y Activos Fuera de las Instalaciones:**

No se aplican medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, no se tienen en cuenta los diferentes riesgos de trabajar fuera de las instalaciones.

No se han aplicado las siguientes directrices para proteger los equipos fuera de las instalaciones:

- ✓ Los equipos y medios retirados de las instalaciones no se deben dejar sin vigilancia en lugares públicos.
- ✓ No se controlan los lugares fuera de las instalaciones, tales como trabajo en la casa, teletrabajo y sitios temporales no se ha realizado una valoración de riesgos, por lo tanto, no se aplican controles adecuados a la situación de riesgo.

**11.2.7. Disposición Segura o Reutilización de Equipos:**

No se verifica que todos los elementos de equipos que contengan medios de almacenamiento, haya sido retirados o sobrescrito en forma segura antes de su disposición o reuso para asegurar que cualquier dato sensible o software con licencia no corre riesgo.

No se encuentra establecido ningún proceso de borrado, ni de encriptación de los discos.

**11.2.8. Equipos de Usuarios Desatendidos:**

No existe procedimiento o políticas para los equipos de usuarios desatendidos:

- ✓ Se encuentra establecido un tiempo muy alto de cierre de las sesiones activas mediante un protector de pantalla protegido con contraseña.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



- ✓ No se encuentra establecida la obligatoriedad de salir de las aplicaciones o servicios de red (incluyendo VPN) cuando ya no los necesiten.

**11.2.9. Política de Escritorio Limpio y Pantalla Limpia:**

Se encuentra adoptada una política de escritorio y pantalla limpia, pero no se encuentra implementada aún.

**12. SEGURIDAD DE LAS OPERACIONES –TECNICA.**

**12.1. Procedimientos Operacionales y Responsabilidades:**

No todas las operaciones son correctas y seguras de las instalaciones de procesamiento de información.

**12.1.1. Procedimientos de Operación Documentados:**

Se encuentran documentados algunos procedimientos de operación y se ponen a disposición de todos los funcionarios que los necesiten.

Las operaciones de la entidad no cuentan con instrucciones operacionales, en las que se definan:

- ✓ Poca documentación con información de instalaciones y configuraciones de los sistemas.
- ✓ Poca documentación con información de manejo de información, tanto automático como manual.
- ✓ Documentación no implementada de la gestión y/o administración de las copias de respaldo, a pesar que se realizan los backup, todos se guardan en la misma infraestructura, generando con esto, un alto riesgo en la pérdida de información y dificultades para la implementación de un Plan de Recuperación de Desastres (DRP).
- ✓ No se encuentran definidos los requisitos en temas de programación.
- ✓ No se encuentra establecida una base de datos que dé instrucciones para manejo de errores u otras condiciones excepcionales.
- ✓ No se tienen definidos los contactos de apoyo y de una instancia superior, incluidos los contactos de soporte externo, en el caso de dificultades operacionales o técnicas inesperadas.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



- ✓ No hay establecidas instrucciones sobre manejo de medios y elementos de salida.
- ✓ No hay documentación definida de reinicio y recuperación del sistema para uso en el caso de falla del sistema.
- ✓ No hay definida la gestión de la información de la auditoria y de información de los log del sistema.

#### 12.1.2. *Gestión de Cambios:*

No se evidencia una gestión de cambios en la entidad, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información.

No hay procedimientos de control de cambios, aplicados en la entidad:

- ✓ No se identifican y registrar los cambios significativos.
- ✓ No hay una planificación y ni puesta a prueba los cambios a realizar.
- ✓ No hay valoración de los impactos potenciales, incluidos los impactos de estos cambios en la seguridad de la información.
- ✓ No hay un procedimiento de la gestión de los cambios, que incluya: las responsabilidades para abortar cambios no exitosos y recuperarse de ellos, y eventos no previstos y suministro de cambio de emergencia que posibilite la implementación rápida y controlada de los cambios necesarios para resolver un incidente.
- ✓ No hay evidencia de la comunicación de todos los detalles de los cambios planeados a todas las personas pertinentes.

#### 12.1.3. *Gestión de Capacidad:*

No hay documentación que permita asegurar el desempeño requerido del sistema ni se hace seguimiento al uso de los recursos, ajustes, y proyecciones de los requisitos sobre la capacidad futura.

#### 12.1.4. *Separación de los Ambientes de Desarrollo, Pruebas y Operación:*

No se separan los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.

No existe documentación para la separación de ambientes, por lo tanto, no cuentan con:



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



- ✓ Definición y documentación de las reglas para la transferencia de software del estatus de desarrollo al de operaciones.
- ✓ Definición de los cambios en los sistemas operativos y aplicaciones se deben probar en un entorno de pruebas antes de aplicarlos a los sistemas operacionales.
- ✓ Definir que solo en circunstancias excepcionales, las pruebas no se deben llevar a cabo en los ambientes de prueba sino en los sistemas operacionales.
- ✓ Establecer que los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no deben ser accesibles desde sistemas operacionales cuando no se requiere.
- ✓ Definir que los datos sensibles no se deben copiar en el ambiente del sistema de pruebas, a menos que se suministren controles seguros para el sistema de pruebas.

## *12.2. Protección Contra Códigos Maliciosos:*

Protección contra códigos maliciosos de la información y por ende las instalaciones de procesamiento de información.

### *12.2.1. Controles Contra Códigos Maliciosos:*

No se encuentran implementados controles de detección, de prevención y de recuperación, tampoco existe una toma de conciencia apropiada de los usuarios, para proteger la entidad contra códigos maliciosos.

No se encuentran implementadas las siguientes directrices (Algunas están documentadas):

- ✓ Política que prohíba el uso de software no autorizado.
- ✓ Controles para evitar o detectar el uso de software no autorizado (listas blancas de aplicaciones).
- ✓ Controles para evitar o detectar el uso de sitios web maliciosos o que se sospecha que lo son (listas negras).
- ✓ Política para proteger contra riesgos asociados con la obtención de archivos y de software, indicando qué medidas externas se deben tomar.
- ✓ Realizar una gestión para el tratamiento de las vulnerabilidades de las que pueda aprovecharse el software malicioso.
- ✓ Llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que apoyan los procesos críticos del negocio.





DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



- ✓ Instalar y actualizar software de detección y reparación de software malicioso en los computadores y medios como una medida de control, en forma rutinaria; el análisis realizado debería incluir:
  - El análisis de cualquier archivo recibido por la red o por cualquier forma de medio de almacenamiento, para detectar el software malicioso, antes de uso.
  - El análisis de los adjuntos y descargas de los correos electrónicos, para determinación del software malicioso antes de uso y cuando se ingresa a la red de la organización; el análisis de páginas web, para determinar el software malicioso.
- ✓ Definir procedimientos y responsabilidades relacionadas con la protección contra el software malicioso en los sistemas, formación acerca del uso de dichos procedimientos, reporte y recuperación de ataques de software malicioso.
- ✓ Preparación de planes de continuidad del negocio apropiados, para la recuperación de ataques de software malicioso, incluidos todos los datos necesarios, copias de respaldo del software y disposiciones para recuperación.
- ✓ Implementar procedimientos para recolectar información en forma regular, (la suscripción a listas de correos o la verificación de sitios web que suministran información acerca de nuevo software malicioso).
- ✓ Listar entornos en donde se pueden obtener impactos catastróficos.

### 12.3. Copias de Respaldo:

Protección contra la pérdida de datos.

#### 12.3.1. Respaldo de la Información:

Se realizan copias de respaldo de la información, pero no del software ni de imágenes de los sistemas, pero no se ponen a prueba regularmente, hay políticas y procedimiento documentados que están acordes, pero no se han aprobado aún por lo tanto no están implementados.

Se revisan las siguientes directrices:

- ✓ Producir registros exactos y completos de las copias de respaldo, y procedimientos de restauración documentados.
- ✓ Está documentada la cobertura (copias de respaldo completas o diferenciales) y la frecuencia con la que se hacen las copias de respaldo, se encuentra implementada parcialmente.





**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARÍA GENERAL**



- ✓ Las copias de respaldo no almacenan en un lugar remoto, se encuentran almacenadas dentro de la misma entidad, generando con esto un alto riesgo catastrófico de pérdida de información.
- ✓ La información de respaldo no se tiene con un nivel apropiado de protección física y del entorno, no existe la aplicación de ninguna norma asociada.
- ✓ No se han definido los medios de respaldo que se deben poner a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso necesario.
- ✓ No se encuentra definida la información confidencial de las copias de respaldo, que deben estar protegidas por medio de encriptación.
- ✓ Existe un alto riesgo de pérdida de información porque no hay un Plan de Recuperación de Desastres (DRP).

#### *12.4. Registro y Seguimiento:*

Se registran muy pocos eventos y se registra muy poca evidencia de los cambios realizados.

##### *12.4.1. Registro de Eventos:*

No se elaboran los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Los registros de eventos que no se realizan deberían de incluir:

- ✓ Identificación los usuarios.
- ✓ Establecimiento de las actividades del sistema, fechas, horas y detalles de los eventos clave (entrada y salida).
- ✓ Identificación del dispositivo y/o ubicación, si es posible, e identificador del sistema.
- ✓ Registros de intentos de acceso al sistema exitosos, rechazados y otros intentos de acceso a recursos.
- ✓ No se encuentra implementado un sistema de control de acceso, por lo tanto, no hay alarmas accionadas por este sistema.
- ✓ No se encuentra implementado un sistema de detección de intrusión.
- ✓ Registro de las transacciones ejecutadas por los usuarios en las aplicaciones.



#### *12.4.2. Protección de la Información de Registro:*

Las instalaciones y la información de registro no se protegen contra alteraciones y acceso no autorizado.

#### *12.4.3. Registros del Administrador y del Operador:*

Las actividades del administrador y del operador del sistema no se registran, por lo tanto no se protegen ni revisan regularmente.

#### *12.4.4. Sincronización de Relojes:*

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la entidad no se sincronizan con una única fuente de referencia de tiempo.

#### *12.5. Control de Software Operacional:*

No se asegura la integridad de los sistemas operacionales.

##### *12.5.1. Instalación de Software en Sistemas Operativos:*

No hay implementados procedimientos para controlar la instalación de software en sistemas operativos.

Las siguientes directrices para control de software operacional no se tiene en cuenta:

- ✓ La actualización del software operacional, aplicaciones y bibliotecas de programas solo se debe llevar a cabo por personal autorizado.
- ✓ La definición de los sistemas operacionales sólo debe contener códigos ejecutables aprobados, no el código de desarrollo o compiladores.
- ✓ El establecimiento de las aplicaciones y el software del sistema operativo solo se debería implementar después de pruebas extensas y exitosas, dentro los ensayos se deberían de abarcar la usabilidad, la seguridad, los



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



efectos sobre otros sistemas y la facilidad de uso, esta se debería llevar a cabo en sistemas separados de la producción.

- ✓ No se usa un sistema de control de la configuración para mantenimiento de la configuración, el control de todo el software implementado, al igual que la documentación del sistema.
- ✓ No se encuentra establecida una estrategia de retroceso (rollback) antes de una implementación de los cambios.
- ✓ No se mantiene un log de auditoría de las actualizaciones de las bibliotecas de programas operacionales.
- ✓ No se definen las versiones anteriores del software de aplicación, estas se deberían de conservar como una medida de contingencia.
- ✓ No está establecido que se debería manejar toda la información del software no se lleva ninguna información de estos se debería tener en cuenta mínimo; la información y parámetros, procedimientos, detalles de configuración, en tanto los datos permanezcan en el archivo.

#### *12.6. Gestión de la Vulnerabilidad Técnica:*

No hay una administración enfocada en la prevención y el aprovechamiento de las vulnerabilidades técnicas por terceros para cualquiera que sea el fin.

##### *12.6.1. Gestión de las Vulnerabilidades Técnicas:*

No hay información acerca de las vulnerabilidades técnicas de los sistemas de información que se usan; no se evalúa la exposición de la organización a estas vulnerabilidades, y tampoco se toman las medidas apropiadas para tratar el riesgo asociado.

Por lo anterior tampoco se toman en cuenta las siguientes directrices para las vulnerabilidades técnicas:

- ✓ La definición y establecimiento de los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad y por lo tanto la solución o control de estas.
- ✓ Definición de los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la toma de conciencia acerca de ellas.
- ✓ Un control para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



- ✓ Establecer que una vez que se haya identificado una vulnerabilidad técnica, la organización debería identificar los riesgos asociados y las acciones por tomar y la aplicación de controles.
- ✓ Definir procedimiento de respuesta a incidentes de seguridad de la información.
- ✓ Llevar un log de auditoría para todos los procedimientos que se hayan realizado.
- ✓ Establecer un proceso de gestión eficaz y eficiente de la vulnerabilidad técnica alineada con las actividades de gestión de incidentes y suministrar los procedimientos técnicos para realizarse si llegara a ocurrir un incidente.

#### *12.6.2. Restricciones Sobre la Instalación de Software:*

No se encuentran establecidas e implementadas las reglas para la instalación de software por parte de los usuarios. Se encuentra algunas restricciones, pero estas no son suficientes.

#### *12.7. Consideraciones Sobre Auditorías de Sistemas de Información:*

No hay actividades de auditoría sobre los sistemas operacionales.

##### *12.7.1. Controles Sobre Auditorías de Sistemas de Información:*

Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos no se realizan, por lo tanto, no se planifican ni se ejecutan este tipo de actividades.

### **13. SEGURIDAD DE LAS COMUNICACIONES –TECNICA.**

#### *13.1. Gestión de la Seguridad de las Redes:*

Se tienen implementadas algunas medidas de protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.



**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARÍA GENERAL**



**13.1.1. Controles de Redes:**

Las redes se gestionan y controlan medianamente para la protección de la información en sistemas y aplicaciones.

Se Revisan las siguientes directrices implementadas para la gestión de seguridad de redes:

- ✓ No se encuentran establecidas las responsabilidades operacionales y procedimientos para la gestión de equipos de redes.
- ✓ No se encuentran establecidos controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes inalámbricas, y para proteger los sistemas y aplicaciones conectados.
- ✓ No se aplican logging y seguimientos adecuados para posibilitar el registro y detección de acciones que puedan afectar, o son pertinentes a la seguridad de la información.
- ✓ No se definen actividades de gestión para optimizar tanto el servicio de la organización, como para asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información.
- ✓ No hay restricciones de conexión a la red la conexión física y de los sistemas a la red.

**13.1.2. Seguridad de los Servicios de Red:**

No se tienen identificados los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red.

No se tiene establecido:

- ✓ Una revisión de las tecnologías aplicadas a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red.
- ✓ Una definición de los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red.
- ✓ Los procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red.



**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARÍA GENERAL**



**13.1.3. Separación en las Redes:**

Se encuentra implementada una segregación en las redes, por secretaria, pero esta se ha ido deteriorando porque se han implementado nuevas secretarías y oficinas y no se ha ido actualizando esta separación a medida de los cambios físicos y administrativos que se han venido presentando.

**13.2. Transferencia de Información:**

**13.2.1. Políticas y Procedimientos de Transferencia de Información:**

De acuerdo a la NIST: Se deben mapear los flujos de comunicaciones y datos lo cual no se cumple, como se revisan las siguientes directrices:

- ✓ No se han definido procedimientos diseñados para proteger la información transferida contra interceptación, copiado, modificación, enrutado y destrucción.
- ✓ No se ha definido procedimientos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas (Se encuentra implementado un Antivirus que permite la protección contra este tipo de software).
- ✓ No se han definido las responsabilidades del personal, las partes externas y cualquier otro usuario para no comprometer a la organización, (por difamación, acoso, suplantación, envío de cadenas, compras no autorizadas, etc.).
- ✓ No se ha establecido el uso de técnicas criptográficas, (proteger la confidencialidad, la integridad y la autenticidad de la información).
- ✓ No se ha establecido las directrices sobre retención y disposición para toda la correspondencia del negocio (Información electrónica).
- ✓ No se ha brindado asesoría al personal para que tome las precauciones apropiadas acerca de no revelar información confidencial.

**13.2.2. Acuerdos Sobre Transferencia de Información:**

No existen acuerdos para la transferencia segura de información de la entidad entre esta y las partes externas.

No se encuentran establecidas las siguientes directrices para transferencia segura de la información:



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



- ✓ No están establecidas las responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo.
- ✓ No hay definidos procedimientos para asegurar trazabilidad y no repudio.
- ✓ No están definidos estándares técnicos mínimos de empaquetado y transmisión.
- ✓ No se encuentran definidas las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información.
- ✓ No se mantener una cadena de custodia para la información mientras está en tránsito.

**13.2.3. Mensajería Electrónica:**

No se aplican las siguientes directrices de mensajería electrónica:

- ✓ No se han definido las consideraciones legales, (los requisitos para firmas electrónicas).
- ✓ No se ha establecido una obtención de aprobación antes de usar servicios públicos externos como mensajería instantánea, redes sociales o intercambio de información).

**13.2.4. Acuerdos de Confidencialidad o de no Divulgación:**

No se ha documentado los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la entidad para la protección de la información, estos solo se manejan en contratos, pero los empleados no firman este tipo de acuerdos.

No se tiene implementadas las siguientes directrices para acuerdos de confidencialidad:

- ✓ No se ha definido la información que se va a proteger (información confidencial).
- ✓ No se ha determina la duración esperada de un acuerdo, incluidos los casos en los que podría ser necesario mantener la confidencialidad indefinidamente.
- ✓ No se han establecido acciones requeridas cuando termina el acuerdo.
- ✓ No se han definido las responsabilidades ni acciones de los firmantes para evitar la divulgación no autorizada de información.
- ✓ No se ha definido el procedimiento de notificación y reporte de divulgación no autorizada o fuga de información confidencial.
- ✓ No se han establecido las acciones que se espera tomar en caso de violación del acuerdo.





## **14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN –TECNICA.**

### *14.1. Requisitos de Seguridad de los Sistemas de Información:*

No se asegura que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida.

#### *14.1.1. Análisis y Especificación de Requisitos de Seguridad de la Información:*

No existen requisitos relacionados con seguridad de la información que se incluyan como requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

#### *14.1.2. Seguridad de Servicios de las Aplicaciones en Redes Públicas:*

La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas no se protege de actividades fraudulentas, disputas contractuales y divulgación o modificación no autorizadas.

#### *14.1.3. Protección de Transacciones de los Servicios de las Aplicaciones:*

La información involucrada en las transacciones de los servicios de las aplicaciones, no se protege 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 autorizado.

No se ha definido el uso de firmas electrónicas en los aspectos de la transacción.

No se ha definido la trayectoria de las comunicaciones entre todas las partes involucradas esté encriptada y los protocolos usados para comunicarse entre todas las partes involucradas estén asegurados.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



*14.2. Seguridad en los Procesos de Desarrollo y de Soporte:*

No se asegura que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

*14.2.1. Política de Desarrollo Seguro:*

No se han establecido reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.

No se ha definido la seguridad del ambiente de desarrollo.

No orienta la seguridad en el ciclo de vida de desarrollo del software.

No se ha definido la seguridad en la metodología del desarrollo de software.

No se ha establecido directrices de codificación seguras para cada lenguaje de programación usado.

No se ha definido requisitos de seguridad en la fase diseño.

*14.2.2. Procedimientos de Control de Cambios en Sistemas:*

Los cambios a los sistemas dentro del ciclo de vida de desarrollo no se controlan ni se usan procedimientos formales de control de cambios.

No se mantiene un control de versiones para todas las actualizaciones de software.

*14.2.3. Revisión Técnica de las Aplicaciones Después de Cambios en la Plataforma de Operación:*

Cuando se cambian las plataformas de operación, no se evidencia la revisión de las aplicaciones críticas del negocio, y tampoco se ponen a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la entidad.

Asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



No se asegura que se hacen cambios apropiados en los planes de continuidad del negocio (Este no lo hay).

*14.2.4. Restricciones en los Cambios a los Paquetes de Software:*

No hay evidencia de las restricciones de las modificaciones, a los paquetes de software, no hay una documentación que controle un límite a los cambios necesarios, que permita un control más estricto a los cambios.

*14.2.5. Principios de Construcción de Sistemas Seguros:*

No están establecido ni documentado principios para la construcción de sistemas seguros, por lo tanto, estos no se aplican a ninguna actividad de implementación de sistemas de información.

*14.2.6. Ambiente de Desarrollo Seguro:*

La entidad no ha establecido un ambiente de desarrollo seguro para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas, para que este sea protegido adecuadamente.

No se almacenan las copias de respaldo en lugares seguros fuera del sitio.

*14.2.7. Desarrollo Contratado Externamente:*

La entidad supervisa y hace seguimiento a la actividad de desarrollo de sistemas contratados externamente, aunque esta no se hace de una forma exhaustiva.

Revisadas las siguientes directrices desarrollo contratado externamente no se cumple con las siguientes:

- ✓ No hay una definición clara de los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el desarrollo contratado externamente.
- ✓ No están establecidos requisitos contractuales para prácticas seguras de diseño, codificación y pruebas.



**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARÍA GENERAL**



- ✓ No se realizan ensayos pertinentes de aceptación para determinar la calidad y exactitud de los entregables, esta prueba se hace directamente en producción.
- ✓ No hay una documentación de ningún tipo acerca del software contratado.

#### *14.2.8. Pruebas de Seguridad de Sistemas:*

No se han realizado pruebas durante el desarrollo de software para asegurar la funcionalidad de la seguridad. No se realizan pruebas de seguridad a los desarrollos antes de pasar a producción.

#### *14.3. Datos de Prueba:*

##### *14.3.1. Protección de Datos de Prueba:*

Los de ensayo que se seleccionan no sé, protegen y por ende no se controlan cuidadosamente.

### **15.RELACIÓN CON PROVEEDORES – ADMINISTRATIVA.**

#### *15.1. Seguridad de la Información en las Relaciones con los Proveedores:*

Hay algunas acciones que protegen los activos de la entidad que son accesibles para los proveedores.

- ✓ No hay una política de seguridad de la información relacionada con el acceso de los proveedores a los activos de la entidad, tampoco se refleja esta en los acuerdos o en los pliegos de condiciones con los proveedores lo cual debe estar documentado.
- ✓ No hay evidencia que se hayan suscrito acuerdos (ANS) formales donde se establezcan y acuerden todos los requisitos de seguridad de la información pertinentes con cada proveedor.



### *15.2. Gestión en la Prestación de Servicios de Proveedores:*

No hay evidencia de la revisión y/o auditoria con regularidad de los acuerdos (ANS) suscritos con los proveedores en lo cual se verifique el cumplimiento de estos con respecto a la seguridad de la información.

## **16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN – TECNICA.**

### *16.1. Gestión de Incidentes y Mejoras en la Seguridad de la Información:*

Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

#### *16.1.1. Responsabilidades y Procedimientos:*

No se encuentran establecidas las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

No se encuentran establecidas las siguientes directrices responsabilidades y procedimientos:

- ✓ No están establecidos procedimientos para la planificación y preparación de respuesta a incidentes.
- ✓ No están establecidos procedimientos para seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información.
- ✓ No están establecidos procedimientos para el manejo de evidencia forense.
- ✓ No están establecidos procedimientos para la valoración y toma de decisiones sobre eventos de seguridad de la información y la valoración de debilidades de seguridad de la información.
- ✓ No están establecidos procedimientos para respuesta, incluyendo aquellos para llevar el asunto a una instancia superior, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas.
- ✓ No están establecidos procedimientos para asegurar que el personal competente, maneje las cuestiones relacionadas con incidentes de



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



seguridad de la información. Se implemente un punto de contacto para la detección y reporte de incidentes de seguridad y se mantengan contactos apropiados con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información.

- ✓ No están establecidos procedimientos para definir la preparación de formatos de reporte de eventos de seguridad de la información, el procedimiento que se va a seguir en el caso de un evento de seguridad de la información, la referencia a un proceso disciplinario formal establecido para ocuparse de los empleados que cometen violaciones a la seguridad y los procesos de retroalimentación adecuados para asegurar que las personas que reportan eventos de seguridad de la información sean notificadas de los resultados después de que la cuestión haya sido tratada y cerrada.

#### *16.1.2. Reporte de Eventos de Seguridad de la Información:*

Los eventos de seguridad de la información no se informan a través de los canales apropiados, tampoco se encuentra establecido un control de seguridad eficaz que permita definir la violación de la integridad, confidencialidad o expectativas de disponibilidad de la información, errores humanos, no conformidades con políticas o directrices, violaciones de acuerdos de seguridad física, mal funcionamiento en el software o hardware y definir violaciones de acceso.

#### *16.1.3. Reporte de Debilidades de Seguridad de la Información:*

No se ha observado ningún reporte por parte de los empleados o contratistas que usan los servicios y sistemas de información de la entidad, de cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios prestados.

#### *16.1.4. Evaluación de Eventos de Seguridad de la Información y Decisiones Sobre Ellos:*

Los eventos de SI detectados no son analizados para determinar si constituyen un incidente de seguridad de la información por lo tanto no se evalúan y no se



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



decide si se van a clasificar como incidentes de seguridad de la información o no. No existe una categorización para los incidentes por lo tanto no hay planes de respuesta para cada categoría de incidentes presentados.

*16.1.5. Respuesta a Incidentes de Seguridad de la Información:*

Se no hay respuesta a los incidentes de seguridad de la información registrados tampoco hay procedimientos documentados.

No se cuenta con un plan de recuperación de incidentes durante o después del mismo. No hay un sistema de recolección de evidencia que permita hacerlo lo más pronto posible después de que ocurra el incidente. Nunca se ha llevado a cabo un análisis forense de seguridad de la información. No hay un registro de todas las actividades de respuesta involucradas para análisis posterior. No se ha comunicado la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo.

No se realiza un tratamiento a las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente, hasta cerrar formalmente el incidente y hacer un registro de esto.

No hay sistemas de detección para investigar las notificaciones de estos y tomar una decisión sobre el incidente.

*16.1.6. Aprendizaje Obtenido de los Incidentes de Seguridad de la Información:*

De acuerdo a la NIST se debe entender cuál fue el impacto del incidente. Las lecciones aprendidas deben ser usadas para actualizar los planes de respuesta a los incidentes de SI, pero no existe registro de este aprendizaje la entidad no ha gestionado el conocimiento adquirido porque al no analizar los incidentes de seguridad de la información no se puede usar esta información para reducir la posibilidad o el impacto de incidentes futuros de este mismo tipo.

*16.1.7. Recolección de Evidencia:*

La entidad no ha definido procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.





DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



No se aplican las siguientes directrices para recolección de evidencia:

- ✓ No se define una cadena de custodia.
- ✓ No se establece la seguridad de la evidencia.
- ✓ No está definida la seguridad del personal.
- ✓ No se encuentran definidos roles y responsabilidades del personal involucrado.
- ✓ No hay definidas sesiones informativas.

**17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO – ADMINISTRATIVA.**

*17.1. Continuidad de la Seguridad de la Información:*

La continuidad de la seguridad de la información no incluye los sistemas de gestión de la continuidad del negocio de la Entidad.

*17.1.1. Planificación de la Continuidad de la Seguridad de la Información:*

La entidad no cuenta con un BCP (Business Continuity Plan) o DRP (Disaster Recovery Plan), por lo tanto, no se ha incluido en estos planes los requisitos de seguridad de la información.

De acuerdo a la NIST también se deben tener planes de respuesta a incidentes y recuperación de incidentes, pero la entidad no cuenta con ellos.

*17.1.2. Implementación de la Continuidad de la Seguridad de la Información:*

La organización no ha establecido, ni documentado procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.

La entidad:

- ✓ No cuenta con una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



- ✓ No cuenta con personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información.
- ✓ No cuenta con planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la dirección.

*17.1.3. Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información:*

No hay evidencias de la realización de pruebas de la funcionalidad de los procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información.

*17.2. Redundancias:*

No hay implementadas redundancias que permitan asegurar la disponibilidad de las instalaciones de procesamiento de la información, para la entidad.

*17.2.1. Disponibilidad de Instalaciones de Procesamiento de Información:*

La entidad no cuenta con arquitecturas redundantes, en el centro de cómputo principal, centro de datos o centro de procesamiento de información.

No se han definido las necesidades de los procesos para seleccionar que elementos deben ser redundantes.



## **18. CUMPLIMIENTO – ADMINISTRATIVA.**

### *18.1. Cumplimiento de Requisitos Legales y Contractuales:*

Se podría llegar a un incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad, porque no ha sido implementada ninguna de estas normas actuales acerca de este tema, por ejemplo: la ley de protección de datos personales la cual no presenta una evidencia de implementación y seguimiento de esta.

#### *18.1.1. Identificación de la Legislación Aplicable y de los Requisitos Contractuales:*

Se tiene identificado en la entidad una relación de requisitos legales, reglamentarios, estatutarios, que le aplican a la Entidad (Normograma). Pero no hay un responsable de identificarlos y no hay definidos responsables para su cumplimiento o implementación.

#### *18.1.2. Derechos de Propiedad Intelectual:*

- ✓ No hay implementado procedimiento o guía para el cumplimiento de los requisitos y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
- ✓ La Entidad no cuenta con una política publicada sobre el cumplimiento de derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos.

#### *18.1.3. Protección de Registros:*

La entidad cuenta con tablas de retención documental, pero las condiciones en las que se protegen los registros importantes de una pérdida, destrucción o falsificación, no es la más adecuada, los registros, cualquiera que sea el medio de estos tienen un riesgo muy alto por lo menos de sufrir algún percance.



DEPARTAMENTO DE ANTIOQUIA  
**ALCALDÍA DE APARTADÓ**  
SECRETARÍA GENERAL



*18.1.4. Protección de los Datos y Privacidad de la Información Relacionada con los Datos Personales:*

No se asegura la protección y privacidad de la información personal tal como lo exige la ley. La entidad no ha cumplido con el 100% de las disposiciones de la ley estatutaria 1581 de 2012 Régimen General de Protección de Datos Personales y por ende con el decreto 1377 de 2013 que reglamenta la ley.

- ✓ No están definidos los responsables del cumplimiento de esta ley.
- ✓ No se tienen identificados los repositorios de datos personales.
- ✓ No se ha solicitado consentimiento al titular para tratar los datos personales.
- ✓ No se han adoptan las medidas técnicas necesarias para proteger las bases de datos o archivos donde reposan estos datos.

*18.2. Revisiones de Seguridad de la Información:*

*18.2.1. Revisión Independiente de la Seguridad de la Información:*

No se realizan revisiones independientes, ni auditorias de la seguridad de la información.

- ✓ En el plan de auditorías del año 2017, no se evidencia la revisión independiente de temas relacionados con la seguridad de la información.
- ✓ No se han identificado en una auditoria, oportunidades de mejora o cambios en la seguridad de la información.

*18.2.2. Cumplimiento con las Políticas y Normas de Seguridad:*

No se asegura el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

- ✓ No se encuentra implementado el cumplimiento de las políticas y estándares de seguridad.
- ✓ No se encuentra implementada una revisión periódica del cumplimiento del centro de datos con las políticas y normas de seguridad establecidas.



**DEPARTAMENTO DE ANTIOQUIA**  
**ALCALDÍA DE APARTADÓ**  
**SECRETARÍA GENERAL**



**18.2.3.    *Revisión de Cumplimiento Técnico:***

Los sistemas de información no se chequean regularmente para el cumplimiento con los estándares de implementación de la seguridad.

No se realizan evaluaciones de seguridad técnicas por personal autorizado, apoyado en herramientas automáticas o con revisiones manuales realizadas por especialistas.