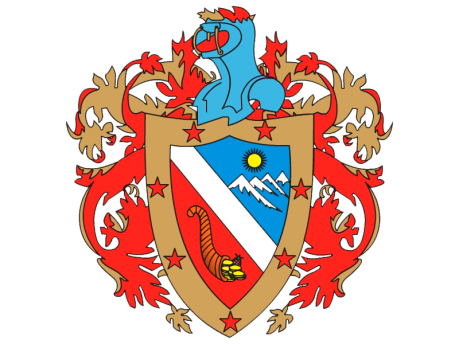
**GRUPO DE TECNOLOGIA, CONECTIVIDAD Y COMUNICACIONES**



**MANUAL DE POLÍTICAS DE USO, SEGURIDAD Y ADMINISTRACIÓN DE ACTIVOS TECNOLÓGICOS Y DE INFORMACIÓN DE LA GOBERNACIÓN DEL HUILA**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Elaboró** | **Revisó** | **Aprobó** |
| **Firma** |  |  |  |
| **Nombre** |  |  |  |
| **Cargo** |  |  |  |

Contenido

[1. INTRODUCCIÓN 7](#_Toc115965527)

[2. JUSTIFICACION 8](#_Toc115965528)

[3. ALCANCE 9](#_Toc115965529)

[4. OBJETIVO 9](#_Toc115965530)

[4.1. Objetivos Específicos 9](#_Toc115965531)

[5. MARCO NORMATIVO 10](#_Toc115965532)

[6. CONDICIONES GENERALES 17](#_Toc115965533)

[7. DIAGNOSTICO INICIAL 18](#_Toc115965534)

[8. METODOLOGIA 19](#_Toc115965535)

[9. ASIGNACIÓN DE RESPONSABILIDADES 23](#_Toc115965536)

[9.1. Nivel Gerencial 23](#_Toc115965537)

[9.2. Grupo De Tecnología, Conectividad Y Telecomunicaciones 23](#_Toc115965538)

[9.3. Proveedores De Redes 24](#_Toc115965539)

[10. ESTRUCTURA DE SISTEMA DE GESTIÓN 25](#_Toc115965540)

[10.1. Mapa De Procesos 25](#_Toc115965541)

[11. INFORMACIÓN GENERAL DE LA GOBERNACIÓN DEL HUILA 26](#_Toc115965542)

[11.1. Visión 26](#_Toc115965543)

[11.2. Misión 26](#_Toc115965544)

[11.3. Objetivos Del Sistema De Gestion 26](#_Toc115965545)

[12. AUTORIDAD Y RESPONSABILIDAD 27](#_Toc115965546)

[12.1. Organigrama De La Gobernación Del Huila 27](#_Toc115965547)

[12.2. Manual De Funciones 27](#_Toc115965548)

[12.3. Sistema De Comunicación Formal En La Gobernación 29](#_Toc115965549)

[CAPITULO 1: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 30](#_Toc115965550)

[13. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA GOBERNACIÓN DEL HUILA 31](#_Toc115965551)

[13.1. Objetivo 32](#_Toc115965552)

[13.2. Objetivos Específicos: 33](#_Toc115965553)

[13.3. Alcance 33](#_Toc115965554)

[CAPITULO 2: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 34](#_Toc115965555)

[14. RESPONSABILIDADES EN MATERIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 35](#_Toc115965556)

[14.1. Cumplimiento 36](#_Toc115965557)

[15. POLÍTICAS DE USO DE LOS RECURSOS TECNOLOGICOS, INFORMATICOS Y TELECOMUNICACIONES DE LA GOBERNACIÓN DEL HUILA 36](#_Toc115965558)

[15.1. Documentación De Las Políticas De Seguridad Y Admiinstración 36](#_Toc115965559)

[15.2. Asignación De Responsabilidades En Materia De Seguridad Y Adminstración De La Plataforma Tecnologica 37](#_Toc115965560)

[15.3. Asignación De Responsabilidades En Materia De Seguridad Y Adminstrración De La Plataforma Tecnologica Dentro Del Grupo De Tecnologia, Conectividad Y Comunicaciones. 38](#_Toc115965561)

[15.4. Perfil Y Funciones De Los Administradores De La Red De La Gobernación Del Huila 39](#_Toc115965562)

[CAPITULO 3: CONTROL Y GESTIÓN DE ACTIVOS 42](#_Toc115965563)

[16. USO, CLASIFICACIÓN Y CONTROL DE ACTIVOS DE TI 43](#_Toc115965564)

[16.1. Responsabilidad Por Rendición De Cuentas De Los Activos 43](#_Toc115965565)

[16.2. Inventarios De Activos 43](#_Toc115965566)

[16.3. Clasificación De La Informacón 44](#_Toc115965567)

[17. METODOLOGÍA DE GESTÓN DE ACTIVOS DE SEGURIDAD DIGITAL 45](#_Toc115965568)

[17.1. Diagnóstico De Activos 45](#_Toc115965569)

[18. POLÍTICA DE DISPOSITIVOS MÓVILES 49](#_Toc115965570)

[19. POLITICAS DE GESTION INFORMATICA 54](#_Toc115965571)

[19.1. Planeación 55](#_Toc115965572)

[19.2. Adquisición Equipos 56](#_Toc115965573)

[19.3. Parametros A Tener En Cuenta En La Compra De Tecnologia Informatica Y Telecomunicaciones 57](#_Toc115965574)

[CAPITULO 4: 60](#_Toc115965575)

[CONTROL DE ACCESO DE USUARIOS 60](#_Toc115965576)

[20. CUENTAS DE LOS USUARIOS 61](#_Toc115965577)

[20.1. Creación Cuentas Usuarios De Planta Gobernación Del Huila 62](#_Toc115965578)

[20.2. Creación Cuentas Usuario Para Contratistas De La Gobernación Del Huila 62](#_Toc115965579)

[20.3. Creación Cuentas De Usuario Para Dependencias E Instituciones Descentralizadas 63](#_Toc115965580)

[21. CONTROL DE ACCESO A SERVIDORES, ESTACIONES DE TRABAJO Y APLICATIVOS 64](#_Toc115965581)

[21.1. Creación Grupos De Trabajo 66](#_Toc115965582)

[22. IDENTIFICACIÓN DE ELEMENTOS DE HARDWARE EN LA RED CORPORATIVA 66](#_Toc115965583)

[22.1. Identificación De Servidores 66](#_Toc115965584)

[22.2. Identificación De Estaciones De Trabajo 66](#_Toc115965585)

[22.3. Identificación De Access Point 68](#_Toc115965586)

[22.4. Impresoras De Red 69](#_Toc115965587)

[22.5. Acceso A Áreas Críticas 69](#_Toc115965588)

[23. POLITICAS DEL USO CONTRASEÑA 69](#_Toc115965589)

[CAPITULO 5: SEGURIDAD FÍSICA Y DEL ENTORNO 73](#_Toc115965590)

[24. SEGURIDAD DE EQUIPOS TECNOLÓGICOS 74](#_Toc115965591)

[24.1. Ubicación Y Protección Del Equipamiento 74](#_Toc115965592)

[24.2. Instalación De Equipos De Cómputo 76](#_Toc115965593)

[24.3. Mantenimiento De Equipos Cómputo 76](#_Toc115965594)

[25. POLÍTICA DE ADMINISTRACIÓN DE RECURSOS TECNOLÓGICOS 77](#_Toc115965595)

[26. POLÍTICAS DE SEGURIDAD DEL CENTRO DE CÓMPUTO 79](#_Toc115965596)

[27. SEGURIDAD PERSONAL 80](#_Toc115965597)

[27.1. Seguridad En La Definición De Puestos De Trabajo Y La Asignación A Recursos A Usuarios 80](#_Toc115965598)

[28. SEGURIDAD Y AMBIENTAL 81](#_Toc115965599)

[28.1. Seguridad De Areas 81](#_Toc115965600)

[28.2. Limpieza De Puestos De Trabajo 83](#_Toc115965601)

[29. SEGURIDAD FISICA DE LAS AREAS DE ENTREGA Y CARGA DE LA GOBERNACIÓN DEL HUILA 86](#_Toc115965602)

[30. POLÍTICA DE MEDIO AMBIENTE 86](#_Toc115965603)

[CAPITULO 6: 88](#_Toc115965604)

[SEGURIDAD DE LAS OPERACIONES 88](#_Toc115965605)

[31. SEPARACION DE AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN 89](#_Toc115965606)

[32. POLÍTICAS DEL USO Y APLICACIÓN DEL ANTIVIRUS 90](#_Toc115965607)

[33. CONTROL DE INSTALACIÓN DEL SOFTWARE 91](#_Toc115965608)

[34. POLITICA DE RESPALDO DE INFORMACIÓN 92](#_Toc115965609)

[CAPITULO 7: 98](#_Toc115965610)

[SEGURIDAD DE LAS COMUNICACIONES 98](#_Toc115965611)

[35. POLÍTICAS DE ADMINISTRACIÓN DE LA RED 99](#_Toc115965612)

[35.1. Políticas De Adminstración Del Cableado 100](#_Toc115965613)

[35.2. Consideraciones Para Dispositivos Activos De Conexion (Hub's, Concentradores, Switches): 101](#_Toc115965614)

[35.3. Consideraciones Para Los Centros De Cableado 102](#_Toc115965615)

[35.4. Consideraciones Para El Cableado Horizontal 104](#_Toc115965616)

[35.5. Consideraciones Para El Cableado Vertical (Backbone) 107](#_Toc115965617)

[35.6. Nomenclatura Par Puntos De Red 107](#_Toc115965618)

[35.7. Seguridad Física Del Cableado 108](#_Toc115965619)

[35.8. Politicas De Seguridad Para Redes Inalambricas 109](#_Toc115965620)

[36. POLÍTICAS DE SEGURIDAD DE LA RED 110](#_Toc115965621)

[36.1. Seguridad De Acceso A Internet Y Conexiones Con Redes Externas 114](#_Toc115965622)

[36.2. Seguridad En El Acceso De Los Recursos De La Red Interna 116](#_Toc115965623)

[37. POLITICA DE TRANSFERENCIA DE INFORMACIÓN 123](#_Toc115965624)

[38. POLÍTICAS DE CORREO ELECTRONICO 128](#_Toc115965625)

[39. POLÍTICAS DEL USUARIO FINAL 131](#_Toc115965626)

[39.1. Procedimientos Para El Uso Y El Manejo Del Sistema 132](#_Toc115965627)

[39.2. Políticas Operativas 133](#_Toc115965628)

[40. CONFIDENCIALIDAD 135](#_Toc115965629)

[CAPITULO 8: 137](#_Toc115965630)

[ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN 137](#_Toc115965631)

[41. ADQUISICIÓN, DESARROLLO, SOPORTE, MANTENIMIENTO, RETIRO, CAMBIO Y/O ACTUALIZACIÓN DE SOFTWARE 138](#_Toc115965632)

[41.1. Ciclo De Vida De Un Software, Aplicativo Y/O Sistema De Información 138](#_Toc115965633)

[CAPITULO 9: 148](#_Toc115965634)

[GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 148](#_Toc115965635)

[42. COMUNICACIÓN DE INCIDENTES EN MATERIA DE SEGURIDAD 149](#_Toc115965636)

[CAPITULO 10: 150](#_Toc115965637)

[DISPONIBILIDAD DE SERVICIOS E INFORMACIÓN 150](#_Toc115965638)

[43. POLÍTICA DE SERVICIOS TIC 151](#_Toc115965639)

[CAPITULO 11: 162](#_Toc115965640)

[CUMPLIMIENTO DE REQUISITOS LEGALES Y NORMATIVOS 162](#_Toc115965641)

[44. PROPIEDAD DE LA INFORMACIÓN 163](#_Toc115965642)

[45. POLITICAS SITIO WEB 163](#_Toc115965643)

[46. POLÍTICA DE DERECHOS DE AUTOR Y/O AUTORIZACIÓN DE USO SOBRE LOS CONTENIDOS DE LA SEDE ELECTRÓNICA 164](#_Toc115965644)

[46.1. Alcances Y Limites En El Uso 164](#_Toc115965645)

[46.2. Política De Derechos De Autor Y/O Autorización De Uso Sobre Los Contenidos 165](#_Toc115965646)

[46.2.1. Materiales Suministrados A La Gobernación Del Huila 166](#_Toc115965647)

[46.2.2. Política Datos Abiertos 166](#_Toc115965648)

[46.3. Responsabilidades De Los Usuarios 166](#_Toc115965649)

[46.4. Notificaciones Y Procedimiento De Reclamos De Violación A Los Derechos De Propiedad 168](#_Toc115965650)

[47. TÉRMINOS Y CONDICIONES DE USO 168](#_Toc115965651)

[47.1. Alcances Y Limites En El Uso 168](#_Toc115965652)

[47.2. Definiciones 169](#_Toc115965653)

[47.3. Condiciones De Uso 170](#_Toc115965654)

[47.3.1. Vínculos A Sitios De Terceros 170](#_Toc115965655)

[47.3.2. Uso De Servicios De Comunicación 170](#_Toc115965656)

[47.3.3. Uso De “Cookies” 171](#_Toc115965657)

[47.3.4. Seguridad De Su Información Personal 172](#_Toc115965658)

[47.3.5. Normas Aplicables 172](#_Toc115965659)

[47.3.6. Renuncia De Obligación 172](#_Toc115965660)

[47.4. Deberes De Los Usuarios 173](#_Toc115965661)

[47.4.1. Política Comentarios 174](#_Toc115965662)

[47.5. Contacto Para Asuntos Relacionados Con Los Términos Y Condiciones 174](#_Toc115965663)

[48. GLOSARIO 175](#_Toc115965664)

[49. CONTROL DE CAMBIOS 177](#_Toc115965665)

# INTRODUCCIÓN

Con este Manual de Políticas, Uso, Seguridad y Administración de Activos Tecnológicos y de Información, se pretende trazar los lineamientos bajo la responsabilidad del Grupo de Tecnología, Conectividad y Telecomunicaciones que orientan al uso adecuado de estas políticas Tecnológicas recomendadas para obtener el mayor provecho de estas. En este sentido, surgen como una herramienta de vital importancia y sensibilidad organizacional de carácter obligatoria, el cual permite a la entidad crecer y mantenerse competitiva.

La Gobernación del Huila y la Secretaria General, en apoyo con el Grupo de Tecnología, Conectividad y Telecomunicaciones, prioriza e identifica los recursos informáticos y tecnológicos como elementos indispensables en la conducción y consecución de los objetivos definidos por la entidad, para ello emprendió la tarea de actualizar el Manual de Políticas de Uso, Seguridad y Administración de Activos Tecnológicos y de Información, con el fin de reglamentar el uso, protección y administración de ellos al interior de la organización.

Conscientes de la importancia del uso adecuado de los de Activos Tecnológicos y de Información, se han planteado políticas que deben ser cumplidas por todos los funcionarios y contratistas que laboren o tengan relación con la entidad. A continuación, en este documento se analizarán las políticas de gestión informática, desarrollo de software, administración de red, uso y aplicación del antivirus, red inalámbrica, seguridad de la red, correo electrónico, sitio web, y usuarios finales.

Debido a los avances tecnológicos y de telecomunicaciones a nivel mundial, se hace necesario que las organizaciones sean flexibles al cambio en sus procesos estratégicos e institucionales los cuales les permitirán mejorar la productividad y competitiva, garantizando la protección de los activos tangibles e intangibles de la Gobernación del Huila.

La Política de Uso, Seguridad y Administración de Activos Tecnológicos y de Información será revisada regularmente por la Gobernación del Huila, en apoyo del Grupo de Tecnología, Conectividad y Telecomunicaciones, y permitirá garantizar a los funcionarios, contratistas tener claridad en el manejo y el cumplimento correcto de los lineamientos estipulados para el buen uso y protección de los recursos tecnológicos de la Gobernación del Huila.

# JUSTIFICACION

El presente documento define las Políticas de Uso, Seguridad y Administración de Activos Tecnológicos y de Información de la Gobernación del Huila, durante el periodo 2020 – 2023. Las Políticas actualizadas y presentadas en este documento se enmarcan dentro del Sistema de Gestión Integrado, que soportan sus directrices en el anterior Manual de Políticas de Uso, Seguridad y Administración de Activos Tecnológicos y de Información de la Gobernación del Huila, versión 6; con código: SGN-C043-M806

La Seguridad Informática y Administración de los Activos Tecnológicos ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información. Es frecuente que las personas involucradas con Seguridad Informática tengan un concepto erróneo de las Políticas de Seguridad, estas incluyen la asignación de responsabilidades y actividades para darlas a conocer y supervisar su cumplimiento.

Es importante resaltar que en esta administración 2020 – 2023 “Huila Crece” se ha logrado gestionar la más grande inversión en materia de Tecnologías en la historia del Huila, es por esta razón que la Gobernación del Huila y la Secretaria General, en apoyo con el Grupo de Tecnología, Conectividad y Telecomunicaciones, ha decidido actualizar sus políticas de Uso, Seguridad y Administración de Activos Tecnológicos y de Información, a medida que se adquieran activos tangibles o intangibles importantes y vitales en la entidad, sin ellos no se contaría con una herramientas para la toma de decisiones y gestión.

Con el uso de este documento, la Gobernación del Huila en apoyo con el Grupo de Tecnología, Conectividad y Telecomunicaciones pretende minimizar los riesgos y amenazas a las cuales están expuestos los activos de la entidad, y en caso que ocurra un incidente grave que refleje alguna vulnerabilidad en los Sistemas Informáticos y Tecnológicos, se deberán tomar las acciones correctivas rápidamente para así reducir los impactos, esto se logrará garantizando el cumpliendo del Manual de políticas de Uso y Administración con apoyo del Plan de Contingencia que actualizó el Grupo de Tecnología, Conectividad y Comunicaciones de la Entidad.

# ALCANCE

El presente Manual de Políticas de Uso, Seguridad y Administración de Activos Tecnológicos y de Información de la Gobernación del Huila, aplica para los directivos, funcionarios, contratistas y terceros no vinculados directamente, en la ejecución de actividades de los procesos de gestión misionales, de apoyo, estratégicos y de evaluación de la entidad, quienes están en la obligación de dar cumplimiento a las políticas y lineamientos de uso, seguridad y administración de los activos de TI de la entidad, y que son emitidas y aprobadas por la alta dirección, en el marco de la implementación de la gestión de seguridad y privacidad de la información.

# OBJETIVO

El objetivo de este documento es actualizar las Políticas de Uso, Seguridad y Administración de Activos Tecnológicos y de Información, con el fin de garantizar el conocimiento y cumplimento de directrices por parte de todos los funcionarios, y contratistas y terceros que presten sus servicios a la Gobernación del Huila a través de proceso de gestión y seguridad de TI.

# Objetivos Específicos

1. Restablecer las Políticas de Uso, Seguridad y Administración de Activos Tecnológicos y de Información, que faciliten ejecutar las actividades y procedimientos en la Gobernación del Huila.
2. Concientizar a los usuarios sobre la importancia de uso racional y seguro de los Activos Tecnológicos y de Información de la organización.
3. Fomentar una cultura de pertenecía hacia los Activos Tecnológicos y de Información.

4. Promover estrategias en pro del mejoramiento continuo de Políticas de TI, mediante encuestas de sugerencias aplicables para todos los usuarios de la Gobernación.

# MARCO NORMATIVO

A continuación, se lista las normas y documentos de referencia para el establecimiento de las políticas contenidas en el presente manual.

| **Normas y Documentos de Referencia** | |
| --- | --- |
| **Marco Normativo** | **Descripción** |
| **Constitución Política de Colombia – 1991** | Artículo 15. “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. |
| **Ley 962 de 2005** | El artículo 14 lo siguiente “Cuando las entidades de la Administración Pública requieran comprobar la existencia de alguna circunstancia necesaria para la solución de un procedimiento o petición de los particulares, que obre en otra entidad pública, procederán a solicitar a la entidad el envío de dicha información. En tal caso, la carga de la prueba no corresponderá́ al usuario.  Será permitido el intercambio de información entre distintas entidades oficiales, en aplicación del principio de colaboración. El envío de la información por fax o por cualquier otro medio de transmisión electrónica, proveniente de una entidad pública, prestará mérito suficiente y servirá́ de prueba en la actuación de que se trate, siempre y cuando se encuentre debidamente certificado digitalmente por la entidad que lo expide y haya sido solicitado por el funcionario superior de aquel a quien se atribuya el trámite”. |
| **Ley 1273 de 2009** | Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones |
| **Ley 1341 de 2009** | Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. |
| **Ley 1581 de 2012** | Por la cual se dictan disposiciones generales para la protección de datos personales. |
| **Ley 1712 de 2014** | Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. |
| **Ley 1753 de 2015** | Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAIS" "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. |
| **Ley 1955 de 2019** | Por el cual se expide el Plan Nacional de Desarrollo 2018-2022 “Pacto por Colombia, Pacto por la Equidad”. Por el cual se expide el plan nacional de desarrollo 2018-2022 - pacto por Colombia, pacto por la equidad. En su artículo 147 “Transformación Digital Pública” establece que las entidades territoriales podrán definir estrategias de ciudades y territorios inteligentes, para lo cual deberán incorporar los lineamientos técnicos en el componente de transformación digital que elabore el Ministerio de Tecnologías de la Información y las Comunicaciones.  Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) |
| **Ley 1978 de 2019** | Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones. |
| **Decreto Ley 019 de 2012** | Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública. |
| **Decreto 2150 de 1995** | Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública |
| **Decreto 1151 de 2008** | Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones. |
| **Decreto 4485 de 2009** | Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública. |
| **Decreto 235 de 2010** | Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas. |
| **Decreto 2364 de 2012** | Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones. |
| **Decreto 2693 de 2012** | Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones. |
| **Decreto 2482 de 2012** | Por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión. |
| **Decreto 1377 de 2013** | Por el cual se reglamenta parcialmente la Ley 1581 de 2012 o Ley de Datos Personales. |
| **Decreto 2573 de 2014** | Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones |
| **Decreto 886 de 2014** | Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos, que permitirá cumplir con la obligación legal de dar publicidad a la existencia de bases de datos de carácter personal y servirá de herramienta de supervisión para la efectiva protección de los derechos de los titulares. |
| **Decreto 2433 de 2015** | Por el cual se reglamenta el registro de TIC y se subroga el título 1 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. |
| **Decreto 1078 de 2015** | Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones |
| **Decreto 103 de 2015** | se reglamenta parcialmente la Ley 1712 de 2014 en lo relativo a la gestión de la información pública y se dictan otras disposiciones. |
| **Decreto 415 de 2016** | Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones. |
| **Decreto 728 2016** | Actualiza el Decreto 1078 de 2015 con la implementación de zonas de acceso público a Internet inalámbrico |
| **Decreto 728 de 2017** | Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico. |
| **Decreto 1413 de 2017** | Por el cual se adiciona el título [17](https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888#2.2.17.1.1) a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales. |
| **Decreto 1499 de 2017** | Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015. |
| **Decreto 612 de 2018** | Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. |
| **Decreto 1008 de 2018** | Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. |
| **Decreto 2106 del 2019** | Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Publica Efectiva |
| **Decreto 620 de 2020** | Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales" |
| **Resolución 3564 de 2015** | Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública. |
| **Resolución 3564 2015** | Reglamenta algunos artículos y parágrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados) |
| **Resolución 2710 de 2017** | Por la cual se establecen los lineamientos para la adopción del protocolo IPv6. |
| **Resolución 500 de 2021** | Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital. |
| **Norma Técnica Colombiana NTC 5854 de 2012** | Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA. |
| **Manual de Gobierno Digital – 2018** | En este documento se desarrolla el proceso de implementación de la Política de Gobierno Digital a través de los siguientes cuatro (4) momentos: 1. Conocer la política; 2. Planear la política; 3. Ejecutar la política; y 4. Medir la política; cada uno de ellos incorpora las acciones que permitirán desarrollar la Política en las entidades públicas de nivel nacional y territorial, teniendo en cuenta los componentes TIC para el Estado, y TIC para la Sociedad, y los elementos habilitadores Arquitectura, Seguridad de la Información, Servicios Ciudadanos Digitales, con el fin de habilitar y mejorar la provisión de servicios ciudadanos digitales de confianza y calidad, lograr procesos internos, seguros y eficientes, tomar decisiones basadas en datos a partir del uso y aprovechamiento de la información, empoderamiento de los ciudadanos a través de un estado abierto, e impulsar el desarrollo de territorios y ciudades inteligentes a través de las TIC. |
| **MAE.G.GEN.01 - Documento Maestro**  **del Modelo de Arquitectura Empresarial** | Documento maestro dirigido a Entidades Públicas, el cual establece la estructura conceptual del Modelo de Arquitectura Empresarial del Marco de Referencia. En este, se definen los dominios o dimensiones las cuales agrupan y organizan los lineamientos de arquitectura empresarial: Planeación de la Arquitectura, Arquitectura Misional, Arquitectura de Información, Arquitectura de Sistemas de Información, Infraestructura Tecnológica, Arquitectura de Seguridad, y Uso y Apropiación de la Arquitectura. |
| **MGPTI.G.GEN.01 - Documento Maestro**  **del Modelo de Gestión de Proyectos TI** | Documento maestro dirigido a Entidades Públicas, el cual establece la estructura conceptual del Modelo de Gestión de Proyectos TI del Marco de Referencia. En este, se definen dominios que abordan todos los procesos y actividades para la dirección y ejecución de proyectos, programas y portafolios desde la necesidad de la administración pública: Legal, Planeación, Ejecución, y Control. |
| **MGGTI.G.GEN.01 - Documento Maestro**  **del Modelo de Gestión y Gobierno de TI** | Documento maestro dirigido a Entidades Públicas, el cual establece la estructura conceptual del Modelo de Gestión y Gobierno de TI del Marco de Referencia. En este, se definen los dominios que permiten alinear las necesidades del negocio mediante el uso adecuado de las TIC: Estrategia de TI, Gobierno de TI, Sistemas de Información, Información, Infraestructura de TI, Uso y Apropiación de TI. |
| **G.ES.06 Guía para la Construcción del PETI – Planeación de la Tecnología para la Transformación Digital – 2019** | Documento técnico dirigido a las entidades públicas del Estado Colombiano, en el que se reestructura la versión anterior de la guía, se incorpora una metodología y se actualiza el contenido para la construcción del PETI con un enfoque de Arquitectura en la planeación de la Tecnología para la Transformación Digital. |
| **Directiva Presidencial 04 de 2012** | Eficiencia administrativa y lineamientos de la política cero papel en la administración pública |
| **Conpes 3292**  **Proyecto de Racionalización y automatización de trámites, del 28 de junio de 2004** | Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos. |
| **Conpes 3920 de Política Nacional de Explotación de Datos - Big Data, del 17 de abril de 2018** | La presente política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales. |
| **Conpes 3854 Política Nacional de Seguridad Digital de Colombia, del 11 de abril de 2016** | El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo. |
| **Conpes 3975**  **Política Nacional de Transformación Digital e Inteligencia Artificial, del 8 de noviembre de 2019** | Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema. |

# CONDICIONES GENERALES

Para la correcta Actualización de este Manual de Políticas de Uso, Seguridad y Administración de Activos Tecnológicos y de Información de la Gobernación del Huila, se debe tomar en cuenta lo siguiente:

* El Manual deberá estar habilitado para todos los estamentos de la Gobernación del Huila, de manera física y electrónica.
* Las diferentes oficinas, y dependencias de la entidad incluyendo el Grupo de Tecnología, Conectividad y Telecomunicaciones deberán difundir las políticas y lineamientos detallados en este Manual y velar porque se dé el cumplimiento.
* Cuando se presenten sugerencias para cambio en la categorización legal actual, o en las políticas que afecten la estructura del Manual, se concebirá también un cambio en su contenido con el fin de adaptarlo a las nuevas políticas formuladas.
* La estructura del Manual es clara y precisa, por lo cual permite al usuario localizar la información sobre sus responsabilidades y las restricciones en el uso de los recursos y servicios TIC en la Gobernación del Huila, al igual que las responsabilidades de quienes los gestionan.
* Con la incorporación paulatina en tecnologías de información y comunicaciones en la institución, el Manual estará sujeto a permanentes cambios, por lo cual está fácil su actualización, convirtiéndose en un documento dinámico que solamente podrá ser modificado por el Grupo de Tecnología, Conectividad y Telecomunicaciones y aprobado por el Gobernador.

# DIAGNOSTICO INICIAL

Hoy en día las organizaciones están en la tarea de optimizar sus recursos Tecnológicos y de Telecomunicaciones, debido a las cambiantes condiciones y nuevos avances Tecnológicos disponibles, las cuales le permiten realizar sus procesos y procedimientos de manera eficiente para lograr cumplir sus expectativas frente a los nuevos horizontes productivos y competitivos de la entidad. Es por ello que en el siguiente diagnóstico inicial se pretende fortalecer las debilidades y amenazas en materia de Políticas de Uso, Seguridad y Administración de Activos Tecnológicos y de Información por parte del Grupo de Tecnología, Conectividad y Telecomunicaciones.

Existen varias inquietudes dentro de la Gobernación del Huila como los son: ¿Dónde estamos?, ¿Qué tan bien los estamos haciendo? ¿Qué expectativas se tienen para el futuro? en el tema de Políticas de Uso, Seguridad y Administración de Activos Tecnológicos y de Información dentro de la entidad, es por ello que se hace necesario, actualizar las estas políticas, las cuales permiten la facilidad y uso de herramientas tecnológicas y así crear en los usuarios una cultura de salvaguardar y administrar los recursos tecnológicos de la organización.

Para la realización del proceso de actualización del Manual de Política, Uso y Administración de los Recursos Tecnológicos de la Gobernación del Huila, el documento guía o base es el *Manual de Políticas de Uso, Seguridad y Administración de Activos Tecnológicos y de Información* con *Código: SGN-C043-M806*; implementado en el Sistema de Gestión Integrado, elaborado por el Grupo de Tecnología, Conectividad y Telecomunicaciones.

Es importante resaltar que estas directrices son de carácter obligatoria para todos los funcionarios y contratistas de la entidad, y de su cumplimiento estará encargado el Grupo de Tecnología, Conectividad y Telecomunicaciones el cual deberá establecer sus responsabilidades y estrategias para el debido control, seguimiento y la mejora continua de este documento.

# METODOLOGIA

La metodología utilizada para el diseño e implementación de las Políticas de Uso, Seguridad y Administración de Activos Tecnológicos y de Información de la Gobernación del Huila, se inicia mediante diagnóstico previo de las falencias y debilidades en materia de Gestión Informática y Telecomunicaciones, es por ello que se hace necesario elaborar y presentar unas directrices las cuales encaminan al mejoramiento de los procesos en Gestión de Información y Recursos Tecnológicos, con el apoyo del Grupo de Tecnología, Conectividad y Telecomunicaciones, y su respectiva aprobación por parte de la Oficina de calidad de la entidad.

Los aspectos a tener en cuenta dentro de las Políticas de tecnología y Telecomunicaciones, los cuales se encamina a través de los objetivos diseñados en el Sistema Integrado de gestión son:

* **FASE DE DESARROLLO:** Durante esta fase la Política es creada, revisada y aprobada.
* **FASE DE IMPLEMENTACIÓN:** En esta fase la política es comunicada y acatada.
* **FASE DE MANTENIMIENTO:** Los usuarios deben ser conscientes de la importancia de la política, cumplimiento, monitoreo y mantenimiento (actualizar).
* **FASE DE VERIFICACIÓN:** En esta fase la política requiere de acciones correctivas.
* ***Creación:*** *Planificación, investigación, documentación y coordinación de la política.*

El primer paso en la fase de desarrollo de la Política es la planificación, la investigación y la redacción de la política o, tomado todo junto, la creación. La creación implica identificar (por ejemplo, requerimientos legales, regulaciones técnicas); determinar el alcance y la aplicabilidad de la política, los roles y las responsabilidades inherentes a la aplicación y garantizar la factibilidad de su implementación. De esta etapa se tendrá como resultado la documentación de la política de acuerdo con los procedimientos de la Gobernación del Huila, con respecto a Tecnología y Telecomunicaciones al igual que la coordinación con organizaciones internas y externas que la política afectará, para obtener información y su aceptación.

* ***Revisión:*** *Evaluación de la política*

La revisión de la política es la segunda etapa en la fase de desarrollo. Una vez la documentación de la política ha sido creada y la coordinación inicial ha sido iniciada, esta debe ser remitida al Área de Tecnología, Conectividad y Telecomunicaciones, para su revisión, una vez revisada se direcciona a la oficina de CALIDAD para su respectivo análisis.

Como parte de esta función, se espera que el creador de la política recopile los comentarios y las recomendaciones para realizar cambios en la política y efectuar todos los ajustes y las revisiones necesarias para obtener una versión final de la política lista para la aprobación por las directivas.

* **Aprobación:** *Obtener la aprobación de la política por parte de las directivas*

El paso final en la fase de desarrollo de la política es la aprobación. El objetivo de esta etapa es obtener el apoyo y aprobación del Gobernador del Huila.

* **Comunicación:** *Difundir la política*

Una vez la política ha sido aprobada formalmente, se pasa a la fase de implementación. La comunicación de la política es la primera etapa que se realiza en esta fase. La política debe ser inicialmente difundida a los miembros de la Gobernación del Huila o a quienes sean afectados directamente por la política (contratistas, proveedores, usuarios de cierto servicio, etc.). Debe planificarse esta etapa con el fin de determinar los recursos necesarios y el enfoque que debe ser seguido para mejorar la visibilidad de la política.

* **Cumplimiento:** *Implementar la política*

La etapa de cumplimiento incluye actividades relacionadas con la ejecución de la política. Implica trabajar para interpretar cuál es la mejor manera de implementar la política en diversas situaciones y oficinas; asegurando que la política es entendida por aquellos que requieren implementarla, monitorearla, hacerle seguimiento, reportar regularmente su cumplimiento y medir el impacto inmediato de la política en las actividades operativas

* **Excepciones:** *Gestionar las situaciones donde la implementación no es posible*

Debido a problemas de coordinación, falta de personal y otros requerimientos operacionales, no todas las políticas pueden ser cumplidas de la manera que se pensó al comienzo. Por esto, cuando los casos lo ameriten, es probable que se requieran excepciones a la política para permitir a ciertas oficinas o personas el no cumplimiento de la política. Debe establecerse un proceso para garantizar que las solicitudes de excepciones son registradas, seguidas, evaluadas, enviadas para aprobación o desaprobación, documentadas y vigiladas a través del periodo de tiempo establecido para la excepción. El proceso también debe permitir excepciones permanentes a la política al igual que la no aplicación temporal por circunstancias de corta duración.

* **Concienciación:** *Garantiza la concienciación continuada de la política*

La etapa de concienciación de la fase de mantenimiento comprende los esfuerzos continuos realizados para garantizar que las personas están conscientes de la política y buscan facilitar su cumplimiento.

Esto es hecho al definir las necesidades de concienciación de los diversos grupos de audiencia dentro de la organización (directivos, jefes de dependencias, usuarios, etc.); en relación con la adherencia a la política, determinar los métodos de concienciación más efectivos para cada grupo de audiencia (es decir, reuniones informativas, cursos de entrenamiento, mensajes de correo, etcétera); y desarrollo y difusión de material de concienciación (presentaciones, afiches, circulares, etc.).

La etapa de concienciación también incluye esfuerzos para integrar el cumplimiento de la política y retroalimentación sobre el control realizado para su cumplimiento. La tarea final es medir la concienciación de los miembros de la comunidad universitaria con la política y ajustar los esfuerzos de acuerdo con resultados de las actividades medidas.

* **Monitoreo:** *Seguimiento y reporte del cumplimiento de la política.*

Durante la fase de mantenimiento, la etapa de monitoreo es realizada para seguir y reportar la efectividad de los esfuerzos en el cumplimiento de la política. Esta información se obtiene de la observación de los docentes, estudiantes, empleados y los cargos de supervisión, mediante auditorias formales, evaluaciones, inspecciones, revisiones y análisis de los reportes de contravenciones y de las actividades realizadas en respuesta a los incidentes. Esta etapa incluye actividades continuas para monitorear el cumplimiento o no de la política a través de métodos formales e informales y el reporte de las deficiencias encontradas a las autoridades apropiadas.

* **Garantía de cumplimiento:** *Afrontar las contravenciones de la política*

La etapa de garantía de cumplimiento de las políticas incluye las respuestas de la administración a actos u omisiones que tengan como resultado contravenciones de la política con el fin de prevenir que sigan ocurriendo. Esto significa que una vez una contravención sea identificada, la acción correctiva debe ser determinada y aplicada a los procesos (revisión del proceso y mejoramiento), a la tecnología (actualización) y a las personas (acción disciplinaria) involucrados en la contravención con el fin de reducir la probabilidad de que vuelva a ocurrir. Se recomienda incluir información sobre las acciones correctivas adelantadas para garantizar el cumplimiento en la etapa de concienciación.

* **Mantenimiento:** *Asegurar que la política esté actualizada*

La etapa de mantenimiento está relacionada con el proceso de garantizar la vigencia y la integridad de la política. Esto incluye hacer seguimiento a las tendencias de cambios (cambios en la tecnología, en los procesos, en las personas, en la organización, etcétera) que puede afectar la política; recomendando y coordinando modificaciones resultado de estos cambios, documentándolos en la política y registrando las actividades de cambio. Esta etapa también garantiza la disponibilidad continuada de la política para todas las partes afectadas por ella, al igual que el mantenimiento de la integridad de la política a través de un control de versiones efectivo. Cuando se requieran cambios a la política, las etapas realizadas antes deben ser re-visitadas, en particular las etapas de revisión, aprobación, comunicación y garantía de cumplimiento.

* **Verificación:** *Asegurar las acciones de mejoramiento de la política*

Después que la política ha logrado su fase de manteamiento, control y seguimiento se busca mejorar los procesos con acciones correctivas, preventivas y de mejora continua.

# ASIGNACIÓN DE RESPONSABILIDADES

## Nivel Gerencial

Gobernador, Secretarios de Despacho y/o Directores. Establece y mantiene el presupuesto, personal y todos los recursos para asegurar el cumplimiento de las políticas. Los responsables del nivel gerencial deben aprobar y publicar el documento que contenga las políticas de uso y administración de los Recursos Tecnológicos y de Comunicación según corresponda.

## Grupo De Tecnología, Conectividad Y Telecomunicaciones

**PROFESIONAL ESPECIALIZADO**: Participar, Asesorar y coordinar con el Gobernador del Departamento en la fijación de políticas y estrategias tendientes a articular las políticas del Gobierno Departamental con las fijadas por el Gobierno Nacional en lo relacionado con la implementación y desarrollo de las Tecnologías de la información y las Telecomunicaciones TIC

**PROFESIONAL UNIVERSITARIO:** Apoyar a la institución con los conocimientos profesionales de tal manera que los recursos tecnológicos e informáticos funcionen adecuadamente para que los objetivos de la institución se cumplan.

**TÉCNICO OPERATIVO:** Apoyar, Aplicar y adaptar tecnologías de Redes y sistemas de información que sirvan de apoyo al desarrollo de las actividades propias de la dependencia y del cargo y al cumplimiento de las metas propuestas.

Participar en la planeación, la programación, la organización, la ejecución, el seguimiento y la evaluación de las actividades propias del cargo y del área de desempeño y elaborar e interpretar cuadros, informes, estadísticas y datos concernientes al área de desempeño.

**CONTRATISTA:** Prestar los servicios profesionales para la asistencia a usuarios, administración y apropiación del Sistema de Gestión de Comunicaciones Oficiales, correo corporativo y sistema de mensajería interna. Prestación de servicios profesionales de apoyo bajo los parámetros establecidos por la coordinación del Grupo de Tecnología, Conectividad y Telecomunicaciones, para adelantar todas las actividades que aseguren el desarrollo y la gestión del TIC de la Gobernación del Huila

**SOPORTE TÉCNICO:**

1. Efectuar una evaluación inicial uno a uno de todos los equipos de cómputo objetos de mantenimiento y cambiar en el transcurso repuesto y elementos dañados, de acuerdo a la disponibilidad de partes que existan.

2. Apoyar y brindar un buen manejo al Sistema de Infraestructura informática (Gestión de IT DEXON SOFTWARE) y la administración help desk, mediante la revisión, mantenimiento preventivo y correctivo de los equipos que se encuentran en la Gobernación del Huila, como también a los equipos que ingresen en el transcurso del desarrollo del contrato incluidos y bajo la responsabilidad y custodia de las Secretaria General, de Educación, Cultura, Salud, Asamblea y conservatorio departamental.

3. Instalar dispositivos de red, configurar y controlar la red y los diferentes enlaces inalámbricos con el fin de ofrecer alta disponibilidad y desempeño, administrando las fallas y solucionando incidentes que se presenten manteniéndola eficientemente y segura.

4. Apoyar a la administración con mínimo dos computadores para soporte y respaldo de sus técnicos dentro de las dependencias de la Gobernación.

5. Garantizar que la red regulada sea estable, segura confiable e integra, con capacidad de efectuar cambios permanentes de acuerdo a los requerimientos de la administración, Secretaria del Salud, Cultura, Educación y Conservatorio.

## Proveedores De Redes

**SISTEMAS DESARROLLOS SYMDE S.A.S:** Prestar los servicios profesionales de apoyo a la Secretaría General, Secretaría de Educación y Secretaría de Salud en la administración y seguridad informática del ambiente de TIC constituido por software de plataforma Microsoft, Linux, bases de datos MS-SQL.Oracle y sistemas de virtualización.

**E&T DESARROLLOS LTDA:** Prestación de servicios para el soporte y asistencia técnica de la extranet corporativa y el sistema de comunicaciones oficiales de la Gobernación del Huila.

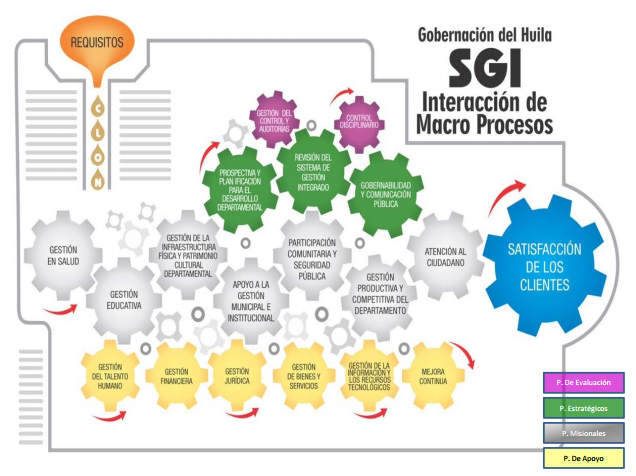
**TECNOMUSIC** Realizar el mantenimiento preventivo, correctivo y dar soporte técnico a todos los computadores, impresoras, periféricos informáticos, UPS y red regulada pertenecientes a la Gobernación del Huila nivel central, en las áreas dependientes de las Secretarías General, de Salud, de Educación y de Cultura incluyendo el suministro de repuestos que se requiera

**PLANTA TELEFONICA:** Prestar el servicio de apoyo a la gestión garantizando el correcto funcionamiento de la planta telefónica (teléfonos y fax) de la Administración Central Departamental, mediante el mantenimiento preventivo y correctivo de los mismos.

# ESTRUCTURA DE SISTEMA DE GESTIÓN

## Mapa De Procesos

Las actividades de la **Gobernación del Huila** se encuentran organizadas en procesos, cuya secuencia e interacción conforma el Mapa de procesos del Sistema de Gestión Integrado. Estos procesos se encuentran clasificados en:



# INFORMACIÓN GENERAL DE LA GOBERNACIÓN DEL HUILA

## Visión

En el año 2020 el Huila será el corazón verde de Colombia, pacífico, solidario y emprendedor; líder de una región dinámica donde florecen los sueños de todos'

## Misión

El Departamento, como ente coordinador y articulador, orientará su desarrollo social, económico, político y ambiental, con enfoque sostenible, humanista e Integrado, asumido con perspectiva de futuro, como respuesta a las necesidades y expectativas de sus habitantes, en el reconocimiento de su identidad como pueblo, en un ambiente de respeto mutuo y tolerancia para garantizar soluciones eficaces a la problemática de la región.

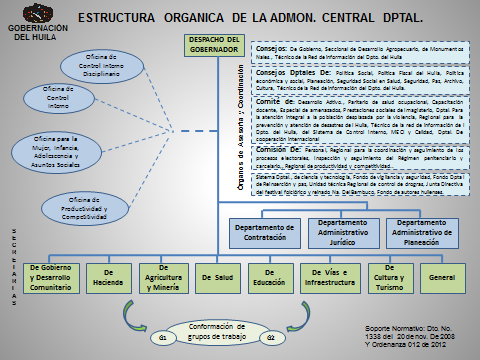
## Objetivos Del Sistema De Gestion

Conforme a la Política de gestión Integral, se han formulado los siguientes objetivos Integrales:

1. Incrementar el nivel de eficacia de planes, programas y proyectos de la Gobernación.
2. Incrementar el nivel de eficiencia en el uso de los recursos asignados.
3. Incrementar la confiabilidad y oportunidad de la información.
4. Incrementar la oportunidad y calidad en el suministro de recursos
5. Fortalecer competencias técnicas y organizacionales del talento humano para facilitar el cambio cultural en la Gobernación
6. Mejorar la oportunidad y calidad de servicio al cliente.

# AUTORIDAD Y RESPONSABILIDAD

## Organigrama De La Gobernación Del Huila



## Manual De Funciones

* **GOBERNADOR**

El Gobernador del Departamento del Huila, ante el Sistema de Gestión Integrado es responsable de:

* Revisar periódicamente que el desempeño del sistema de Gestión Integrado se facilite, mediante el logro de los objetivos afines a su gestión, asegure el conocimiento de la Gobernación y contribuya al mejoramiento del desempeño de los procesos.
* Nombrar el Representante de la Dirección y Gerente del Sistema de Gestión Integrado, para garantizar su operatividad.
* Asignar los recursos necesarios para el buen desempeño del Sistema de Gestión
* La determinación y comunicación del código para los acuerdos, compromisos o protocolos éticos.
* Mantener el estilo de dirección orientado a las necesidades de los grupos de interés y hacia los fines esenciales del estado.
* **SECRETARIOS DE DESPACHO, DIRECTORES DE DEPARTAMENTO Y JEFES DE OFICINA**

Como dueños de procesos, son responsables de:

* Cumplir y hacer cumplir los programas y planes establecidos en el sistema de gestión Integrado.
* Realizar las actividades de control necesarias para garantizar la prevención de eventos de pérdida que incidan adversamente en los objetivos de la Gobernación y el desempeño mismo de los procesos.
* Mantener permanente retroalimentación a los procesos mediante la implementación de acciones correctivas, preventivas y oportunidades de mejora.
* Determinar, efectuar seguimiento y hacer cumplir los planes de acción del Plan de desarrollo, así como para el levantamiento de las no conformidades identificadas.
* Administrar los riesgos determinados en los procesos, que están bajo su responsabilidad.
* **FUNCIONARIOS**

Todos los funcionarios de la **Gobernación del Huila** tienen la responsabilidad:

* Implementar lo establecido en los documentos propios del Sistema de Gestión Integrado y las herramientas que lo integran.
* Ayudar en la detección de no conformidades potenciales y reales, en la determinación de sus causas y en el desarrollo de los planes de acción determinados para su levantamiento.
* Tener presente los principios del Calidad y MECI que soportan el Sistema de Gestión Integrado, conforme a lo establecido en el presente manual de Gestión Integrado.
* Efectuar acciones correctivas, preventivas, de mejora y autocontrol de sus procesos.

## Sistema De Comunicación Formal En La Gobernación

Para asegurar la oportuna comunicación en la Gobernación del Huila, se han establecido como esquemas de comunicación los siguientes:

* Prensa, radio, televisión.
* Mesas de trabajo con la comunidad
* Consejos comunitarios
* Mensajero interno
* Internet
* Extranet
* Mensajero interno
* Página Web
* Correo Institucional
* Publicidad Móvil: Volantes, Porta lapiceros, pendones, botones, carteleras
* Informes de Gestión
* Archivo Fotográfico

# CAPITULO 1: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

# POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA GOBERNACIÓN DEL HUILA

Para la Gobernación del Huila, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de ésta, acorde con las necesidades de los diferentes grupos de interés identificados.

Entendiendo la importancia de una adecuada gestión de la información, la entidad, mediante la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), busca establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad, asegurando la dirección estratégica mediante la compatibilidad de la Política de Seguridad y Privacidad de la Información y los objetivos de seguridad de la información, estos últimos correspondientes a:

* Minimizar el riesgo en las funciones más importantes de la entidad.
* Cumplir con los principios de seguridad y privacidad de la información.
* Cumplir con los principios de la función administrativa.
* Mantener la confianza de sus clientes, socios y empleados.
* Apoyar la innovación tecnológica.
* Proteger los activos tecnológicos.
* Establecer las políticas, procedimientos e instructivos en materia de seguridad y privacidad de la información.
* Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Gobernación del Huila.
* Garantizar la continuidad del negocio frente a incidentes.

A continuación, se establecen los principios de seguridad que la Administración ha decidido definir, implementar, operar y mejorar de forma continua, para soportar el Modelo de Seguridad y Privacidad de la Información de la Gobernación del Huila:

* Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
* La información generada, procesada o resguardada por los procesos de negocio de la Gobernación del Huila, su infraestructura tecnológica y activos, se protegerá del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
* La información creada, procesada, transmitida o resguardada por los procesos de negocio de la Gobernación del Huila se protegerá, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
* La Gobernación del Huila protegerá su información de las amenazas originadas por parte del personal, posibles errores o ataques intencionados.
* Las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos de la Gobernación del Huila serán protegidos.
* La operación de los procesos de negocio de la Gobernación del Huila será contralada, garantizando la seguridad de los recursos tecnológicos y las redes de datos.
* La Gobernación del Huila implementará acciones de mejora en los procedimientos de control de acceso a la información, sistemas y recursos de red.
* La Gobernación del Huila garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
* La Gobernación del Huila garantizará una mejora efectiva de su modelo de seguridad, a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información.
* La Gobernación del Huila garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
* La Gobernación del Huila garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

## Objetivo

Establecer el marco general de actuación para la implementación la política general de seguridad y privacidad de la información de la Gobernación del Huila, que deben seguir los funcionarios, colaboradores y terceros de la Gobernación del Huila, fortaleciendo el enfoque preventivo referente a la seguridad y privacidad de la Información, y garantizando su disponibilidad, integridad y confidencialidad, mediante la aplicación eficaz de controles que permitan la disminución de amenazas y vulnerabilidades asociadas a los activos de información de la entidad, y que pueden afectar o impedir el logro de los objetivos institucionales y estratégicos.

## Objetivos Específicos:

* Fomentar una cultura organizacional orientada hacia la seguridad y la privacidad de la información al interior de la Gobernación del Huila.
* Establecer las responsabilidades de la alta dirección, funcionarios, contratistas y usuarios en general con el Modelo de Seguridad y Privacidad de la Información (MSPI) de la Gobernación del Huila.
* Garantizar la asignación de recursos administrativos y financieros necesarios para alcanzar y mantener los objetivos del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Gobernación del Huila.
* Establecer los lineamientos mínimos necesarios para dar cumplimiento a los estándares que conforman el Sistema Integrado de Gestión -MIPG- de la Gobernación del Huila.

## Alcance

Esta política aplica a todo el personal de la Gobernación del Huila sus funcionarios, contratistas, aprendices, practicantes, proveedores, ciudadanía, y en general a aquellas a todo aquel que en razón del cumplimiento de sus funciones y las de la entidad, compartan, utilicen, recolecten, procesen, intercambien o consulten su información creada, procesada o utilizada por la Administración, sin importar el medio, formato, presentación o lugar en el que se encuentre.

Aplica además a los entes de control y entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación.

# CAPITULO 2: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

# RESPONSABILIDADES EN MATERIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El grupo interno de trabajo denominado **Grupo de Tecnología, Conectividad y Telecomunicaciones de la Secretaría General**, en su calidad de tal, responde ante el Gobernador del Huila, por la existencia, gestión y cumplimiento legal de la Seguridad y Privacidad de la Información, acorde con las necesidades de la Entidad y los recursos disponibles.

**Coordinador del Grupo de Tecnología, Conectividad y Telecomunicaciones**

* Es el responsable de la definición, gestión de implementación y difusión al interior de la Entidad, del Modelo de Seguridad y Privacidad de la Información.
* Es el responsable de velar por el cumplimiento y actualización de la política general de seguridad y privacidad de la información y sus políticas específicas.
* Es el responsable de velar por la implementación de los controles de seguridad y privacidad de la información.
* Es el responsable de gestionar y analizar periódicamente los riesgos de seguridad existentes y proponer soluciones que fortalezcan la seguridad y privacidad de la información en la Entidad.
* Es el responsable de gestionar los incidentes de seguridad y recomendar acciones preventivas y correctivas para evitar afectaciones al interior de la Entidad.
* Es el responsable de la gestión para la divulgación de la seguridad y privacidad de la información.

**Comité Institucional de Gestión y Desempeño**

La Gobernación del Huila a través, del Comité Institucional de Gestión y Desempeño tendrá las funciones relacionadas a continuación y que son requeridas para la implementación y gestión del Modelo de Seguridad y Privacidad de la Información (MSPI):

* Tiene por responsabilidad de asesorar al Gobernador del Huila, en temas de seguridad de la información coordinadamente con el Responsable de Seguridad, el **Coordinador del Grupo de Tecnología, Conectividad y Telecomunicaciones**.
* Monitorear los incidentes de seguridad y establecer acciones preventivas y correctivas para evitar afectaciones al interior de la Entidad.
* Gestionar las actividades de planeación, implementación, seguimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información.
* El **Comité de Seguridad** (cuyas funciones son asumidas por el Comité Institucional de Gestión y Desempeño, mediante Decreto Departamental No. 0364 del 21 de agosto de 2018) deberá realizar un proceso continuo de revisión y aprobación de las políticas de seguridad y privacidad de la Información con el fin de mantenerlas actualizadas, vigentes y operativas para asegurar su permanencia y apropiación por parte de todos los colaboradores.

## Cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán conocer, y cumplir esta y todas las políticas y buenas prácticas de seguridad y privacidad de la información. El incumplimiento a la política de Seguridad y Privacidad de la Información, a las políticas específicas y demás lineamientos, buenas prácticas de seguridad, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al gobierno nacional y territorial en cuanto a seguridad y privacidad de la información se refiere.

# POLÍTICAS DE USO DE LOS RECURSOS TECNOLOGICOS, INFORMATICOS Y TELECOMUNICACIONES DE LA GOBERNACIÓN DEL HUILA

## Documentación De Las Políticas De Seguridad Y Admiinstración

La documentación de las Políticas de Seguridad y administración se realiza con el fin de proporcionar dirección y apoyo gerencial a todos los procesos y procedimientos que realiza el Grupo de Tecnología, Conectividad y Comunicaciones a nivel técnico.

Se debe establecer una dirección política clara y demostrar apoyo y compromiso con respecto a la seguridad de la información, mediante la formulación y mantenimiento de una política de seguridad y administración de la plataforma tecnológica a través de toda la organización.

## Asignación De Responsabilidades En Materia De Seguridad Y Adminstración De La Plataforma Tecnologica

Para la utilización adecuada de los recursos de tecnología informática (computadores personales, servidores, dispositivos y medios de comunicación entre otros), de forma que se garantice la aplicación de las políticas implementas, es necesario disponer de una estructura funcional, con base en la asignación de responsabilidades, pueden verse implicadas en:

- Nivel Gerencial: Gobernador, secretarios de Despacho y/o directores. Establece y mantiene el presupuesto, personal y todos los recursos para asegurar el cumplimiento de las políticas, debe existir una clara dirección y apoyo manifiesto del nivel gerencial a las iniciativas de seguridad.

Los responsables del nivel gerencial deben aprobar y publicar el documento que contenga las políticas de seguridad y administración, comunicarlo a todos los funcionarios, según corresponda. Este debe poner de manifiesto su compromiso y establecer el enfoque de la Organización con respecto a la gestión de la seguridad y administración de la plataforma tecnológica. Como mínimo, dicho documento debe estar acompañado de las siguientes pautas:

* Una declaración del propósito de los responsables del nivel Gerencial, apoyando los objetivos y principios de la seguridad de la Información y la administración de la plataforma tecnológica.
* El compromiso que la política debe ser comunicada a todos los usuarios de la Organización de manera pertinente, accesible y comprensible.
* Administradores de redes y sistemas. Es el personal encargado de identificar requerimientos de seguridad, evaluar los riesgos que enfrenta la Organización, de elaborar, implementar estándares o conjunto especifico de principies para la administración de la seguridad, proyectar las políticas para cada sistema sobre el que tienen responsabilidades asignadas, presentan informes de los sistemas de seguridad, hacer seguimiento y asegurar el cumplimiento de las políticas entre otras actividades; en la Gobernación del Huila estas responsabilidades estarán a cargo del Grupo de Tecnología, Conectividad y Comunicaciones perteneciente a la Secretaria General.
* El ente regulador en materia de informática y comunicaciones será el Grupo Informática y de Telecomunicaciones, con el aval del secretario general.
* Las normas y directrices en materia de informática que tengan aplicabilidad en la Administración Departamental, serán acogidas, diseñadas dirigidas e implementadas al interior de la Gobernación del Huila bajo el liderazgo del Grupo de Tecnología, Conectividad y Comunicaciones
* Los Administradores de redes y sistemas deben ser los encargados de la proyección y actualización del documento que contenga las políticas y procedimientos de administración de la plataforma tecnológica de la Organización.
* Usuarios finales. Comprende a todos los funcionarios que tienen acceso a los sistemas y servicios corporativos de la administración departamental, deben tener un cabal cumplimiento de las políticas de seguridad implementadas.
* Los Usuarios finales deben conocer y cumplir cabalmente el documento que contenga las políticas y procedimientos de administración de la plataforma tecnológica de la Organización una vez sea publicado.

## Asignación De Responsabilidades En Materia De Seguridad Y Adminstrración De La Plataforma Tecnologica Dentro Del Grupo De Tecnologia, Conectividad Y Comunicaciones.

El Grupo de Tecnología, Conectividad y Comunicaciones en cuestión es el encargado de identificar y definir claramente y minuciosamente los diversos recursos y servicios con los que cuenta la Gobernación del Huila. Una vez identificados se debe designar un responsable de cada recurso, servicio o proceso de seguridad y se deben documentar claramente los detalles y tareas de esta responsabilidad. Es esencial que se establezcan claramente las áreas sobre las cuales es responsable cada miembro del grupo.

La asignación de funciones de seguridad y responsabilidades dentro la Organización debe complementarse, cuando corresponda, con una guía más detallada para sitios, sistemas, recursos o servicios específicos, estas guías deben plasmarse de forma obligatoria.

Se debe asignar a un miembro del Grupo de Tecnología, Conectividad y Comunicaciones la responsabilidad general por el desarrollo e implementación de la seguridad y por el soporte a la identificación de controles de toda la Plataforma. No obstante, la responsabilidad por la reasignación e implementación de controles puede ser retenida y propuesta por cada uno de los miembros responsables de un recurso o servicio específico en coordinación directa con el responsable General de la Seguridad.

Los niveles de autorización deben ser claramente definidos y documentados. Los responsables de los recursos tecnológicos específicos (funcionario que pertenece al Grupo de Tecnología, Conectividad y Comunicaciones) pueden delegar sus responsabilidades de seguridad, administración y ejecución a proveedores y prestadores de servicios si fuera el caso. No obstante, el responsable asignado es en último término responsable de la seguridad y administración del recurso y debe estar en capacidad de determinar si las responsabilidades delegadas fueron cumplidas correctamente. (En último término, el usuario designado del activo debe rendir cuentas por el mismo).

Una vez asignadas todas las responsabilidades dentro del Grupo de Tecnología, Conectividad y Comunicaciones es obligación informar a toda la Organización legalmente los nombres de los responsables de la administración de determinado recurso, logrando así establecer el conducto regular en la prestación de los servicios a los funcionarios.

## Perfil Y Funciones De Los Administradores De La Red De La Gobernación Del Huila

El perfil o administrador de la Red de la Gobernación del Huila se caracteriza por poseer conocimientos en mantenimiento del hardware y el software. El Administrador de la red, identificará problemas en el funcionamiento logrando a partir de los recursos del sistema que opera obtener información sobre velocidades, respuesta, números de usuarios conectados, suspensiones, correo electrónico entre otras particularidades. De esta forma podrá reportar el desempeño de la red y adoptar las soluciones necesarias propias del sistema que se llevarán a cabo por el profesional o administrador de la red en la entidad, trabajando con el apoyo constante de los técnicos que soportan su servicio del mantenimiento técnico.

La finalidad del Administrador de red es la de compartir información y recursos tecnológicos operándolo bajo un ambiente de servicio de sistema operativo que permita hacer más efectivos los propósitos de red de la organización.

El administrador de red está a cargo de implementar medidas de protección adecuadas, supervisar los registros de actividades y controlar las alertas de seguridad. Para anticiparse a peligros posibles, debe implementar un plan de recuperación definiendo lo que se debe hacer para reestablecer el acceso lo antes posible, de acuerdo con la política de seguridad de la entidad.

Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos, hacer uso eficiente de la red y utilizar mejor los recursos, como, por ejemplo, el ancho de banda, detección de fallas, diagnóstico del problema, recuperación, seguimiento, control y monitoreo de redes.

El administrador de la Red debe realizar mantenimiento a los diferentes Rack de comunicación conservándolos en buen estado, orden y limpieza. Además de sugerir y efectuar los cambios que sean necesarios al interior de los dispositivos de red de la administración.

Instalar dispositivos de red, configurar y controlar la red y los diferentes enlaces inalámbricos con el fin de ofrecer alta disponibilidad y desempeño, administrando las fallas y solucionando incidentes que se presenten manteniéndola eficiente y segura.

Organizar el cableado, marcación, prueba de fibra certificada y los cambios cuando sean necesarios, llevando los respectivos registros.

Presentar reportes mensuales del monitoreo de todos los dispositivos de red de la administración tales como: Routers, Acces Point, Switches, Enlaces inalámbricos, en el cual deberá reportase los tiempos de servicio de cada uno de los elementos monitoreados con sus respectivos soportes.

El administrador de red debe conocer las claves de las máquinas que administra. Desde estas puede configurar servicios y establecer políticas que afectaran a todos los usuarios. Algunas de las labores que debe poder realizar en esta estación de trabajo o cuenta de usuario son:

* Apagar el equipo
* Configurar los programas que se inician junto con el sistema.
* Administrar cuentas de usuarios.
* Administrar los programas y la documentación instalada.
* Configurar los programas y los dispositivos.
* Configurar la zona geográfica, fecha y hora.
* Administrar espacio en discos y mantener copias de respaldo.
* Configurar servicios que funcionaran en red.
* Solucionar problemas con dispositivos o programas.
* Revisar bitácoras solucionar y prevenir inconvenientes de seguridad.

La administración, mantenimiento, desarrollo, operación y análisis de desempeño de la red corporativa de datos, están bajo la responsabilidad de profesionales universitarios y administradores de la red adscritos al Grupo de Tecnología, Conectividad y Comunicación.

# CAPITULO 3: CONTROL Y GESTIÓN DE ACTIVOS

# USO, CLASIFICACIÓN Y CONTROL DE ACTIVOS DE TI

## Responsabilidad Por Rendición De Cuentas De Los Activos

Se debe rendir cuentas por todos los Recursos Informáticos y Tecnológicos de la Gobernación del Huila, con apoyo del Grupo de Tecnología, Conectividad y Telecomunicaciones el cual tiene la facultad de asignar responsabilidades en materia de administración y seguridad de cada uno de ellos, por tal razón cada funcionario es responsables del uso y protección del equipo (s), obligación contemplada en las políticas de la entidad.

La rendición de cuentas por los activos (tangibles e intangibles) ayuda a garantizar que se mantenga una adecuada protección. Se deben identificar a los responsables para todos los activos importantes y se debe asignar la responsabilidad por el mantenimiento de los controles apropiados.

## Inventarios De Activos

Los inventarios de activos ayudan a garantizar la vigencia de una protección eficaz de los recursos, y también pueden ser necesarios para otros propósitos de la empresa, como los relacionados con sanidad y seguridad, toma de decisiones, informes de estado de los activos, seguros o finanzas (administración de recursos). El proceso de compilación de un inventario de activos es un aspecto importante de la administración de riesgos.

Una Organización debe contar con la capacidad de identificar sus activos y el valor relativo e importancia de los mismos. Sobre la base de esta información, la entidad puede entonces, asignar niveles de protección proporcionales al valor e importancia de los activos.

Se debe elaborar y mantener un inventario de los activos importantes asociados a cada sistema de información y recursos tecnológicos. Cada activo debe ser claramente identificado y su funcionario a cargo. El inventario debe contener los datos de los siguientes activos:

a) Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información perdida ("fallback"), información archivada.

b) Recursos de software: software de aplicaciones, software de sistemas (Licencias de sistemas operativos y programas), herramientas de desarrollo y utilitarios.

c) Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems, servidores), equipos de comunicaciones (Routers, Switches, Máquinas de fax, equipos inalámbricos contestadores automáticos), medios magnéticos (cintas y discos), otros equipos técnicos (suministro de electricidad, unidades baterías, UPS).

d) Servicios utilizados en la plataforma.

e) Grabar y marcar todos los números de serie de los recursos informáticos pertenecientes a la Gobernación del Huila, para indicar quien es el propietario al usuario al que se le asignó el recurso.

## Clasificación De La Informacón

**Objetivo:** Garantizar que los recursos de información reciban un apropiado nivel de protección.

La información debe ser clasificada para señalar la necesidad, las prioridades y el grado de protección. La información tiene diversos grados de sensibilidad y criticidad. Algunos ítems pueden requerir un nivel de protección adicional o un tratamiento especial. Se debe utilizar un sistema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de tratamiento especial.

Se deben clasificar los recursos más importantes en materia de información y de esta forma poder señalar como va a ser tratada y definir quienes tendrán acceso a ella. La clasificación debe hacerse de acuerdo al grado de sensibilidad para la Organización.

La responsabilidad por la definición de la clasificación de un ítem de información, por ejemplo, un documento, registro de datos, archivo de datos, y por la revisión periódica de dicha clasificación, debe ser asignada al propietario designado de este recurso de información.

# METODOLOGÍA DE GESTÓN DE ACTIVOS DE SEGURIDAD DIGITAL

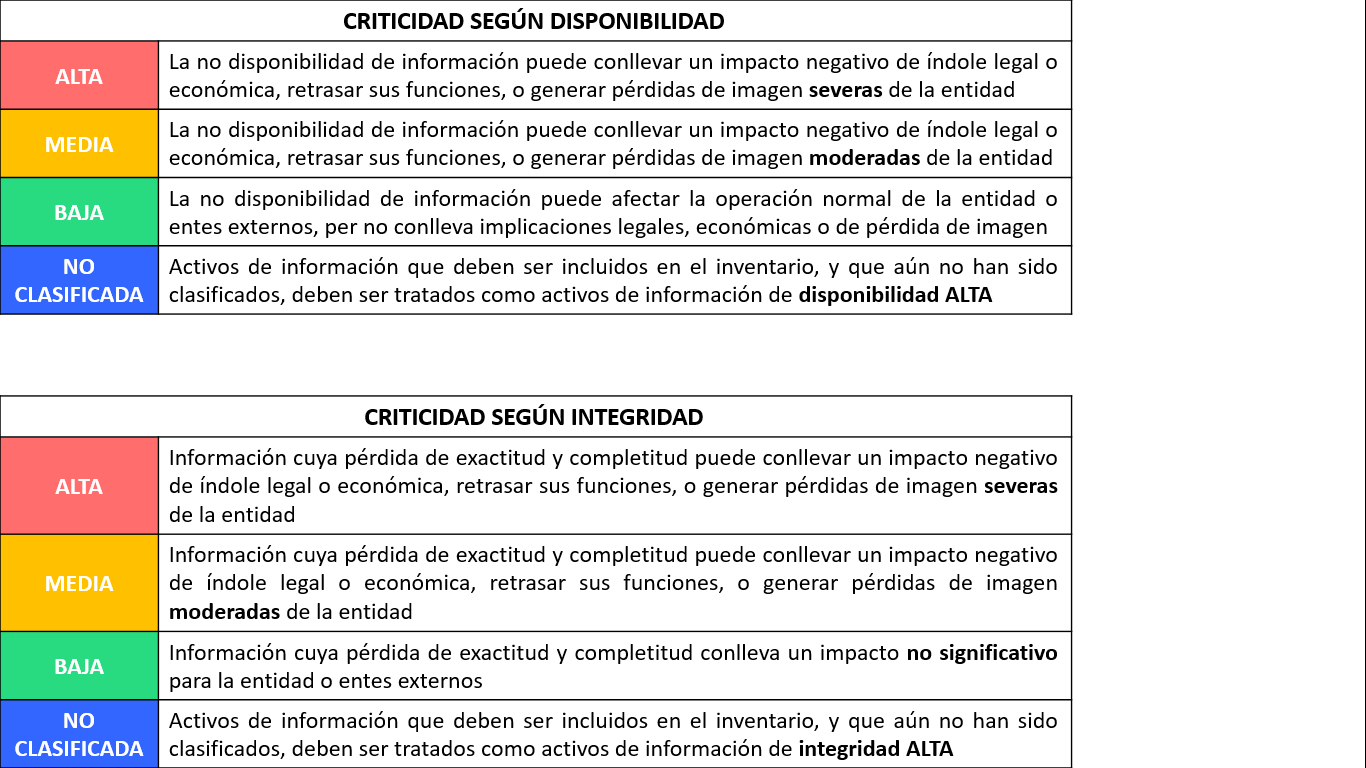
La Gobernación del Huila, adoptando los lineamientos establecidos por el Departamento Administración de la Función Pública, en la “*Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas”*, *Versión 5 de diciembre de 2020*, y en el anexo 4 “*Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas*”, ha establecido la siguiente metodología, a fin de gestionar sus activos de seguridad digital:

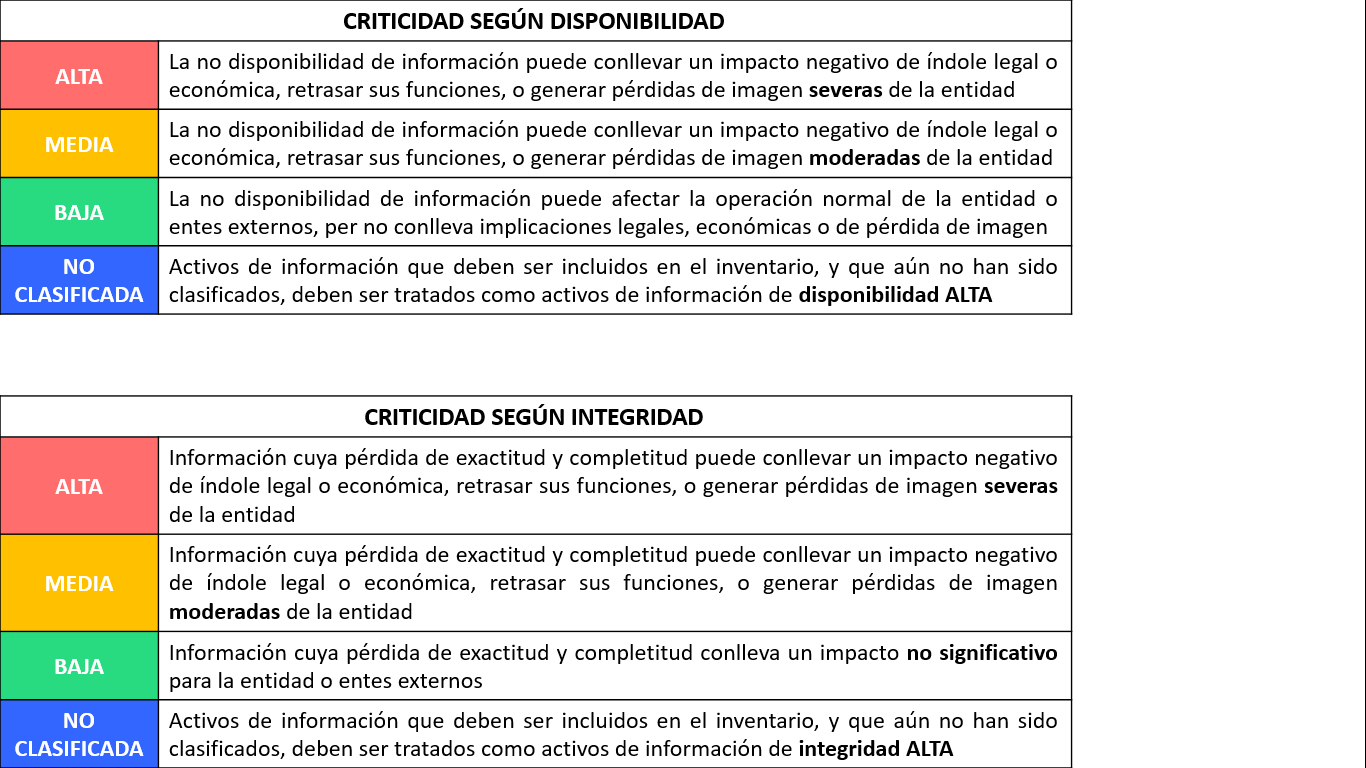
## Diagnóstico De Activos

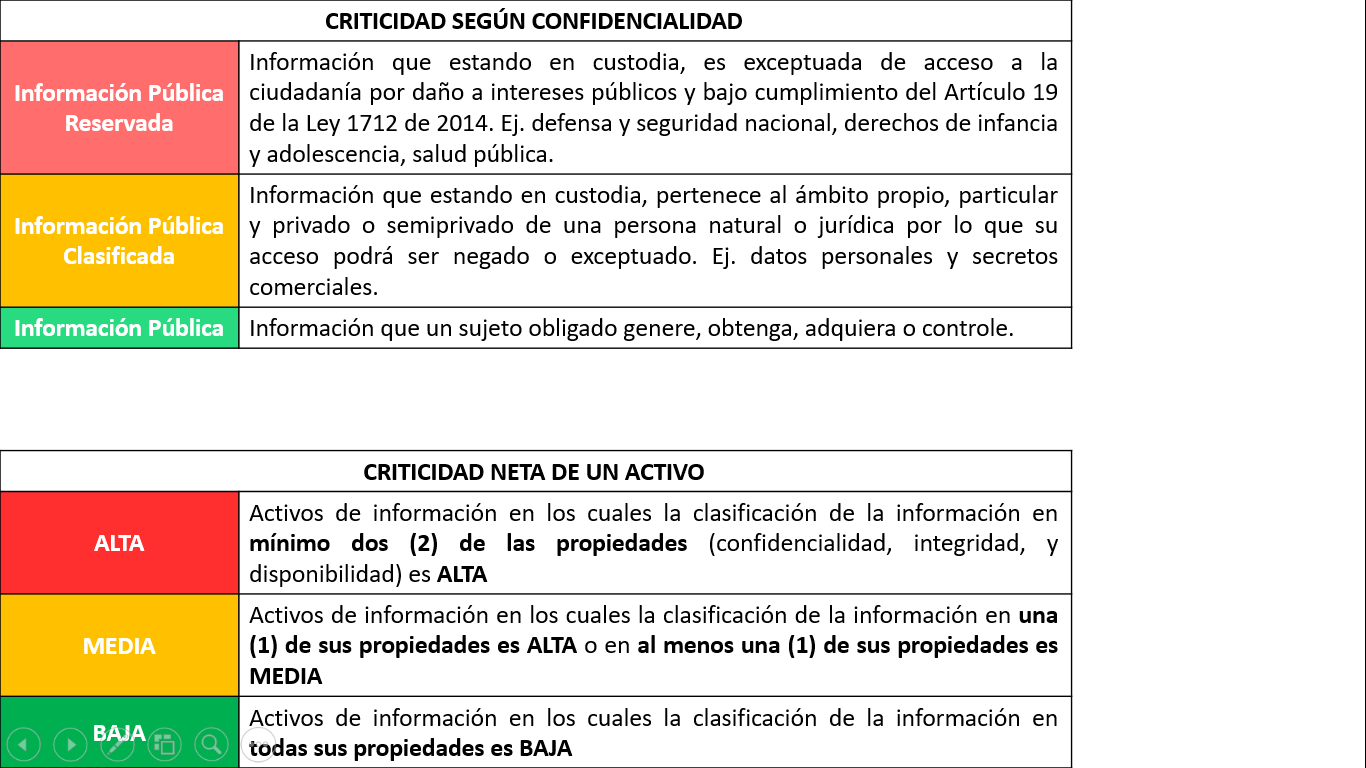
Es necesario identificar los activos de TI y documentarlos mediante un inventario de activos, así podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (FrontOffice), aumentando así su confianza en el uso del entorno digital para interactuar con el Estado. Lo anterior se realiza mediante encuestas y entrevistas con funcionarios líderes de procesos de gestión de la entidad. Se clasifican y cuantifican según funcionalidades, y se valoran según criterios de la norma técnica ISO/IEC 27001:2013, evaluando de manera acertada cada una de las dimensiones de seguridad para cada activo. Esta información se recopiló en un cuadro denominado “*Matriz de Identificación de Activos de Seguridad Digital*”, diseñado en formato de archivo xlsx -basado en el Modelo de Seguridad y Privacidad de la Información del MinTIC, y en el que se incluyen una serie de pasos que permiten realizar una valoración de cada activo- de forma que se facilitara su integración a la metodología de gestión de riesgos de la entidad, y su uso por parte de personal de la Coordinación del Sistema Integrado de Gestión.



* **Paso 1 - Listar activos:** Se listan los activos de seguridad digital, correspondientes a los activos de TI que se identifican en cada proceso de gestión, indicando nombre y descripción breve de cada uno.
* **Paso 2 - Identificar tipo de activo:** Cada activo se clasifica en un determinado grupo de activos según su naturaleza cómo sigue a continuación: Información, Software, Hardware, Servicios, Intangibles, Componentes de Red, Personas, Instalaciones.
* **Paso 3 - Identificar dueño del activo:** Cada uno de los activos identificados debe tener un dueño designado, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.
* **Paso 4 - Identificar custodio del activo:** Cada uno de los activos identificados debe tener una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que posteriormente se definan.
* **Paso 5 - Clasificar activo según criticidad:** Se realiza la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable. Posteriormente se evalúa la criticidad de los activos, determinando el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada de cada caso. Teniendo en cuenta lo anterior, se plantean las siguientes escalas valorativas para determinar la criticidad del activo en cada una de sus propiedades.
* **Paso 6 - Determinar nivel de criticidad neta del activo:** Se indica el nivel de criticidad neta del activo, con base en el resultado de la criticidad en cada una de sus propiedades.
* **Paso 7 y 8 - Identificación de Amenazas y Vulnerabilidades:** Existen diversos lineamientos y estándares como la Norma Técnica ISO/IEC 27005 y MAGERIT, que muestran posibles amenazas y vulnerabilidades que pueden materializar los tres tipos de riesgos de seguridad digital (pérdida de confidencialidad, pérdida de integridad, pérdida de disponibilidad). En este caso, se utiliza el cuadro denominado “*Matriz de Identificación de Activos de Seguridad Digital*”, en el que a partir del paso 7, se identifican las diferentes amenazas que, según su origen, pueden llegar a afectar el activo identificado, y en el paso 8 las posibles causas que permitirían la materialización de estas amenazas, y las vulnerabilidades que presentan estos activos, y que pueden llegar a ser explotadas.







Texto, Carta

Descripción generada automáticamente

* **Paso 9 - Identificar infraestructuras críticas cibernéticas – ICC:** Se identifican y reportan a instancias y autoridades respectivas en el Gobierno nacional si la Gobernación del Huila posee ICC. Un activo es considerado infraestructura crítica cibernética si su impacto o afectación podría superar alguno de los siguientes 3 criterios: Impacto Social mayor a 250.000 personas (0,5% de Población Nacional), Impacto Económico mayor a $464.619.736 (PIB de un Día o 0,123% del PIB Anual), o Impacto Ambiental mayor a 3 años de recuperación.

Para esta identificación, se sigue utilizando el cuadro denominado “*Matriz de Identificación de Activos de Seguridad Digital*”, en el que, en el 9no paso, se indica si el activo corresponde a un activo de infraestructura crítica cibernética, y en el paso 10 se incluyen observaciones adicionales que se consideren relevantes sobre el activo para su análisis y diagnóstico.



# POLÍTICA DE DISPOSITIVOS MÓVILES

**Alcance:** Esta política aplica para toda la Administración Central Departamental de la Gobernación del Huila, todos sus funcionarios (personal de planta administrativa, personal de libre nombramiento y remoción, y contratistas de prestación de servicios), terceros, aprendices, practicantes, proveedores y ciudadanía en general, que ingresa a las instalaciones de la entidad, con dispositivos móviles electrónicos (celulares, equipos de cómputo portátiles, tabletas).

**Definiciones:**

***Dispositivo móvil:*** Elemento electrónico de tamaño pequeño, con capacidades de procesamiento de datos, conexión a Internet y memoria. Son ejemplos de estos: celulares, equipos de cómputo portátiles, tabletas.

***Personal:*** Es aquella persona que tiene una relación con la Gobernación del Huila de forma directa o a través de un tercero, bajo cualquier tipo de vinculación: planta, contratistas, proveedores, estudiantes en práctica, etc.

**Objetivo:** Establecer lineamientos para gestionar el uso correcto de los dispositivos móviles corporativos y personales en las instalaciones de la Gobernación del Huila y entes descentralizados beneficiarios.

**Responsabilidades:**

* Alta dirección (Secretarios de Despacho, Directores de Departamentos, Jefes de Oficinas Asesoras)
* Reportar al área de Almacén (Líder de Recursos Físicos) los funcionarios responsables de todos y cada uno de los dispositivos móviles corporativos asignados a la dependencia que lidera. En caso de que el responsable sea un contratista, deberá reportar el periodo de vinculación de éste, y el funcionario responsable del dispositivo una vez finalizado el contrato.
* Notificar al Grupo de Tecnologías, Conectividad y Telecomunicaciones (Grupo TIC) la asignación de los dispositivos móviles corporativos a funcionarios de la entidad ya sea de planta administrativa o contratistas, con el fin de realizar la asignación de usuario de dominio, y demás verificaciones y configuraciones que sean necesarias y pertinentes, de acuerdo con lo expuesto en políticas y lineamientos de uso de recursos y servicios tecnológicos de la entidad.
* En caso de que el dispositivo móvil sea asignado a un contratista, se debe notificar al supervisor del contrato, para que éste realice el respectivo seguimiento a la información gestionada a través de este dispositivo, y solicite al contratista el respectivo backup o copia de respaldo de información de los archivos de gestión donde se relacione la documentación producida durante la ejecución del contrato, con el objetivo de garantizar la seguridad de la información y la continuidad de la operación de la dependencia, como se indica en las obligaciones de los respectivos contratos de prestación de servicios.
* Grupo de Tecnologías, Conectividad y Telecomunicaciones
* Verificar que las configuraciones y opciones de protección de los dispositivos móviles corporativos y personales que se adquieren en la entidad, y que hagan uso de los servicios tecnológicos provistos por la institución sean aceptables, acordes y alineadas con las políticas y lineamientos de uso de recursos y servicios tecnológicos de la entidad.
* Configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
* Llevar registro de los dispositivos móviles corporativos y personales que acceden a recursos y servicios tecnológicos de la Gobernación del Huila.
* Capacitar y concientizar a los funcionarios de la entidad respecto a la presente política de uso de dispositivos móviles, y al uso de éstos dentro y fuera de las instalaciones de la Gobernación.

**Responsabilidades de los usuarios:**

* Sobre dispositivos móviles corporativos
* El funcionario es el responsable del dispositivo móvil que se le ha facilitado para el desempeño de sus tareas fuera de las instalaciones corporativas. Por tanto, es el funcionario el que debe garantizar la seguridad, tanto del equipo como de la información que contiene.
* Evitar usar los dispositivos móviles asignados por la entidad, en lugares que no ofrezcan garantías de seguridad física necesarias para prevenir la pérdida o robo de éstos.
* Los dispositivos móviles que contiene información importante, sensible o crítica no deben ser desatendidos y, en lo posible, debe quedar resguardados bajo llave o se deben utilizar trabas o guayas especiales para asegurarlos.
* Sobre dispositivos móviles personales
* El funcionario es responsable de su dispositivo móvil personal, y de utilizarlo de acuerdo con las políticas para el uso de recursos y servicios tecnológicos de la Gobernación del Huila que le hayan sido autorizados.
* El funcionario es responsable por las reparaciones y soporte técnico que requiera su dispositivo móvil personal, los materiales y los costos que para ello sean necesarios.
* El funcionario es responsable de mantener actualizado el sistema operativo y de las aplicaciones en su dispositivo móvil personal, en especial, disponer de un antivirus que lo proteja de posibles ataques y accesos no autorizados, que puedan afectar los servicios tecnológicos de la Gobernación del Huila.
* El funcionario es responsable de las herramientas de software instaladas en su dispositivo móvil, licenciamiento y demás condiciones legales del uso del software instalado allí, dejando constancia que la legitimidad de las mismas son compromiso único y exclusivo del contratista, liberando de cualquier responsabilidad legal a la Gobernación del Huila.

**Directrices:**

* Sobre dispositivos móviles corporativos
* La alta dirección (secretarios de despacho, directores de departamentos administrativos, jefes de oficinas asesoras) es la única instancia autorizada para realizar solicitudes y asignación de dispositivos móviles corporativos de la entidad.
* Todo dispositivo móvil corporativo (portátil, celular o tableta) debe tener un funcionario responsable asignado y dicha asignación debe ser reportada al área de Almacén (Líder de Recursos Físicos) de la Gobernación del Huila.
* Los dispositivos móviles corporativos deberán contar con una contraseña que permita el acceso solo al funcionario responsable de éste.
* Los dispositivos móviles corporativos deben contar con un antivirus instalado y activo.
* Los dispositivos móviles no deben quedar expuestos a altas temperaturas que puedan dañar sus componentes.
* Registrar en la planilla de la empresa de vigilancia contratada por la entidad, el ingreso y salida de los dispositivos móviles corporativos a las diferentes sedes y edificaciones de la Gobernación del Huila, con su respectiva marca, modelo y serial.
* Los funcionarios que requieren acceso a recursos y servicios tecnológicos de la Gobernación del Huila a través de dispositivos móviles corporativos deben realizar la solicitud respectiva, de acuerdo con el Catálogo de Servicios TIC de la entidad, a través de la mesa de servicios del Grupo TIC (*correo electrónico* [*soporte.tic@huila.gov.co*](mailto:soporte.tic@huila.gov.co)*, o a la línea telefónica (8) 8671300 Extensión 1104*), para que se preste la atención y el soporte necesario. Lo anterior incluye también fallas, incidentes o requerimientos relacionados con inconvenientes técnicos de los equipos portátiles corporativos.
* Los funcionarios con dispositivos móviles corporativos bajo su responsabilidad deben realizar periódicamente copias de respaldo de la información, archivos y documentos almacenados y procesados en éstos.
* Los funcionarios no deben modificar las configuraciones de seguridad de los dispositivos móviles corporativos asignados, ni instalar programas o aplicaciones desde fuentes desconocidas que no correspondan con el desarrollo de sus funciones u obligaciones, ni desinstalar el software provisto con ellos al momento de su entrega. Solo el personal autorizado del Grupo TIC puede realizar estas labores, bajo solicitud expresa del funcionario y/o del jefe de la dependencia, y justificando la necesidad según el caso.
* Abstenerse de almacenar videos, fotografías o cualquier otro tipo de información personal en los dispositivos móviles corporativos asignados.
* Evitar hacer uso de redes inalámbricas de uso público en los dispositivos móviles corporativos, con el fin de evitar acceso y divulgación no autorizada de la información almacenada y/o procesada en ellos.
* En caso de pérdida, o hurto del dispositivo móvil corporativo asignado, o algún caso fortuito o fuerza mayor se haya presentado, se debe reportar inmediatamente al área de Almacén (Recursos Físicos) y a la mesa de servicios del Grupo TIC para que se trate como un incidente de seguridad de la información (*correo electrónico* [*soporte.tic@huila.gov.co*](mailto:soporte.tic@huila.gov.co)*, o a la línea telefónica (8) 8671300 Extensión 1104*), y seguidamente realizar la respectiva denuncia ante las autoridades competentes, para que se aplique el respectivo egreso y reposición del equipo, mediante procedimiento de Código SGN-C042-P810 “EGRESOS POR PERDIDA, HURTO, CASO FORTUITO Y FUERZA MAYOR” o el que sea definido en el proceso de Gestión de Recursos Físicos (Almacén).
* Participar en las jornadas de capacitación y sensibilización respecto a la presente política de dispositivos móviles, y en general las relacionadas con seguridad y privacidad de la información que realice la Gobernación del Huila.
* Sobre dispositivos móviles personales
* Los dispositivos móviles personales deben contar con un sistema operativo y aplicaciones actualizadas y en especial, contar con un antivirus activo y actualizado, que lo proteja de posibles ataques y accesos no autorizados, que puedan afectar eventualmente los servicios tecnológicos de la Gobernación del Huila.
* Registrar en la planilla de la empresa de vigilancia contratada por la entidad, el ingreso y salida de los dispositivos móviles personales a las diferentes sedes y edificaciones de la Gobernación del Huila, con su respectiva marca, modelo y serial.
* Evitar desatender los dispositivos móviles personales al interior de la entidad, para prevenir la pérdida o robo de éstos, así como de la información que contiene.
* En lo posible los dispositivos móviles personales deben quedar resguardados bajo llave o se deben utilizar trabas o guayas especiales para asegurarlos al interior de la entidad.
* La Gobernación del Huila no se hace responsable por pérdida o robo de dispositivos móviles personales al interior de la entidad.
* Solo los dispositivos móviles personales que sean registrados por el Grupo TIC podrán tener acceso a los diferentes recursos y servicios tecnológicos establecidos en el Catálogo de Servicios TI de la Gobernación del Huila.
* Los funcionarios y contratistas que requieren acceso a recursos y servicios tecnológicos de la Gobernación del Huila a través de dispositivos móviles personales deberán informar a sus supervisores, quienes deberán realizar la solicitud respectiva, de acuerdo con el Catálogo de Servicios TIC de la entidad, a través de la mesa de servicios del Grupo TIC (*correo electrónico* [*soporte.tic@huila.gov.co*](mailto:soporte.tic@huila.gov.co)*, o a la línea telefónica (8) 8671300 Extensión 1104*), para que se preste la atención y el soporte necesario. Lo anterior NO incluye fallas, incidentes o requerimientos relacionados con inconvenientes técnicos de los equipos portátiles personales.
* El acceso a portales web en internet a través de dispositivos móviles personales debe ser restringido con el fin de controlar el acceso de software y/o aplicaciones que puedan poner en riesgo la información sensible, confidencial y la infraestructura tecnológica de la Gobernación del Huila.
* En caso tal de que el funcionario y contratistas requiera acceder remotamente mediante dispositivos móviles o equipos personales, a sistemas de información que no cuenten con entornos web, y que gestionen información confidencial y sensible para la entidad, el jefe de la dependencia a la que se encuentra adscrito o vinculado deberá solicitar acceso seguro mediante una red privada virtual (VPN), que puede ser provista por el Grupo TIC de la entidad de acuerdo con la disponibilidad existente de licenciamiento, de modo que se asegure la confidencialidad de la información y las comunicaciones establecidas.
* Se prohíbe la conexión de dispositivos móviles portátiles de propiedad de funcionarios de la entidad, a la red cableada de la Gobernación del Huila. Estos dispositivos solo se podrán conectar a las redes inalámbricas WiFi, previa solicitud respectiva del servidor público, de acuerdo con el Catálogo de Servicios TIC de la entidad, a través de la mesa de servicios del Grupo TIC (*correo electrónico soporte.tic@huila.gov.co, o a la línea telefónica (8) 8671300 Extensión 1104*), para que se realice la conexión solicitada.
* Participar en las jornadas de capacitación y sensibilización respecto a la presente política de dispositivos móviles, y en general las relacionadas con seguridad y privacidad de la información que realice la Gobernación del Huila.

**Requerimientos mínimos:**

* Dispositivo móvil (celular, equipo de cómputo portátil, Tablet).
* Licenciamiento de sistema operativo y aplicaciones básicas.
* Licenciamiento de software antivirus.
* Aplicativo o herramienta de gestión de servicios de TI para la gestión de solicitudes de recursos y servicios tecnológicos que requieran los dispositivos móviles.
* Servicio de conectividad en red y conexión a internet en las instalaciones de la Gobernación del Huila.

# POLITICAS DE GESTION INFORMATICA

**Objetivo:**

* Preservar los lineamientos sobre lo que se considera el uso adecuado de los recursos tecnológicos asignados.

**Aplicabilidad:**

Estas son políticas que aplican a los usuarios (funcionarios, contratistas y cualquier otra persona o entidad) que por razón de su trabajo se le permita acceso o tenga relación con la Gobernación del Huila.

## Planeación

* La Gobernación del Huila dentro de su Plan de Desarrollo Departamental, planifica Estrategias administrativas en pro del cumplimiento de sus objetivos institucionales.

La Secretaría General en apoyo del Grupo de Tecnología, Conectividad y Telecomunicaciones debe contribuir a la consecución de dichos objetivos y metas propuestas, es por ello que diseña una planificación y proyección financiera anual de los Recursos Tecnológicos (equipos de cómputo, servidores, licencias, software entre otros), además del Recurso humano idóneo que requieren para desempeñar las labores de manera satisfactoria durante el año.

* El Grupo de Tecnología, Conectividad y Telecomunicaciones, son los encargados de realizar análisis y proyecciones (presupuestales, cálculos, soporte técnico) y además adiciones de ser necesarias para el cumplimiento de sus metas y objetivos en materia de Tecnología y Telecomunicaciones.
* La Gobernación del Huila debe llevar a cabo una planeación estratégica de tecnologías informáticas y de comunicaciones periódicamente considerando aspectos tales como: sistemas de información, los entes reguladores, la evaluación, la planeación, entre otros con el fin de estar a la vanguardia de las nuevas tecnologías y requisitos propios impuestos por entidades gubernamentales de alto nivel.
* Los sistemas de información serán el resultado de planes estratégicos de información, elaborados al comienzo de un periodo de gobierno y su terminación se da a la finalización del periodo de dicho gobierno.
* Los planes estratégicos de tecnologías informáticas y de comunicaciones deben ser evaluados y ajustados a la vigencia fiscal del periodo de gobierno.

## Adquisición Equipos

* La Gobernación del Huila acepta la utilización de diversas tecnologías informáticas, en sus distintos componentes de hardware, software y telecomunicaciones; siempre que exista compatibilidad entre las mismas, de tal manera que haya una integración entre ellas y faciliten las operaciones de los usuarios.
* La Gobernación del Huila en el año 2013, con el apoyo del Grupo de tecnología, Conectividad y Telecomunicaciones idéntico la necesidad de renovar mediante equipos nuevos a las dependencias más críticas, pero además planifico la reubicación de equipos existen para el aprovechamiento de estos, con el fin de ajustarlos a los requerimientos de la gobernación del Huila.
* Toda compra de Tecnología Informática debe tener el aval previo del Grupo de Tecnología, Conectividad y Telecomunicaciones, la forma de adquisición de los bienes tecnológicos debe ser el resultado de un estudio en donde la relación necesidad/costo/beneficio sea la variable determinante y cuenta con la total asesoría y respaldo del Grupo de Tecnología, Conectividad y Comunicaciones.
* El procedimiento para la compra de bienes y tecnología informática en general, debería ser establecido por el Grupo de Tecnología y Telecomunicaciones, garantizando obtener precios favorables mediante el manejo de economía de escala.
* Cada dependencia de la Gobernación del Huila será la encargada de realizar las compras de tecnología informática con el presupuesto asignado y sus necesidades, por lo cual deberá solicitar cotizaciones a los proveedores activos de la lista suministrada por El Grupo de Tecnología, Conectividad y Comunicaciones de la Gobernación del Huila, siempre y cuando este previamente aprobada la compra por dicha dirección.
* El proceso de adquisición de bienes informáticos se rige por lo establecido en la Ley 80 de 1993 los artículos en los que aplique y los decretos reglamentarios que la regulen.
* Se debe establecer un sistema de evaluación de los proveedores de soluciones tecnológicas (establecer un formato de calificación en lo posible) cuyos evaluadores no sean otros que el Grupo de Tecnología, Conectividad y Comunicaciones para garantizar un óptimo nivel de cumplimiento y transparencia. Así como implementar una base de datos de los mismos proveedores.

## Parametros A Tener En Cuenta En La Compra De Tecnologia Informatica Y Telecomunicaciones

* Las especificaciones técnicas de las actualizaciones de los equipos corporativos o de los servidores, como la de sus equipos reemplazantes, se dimensionarán a través de estudios formales de planeación de la capacidad de almacenamiento, procesamiento, compatibilidad y tecnología, con un horizonte acorde con los niveles de obsolescencia, lo que permitirá un crecimiento apropiado.
* Los equipos a cotizar generalmente deben ajustarse a la necesidad, ser compatibles, de marca, de última tecnología, técnicamente comparables, bajo ninguna circunstancia CLONES.
* Propender por reponer y renovar los equipos informatices antes de producirse su obsolescencia tecnológica, mientras tengan un valor en el mercado, de tal forma que sean negociables a un costo significativo y no meramente de salvamento.
* Buscar que los equipos a reponer se puedan utilizar para otros propósitos o tareas dentro de la Gobernación del Huila, de lo contrario negociarlos como parte de pago de los equipos reemplazantes; de no ser posible, realizar donaciones a entidades públicas descentralizadas (como escuelas) o sin ánimo de lucro.
* Se repondrán los equipos cuando el rendimiento y/o tiempo de respuesta no sea aceptable para los usuarios en la realización de sus funciones, esto será con el previo análisis del Grupo de Tecnología, Conectividad y Comunicaciones.
* Se deben adquirir solo equipos electrónicos que sean fácilmente escalables, para asegurar una mayor permanencia en el tiempo de las arquitecturas y compatibles con la plataforma tecnológica de la Gobernación del Huila.
* Los programas que se instalen en los equipos de cómputo no deben ser totalmente de última versión, ya que en ocasiones no se cuentan con su respectiva licencia, por tanto, se deben ajustar a las características y requisitos del sistema.
* El software que se adquiera en la Gobernación del Huila deberá ser de última versión estable; en cuanto a las versiones de prueba, se aceptaran temporalmente y solamente por cortesía del proveedor para su estudio, prueba e implementación por el Grupo de Tecnología.
* Al comprar software operativo se debe solicitar al proveedor una certificación de su nivel de seguridad.
* Solo se podrá utilizar software que sea legalmente licenciado o que sea expresamente autorizado su uso por parte del dueño de los derechos y se cuente con las respectivas licencias de uso por parte del proveedor contratista a nombre de la Gobernación del Huila.
* La reposición de software básico y de automatización de oficina tendrá en cuenta los cambios de versiones de los proveedores y los tiempos límites de soporte del proveedor a las versiones antiguas.
* Toda negociación de hardware y/o software debe presentarse bajo la figura de esquema de proyecto con objetivos, alcances, recursos, cronogramas y responsabilidades claramente definidas, involucrando todas aquellas dependencias y personas que tienen que ver con dicho proceso.
* Para la obtención de los sistemas de información y desarrollos requeridos se tendrá en cuenta el siguiente orden de preferencias: Comprar o licenciar un paquete de aplicaciones probado en el mercado, contratar el desarrollo del sistema con terceros y en última instancia, desarrollo internamente. La selección de la alternativa de adquisición será la que determine el correspondiente estudio de conveniencia.
* En toda negociación de tecnología se deben obtener los productos y servicios que son objeto de la contratación, buscando la creación de relaciones de trabajo efectivas con el proveedor, que permitan el beneficio mutuo acordado, la flexibilidad y la actualización tecnológica adecuada.
* Antes de adquirir un producto es necesario realizar un estudio adecuado acerca de su coherencia con las políticas y medidas de seguridad adoptadas por El Grupo de Tecnología, Conectividad y Comunicaciones.
* El Grupo de Tecnología, Conectividad y Comunicaciones será el encargado de la administración total de todos los recursos de tecnología informática con los que cuente la Gobernación del Huila.
* El Grupo de Tecnología, Conectividad y Telecomunicaciones validaran las diversas solicitudes de oferta expuestas por los proveedores. Se debe poseer una cláusula de actualización tecnológica y un soporte técnico adecuado y oportuno por parte del proveedor designado.
* Todo contrato de tecnología informática llevado a cabo con la Gobernación del Huila debe tener cláusulas de actualización tecnológica, cambios durante la ejecución, manejo de actas de acuerdo, coordinación entre contratistas, calidad, seguimiento a las metodológicas en lo referente a los productos a entregar, pruebas, aplicación de las garantías de uso y proceso de aceptación.
* Antes de llegar a la etapa de contratación debe realizarse una investigación de mercado. Dentro de los tópicos a considerar se deben incluir aspectos como: Esquemas de prestación de servicios, licenciamientos de software, derechos de autor. Estos resultados deberán quedar plasmados en el respectivo pliego de condiciones de acuerdo con la conveniencia para la Gobernación del Huila.

# CAPITULO 4:

# CONTROL DE ACCESO DE USUARIOS

# CUENTAS DE LOS USUARIOS

Cuando un usuario recibe una cuenta, debería firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.

La solicitud de una cuenta de usuario ya sea para tener acceso al correo electrónico institucional o a un aplicativo administrativo, el cambio de privilegios o el bloqueo a la misma debe ser efectuado por el jefe inmediato del usuario solicitante y la misma debe ser hecha de manera escrita y dirigida al Grupo de Tecnología, Conectividad y Comunicaciones.

No debe concederse cuentas de usuarios a personas que no tengan vínculos laborales con La Gobernación del Huila a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso no mayor de 30 días.

Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos funcionarios directamente responsable de la administración o la seguridad de los sistemas.

No deben otorgarse cuentas con privilegios de Administrador a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas determine que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como, por ejemplo, el mantenimiento remoto). Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto.

Se prohíbe el uso de cuentas anónimas o de invitado (guest) en los aplicativos administrativos.

Los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad; esto también implica que los administradores de los servidores y sus respectivos sistemas operativos deben entrar empleando su propio username (usuario). En cualquier caso, debe registrarse en una bitácora todos los cambios de usuario.

Toda cuenta debe ser suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 90 días.

El Administrador de los recursos informáticos debe inactivar la cuenta o los privilegios de un usuario cuando reciba una orden escrita del jefe de dicho usuario, y en particular cuando el empleado cesa en sus funciones.

Cuando un empleado se retira de la Gobernación del Huila, debe inactivarse sus cuentas después de que deje el cargo.

El área de Talento Humano debe reportar al Grupo de Tecnología, Conectividad y Comunicaciones cada vez que ingresen nuevos funcionarios, para proceder a crear o a inactivar las cuentas de correo electrónico a que haya lugar.

## Creación Cuentas Usuarios De Planta Gobernación Del Huila

Para la creación de una cuenta de usuario para el correo electrónico del personal de planta de la Gobernación del Huila se utiliza la siguiente convención:

Ejemplo: El primer nombre, seguido de punto, seguido del primer apellido

luz.cardenas

**Observación:** Si se presenta duplicidad en las cuentas de usuario se debe aplicar la siguiente convención: El primer nombre, seguido del segundo nombre, seguido de punto, seguido del primer apellido.

Si nuevamente se presentan duplicidad en las cuentas de usuario de debe aplicar la siguiente convención: El primer nombre, seguido del segundo nombre, seguido de punto, seguido del primer apellido, seguido segundo apellido.

**NOTA:** La longitud máxima de caracteres por usuario es de 20 caracteres (letras, números, y símbolos).

## Creación Cuentas Usuario Para Contratistas De La Gobernación Del Huila

Para la creación de una cuenta de usuario de dominio para contratistas de la Gobernación del Huila se utiliza la siguiente convención:

Ejemplo: La letra **c**, seguida de (\), seguido del primer nombre, seguido de punto, seguido del primer apellido.

c\luz.cardenas

**Observación:** Si se presenta duplicidad en las cuentas de usuario se debe aplicar la siguiente convención: La letra **c**, el primer nombre, seguido del segundo nombre, seguido de punto, seguido del primer apellido.

Si nuevamente se presentan duplicidad en las cuentas de usuario de debe aplicar la siguiente convención: El primer nombre, seguido del segundo nombre, seguido de punto, seguido del primer apellido, seguido segundo apellido.

**NOTA:** La longitud máxima de caracteres por usuario es de 20 caracteres (letras, números, y símbolos).

## Creación Cuentas De Usuario Para Dependencias E Instituciones Descentralizadas

Para la creación de una cuenta de usuario para dependencias e institutos descentralizados se utilizará la siguiente convención:

* Para las secretarias, aplicar la siguiente convención: la palabra secretaria, seguida de punto, seguido primer nombre. Ej: secretaria.
* Para las Oficinas aplicar la siguiente convención: primer nombre, seguida de punto, seguido de segundo nombre.
* Para la Departamentos Administrativos aplicar la siguiente convención: la palabra departamento, seguido de punto, seguido de primer nombre.
* Para la Institutos Descentralizados aplicar la siguiente convención: la palabra instituto, seguido de punto, seguido de primer nombre.

# CONTROL DE ACCESO A SERVIDORES, ESTACIONES DE TRABAJO Y APLICATIVOS

Todos y cada uno de los equipos que son asignados a los funcionarios y/o contratistas, por lo que es de su competencia y responsabilidad hacer buen uso de los mismos.

Las áreas donde se tiene equipos de propósito general cuya misión es crítica estarán sujetas a los requerimientos que el Grupo de Tecnología, Conectividad y Comunicaciones emita.

Las áreas de cómputo de las dependencias donde se encuentre equipo cuyo propósito reúna características de imprescindible y de misión crítica, deberán sujetarse a las normas que establezca el Grupo de Tecnología, Conectividad y Comunicaciones.

Los accesos a las áreas críticas deberán ser restringidos de acuerdo a las políticas que emite el Grupo de Tecnología, Conectividad y Comunicaciones.

Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, el Grupo de Tecnología, Conectividad y Comunicaciones tiene la facultad de acceder a cualquier equipo de cómputo que no esté bajo su supervisión.

Las auditorias de cada actividad donde se involucren aspectos de seguridad lógica y física deberán realizarse periódicamente y deberá sujetarse al calendario que establezca el Grupo de Tecnología, Conectividad y Comunicaciones.

Para efectos de que la Gobernación disponga de una red con alto grado de confiabilidad, será necesario que se realice un monitoreo constante sobre todos y cada uno de los servicios que las tecnologías de la Internet e Intranet dispongan.

Evitar al máximo que los usuarios utilicen aplicativos no autorizados y usen los recursos informáticos de la Gobernación del Huila.

Se deben utilizar controles de acceso lógico a los servidores, estaciones de trabajo, sistemas operativos y programas, es decir las aplicaciones deben estar desarrolladas de tal manera que prevean el acceso no autorizado a la información a la que tienen acceso.

El acceso de los usuarios será únicamente a los recursos informáticos que requiera para desarrollar su trabajo.

Se debe llevar registro de altas, bajas y cambios de usuarios con acceso a los sistemas informáticos y a la red.

Se deben crear y mantener perfiles de seguridad para todos los usuarios con base en sus roles y responsabilidades.

Al momento de hacer entrega a los usuarios de recursos informáticos, se les debe recordar del uso apropiado de los mismos y del conocimiento que dichos usuarios deben tener del “MANUAL DE POLÍTICAS DE USO, SEGURIDAD Y ADMINISTRACIÓN DE ACTIVOS TECNOLOGICOS Y DE INFORMACIÓN”.

Los privilegios de acceso de usuarios deben ser revisados periódicamente.

Deben existir mecanismos que limiten el número de intentos fallidos para autenticarse en los sistemas informáticos.

En lo posible, limitar los lugares desde donde el usuario puede acceder a los recursos informáticos.

Los usuarios deben entrar a la red y sus recursos utilizando el nombre de usuario asignado (propio).

Emplear autenticación fuerte para acceso a sistemas críticos.

Inactivar cuentas de usuario después de un periodo establecido (3 meses) de inactividad y en el caso de correo electrónico, eliminarlas después de un periodo más largo previamente definido (6 meses).

La longitud mínima de los password es de ocho (8) caracteres y estos deben incluir la combinación de letras (mayúsculas y minúsculas), números y signos.

Como sugerencia se recomienda cambiar los passwords periódicamente.

Cambiar los "passwords por defecto" de las instalaciones de sistemas operativos, software y aplicaciones

Emplear un firewall como parte de la solución de seguridad y debe ser el único punto de acceso entre la red interna y redes externas.

## Creación Grupos De Trabajo

Un grupo de trabajo ejemplo (ftp) es la agrupación simple de equipos de cómputo, destinada únicamente a ayudar a buscar elementos como impresoras y carpetas compartidas en el ese grupo.

La creación de un grupo está determinada por los miembros de una dependencia, área u oficio laboral común y debe ser solicitada mediante oficio dirigido al Grupo de Informática, Conectividad y Comunicaciones, indicando en ella los integrantes del mismo.

La responsabilidad del uso de las cuentas de grupo recae en el jefe de la dependencia u oficina que hace la petición de creación del grupo.

# IDENTIFICACIÓN DE ELEMENTOS DE HARDWARE EN LA RED CORPORATIVA

## Identificación De Servidores

Los servidores se identifican con la siguiente convención: la palabra srv seguida de guion seguida del nombre del servicio. Ejemplo: srv-ftp

## Identificación De Estaciones De Trabajo

Las estaciones de trabajo de los funcionarios de planta de la Administración Central Departamental se identificarán con la siguiente nomenclatura para cada una de las dependencias:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| | **NOMBRE DE EQUIPOS EN DOMINIO *HUILA.LOCAL*** | | | --- | --- | | **PREFIJO** | **DEPENDENCIA** | | ALM | Almacén | | ARC | Archivo Departamental | | ASA | Asamblea Departamental | | AGR | Secretaria de Agricultura | | COR | Oficina de Correspondencia | | PAS | Oficina de Pasaportes | | GOB | Secretaria de Gobierno | | CDI | Oficina de Control Disciplinario | | GRI | Oficina de Gestión del Riesgo | | DCO | Desarrollo Comunitario | | DES | Despacho del Gobernador | | PRE | Oficina de Prensa | | DAC | Departamento Administrativo de Contratación | | OVI | Oficina de Victimas | | DAJ | Departamento Administrativo Jurídico | | | **NOMBRE DE EQUIPOS EN DOMINIO *HUILA.LOCAL*** | | | --- | --- | | **PREFIJO** | **DEPENDENCIA** | | SVI | Secretaria de Vías e Infraestructura | | COM | Oficina de Competitividad | | CIT | Oficina de Ciencia y Tecnología | | DAP | Departamento Administrativo de Planeación | | SED | Secretaria de Educación | | HDA | Secretaria de Hacienda | | GEN | Secretaria General | | CIN | Oficina de Control Interno | | OAS | Oficina de Mujer y Asuntos Sociales | | CUL | Secretaria de Cultura | | TIC | Grupo de Tecnología | | SAL | Secretaria de Salud | |

Así mismo, los equipos de cómputo también se identificarán según su tipo, de la siguiente forma:

|  |  |  |
| --- | --- | --- |
| **TIPO DE EQUIPOS** | | |
| COMPUTADOR PORTATIL | LAPTOP | LT |
| COMPUTADOR ESCRITORIO | DESKTOP | DT |
| ESTACION DE TRABAJO | WORK STATION | WS |

Por consiguiente, las estaciones de trabajo se identificarán con la siguiente convención: la sigla o prefijo de la dependencia, seguida de guion, seguida del tipo de equipo de cómputo (LT, DT, WS), seguida de guion, seguida del nombre del funcionario. Si es contratista, se denota con el nombre del contratista antecedido por c. Nota: Si se presenta que varios contratistas presentan nombres homónimos, se adiciona inicial del 1er apellido, y del segundo apellido si es necesario.

Ejemplo:

GEN-DT-JAIME

PREFIJO

DEPENDENCIA

TIPO DE EQUIPO DE CÓMPUTO

NOMBRE FUNCIONARIO

Para funcionarios de planta: GEN-WS-YESINITH

Para contratistas: GEN-LT-CJAIMEAC

## Identificación De Access Point

Los Access Point se identificarán con la siguiente convención: las letras ap que significa que son Access point seguida de un número el cual significa el orden de instalación del mismo en el piso seguida de guion, seguida del nombre de la dependencia según se describieron en la identificación de Estaciones de Trabajo terminando con la letra p y el número del piso donde se encuentra ubicado.

Ejemplo: ap1-gobp2

Los equipos de red inalámbrica se conectarán previa autorización del Grupo de Tecnología, Conectividad y Comunicaciones.

Los equipos que se conecten al Access point del despacho del Gobernador y la Secretaría de Hacienda lo realizaran mediante contraseña la cual se cambiara cada seis meses. En las demás dependencias se concretarán por medio de la de la maquina con previa autorización.

Anualmente se limpiarán las listas de cada Access point con el fin de actualizar y permitir a nuevos usuarios el ingreso a los mismos. Es de aclarar que los usuarios que soliciten este servicio se harán responsables de la integridad de sus equipos y solo se les prestara el servicio de internet bajo las políticas establecidas en la Administración Central.

## Impresoras De Red

Las impresoras de red se identificarán con la siguiente nomenclatura: el nombre de la dependencia según se describieron en la Identificación de Estaciones de Trabajo, seguida de guion, seguida de ptr, seguida de guion, seguida del grupo de trabajo. Ejemplo: gen-ptr-talento.

Las impresoras de red estarán dentro del rango 10.0.153.1 al 10.0.153.100. Es de anotar que la dirección IP de cada una de las impresoras de red tendrá reserva en el servidor y se establecerá la IP de forma manual.

## Acceso A Áreas Críticas

El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta el Grupo de Tecnología, Conectividad y Comunicaciones.

En concordancia con la política de la institución y debido a la naturaleza de estas áreas se llevará un registro permanente del tráfico de personal.

Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de la institución.

# POLITICAS DEL USO CONTRASEÑA

**Objetivo:**

* Garantizar las directrices estipuladas para el uso de las contraseñas

**Aplicabilidad:**

Estas son políticas que aplican usuarios (funcionarios, contratistas y cualquier otra persona o entidad) que por razón de su trabajo se le permita acceso o tenga relación con la Gobernación del Huila.

**Directrices:**

* Las contraseñas son un importante aspecto de la seguridad de los computadores. Ellas son la línea frontal de protección para las cuentas de los usuarios. Una contraseña pobremente escogida puede comprometer la seguridad de toda la red de la Gobernación del Huila, en consecuencia, todos los funcionarios, contratistas y demás personas externas que tengan acceso a los sistemas de la entidad, son responsables de seguir los pasos que se estipulan en este documento para escoger y mantener una contraseña segura.
* El propósito de este reglamento es establecer un estándar para la creación de contraseñas robustas, la protección de esas contraseñas, y la frecuencia con que deben ser cambiadas.
* El ámbito de esta política incluye todas las personas que son responsables de una cuenta o cualquier forma de acceso a los sistemas de la Gobernación del Huila que requieran una contraseña tales como: la red corporativa, el correo electrónico, u otras.
* Es responsabilidad de cada persona manejar la confidencialidad de esta identificación, por lo tanto, se le recomienda no entregar su cuenta de usuario, ni contraseña a nadie.
* Cada usuario es responsable de cambiar periódicamente su clave de acceso al sistema, de acuerdo a su conveniencia.
* Ninguna persona debe utilizar la contraseña de otro usuario para acceder a los servicios de la red (por ejemplo: los diferentes sistemas de información, el correo electrónico, la agenda y todos los servicios en general).
* Las contraseñas son usadas con diferentes propósitos en la Gobernación del Huila. Entre los más comunes están: cuentas de acceso a red, cuentas de acceso a sistemas de información, buzones de correo, protectores de pantalla, contraseñas de inicio de sesión, etc. Las contraseñas usadas en la Gobernación del Huila, deberán tener las siguientes características y cumplir los siguientes criterios:
* Deberán ser cambiadas cada 3 meses,
* Longitud mínima de 8 caracteres alfanuméricos.
* Se deben emplear letras mayúsculas y minúsculas.
* Se deben combinar letras, números, signos de puntuación y caracteres especiales.
* No deben estar basados en información personal, nombres, apellidos, número de la cédula, nombres de familiares, mascotas, fechas conmemorativas, placas de sus vehículos, cedulas, etc. colocar nombres de dioses mitológicos, personajes de series o caricaturas, o lugares familiares.
* No debe escribirla en una parte visible de su escritorio, agenda personal, recordatorios o post stick.
* No compartir ni revelar a nadie la contraseña. Toda acción con su clave es responsabilidad del usuario dueño de esta.
* Al ausentarse del puesto trabajo bloquear sesión de usuario (Ctrl+Alt+Supr opción bloquear)
* La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.
* En el caso de ser necesario, las contraseñas deberán estar almacenadas en sobre cerrado en una ubicación segura, y este solo será abierto por las personas autorizadas para ello por el jefe de la Dependencia.
* Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.
* Para prevenir ingresos no autorizados o ataques cuando el software lo permita, se limita a 3 el número consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema.
* Ningún usuario debe tener la clave de administrador o administración de los equipos de escritorio, de detectarse se debe cambiar e informar al Grupo de Tecnología, Conectividad y Telecomunicaciones.
* Para el acceso remoto a los recursos tecnológicos de la Gobernación del Huila, la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.
* Si no ha habido actividad en una terminal o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente bloquear la Terminal y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El restablecimiento de la sesión requiere que el usuario se autentique mediante su contraseña (o utilice otro mecanismo, por ejemplo, tarjeta inteligente o de proximidad).
* Para evitar el uso no autorizado, abuso, fraude u otro acto mal intencionado que involucre a los sistemas de información, se deben llevar logs de auditoría que contengan información detallada las actividades realizadas.
* Los archivos de bitácora (logs) y los registros de auditoría (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres años. Dichos archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y sólo pueden ser consultados por personas debidamente autorizadas.
* Los servidores de red y los equipos de comunicación (PABX, routers, etc.) deben estar ubicados en lugares apropiados, protegidos contra daños y robo. Debe restringirse el acceso a estos lugares y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras u otros sistemas de acceso (por ejemplo, tarjetas de proximidad).

# CAPITULO 5: SEGURIDAD FÍSICA Y DEL ENTORNO

# SEGURIDAD DE EQUIPOS TECNOLÓGICOS

**Objetivo:** Impedir perdidas, daños o exposiciones al riesgo de los activos e interrupción de las actividades de la empresa.

## Ubicación Y Protección Del Equipamiento

Los equipos tecnológicos de la Gobernación del Huila deben ser ubicados o físicamente protegidos de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado a los recursos y datos, para prevenir pérdidas o daños de estos, se deben tener en cuenta los siguientes puntos:

Los equipos deben ser ubicados en un sitio que permita minimizar el acceso innecesario a las áreas de trabajo.

Las instalaciones de procesamiento y almacenamiento de información, que manejan datos sensibles, deben ubicarse en un sitio que permita reducir el riesgo de falta de supervisión de las mismas durante su uso y mantenimiento.

Los ítems que requieren protección especial deben ser aislados para reducir el nivel general de protección requerida.

Se deben adoptar controles para minimizar el riesgo de amenazas potenciales como:

* Robo
* Incendio
* Explosivos Humo
* Agua (o falta de suministro)
* Polvo
* Vibraciones
* Efectos químicos
* Interferencia en el suministro de energía eléctrica.
* Radiación electromagnética.

Todo usuario debe velar por la preservación y uso de los equipos de cómputo:

* Mantener limpia la zona donde se encuentran los equipos de cómputo.
* No ingerir alimentos ni líquidos cerca o sobre los equipos; con ello se evita la caída o derrame que cause posible deterioro a los componentes de los equipos.
* El teclado y mouse deben ser tratados con suavidad, no hay necesidad de golpear o presionar fuertemente las teclas; por ningún motivo agarre estos elementos por el cable, puede ocasionar averías.
* Realice el apagado del computador con el procedimiento adecuado para ello.
* Los equipos y demás recursos informáticos asignados a cada funcionario son para uso en actividades de la Entidad y no para realizar trabajos de tipo personal.
* Está totalmente prohibido el uso de los computadores, y recursos informáticos en general, por parte de personal ajeno a la Organización.
* Informar al Grupo de Tecnología, Conectividad y Telecomunicaciones cualquier novedad que se presente en la red, las aplicaciones, los equipos o sus instalaciones.

Cumpliendo con las normas para instalaciones eléctricas, ambientales y de seguridad.

* No se deben intercambiar elementos entre equipos sin la autorización del Grupo de Tecnología, Conectividad y Telecomunicaciones.
* Solo el personal de Soporte Técnico está autorizado para realizar las configuraciones de los equipos e instalar el software en los mismos.
* No se deben conectar equipos diferentes al computador, en las tomas color naranja (tomas de la UPS).
* Por ningún motivo desconecte los equipos que están en red, ni conecte equipos o impresoras adicionales sin previa autorización.

Respecto a los cables:

* No pararnos en ellos o presionar con cualquier tipo de objeto.
* No doblarlos o halarlos fuerte.
* No cortarlos.
* No maltratar, ni pisotear las canaletas por donde ellos pasan.

Se debe tener especial cuidado con los cables, ya que de este depende una buena comunicación de los datos a través de la red.

**Nota:** Para contrarrestar y reducir los impactos de los Riesgos y Amenazas a los cuales están expuestos los activos tangibles e intangibles de la Gobernación del Huila, se Diseñó el Plan de contingencia, el cual apoya las políticas institucionales contempladas en el Manual de Políticas de Uso, Seguridad y Administración de los Activos Tecnológicos y de Información.

## Instalación De Equipos De Cómputo

La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar las solicitudes de movimientos en caso de que existan, al área de Almacén y al Grupo de Tecnología, Conectividad y Comunicaciones quienes tienen la obligación de supervisarlo.

Los computadores portátiles, laptops y cualquier equipo que se pueda conectar a la red de la institución deben estar protegidos con sistemas antivirus actualizados para minimizar el riesgo de propagación de virus y software mal intencionado o ser escaneados con un programa antivirus antes de conectarse a la misma.

Todo personal ajeno a la entidad que necesite conectarse a la red deberá informar al Grupo de Tecnología, Conectividad y Comunicaciones, donde se revisara su equipo antes de conectarlo y en caso de ser necesario deberá instalar los mecanismos de seguridad apropiados a fin de cumplir con las políticas de seguridad existentes en la Institución.

## Mantenimiento De Equipos Cómputo

El Grupo de Tecnología, Conectividad y Comunicaciones a través de las personas que ella designe, realiza el mantenimiento preventivo y correctivo de los equipos de cómputo dos veces al año, su instalación, la verificación de la seguridad física y el acondicionamiento específico a que tenga lugar, dando cumplimiento a los procedimientos existentes.

En el caso de los equipos atendidos por terceros, el Grupo de Tecnología, Conectividad y Telecomunicaciones deberá supervisar su aplicación, es decir, garantías, contratos de mantenimiento, etc. Queda estrictamente prohibido solicitar y dar mantenimiento a equipo de cómputo que no es propiedad de la institución.

Todo equipo tecnológico y de telecomunicaciones (computador portátil, estación de trabajo, servidor y demás relacionados) que sea propiedad de la Gobernación del Huila, debe actualizarse siempre que pueda hacerse, tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

Esta actualización deberá realizarse, previa evaluación del perfil de uso del equipo, y por consiguiente del desempeño, funcionalidad y rendimiento del equipo tecnológico, siendo necesario determinar el estado funcional de éste para tal fin. De esta manera se valoran los equipos como *aceptables, adecuados, o inadecuados*, por parte del personal de soporte técnico de la Gobernación del Huila, y documentándose en los formatos dispuestos en los procedimientos de gestión asociados a esta actividad.

# POLÍTICA DE ADMINISTRACIÓN DE RECURSOS TECNOLÓGICOS

**Objetivo:**

* Preservar y garantizar las directrices para el uso óptimo de los recursos tecnológicos.

**Aplicabilidad:**

Estas son políticas que aplican usuarios (funcionarios, contratistas y cualquier otra persona o entidad) que por razón de su trabajo se le permita acceso o tenga relación con la Gobernación del Huila.

**Directrices:**

* Las políticas de administración de los recursos tecnológicos buscan que todos los bienes y servicios informáticos sean administrados y operados de una manera fácil y segura permitiéndole a la Gobernación del Huila tanto su optimización como la minimización de los costos de funcionamiento en procura de llevar un mejor servicio a los usuarios.
* Los recursos informáticos de la Organización deben estar siempre a disposición de los usuarios que los requieran. Para cada perfil de usuario se dimensionarán en su justa medida, los recursos informáticos y servicios que debe tener dicho tipo de usuario.
* El equipamiento Tecnológico debe mantenerse en forma adecuada para asegurar que su disponibilidad e integridad sean permanentes.
* El soporte de los sistemas, es decir, el mantenimiento preventivo y correctivo de los equipos deberá gestionarse por medio del Grupo de Tecnología, Conectividad y Comunicaciones, y este a su vez autoriza al personal asignado para la realización de sus actividades.
* Se debe respetar permanentemente las instrucciones del fabricante de los equipos y seguir las recomendaciones con respecto a los tiempos de mantenimiento y aplicación de la garantía.
* El movimiento de equipos y el traslado a otro lugar dentro de las instalaciones deberá ser autorizado previamente por el Grupo de Tecnología, Conectividad y Comunicaciones.
* Se debe mantener registro de todas las fallas supuestas o reales y de todo el mantenimiento preventivo y correctivo. Los administradores deben Llevar un registro histórico de los principales errores y problemas que ocurren en los dispositivos tanto de hardware como software y el método usado para normalizar la situación.
* El usuario debe responsabilizarse de realizar las copias de seguridad de sus archivos o datos importantes de su PC, acuerdo o según lo requiera la importancia de los documentos.
* Mantener actualizada la documentación relacionada con: configuración de equipos de cómputo y servidores, direccionamiento IP de los equipos, diagramas esquemáticos de conectividad de los equipos en la red, diagrama esquemático del sistema de cableado estructurado, planos con la ubicación exacta de los elementos del cableado (racks, tomas lógicas, puntos de conexión cruzada, canalización, etc.), diagrama de distribución de los gabinetes y organizadores instalados.
* Publicar y difundir los procedimientos de uso para y entre los usuarios de los bienes y recursos informáticos provistos a través de la red.
* Debe propiciar el uso de las tecnologías de la información con el fin de contribuir con las directrices económicas y ecológicas de la institución.
* No revelar información a personas que la soliciten a nombre terceros.
* El grupo de Tecnología, Conectividad y Telecomunicaciones es el responsable de emitir y dar seguimiento a las políticas del uso de la red.
* El Grupo de Tecnología, Conectividad y Comunicaciones es responsable por la coordinación de la reparación de las computadoras de los usuarios y por las actualizaciones de los mismos, con la elaboración de un respectivo plan de mantenimiento de acuerdo con el registro de todas las fallas reportadas.
* No se permite ejecutar programas portables.
* Controlar el uso de todo tipo de software de dominio público, solo deber ser instalado el software necesario y aprobado por El Grupo de Tecnología, Conectividad y Comunicaciones dicho software o utilidades deben darse a conocer a encargados de la instalación de estos en los equipos de cómputo.
* Los administradores encargados de los recursos informáticos, deben hacer funcionar el software sobre el hardware en el que este sea más óptimo, evitando así posibles resultados inesperados y fallas que puedan dañar seriamente la seguridad del sistema, ya que la incompatibilidad entre hardware y software crea agujeros de seguridad.
* Todos los recursos que hacen parte de la infraestructura tecnológica deberán estar interconectados a través de red LAN.

# POLÍTICAS DE SEGURIDAD DEL CENTRO DE CÓMPUTO

El acceso al centro de cómputo se realizará de manera controlada y restringida, las personas que requieran ingresar deberán estar acompañadas por un funcionario del Grupo de Tecnología, Conectividad y Comunicación, habiendo previamente solicitado el permiso de acceso existiendo una razón suficiente que lo amerite.

Queda prohibido fumar, introducir líquidos o alimentos o cualquier elemento que ponga en peligro la integridad de los equipos y el medio ambiente de trabajo dentro del centro de cómputo.

El diseño y construcción del centro de cómputo deberá tener en cuenta las normas, códigos y estándares NFPA 2001, NFPA 72, Código Eléctrico Nacional, ANSIITIA/EIA-568-B.1, ANSIITIA/EIA-569-A, ANSlITl/EIA-607.

Tener identificados todos los elementos que conforman la plataforma tecnológica utilizando para tal fin el rotulado de los mismos.

El Centro de Cómputo deberá tener documentado el control y registro de acceso; el mantenimiento del sistema de detección, alarma y extinción de incendios, el mantenimiento del sistema de aire acondicionado y el mantenimiento de los servidores y equipos de cómputo, entre otros.

Deberá contar con sistemas aire acondicionado, detección, alarma y extinción de incendios, y mecanismos para impedir el acceso no autorizado de terceros

Minimizar el interés de entidades ajenas en las áreas críticas, evitar en lo posible visitas guiadas a los centros de cómputo y comunicaciones.

El centro de cómputo deberá realizar y mantener copias de respaldo (back-up) de la información, y realizar monitoreo al desempeño de sus servidores, con el propósito de mejorar su rendimiento.

# SEGURIDAD PERSONAL

## Seguridad En La Definición De Puestos De Trabajo Y La Asignación A Recursos A Usuarios

**Objetivo:** Reducir los riesgos de error humano, robo, fraude, daño o uso inadecuado de instalaciones y recursos tecnológicos por parte de los usuarios.

Las políticas y responsabilidades en materia de seguridad y utilización de los recursos deben ser dadas a conocer en la etapa de entrega de estos a los funcionarios, incluidas en los contratos y monitoreadas durante el desempeño del individuo.

La responsabilidad por la utilización y administración de los datos del usuario se extienden más allá de los límites de la Gobernación y del horario normal del trabajo, por ejemplo, cuando el usuario desempeña tareas en su domicilio.

Todos los empleados de la Organización y, cuando sea pertinente, los usuarios externos, deben recibir una adecuada capacitación y actualizaciones periódicas en materia de políticas y procedimientos de la Organización. Esto comprende los requerimientos de seguridad, las responsabilidades legales y controles de la Gobernación, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información, servicios y recursos por ej. El procedimiento de entrada al sistema ("Iog-on") y el uso de paquetes de software, antes de que se le otorgue acceso a la información o a los servicies.

Deshabilitar en las estaciones de trabajo el uso del protocolo NetBios con el fin de prevenir ataques de usuarios maliciosos.

Las impresoras, plotter's, faxes o cualquier dispositivo por el que pueda salir información esencial del sistema ha de estar situado en un lugar de acceso restringido solo a empleados autorizados o en un lugar donde pueda ser supervisado su funcionamiento.

Es conveniente tener un grado de control así sea mínimo de lo que sale por las impresoras; si un atacante sabe que el acceso a los documentos está controlado, lo pensara varias veces antes de intentar conseguir algo que otro usuario ha impreso.

Los equipos de cómputo se asignarán de acuerdo a los requerimientos técnicos exigidos por las herramientas que utilizadas para el desempeño de sus o tareas asignadas.

# SEGURIDAD Y AMBIENTAL

## Seguridad De Areas

**Objetivo:** Impedir accesos no autorizados, daños e interferencia a las sedes e información de la Gobernación del Huila.

Las instalaciones de procesamiento de información crítica o sensible de la Gobernación deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con controles de acceso apropiados deben estar físicamente protegidas contra accesos no autorizados, daños e intrusiones.

Se recomienda la implementación de políticas de escritorios y pantallas limpios para reducir el riesgo de acceso no autorizado o de daño a papeles, medios de almacenamiento e instalaciones de procesamiento de información o recursos te/enológicos.

La protección física debe llevarse a cabo mediante la creación de diversas barreras físicas alrededor de las sedes de la Organización y de las instalaciones de procesamiento de información. Cada barrera establece un perímetro de seguridad, cada uno de los cuales incrementa la protección total provista. Por ejemplo: una pared una puerta de acceso controlada o un escritorio u oficina de recepción atendidos por personal.

Se deben considerar el diseño de un sistema General de acceso para todas las instalaciones de la Gobernación del Huila que administre correctamente las visitas de usuarios externos y controle los movimientos de los funcionarios y contratistas, este sistema debe contener como mínimo los siguientes lineamientos y controles, según corresponda,

a) El perímetro de seguridad debe estar claramente definido

b) El perímetro de un edificio o área que contenga instalaciones de procesamiento de información debe ser físicamente solido (por ej. No deben existir claros o aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados, por ej., mediante mecanismos de control, vallas, alarmas, cerraduras, etc.

c) Debe existir un área de recepción atendida por personal u otros medios de control de acceso físico al área o edificio. El acceso a las distintas áreas y edificios debe estar restringido exclusivamente al personal autorizado.

d) Las barreras físicas deben, si es necesario, extenderse desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, la ocasionada por incendio e inundación.

e) Todas las puertas de incendio de un perímetro de seguridad deben tener alarma y cerrarse automáticamente.

f) Los visitantes de áreas protegidas deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y egreso deben ser registrados. Solo se debe permitir el acceso a los mismos con propósitos específicos y autorizados, instruyéndose en dicho momento al visitante sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

g) El acceso a la información sensible, y a las instalaciones de procesamiento de información, debe ser controlado y limitado exclusivamente a las personas autorizadas. Se deben utilizar controles de autenticación, por ej. Tarjeta y número de identificación personal (PIN), para autorizar y validar todos los accesos. Debe mantenerse una pista protegida que permita auditar todos los accesos.

h) Se debe requerir que todo el personal exhiba alguna forma de identificación visible y se lo debe alentar a cuestionar la presencia de desconocidos no escoltados y a cualquier persona que no exhiba una identificación visible.

i) Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas.

j) Adecuados sistemas de detección de intrusos. Los mismos deben ser instalados según estándares profesionales y probados periódicamente. Estos sistemas comprenderán todas las puertas exteriores y ventanas accesibles. Las áreas vacías deben tener alarmas activadas en todo momento. También deben protegerse otras áreas, como la sala de cómputo o las salas de comunicaciones.

## Limpieza De Puestos De Trabajo

**Objetivo**:

* Proteger documentos sensibles y reducir riesgos de incidentes sobre los servicios tecnológicos de la Gobernación, mediante la limpieza de los puestos de trabajo y el despeje y mantenimiento en buen estado de las conexiones eléctricas y de red.

**Alcance:**

* Aplica a usuarios (funcionarios, contratistas y cualquier otra persona o entidad) que por razón de su trabajo se le permita acceso o tenga relación con la Gobernación del Huila.

**Directrices:**

* Todos los recursos físicos inherentes a la Gobernación del Huila como las instalaciones, equipo, cableado, medios de almacenamiento deben ser protegidos y utilizados eficientemente por parte de los funcionarios.
* Las unidades de almacenamiento (CD’s, memorias USB, discos portátiles, etc.) deben ser tratados como sensibles y guardadas bajo llave en cajones cerrados, y no deben dejarse olvidadas en los computadores.
* Todos los escritorios o puestos de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento, a fin de reducir riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo.
* Evita usar resmas de papel, libros y otros elementos como soporte para monitores y computadores todo en uno. Solicita verificación de tu puesto de trabajo al área de Seguridad y Salud en el Trabajo, con el fin de definir qué elementos pueden mejorar tu postura de trabajo, y proteger de paso los equipos de cómputo, monitores, y demás periféricos.
* Guardar bajo llave documentos sensibles del trabajo, en largos periodos de tiempo fuera del escritorio.
* Al finalizar la jornada de trabajo, poner en orden su escritorio, guardar todos los papeles de oficina, y cerrar con llave escritorio y archivadores.
* Todos los puestos de trabajo cuentan con un tomacorriente/conector a la red corporativa, este debe estar debidamente instalado en un faceplate (caja plástica) bien sea empotrada en la canaleta o sobrepuesta en la cancelería, de uno o varios tomacorrientes.
* Todos los elementos instalados en los puestos de trabajo para conformar él toma/conector, así como el cable que conecta el computador al tomacorriente/conector deben protegerse de daño físico, humedad y calor.
* Las canaletas del cableado estructurado deben estar despejadas, sin objetos (cajas, carpetas, documentos, etc.) que las aprisionen, deterioren, obstaculicen o que estén acumulados sobre ellas, ya que, del buen estado de dicho cableado, depende el acceso a los diferentes servicios tecnológicos dispuestos para el desarrollo de las labores (internet, FTP, correo electrónico, extranet, acceso a sistemas de información y aplicativos, etc.).
* Los cordones (cables) de la red de computadores deben tener libre acceso a las tomas instaladas para el buen funcionamiento de la red de datos y todos los servicios que de ella depende.
* No bloquear las ranuras de ventilación de los equipos. Si los equipos deben estar uno al lado del otro, la distancia de separación entre ellos deberá estar entre 5 y 10 cm. La distancia de separación entre la parte trasera del equipo y cualquier obstáculo deberá estar entre 20 y 30 cm.

De igual forma, desde la Coordinación del Sistema Integrado de Gestión se estableció el programa 5’S cuyo objetivo es la creación de una cultura organizacional y cambio de hábitos para mejorar y mantener las condiciones de organización, orden y limpieza en el lugar de trabajo y zonas comunes donde se desarrollan los procesos internos, con el fin de mejorar productividad, motivación y bienestar de los servidores públicos de la entidad, y bajo el cual se establecen las siguientes directrices:

* Identificación y clasificación de los elementos innecesarios en el puesto de trabajo, para posterior eliminación gradual de los elementos innecesarios, limpieza y aseo.
* Reubicación y reorganización de elementos innecesarios en un sitio adecuado, que no perturbe y por el contrario agilice las actividades del proceso en el puesto de trabajo, en caso tal de que se pueda realizar una eliminación de los mismos.
* Ubicación y organización de elementos de un área o puesto de trabajo en el lugar que le corresponde o que fue diseñado para tal fin.
* Crear el hábito de mantener el sitio de trabajo en correctas condiciones, gracias al suministro de los elementos necesarios para su realización, como también destinación del tiempo requerido para su ejecución.
* Planificar el mantenimiento y rutina de la limpieza, desde la inspección antes del comienzo del día, durante el día, hasta las que se hacen al final del día, pasando por el almacenamiento de información en los computadores de la entidad, manejo del archivo y forma de organización.
* Establecer tiempos para actividades de limpieza, de modo que lleguen a formar parte natural del trabajo diario.
* Realizar campañas o jornadas periódicas de limpieza, para la eliminación de elementos innecesarios.
* Cada funcionario debe conocer exactamente cuáles son sus responsabilidades y acciones por cumplir, en relación con los trabajos de limpieza y mantenimiento autónomo. Los estándares pueden ser preparados por el personal, pero esto requiere una formación y práctica de mejoramiento continuo, que progresivamente vayan mejorando los tiempos de limpieza y métodos.

# SEGURIDAD FISICA DE LAS AREAS DE ENTREGA Y CARGA DE LA GOBERNACIÓN DEL HUILA

El acceso a las áreas del almacén, desde el exterior de la sede de la Organización, debe estar limitado a personal que sea previamente identificado y autorizado.

El área del almacén debe ser asegurada de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.

El material entrante debe ser inspeccionado para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.

# POLÍTICA DE MEDIO AMBIENTE

**Directrices:**

* El grupo de Tecnología, Conectividad y Telecomunicaciones debe garantizar la seguridad física en la entidad, para prevenir e impedir accesos no autorizados, daños e interferencias, así como la información que recibe y genere.
* Prohíbase la existencia de cualquier material que pudiera poner en riesgo la integridad física o lógica de los recursos informáticos de la Gobernación del Huila.
* No bloquear las ranuras de ventilación de los equipos, si los equipos deben estar uno al lado el otro la distancia de separación entre ellos deberá estar entre 5 y 10 cm., la distancia de separación entre la parte trasera del equipo y cualquier obstáculo deberá estar entre 20 y 30 cm.
* Maximizar la protección estructural, evitar en posible el empleo de muros falsos o cancelas de vidrio.
* Se debe contar con protección contra incendios, detectores de humo, extintores y control de clima (rango de 10 a 25 grados centígrados).
* Se debe retirar el material no necesario y que en un momento dado se convierta en obstáculo de los centros de cómputo y comunicaciones
* Solo personal autorizado puede acceder a los centros de cómputo y comunicaciones, previo el diligenciamiento del respectivo permiso escrito o verbal por parte del Grupo de Tecnología, Conectividad y Telecomunicaciones.
* Todos los recursos físicos inherentes a la Gobernación del Huila como las instalaciones, equipo, cableado, medios de almacenamiento deben ser protegidos y utilizados eficientemente por parte de los funcionarios.
* Mantener los centros de cableado (racks de cableado) cerrados con llave.
* Establecer periódicamente programas de mantenimiento preventivo. Contar con planes de reparación de emergencia de equipo crítico.
* Deben existir equipos de protección contra fluctuaciones de energía (reguladores de voltaje, UPS, plantas de energía, etc.)
* Proteger las fuentes de energía de amenazas del medio ambiente (las instalaciones eléctricas deben ser resistentes al fuego, inundaciones y otros desastres.
* Los sitios de cómputo y comunicaciones no deben estar alfombrados.
* Las impresoras, copiadoras, faxes y cualquier otro periférico compartido deben encontrarse fuera del centro de cómputo y comunicaciones.
* Los centros de cómputo y comunicaciones deben contar con una línea y aparato telefónico que se empleará en caso de emergencia, así como una lista con los números telefónicos del personal a contactar en el evento de un siniestro.
* Se debe capacitar al personal en el empleo de extintores, sistemas de alarma y cualquier mecanismo de seguridad.

# CAPITULO 6:

# SEGURIDAD DE LAS OPERACIONES

# SEPARACION DE AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN

En el marco del ciclo de vida de un sistema de información, específicamente en la etapa de planeación, los jefes de dependencias, responsables funcionales y responsables técnicos designados establecen las **especificaciones y requerimientos** que soportan las necesidades expresadas para la adquisición, desarrollo, mantenimiento y/o actualización, cambio y/o retiro de software.

Dentro de las **especificaciones y requerimientos** se deben considerar

* Habilitar ambientes de pruebas antes de paso a producción.
* Realizar un plan de pruebas para la realización de casos o escenarios de prueba, que permitan evaluar las funcionalidades y verificar los resultados esperados, teniendo en cuenta no utilizar para ello datos sensibles y/o datos personales en este proceso.
* Realizar pruebas de carga, estrés y rendimiento del software, con el fin de evaluar la cantidad de peticiones que puede soportar.
* Realizar pruebas de regresión, posterior a las anteriores pruebas descritas, con el fin de verificar la no existencia de defectos o errores en el software, producto de las pruebas o modificaciones que se realicen sobre éste.
* Realizar las pruebas de aplicación del procedimiento de backup programados para el respaldo y restauración del software, validando la información almacenada y restaurada.

Posteriormente en la etapa de **Pruebas de Software y validación de requerimientos,** la supervisión asignada, los responsables técnicos y responsables funcionales junto con los proveedores contratados, deben velar por el cumplimiento de las especificaciones del producto de software desarrollado/implementado, realizando el seguimiento de las pruebas en los ambientes de pruebas y producción respectivamente, hasta obtener la funcionalidad y operación adecuada.

El ***Formato de recolección y especificación de requerimientos / SGN-C043-P808-F01 / v1***, los documentos técnicos de la etapa de análisis y diseño detallado y las demás obligaciones estipuladas en los documentos contractuales, corresponden a insumos para la verificación y ejecución de las pruebas.

Todas las pruebas que se realicen deben documentarse en un informe, que incluya al menos la siguiente información:

* Nombre del software y/o sistema de información objeto de la prueba.
* Fecha de realización.
* Ambiente en el que se desarrolló la prueba.
* Resultados obtenidos.
* Observaciones y opciones de mejora si aplican.
* Participantes y/o asistentes.

Después, en la etapa de **Puesta en Producción,** el supervisor del contrato debe coordinar con el Grupo de Tecnología de la Entidad, el proceso de puesta en producción y despliegue del software en el Centro de Datos, y suscribir acta de entrega al Grupo de Tecnología del software y hardware pertinente, si es el caso.

Cabe recordar que, dentro de la planificación de la puesta en producción, debe incluirse la migración de bases de datos actuales, en caso de que corresponda a cambio o reemplazo del software y la configuración y parametrización del software para entrar en producción.

# POLÍTICAS DEL USO Y APLICACIÓN DEL ANTIVIRUS

**Objetivo:**

* Utilizar los lineamientos y aplicación del antivirus

**Directrices:**

* Todas las computadoras de la red deben tener instalado el mismo paquete de antivirus adquirido por la Gobernación del Huila.
* El servidor de Antivirus debe ser el que gestione la descarga de actualizaciones y las distribuya a los clientes periódicamente, siendo una tarea transparente para el responsable del equipo.
* Asegurar que el antivirus este siempre activo vigilando constantemente todas las operaciones realizadas por los sistemas de información utilizados por los funcionarios de la Gobernación del Huila.

El Antivirus que funcione dentro de la entidad debe cumplir con las siguientes características:

* Deben actualizar los patrones o firmas, por lo menos una vez par semana.
* La empresa que los promueve debe contar con un equipo de soporte técnico con acceso a un laboratorio especializado en códigos maliciosos y un tiempo de respuesta no mayor a 48 horas, el cual me pueda orientar, en mi idioma, en caso de que yo contraiga una infección.
* Deben contar con distintos métodos de verificación y análisis de posibles códigos maliciosos, incluyendo el heurístico, el cual no se basa en firmas virales sino en el comportamiento de un archivo, y así poder detener amenazas incluso de posibles virus nuevos.
* Se deben poder adaptar a las necesidades de diferentes usuarios.
* Deben poder realizar la instalación remota tanto en una red LAN como en una WAN.
* Deben constar de alguna consola central en donde se puedan recibir reportes de virus, mandar actualizaciones y personalizar a distintos usuarios.
* Deben ser verdaderamente efectivos para efectos de defección y eliminación correcta y exacta de los distintos virus que puedan amenazar a los sistemas.
* Deben de permitir la creación de discos de emergencia o de rescate de una manera clara y satisfactoria.
* No deben de afectar el rendimiento o desempeño normal de los equipos, y de ser preferible lo que se desea es que su residente en memoria sea de lo más pequeño.
* El número de falsos positivos que se den tanto en el rastreo normal como en el heurístico debe de ser la mínima posible.
* Su mecanismo de auto-protección debe de poder alertar sobre una posible infección a través de las distintas vías de entrada, ya sea Internet, correo electrónico, red o discos flexibles, etc.
* Deben tener posibilidad de chequear el arranque, así como los posibles cambios en el registro de las aplicaciones.

# CONTROL DE INSTALACIÓN DEL SOFTWARE

Solo personal autorizado por el Grupo de Tecnología, Conectividad y Telecomunicaciones puede instalar software y en el caso de no ser "software de libre distribución", este debe contar con la respectiva licencia de uso.

Corresponde al Grupo de Tecnología, Conectividad y Telecomunicaciones emitir los procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.

En los equipos de cómputo, de Telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual.

El Grupo de Tecnología, Conectividad y Telecomunicaciones es el responsable de brindar asesoría y supervisión para la instalación de software informático.

La instalación de software que desde el punto de vista del Grupo de Tecnología, Conectividad y Telecomunicaciones pudiera poner en riesgo los recursos tecnológicos de la entidad, no está permitida.

Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, privilegios de acceso, y otros que apliquen).

La protección física y lógica de los recursos informáticos corresponde a quienes en un principio se les asigna y le compete notificar cualquier movimiento al Grupo de Tecnología, Conectividad y Telecomunicaciones y el área de almacén.

# POLITICA DE RESPALDO DE INFORMACIÓN

**Alcance**: Esta política de Seguridad abarca además de la información alojada en servidores y sistemas de información, la información de gestión priorizada que se encuentra alojada en equipos de cómputo administrados por funcionarios de la Gobernación del Huila (personal de planta administrativa, personal de libre nombramiento y remoción, y contratistas de prestación de servicios), con el fin de que ésta esté disponible, mantenga su integridad y sea restaurable en el momento en que sea necesario y requerido.

**Objetivo**: Especificar los lineamientos generales para desarrollar un apropiado proceso de generación de copias de seguridad de la información alojada en servidores, sistemas de información, y equipos de cómputo de la Gobernación del Huila, estableciendo lineamientos de respaldo, almacenamiento, aseguramiento y restauración de la información.

**Responsabilidades**:

* + *Coordinador TIC*: realiza las funciones de Líder de la gestión y respaldo de información de la Gobernación del Huila, garantizando la disponibilidad, integridad y confidencialidad de ésta, y además, que sea restaurable en el momento en que sea necesario y requerido.
  + *Profesional Universitario*: realiza las funciones de supervisor de los contratos de soporte técnico, administración y seguridad informática del centro de datos y redes de datos, con capacidad de resolución de incidentes y requerimientos con cierto nivel de acceso, y gestión de respaldo de información relacionada con la infraestructura del centro de datos y redes de datos de la entidad, o en su defecto, debe contar con capacidad de análisis para escalar el requerimiento a un experto que brinde el servicio de gestión de respaldo y backup de información.
  + *Profesional de Apoyo o Personal de outsourcing de soporte técnico*: realiza las funciones de analista de requerimientos de respaldo y backup de información, siendo el contacto directo con los usuarios, velando siempre por atender las solicitudes y requerimientos lo más pronto posible, registrando, organizando y priorizando las solicitudes de acuerdo con el nivel de interrupción de las actividades de uso y acceso a la información relacionada, para asignar adecuadamente los recursos disponibles.

**Responsabilidades de los usuarios**:

* + Los funcionarios de la Gobernación del Huila son responsables por la realización de copias de seguridad de la información de gestión que administren en sus equipos de cómputo.
  + Los jefes de dependencia, líderes de procesos, o funcionarios encargados que desarrollan labores de administración de sistemas de información alojados en el centro de datos del 6to piso – Secretaría General, pueden solicitar respaldo o restauración de copias de seguridad, según la necesidad del área, a los medios establecidos por el Grupo TIC (correo electrónico [soporte.tic@huila.gov.co](mailto:soporte.tic@huila.gov.co)).
  + Los funcionarios de la Gobernación del Huila que tienen información de gestión priorizada para backup y respaldo, deben facilitar la atención al personal de soporte técnico o profesionales de apoyo asignados por el Grupo TIC, para realizar las labores relacionadas con la transferencia de la información a respaldar.

**Directrices**:

* El Grupo de TIC de la Gobernación del Huila realizará copias de seguridad sobre los activos que son administrados por el Grupo TIC, en el centro de datos de la Secretaría General, ubicado en el 6to piso, (sistemas de información, bases de datos, información alojada, etc.), según su nivel de criticidad, asegurándose de tener la capacidad de restaurar de forma completa y oportuna la información en caso de requerirla.
* Las aplicaciones, sistemas de información, bases de datos, entre otros, que son alojados en el centro de datos de la Secretaría General, y que son administrados por funcionarios de otras dependencias que desarrollan labores de administración de sistemas de información, deben contar con sus respectivas copias de seguridad, debidamente probadas en su capacidad de restauración, y será responsabilidad de estos el realizar dichas copias de seguridad.
* Las copias de seguridad deben estar almacenadas en lugares apropiados cumpliendo con las condiciones ambientales y de seguridad, para garantizar la integridad, disponibilidad, y realizar una verificación periódica de que la información respaldada es fiable, garantizando la recuperación de los sistemas.
* Respaldo de sistemas de información: Las copias de respaldo de todos los sistemas de información y/o aplicativos contenidos en los servidores de la Gobernación del Huila se deben realizar bajo los lineamientos descritos en el instructivo de Código SGN-C043-I820 “Elaboración de Backups de Servidores”, que se encuentre vigente, bajo la responsabilidad del Grupo TIC.
* Respaldo de activos de información: Las copias de respaldo de los activos de información gestionados por los funcionarios y usuarios se deben realizar bajo los lineamientos descritos en el instructivo de Código SGN-C043-I821 “Elaboración de Backups de Usuarios”, que se encuentre vigente.
* El Grupo TIC de la Gobernación del Huila no realiza copias de respaldo de los equipos de cómputo de los funcionarios, dado que la relevancia e importancia de la información debe ser definida por el funcionario a cargo de ésta. Por lo tanto, en casos donde se necesite realizar copia de respaldo de información a cargo de funcionarios de la entidad y que esté alojada en equipos de cómputo de propiedad de la Gobernación del Huila, la solicitud se debe realizar a través de los medios establecidos por el Grupo TIC (mesa de servicios de TI - correo electrónico [soporte.tic@huila.gov.co](mailto:soporte.tic@huila.gov.co)) por parte del jefe de la dependencia o líder de proceso.
* El Grupo TIC de la Gobernación del Huila incluirá dentro de las actividades de capacitación y sensibilización en seguridad de la información, dirigidas a los funcionarios de la entidad, temáticas relacionadas con la realización de copias de seguridad de la información de gestión, indicando aspectos importantes a tener en cuenta para mantener la disponibilidad e integridad de esta información (medios, periodicidad, resguardo, pruebas, restauración, entre otros), y que se encuentran descritos en el instructivo de Código SGN-C043-I821 “Elaboración de Backups de Usuarios”, que se encuentre vigente.
* Registro de copias de seguridad: cada respaldo que se realice, manual o automático, de los servidores, o sistemas de información, deberá quedar registrado mediante notificación en la mesa de servicios de TI (correo electrónico [soporte.tic@huila.govco](mailto:soporte.tic@huila.govco)) del Grupo TIC.
* Frecuencia y tipo de respaldo: el Grupo TIC debe definir los tipos de copias de seguridad que realiza para los sistemas de información, servidores y bases de datos, y que administra en el centro de datos de la Secretaría General, ubicado en el 6to piso de la Gobernación del Huila. Así mismo, se deberá considerar la frecuencia, los medios de almacenamiento, tipo de contenido, tiempo de almacenamiento, y borrado, de cada copia de respaldo de información.
* Custodia y protección de medios de respaldo de información: los medios de respaldo que contienen información de sistemas, servidores y bases de datos administrados por el Grupo TIC en el centro de datos de la Secretaría General, ubicado en el 6to piso de la Gobernación del Huila, deben estar debidamente custodiados por personal responsable de ésta, de modo que garantice la protección adecuada de la información almacenada, y que se pueda poner en funcionamiento en el momento que sea requerido.
* Periodo de existencia de las copias de respaldo:
  + El jefe de cada dependencia deberá determinar el período de conservación del respaldo de la información priorizada de sus procesos, teniendo en cuenta los requisitos de conservación de las tablas de retención documental, la normativa legal vigente, el uso eficiente del espacio físico y los medios de almacenamiento disponibles.
  + Para el caso de la información administrada por el Grupo TIC en sistemas de información, servidores, bases de datos, del centro de datos de la Secretaría General, el Grupo TIC define el periodo de conservación de la copia de respaldo, teniendo en cuenta las condiciones establecidas en los contratos de soporte y mantenimiento de cada uno de los sistemas de información o bases de datos, o en su defecto, a través del contrato de soporte técnico, administración, y seguridad informática del centro de datos y de la red de datos de la entidad.
* Pruebas de restauración de copias de respaldo:
  + El Grupo TIC deberá realizar las pruebas de restauración de las copias de respaldo que se realicen de la información que administra en el centro de datos de la Secretaría General, de manera controlada y en un ambiente seguro, que contenga los mismos niveles de seguridad del ambiente original, y con una periodicidad mínima de 1 vez al año.
  + Las aplicaciones, sistemas de información, bases de datos, entre otros, que son administrados por funcionarios que desarrollan labores de administración de sistemas de información, deben contar con sus respectivas copias de seguridad, debidamente probadas en su capacidad de restauración.
* Respaldo de información de sistemas alojados en la web o en sitios externos:
  + A través de los contratos con proveedores de servicios web o hosting, se deben establecer las obligaciones que garanticen la realización de copias de respaldo a la información y aplicaciones, de acuerdo con los requerimientos y necesidades del servicio.
  + Las copias de respaldo realizadas por los proveedores deben ser entregadas de forma periódica al supervisor designado del contrato de soporte técnico y mantenimiento de cada uno de los sistemas de información o aplicaciones de la Gobernación del Huila, ya sea en medios magnéticos o mediante el acceso a un repositorio de documentos, y deben ser verificadas por los supervisores de los contratos.
  + El proveedor debe garantizar mediante clausula u obligación contractual, la confidencialidad de la información que se encuentre alojada en sus equipos, teniendo en cuenta la política de seguridad y privacidad de la información, y la política de tratamiento de datos personales de datos personales, establecidas por la Gobernación del Huila.
  + El proveedor debe tener en cuenta, para la realización y conservación de las copias de seguridad, la normatividad vigente, la cual debe ser suministrada por el supervisor del contrato de soporte técnico y mantenimiento de cada sistema de información, servidor o base de datos, o en su defecto, el supervisor deberá indicar los tiempos de conservación necesarios.
  + El proveedor deberá entregar copia de toda la información resguardada al finalizar el contrato de soporte técnico y mantenimiento, al supervisor de éste, en un formato estándar y legible.

**Requerimientos mínimos**:

* + Servicio de almacenamiento y backup de información de sistemas de información, servidores, bases de datos, entre otros, administrados por el Grupo TIC de la Gobernación del Huila.
  + Aplicativo o herramienta de gestión de servicios de TI para la gestión de solicitudes de respaldo de información.
  + Servicio de conectividad en red y conexión a internet en las instalaciones de la Gobernación del Huila.

# CAPITULO 7:

# SEGURIDAD DE LAS COMUNICACIONES

# POLÍTICAS DE ADMINISTRACIÓN DE LA RED

**Objetivo:**

* Lograr mantener las directrices para la administración eficiente y eficaz de la red

**Directrices:**

* Para el Grupo de Tecnología, Conectividad y Comunicaciones como unidad organizacional encargada de liderar la transformación tecnológica en lo pertinente a sistemas de cómputo y telecomunicaciones de la Administración Departamental a través de diversos procesos, es de trascendental importancia determinar la metodología con la cual se deben llevar a cabo las actividades que comprometan la instalación, ampliación, traslado y transformación de los elementos de la red corporativa (puntos de red, concentradores y centros de cableado, entre otros).
* En términos generales, aplicando las definiciones tornadas al interior de la institución y la Norma 802 del IEEE (Instituto of Eléctrica and Electronic Engineeres - Instituto de Ingenieros Eléctricos y Electrónicos), en este manual se define la metodología con la cual se pretende que la red corporativa de datos de la Gobernación del Huila sea un elemento administrado y manejado en forma coordinada por las partes que en ella intervienen directamente, es decir, por El Grupo de Tecnología, Conectividad y Comunicaciones y el Grupo de Servicios Generales.
* Todos los cambios en el sistema integrado, en los servidores y equipos de desempeño de la red de la Gobernación del Huila, incluyendo la instalación de software nuevas aplicaciones, el cambio de direcciones IP, la reconfiguración de routers y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.
* El grupo de Tecnología, Conectividad y Telecomunicaciones es responsable de emitir y dar seguimiento a las políticas de uso de la red y de procurar su cumplimiento.
* El grupo de Tecnología, Conectividad y Comunicaciones es responsable de proporcionar a los usuarios el acceso a los recursos informáticos, aplicaciones, programas y herramientas tecnológicas dependiendo de las funciones de cada grupo.
* Dado el carácter unipersonal del acceso a la red de la Gobernación del Huila, el Grupo de Tecnología, Conectividad y Comunicaciones verificará el uso responsable, de acuerdo a las políticas para el uso de la red.

## Políticas De Administración Del Cableado

**Objetivo:**

* Garantizar los lineamientos establecidos para el cableado en los puestos de trabajo

**Directrices:**

**Normas relacionadas**

Existen a nivel mundial varias entidades (asociaciones) que compilan y armonizan los diversos estándares de telecomunicaciones a través de normas, siendo la más importante las que se detallan a continuación:

ANSI: Instituto Americano Nacional de Estándares.

TIA: Asociación de Industrias de Telecomunicaciones.

EIA: Asociación de Industrias Electrónicas.

IEEE: Instituto de Ingenieros y Electrónicos

ISO: Organización Internacional de Normalización

Estas cinco asociaciones definen estándares principales que gobiernan el cableado de telecomunicaciones en edificios, cada estándar cubre una parte especifica como el cable, el hardware, los equipos, el diseño y prácticas de instalación requeridas; adicionalmente cada estándar menciona otros estándares relacionados y materiales de referencia, también incluyen secciones que definen términos importantes, acrónimos y símbolos.

Los estándares principales de ANSI/TIA/EIA que gobiernan el cableado de telecomunicaciones en edificios son:

1. ANSI/TIA/EIA-568-B, Estándar de Cableado de Telecomunicaciones en Edificios Comerciales.
2. ANSI/TIA/EIA-569-A, Estándar para Ductos y Espacios de Telecomunicaciones en Edificios Comerciales.
3. ANSI/TIA/EIA-570-A, Estándar de Alumbrado de Telecomunicaciones Residencial y Comercial Liviano.
4. ANSI/TIA/EIA-758, Cableado de planta externa perteneciente al cliente.
5. ANSI/TIA/EIA-606-A, Estándar de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales.
6. ANSI/TIA/EIA -607-A, Requerimientos para Telecomunicaciones de Puesta a Tierra y Puenteado de Edificios Comerciales.
7. ANSI/EIA/TIA 942: Estándar para la infraestructura de telecomunicaciones de los data center.

Existen estándares y documentación complementaria de importancia en la planificación, mejoramiento o diseño de una red integrada de trasmisión de Red de Datos, la cual garantizan el óptimo desempeño de la Red, como:

TIA/EIA- 568-B.1 especifica un sistema de cableado de telecomunicaciones genérico para edificios comerciales que soporta un entorno de varios productos y proveedores.

TIA/EIA-568-B.2 especifica los componentes de cableado, de transmisión, los modelos de sistemas y los procedimientos de medición necesarios para la verificación del cableado de par trenzado.

TIA/EIA-568-B.3 especifica los componentes y requisitos de transmisión para un sistema de cableado de fibra óptica

Guía para el Cableado de Fibra Óptica Centralizada. ANSI/TIA/EIA TSB-72.

Gabinetes, Andenes, Paneles y Equipo Asociado. ANSI/TIA/EIA 310-D-92.

## Consideraciones Para Dispositivos Activos De Conexion (Hub's, Concentradores, Switches):

Para la instalación de estos dispositivos en los centros de cableado, racks, gabinetes o armarios, se debe seguir las normas y estándares de instalación, marcación y las conexiones de todos los componentes activos y no activos de los centros de cableado.

En todos los casos, los dispositivos activos de la red deben estar correctamente instalados (montados) en un centro de cableado que corresponda al diseño de la red del piso o área, es importante aclarar, que estos dispositivos no se deben de instalar en forma provisional o definitiva en oficinas, escritorios o adaptaciones similares. Los dispositivos deben quedar instalados con sus KIT MOUNTING en los centros de cableado, racks o gabinetes, se deben identificar con las letras del alfabeto en mayúscula, en orden ascendente, de arriba hacia abajo, con cintas autoadhesivas y preimpresas, en la esquina superior izquierda.

Se deben instalar dispositivos de la misma marca o qua sean compatibles entre sí y siguiendo las recomendaciones del fabricante, para estandarizar conectividad.

En caso de ser necesario verificar el modelo del equipo a instalar (conexión entre dispositivos), la instalación entre ellos se debe tratar de hacer por los puertos de la parte trasera de los dispositivos, con los cables propietarios de la marca, conservando las limitantes y recomendaciones dadas por el fabricante en cuanto a la cantidad de dispositivos interconectados. Esto beneficia el rendimiento de la red, los puertos y del dispositivo como tal en la transmisión de información.

La Gobernación del Huila actualmente en pro de mejorar el rendimiento de la red cuenta dentro de sus edificaciones, diseñó conexiones tipo cascadas, estrella, stock (1° Piso todo; 2° Piso estrella; 3° Piso stock; 4° Piso stock; 5° Piso stock; 6° Piso Cascada), las cuales se ajustan a sus requerimientos en materia de Tecnología e información.

## Consideraciones Para Los Centros De Cableado

Los centros de cableado en general deben cumplir con las especificaciones de la norma EIA/TIA 569-A/B, las cuales deben ser tenidas en cuenta a la hora de instalar uno de ellos. Dentro de las recomendaciones se destacan en forma especial las siguientes:

En la Administración Central tiene implementado la Red de estrella, en este esquema todas las estaciones están conectadas a un concentrador o Switch de alto rendimiento con cable UTP de la red de cableado estructurado. Por ejemplo, en la estructura CLIENTE-SERVIDOR: el servidor está conectado al HUB activo, de este a los pasivos y finalmente a las estaciones de trabajo la cual tiene como punto principal.

Por piso solo debe existir un centro de cableado diferente al ubicado en el centro de cómputo principal del Back Bone IP, en caso de necesitarse la instalación de otro centro de cableado, el requerimiento será estudiado por parte del Grupo Tecnología, Conectividad y Telecomunicaciones para definir su ubicación y área de cubrimiento, entre otros aspectos.

Todos los centros de cableado existentes en los pisos deben ser instalados en gabinetes cerrados con puerta frontal en vidrio, con bisagras que permitan abrirla hacia fuera o desmontarla, con chapa de seguridad y sus respectivas llaves, no deben estar provistos de techos falsos, de ser posible las tapas laterales y trasera deben permitir ser desmontadas.

Los centros de cableado deben tener buena iluminación de emergencia y estar provistos de un sistema de ventilación (ventilador y/o extractor).

Los centros de cableado deben permanecer cerrados, y solo deben ser abiertos y manipulados por el personal encargado y autorizado por el Grupo de Informática y Telecomunicaciones y Servicios Generales cuando se requiera.

De la chapa de seguridad deben existir por lo menos 3 juegos de llaves con la siguiente distribución: 1 en el Grupo Informático y de Telecomunicaciones y los 2 restantes en Servicios Generales.

Deben estar provistos de la cantidad necesaria de tomas eléctricas para conectar los equipos que en él se instalaran. Las tomas eléctricas deben ser dúplex AC con polo a tierra y conectados a los circuitos de UPS.

Por ningún motivo se deben instalar o conectar definitiva o temporalmente dispositivos que no sean parte integral del centro de cableado o que no sean parte de la red corporativa de datos.

No se deben dejar por fuera del centro de cableado, equipos que estén conectados a las tomas eléctricas del centro de cableado, o dispositivos que sean equipos activos de la red corporativa de datos.

Los centros de cableado deben quedar debidamente identificados en los planos correspondientes del edificio.

Los centros de cableado que se instalen deben tener la capacidad de poder instalar en ellos la cantidad de equipos activos necesarios para cubrir los requerimientos de puntos de red en los puestos de trabajo del área a ser cubierta. Estas instalaciones deben cumplir con las normas y consideraciones dadas para instalación de cableado.

Los centros de cableado deben estar provistos de organizadores de cableado frontal para prestar una completa protección al cable y facilitar el mantenimiento.

En los centros de cableado se debe implementar la instalación de patch panel, esto facilita el uso de herramientas de poncheo y la identificación del cableado. No se deben hacer instalaciones directas de equipos de cómputo, es decir, del puesto de trabajo directamente al dispositivo activo (switch, concentrador, hub).

Los centros de cableado deben estar dotados del manejador de cable vertical y deben ser utilizados para organizar el cable dentro del rack, esto provee una completa protección al cable y facilita movimientos en caso de hacer cambios.

Los centros de cableado ubicados en los pisos deben estar conectados directamente al sitio donde la red del piso se conecta a la red corporativa.

## Consideraciones Para El Cableado Horizontal

Las consideraciones que se deben tener en cuenta para la instalación del cableado horizontal en la red corporativa de datos, se relacionaran para cada uno de los elementos que lo conforman, tales como: cables horizontales, tomas/conectores de telecomunicaciones en el puesto de trabajo, terminaciones en centros de cableado e interconexiones localizadas en centros de cableado. Adicionalmente se toman como referencia las normas y estándar internacional como la Norma IEEE 802.3 (Institute of Electrical and Electronic Engineeres - lnstituto de Ingenieros Eléctricos y Electrónicos) que es la norma asociada a las categorías del cableado estructurado.

* **Cables Horizontales**

Las rutas del cableado deben ceñirse estrictamente a las normas con respecto a las distancias máximas permitidas de acuerdo a cada tipo de cable usado y la utilización que se le dé.

El cable siempre debe ser transportado desde el centro de cableado hasta el puesto de trabajo en forma segura y confiable, por medios que tengan la capacidad y espacio suficiente para crecimiento futuro, tales como: bandejas o canaletas de aluminio o lamina, tuberías metálicas, duetos metálicos o en mampostería, zócalos de divisiones o de ventanas y muebles, canaletas perimetrales o por cielo raso, escalerillas, entre otros.

En la instalación de los medios de transporte del cable se deben cumplir los aspectos descritos en la norma EIA/TIA 568 y recomendaciones de los fabricantes respectivos, especialmente en lo relacionado con la capacidad de los mismos materiales, curvaturas máximas, exposición a campos magnéticos, compartiendo con otros cables.

Este cableado debe seguir la topología de red conocida estrella.

No se permiten empalmes de ningún tipo.

La distancia horizontal máxima no debe exceder 90 mts., la cual se mide desde la terminación en el patch panel hasta la toma/conector en el área de trabajo.

En la distancia del cableado horizontal se deben conservar 10 mts., para los cables del área de trabajo (de la toma/conector a la estación de trabajo) y del patch panel al equipo activo en el centro de cableado (switch, hub, concentrador).

Se debe realizar y obtener certificación de todos los cables instalados, esta certificación debe cumplir los parámetros (distancia, resistencia, impedancia, entre otros) determinados por la norma de acuerdo a la utilización del cable.

La certificación se debe realizar de punta a punta, es decir, desde el conector (plug) al computador en el puesto de trabajo hasta el conector (plug) que va al dispositivo activo (switche, hub, concentrador) en el centro de cableado al que está conectado el punto de red.

De la certificación obtenida se debe guardar copia (impresa y en archivo magnético) en Secretaría General y en el Grupo de Tecnología.

La certificación obtenida debe ser documentada con la identificación que se le haya dado al cable certificado, localización del puesto de trabajo, especificación del puerto del patch panel, concentrador y numero de puerto en el concentrador, y todos los datos que se considere ayuden a tener una ubicación rápida y clara del cable.

* **Tomas/ Conectores en el Puesto de Trabajo**

Todos los puestos de trabajo deben tener una toma/conector a la red corporativa, este debe estar debidamente instalado en un faceplate (caja plástica) bien sea empotrada en la canaleta o sobrepuesta en la cancelería, de uno o varias tomas.

Cada toma/conector de datos debe terminar su conexión en el patch panel del centro de cableado, es decir, no debe ir conectado directamente al dispositivo de la red (hub, concentrador o switch).

No se debe conectar equipos de cómputo directamente a los dispositivos de los centros de cableado.

Cada puesto de trabajo debe tener acceso a una toma de corriente eléctrica, el cual debe ser perteneciente al circuito de la UPS (unidad continua de potencia).

Todas las tomas/conectores de la red corporativa deben tener una nomenclatura que identifica el punto de red.

La nomenclatura que se le asigne a los puntos de red en los puestos de trabajo debe coincidir con la nomenclatura en el patch panel en el centro de cableado en el cual termina la conexión del punto.

Los cables que conectan los equipos (computadores) al torna/conector de la red corporativa no pueden exceder los 3 mts, de longitud y debe de ser cable UTP de contextura no rígida.

Todos los elementos instalados en los puestos de trabajo para conformar él toma/conector, así como el cable que conecta el computador a la toma/conector se trataran de proteger de daño físico, humedad y calor.

* **Terminaciones en los Centros de Cableado**

En los centros de cableado deben terminar todas las instalaciones de las tomas/conectores de los puestos de trabajo, terminando cada una de ellas en un conector en el patch panel, esto para no permitir la conexión directa de un equipo de cómputo al dispositivo de red (hub, concentrador o switch).

Todos los puertos del patch panel deben llevar la nomenclatura correspondiente a la toma/conector del puesto de trabajo al que está conectando.

En los centros de cableado no se deben tener conexiones directas de equipos de cómputo desde el puesto de trabajo al dispositivo de red (hub, concentrador o switch).

Las tomas/conectores de puestos de trabajo que se encuentren activos (equipo de cómputo trabajando en red), deben tener la conexión del respectivo puerto en el patch panel y dispositivo de red (hub, concentrador o switch) por medio de un patch lord y debe ser con cable UTP de contextura no rígida.

En todos los centros de cableado debe existir una o varias regletas de patch panel que permitir la conexión entre el puerto del patch panel y el puerto del dispositivo (hub, concentrador o switch) al que corresponda.

El orden en que se deben hacer las conexiones entre los puertos del patch panel y los puertos de los dispositivos será comenzando en la parte de arriba y de izquierda a derecha en los dos elementos.

Este procedimiento es repetitivo para los todos los dispositivos que se encuentren instalados en el centro de cableado y haciendo un buen uso de los organizadores de cable horizontales que se encontraran ubicados entre los patch panel y los dispositivos.

## Consideraciones Para El Cableado Vertical (Backbone)

El cableado vertical (Backbone) de la red corporativa de datos de la Gobernación del Huila, está conformado por un enlace principal en fibra óptica, debe existir como enlace de respaldo una fibra de las mismas características técnicas, estos enlaces deberán converger en el piso o en el centro de cómputo principal en un switch central de nivel preferiblemente que sea nivel 3.

Por las características tan especializadas del material utilizado para el cableado vertical de esta red, se opta por que todo trabajo en el que se vea implicado este cableado debe ser contratado con terceros que tengan la tecnología, el conocimiento y que puedan certificar lo realizado.

## Nomenclatura Par Puntos De Red

En esta parte se define el estándar para la marcación de los puntos de red, y así poder identificar los puntos, tanto en el puesto de trabajo como en los centros de cableado. Por ejemplo, el punto de Red CC1 - PP4 -30 (Centro de Cableado N° 1, Patch panel N° 4 y puerto de conexión 30)

Es importante tener en cuenta que todos los puntos de la red corporativa están bajo unos principios que facilitan la definición de este estándar, uno de estos principios es: "Por piso solo debe existir un centro de cableado, en caso de necesitarse la instalación de otro(s) centros de cableado, el requerimiento será estudiado por parte del Grupo de Tecnología, Conectividad y Comunicaciones y para definir su ubicación, área de cubrimiento, entre otros aspectos".

## Seguridad Física Del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe ser protegido contra interceptación o daño.

Dentro de las Recomendaciones tanto física y de Seguridad se debería tener en cuenta:

1. Se deben asegurar físicamente todas las áreas por donde se instalen o transporten cables.

2. Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de información deben ser subterráneas, siempre que sea posible, o sujetas a una adecuada protección alternativa.

3. El cableado de la red no debe estar al alcance de cualquier persona, es necesario apartarlo del acceso directo, esto por medio de canaletas, piso falso, cielo raso, entre otros.

4. Controlar todas las actividades realizadas por técnicos de servicio externo y consultores puestos que podrían intervenir en la red interna.

5. Los puntos de conexión de red no utilizados deben estar deshabilitados, porque cualquier persona puede utilizar un portátil para extraer información por uno de estos. Los cables UTP no deben circular junto a cables de energía dentro de los mismos medios de transporte por más corto que sea el trayecto.

6. En tendidos verticales se deben fijar los cables a intervalos regulares para evitar el efecto del peso en el acceso superior.

7. Al utilizar fijaciones (grampas, precintos o zunches) no excederse en la presión aplicada (no arrugar la cubierta), pues puede afectar a los conductores internos.

8. El destrenzado de pares individuales en los conectores y paneles de empate debe ser menor a 1.25 cm., para cables UTP categoría 6.

En la ruta del cableado se debe evitar el paso del cable por los siguientes dispositivos:

* Motores eléctricos grandes o transformadores (mínimo 1.2 metros).
* Cables de corriente alterna
* Luces fluorescentes y balastros (mínimo 1.2 centímetros)
* El dueto debe ir perpendicular a las luces fluorescentes, cables o duetos eléctricos.
* Equipo de soldadura.
* Aires acondicionados, ventiladores, calentadores (mínimo 1.2 metros).
* Otras fuentes de interferencia electromagnética y de radio frecuencia.

## ***Politicas De Seguridad Para Redes Inalambricas***

**Objetivo:**

* Garantizar las directrices en materia de seguridad en redes inalámbricas

**Directrices:**

* No divulgar innecesariamente la presencia de su instalación WiFi. Se debe cambiar periódicamente el SSID de sus equipos Inalámbricos y no dejar el que viene de fábrica.
* Instalar las antenas de punto de acceso (AP) en sitios fijos y seguros, con el estudio de cobertura de la señal a las aéreas requeridas.
* Los dispositivos perdidos o robados son también una amenaza. El filtrado - Autenticación por direcciones de Control de Acceso de Medios (MAC) son métodos de los dispositivos y adicionalmente los equipos se deben autenticar en la RED por medio de nombres de usuarios y contraseñas (servidores).
* Si la red inalámbrica va a ser usada para un propósito determinado, como el acceso a recursos empresariales específicos, entonces se configura los filtros de paquetes para que los datos que provienen de la red inalámbrica no puedan llegar a lugares indeseados. El firewall es la herramienta ideal para esta tarea.
* A los Access Point (AP) se monitorea activamente las configuraciones, su desempeño y toma de estadísticas de equipos conectados. Extreme la atención si no usa puntos de acceso y Cancelar puertos que no se emplean.

* Implementar políticas de administración en tiempo real. En muchas ocasiones las redes WiFi están ampliamente distribuidas. Por ejemplo, abarcan campus enteros e incorporan múltiples sitios globales. Las políticas de seguridad (Ej. listas de usuarios validados o derechos de acceso). El acceso esta complementado con normas WPA y 802.11i. Una WEP con un mínimo de encriptación de 128 bits y protección antivirus en todos los dispositivos móviles.

# POLÍTICAS DE SEGURIDAD DE LA RED

**Objetivo:**

* Establecer lineamientos en la seguridad de la red

**Directrices:**

* Al crear una política de seguridad de red, es importante entender que la razón para crear tal política es, en primer lugar, asegurar que los esfuerzos invertidos en la seguridad son costeables. Esto significa que se debe entender cuáles recursos de la red vale la pena proteger y que algunos recursos son más importantes que otros. También se deberá identificar la fuente de amenaza de la que se protege a los recursos. A pesar de la cantidad de publicidad sobre intrusos en una red, varias encuestas indican que, para la mayoría de las organizaciones, la pérdida real que proviene de los "miembros internos" es mucho mayor (tal cual se ha explicado anteriormente).

El análisis de riesgos implica determinar lo siguiente:

· Qué se necesita proteger

· De quién protegerlo

· Cómo protegerlo

* Los riesgos se clasifican por el nivel de importancia y por la severidad de la pérdida. No se debe llegar a una situación donde se gasta más para proteger aquello que es menos valioso.
* Si se quieren minimizar los riesgos (nunca hay un sistema 100%protegido), se debe tomar conciencia del problema y adoptar una metodología o guías para enfrentarlo. Esto comienza con el conocimiento profundo de la red, un análisis de amenazas y riesgos, la adopción de políticas de seguridad y finalmente la utilización de las tecnologías adecuadas para implantar un sistema de seguridad, el cual incorpore herramientas tales como criptografía, cortafuegos (Firewalls), monitoreo, auditoria junto con esquemas productivos que permitan adelantarse a los ataques y prevenirlos disminuyendo los impactos en las actividades normales de la Gobernación.
* Es responsabilidad de los administradores de las tecnologías informáticas y de telecomunicaciones, proveer la suficiente garantía y contabilidad que permita operar en las mejores condiciones y lograr un funcionamiento continuo de los sistemas bajo el mejor clima de confianza de los usuarios, garantizando el respeto por niveles adecuados de confidencialidad e integridad de la información que se procesa.
* Aunque son varios los elementos que conforman un sistema informático, es la INFORMACIÓN el recurso más preciado sobre el cual se enfocan todos los esfuerzos para asegurar un nivel aceptable de seguridad. Por esto, se destinan los objetivos básicos de la seguridad de la información y los cuales deben estar siempre presentes en las tareas de los administradores:

1. Confidencialidad: Asegurar que la información no este expuesta o sea revelada a personas no autorizadas.
2. Integridad: Asegurar consistencia de los datos, en particular prevenir la creación, alteración o borrado de datos de entidades no autorizadas.
3. Disponibilidad: Asegurar que los usuarios legítimos no obtengan acceso denegado a su información y recursos.
4. Uso legítimo: Asegurar que los recursos no sean usados por personas no autorizadas o en formas no autorizadas.

Riesgos

* Utilización del sistema por personas no autorizadas.
* Manipulación de información o aplicaciones por suplantación de usuarios
* Al interactuar en una red como Internet los posibles atacantes crecen en forma considerable y podrían realizar acciones como: Robo de información, espionaje industrial, estafas, extorsión, daño de sistemas, terrorismo, virus etc.

Amenazas

Amenazas fundamentales: Fugas de información, violación a la integridad, negación de servicios y uso ilegitimo.

Amenazas habilitadoras de las fundamentales: Suplantación, sobrepasar los controles, violación con autorización, caballo de Troya, puerta trasera, bombas lógicas, virus.

Amenazas subyacentes: Escuchar sin autorización, análisis de tráfico, indiscreción por personal, reciclaje de medios.

De todas las amenazas anteriores se dice que las más predominantes son:

Violación con autorización, suplantación, sobrepasar los controles, caballos de Troya y puertas traseras.

Que se debe proteger

1) Los típicos servidores con sistemas operativos como UNIX, Windows, Netware, etc. los cuales, de alguna forma, representan grandes riesgos.

2) Los protocolos de comunicaciones representan uno de los puntos de vulnerabilidad más utilizado en las redes.

3) Las aplicaciones del sistema o de los usuarios.

4) Bases de datos, entre otros tópicos.

5) Hardware: CPU, Tarjetas, teclados, terminales, estaciones de trabajo, impresoras, unidades de almacenamiento, líneas de comunicación, enrutadores, servidores de acceso remoto.

6) Software: Programas fuentes, programas objeto, utilidades, programas de diagnóstico, sistemas operacionales, programas de comunicaciones.

7) Datos: Durante la ejecución, almacenados en línea, almacenados fuera de línea, respaldos, rastreos de auditoría, bases de datos, en tránsito sobre los medios físicos de comunicación.

8) Personas: Usuarios, personal externo con uso de servicios locales.

9) Documentación: de programas, hardware, procedimientos de administración local.

10) Otros: Medios magnéticos, licencias, papel, formas, etc.

Son la respuesta a las amenazas, y responden al que se debe hacer para satisfacer los requerimientos de seguridad de la Organización y hacer frente a las amenazas.

Los servicios básicos que se deben desarrollar en un ambiente de comunicaciones son: Servicio de autenticación: Provee aseguramiento de la identidad de alguna entidad. Las contraseñas o passwords son la forma más común de proveer este servicio.

Autenticación es el servicio más importante ya que todos los otros servicios dependen en gran medida de este. Se puede implementar dos contextos de autenticación:

1. Autenticación de entidad: En el cual la entidad remota se identifica ante el servicio, también se conoce como autenticación simple.

2. Autenticación del0 origen de los datos: Autentica la fuente real de los datos sin importar que pase por muchos sistemas intermedios.

Servicio de control de acceso: Protege contra acceso e manipulación de recursos no autorizados. Contribuye directamente a lograr las metas de seguridad de confidencialidad, integridad, disponibilidad y uso legítimo. El modelo general para un control de acceso asume un conjunto de entidades activas llamadas Sujetos (Iniciadores) los cuales intentan acceder un miembro de un conjunto de recursos pasivos llamadas Objetos (Destinos).

Servicio de confidencialidad: Protege que la información sea divulgada o distribuida a entidades no autorizadas. Se distinguen dos tipos de confidencialidad:

1. Confidencialidad de datos: El cual está relacionada con el almacenamiento de la información.

2. Confidencialidad del flujo de tráfico: El cual está relacionada con el proceso de transmisión de información. Se dan tres casos diferentes de confidencialidad del flujo: Confidencialidad de un servicio orientado a la conexión, confidencialidad de un servicio no orientado a la conexión y servicio de confidencialidad de campo selectivo.

Servicio de integridad de datos: Asegura que los datos no sean cambiados, borrados o sustituidos sin autorización, al igual que el servicio de confidencialidad, diferencia entre integridad de datos e integridad de la comunicación.

Servicio de no repudio: Protege que cualquiera de las dos entidades que participen en una comunicación nieguen que el intercambio ha ocurrido. A diferencia de los anteriores servicios, el objetivo de este es proteger a los usuarios de la comunicación contra amenazas del otro usuario legitime más que de atacantes.

Cada una de las partes posee pruebas irrefutables ante desacuerdos del origen o destine de los datos. Sin embargo, la provisión de este servicio debe considerar el concurso de una tercera parte que ambos extremos de una comunicación continua:

Podemos distinguir dos casos:

1. Repudio de origen: El destino tiene pruebas demostrables, ante terceros de la autenticidad del origen de los datos.

2. Repudio de destino: El origen tiene pruebas demostrables ante terceros de la Autenticidad del receptor y recepción de los datos.

Las amenazas que se pueden presentar en un sistema operacional son las más variadas ya que aparte de las propias del sistema operacional, se le agrega la de todos los protocolos de comunicaciones.

## Seguridad De Acceso A Internet Y Conexiones Con Redes Externas

Los servicios de seguridad de control de acceso tienen por objeto garantizar que sólo accedan a la información y a los diversos recursos del sistema aquellos usuarios que tienen los derechos para ello. Los mecanismos a utilizar van desde una adecuada gestión de claves de acceso o passwords hasta las más complejas técnicas de cortafuegos o Firewall.

Acceso a la red de la Gobernación del Huila debe implementarse por un punto de acceso principal legalmente reconocido, en lo posible evitar diversas puertas de salida y entrada a la red.

El acceso a la red de la Gobernación del Huila, no debe restringirse solo a usuarios autorizados (quienes ingresan a la red corporativa por medio de terminales conectadas directamente, puertos de comunicaciones, redes de área local, estaciones remotas y redes públicas), también se deben tener restricciones y/o controles en los siguientes casos:

Se deben implementar por lo menos uno de los siguientes métodos de acceso remoto (como una VPN, ROSI, Frame Relay, Cable Modem, entre otros) para usuarios externos que requieran acceso a los recursos de la red corporativa de la Gobernación del Huila.

Servicios de información nacionales e internacionales; usuarios y empleados fuera de sus oficinas; clientes, contribuyentes, redes de institutos descentralizados, contratistas, bancos, proveedores, redes externas, es decir, brindar acceso a toda la comunidad en general; sin embargo, la seguridad interna y la integridad de la red. La red corporativa debe ser capaz de interactuar con el mundo exterior, utilizar los no debe verse comprometida.

No se debe permitir a los usuarios centralizados la conexión por modem y a la red interna simultáneamente. Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Gobernación.

El acceso a Internet en la Gobernación del Huila debe hacerse desde una estación debidamente registrada y/o autorizada. Dicho de otra forma, el computador debe estar registrado localizado con una dirección IP legitima de la Gobernación y este acceso debe estar totalmente administrado desde una consola que me permita tener registros del uso del servicio como, por ejemplo: páginas visitadas, tráfico generado por el equipo, hora de conexión y acceso a los servicios.

Por fuera del horario normal el acceso a intranet solo página como: www.huila.gov.co o de educación, es decir solo páginas con extensión gov.co y edu.co para evitar que los usuarios utilicen los recursos de la Gobernación de una forma inadecuada y dejen descargando durante toda la noche archivos de música o videos.

## Seguridad En El Acceso De Los Recursos De La Red Interna

Se debe poseer un sistema de identificación y autenticación de usuarios autorizados en el sistema y un sistema de control de acceso a la información y recursos de la plataforma tecnológica.

La identificación y autenticación de los usuarios en la red debe ser llevada a cabo por medio de un proceso normal de inicio de sesión en un servidor. Controladores de Dominio.

Todos los usuarios que acceden a los recursos informáticos de la Red Corporativa de la Gobernación del Huila requieren de una única e intransferible identidad, normalmente un username (nombre de usuario en la red) y un password (contraseña) para una persona y una identificación de la estación de trabajo. Esta identidad se usa para representar un usuario o un dispositivo en los ambientes informáticos de la red.

La Gobernación no debe permite la transferencia de claves o cuentas de identificación Personal entre cualesquiera individuos tanto a nivel interno como externo. Tal acción es considerada inaceptable y será sujeta a acción disciplinaria.

El control de acceso lógico a la Red Corporativa debe:

* Estar activo todo el tiempo.
* Controlar la entrada a cualquier sistema o aplicación.
* Utilizar perfiles de usuario y contraseñas individuales.
* Permitir el rastreo de actividades de usuario y recursos.
* Prevenir accesos no autorizados a recursos informáticos.
* Estos servicios se pueden implementar en los diferentes dispositivos de comunicación de la plataforma tecnológica como el Firewall, routers, servidores de dominio, etc.

Para prevenir ataques, cuando el software lo permita, cebe limitarse a 3 los intentos consecutivos infructuosos al introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al administrador del sistema.

Debe evitarse al máximo, el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes y otros recursos del sistema.

Si un PC tiene acceso a datos confidenciales, debe implementarse un mecanismo de control de acceso especial, preferiblemente por hardware.

El sistema debe llevar un registro de las claves anteriores de los usuarios con el fin de que estas no se repitan posteriormente. Debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

Cuando se vaya a efectuar una reparación a los computadores o equipos de red por personas distintas al personal del Grupo de Tecnología, Conectividad y Telecomunicaciones fuera de las instalaciones de la entidad se debe eliminar la información confidencial de estos o extraer las unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante de la Gobernación del Huila.

El acceso a archivos y carpetas de los servidores, debe controlarse por permisos y estos deben ser configurados por el administrador o por el propietario del recurso. Se pueden asignar recursos de solo lectura, escritura, ejecución, borrado y cambio de permisos o combinación de ellos.

Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 30 minutos. El re-establecimiento de la sesión requiere que el usuario se autentique mediante su contraseña.

El acceso de los usuarios a los sistemas de información y aplicaciones debe ser restringido a la información necesaria para ejecutar sus funciones y debe ser otorgado con la previa evaluación y autorización del administrador de la red.

Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada mes o meses.

Prohibir a ciertos usuarios permisos de escritura o borrado de algunos archivos, directorios o llaves de registro; con excepción de directorios donde la información pueda ser modificada.

Todos los perfiles y accesos de usuarios asignados a terceros (proveedores de servicios, personas de mantenimiento, contratistas temporales, etc.) Deben tener una fecha de expiración.

Cada usuario que se encuentre registrado en el sistema debe poseer una identificación y una clave de acceso únicas; el administrador de la red es el encargado de dar un adecuado control a dichas cuentas. Esta es una función compartida con el administrador de un sistema de información específico en el cual se deba crear un usuario y una contraseña con sus respectivos permisos de acuerdo a un perfil de usuario.

Definir una estructura estándar para la identificación de los usuarios dentro de la red y para acceder a los diferentes recursos a los cuales tenga permiso. Dicha estructura podría ser la siguiente:

Primer \_ Nombre. Primer \_apellido

Debe existir una cuenta única para cada usuario preferiblemente, cuando las circunstancias lo ameriten se puede crear cuentas compartidas.

Características mínimas que deben ser controladas para el manejo de contraseñas son:

 La longitud mínima debe ser de 8 caracteres.

 No debe tener relación directa con las características del usuario.

 Debe permitir caracteres alfanuméricos, mayúsculas, minúsculas, números y signos de puntuación y la combinación de estos.

Es necesario que los administradores motiven a los usuarios para que creen contraseñas fáciles de recordar solamente para ellos mismos, pero bastante difíciles de conseguir para otras personas.

Las cuentas privilegiadas deben tener un periodo de caducidad menor al establecido para los usuarios.

Se deben realizar revisiones periódicas (una vez cada treinta días) sobre el uso de las cuentas y los permisos de acceso establecidos, con el propósito de garantizar que los privilegios asignados a cada usuario del sistema si son los correspondientes de acuerdo a sus actividades operativas y funciones.

Los usuarios administradores deben poseer dos cuentas, una con privilegios extendidos que solo se utilice para administrar el sistema y la otra con privilegios limitados para utilizarse en el resto de actividades.

Periódicamente (semanalmente) el administrador del sistema es decir el ROOT o responsable general de la seguridad deberá chequear las acciones desempeñadas con las cuentas de administradores.

Cuando a un (unos) usuario(s) de la red le sean asignadas otras funciones laborales, inmediatamente debe ser notificado al administrador de red, por medio de peticiones especiales dirigidas al Grupo de Tecnología, Conectividad y Telecomunicaciones para que este proceda a su estudio y posterior modificación de su perfil de usuario, de acuerdo a sus nuevas funciones y permisos de acceso a los que tendrá derecho.

Cuando a un (unos) usuario(s) de la red no acceda a los recursos ya sea parcial (vacaciones, licencias, incapacidades, entre otros) o totalmente (despido o retiro) debe ser notificado al administrador de la red y al Grupo de Tecnología, Conectividad y Telecomunicaciones para que este proceda a bloquear o eliminar si es el caso su cuenta de usuario.

Es conveniente limitar el horario del uso de la cuenta de los usuarios a horarios estrictamente laborales (lunes a viernes de 7 a.m hasta las 6 p.m).

Los usuarios no pueden ser los encargados de crear perfiles y especificar quien tiene o no acceso, esta función es restringida solo a los administradores red encargados.

Si el sistema de control de acceso no está funcionando apropiadamente, debe rechazar el acceso de los usuarios, hasta que el problema se haya solucionado.

Configurar adecuadamente los permisos estándares e individuales que los usuarios tienen sobre los archivos y carpetas del sistema. Implementar el método de listas de control de acceso (ACL) para asignar permisos a usuarios y grupos concretos.

La aplicación para administrar los datos de usuarios solo deberá ejecutarse en máquinas designadas en el centro de cómputo o consolas remotas operadas únicamente por el administrador.

No permitir el ingreso a otros correos distintos al correo corporativo dentro de la red de datos de la Gobernación del Huila.

Implementar un sistema de detección de intrusos para identificar accesos indebidos a los recursos de la red corporativa de datos de la Gobernación del Huila. Herramientas como tcp­ wrapper, netlog, argus, tcpdump, SATAN, ISS, courtney, gabriel, nocol, tcplist, permiten tener información sobre los intentos de conexión que se han producido sobre un determinado sistema así como intentos de ataque de forma sistemática a puertos tanto de TCP como de UOP, nos permiten tener un control sobre todos los paquetes que entran por el interfaz de red de la maquina: IP (TCP, UOP) e ICMP, o analizar paquetes a nivel de aplicaciones (TELNET, FTP, SMTP, LOGIN, SHELL ... ) pueden ser utilizadas junto con otras que nos permitan definir desde que maquinas permitimos ciertas conexiones y de cuales se prohíben.

Algunas de estas herramientas pueden tener doble uso, es decir nos permiten protegernos ante posibles ataques, pero también podrían ser utilizadas para intentar comprometer los sistemas. Por eso es importante que el uso de estas herramientas este restringido para que no todo el mundo esté utilizándolas de forma aleatoria y nos oculten realmente un ataque.

También podrán ser utilizadas para hacer seguimientos en la red cuando creamos que alguna de nuestras maquinas ha sido comprometida. Existen también herramientas que chequean la integridad del sistema, estas ayudan a proteger el sistema. Se tienen dos tipos de estas herramientas. Las primeras se basan en chequeos a los ficheros y las segundas alertan de posibles modificaciones de ficheros, y, de programas "sospechosos" que puedan estar ejecutándose en la máquina de forma camuflada. Algunas de estas herramientas son: COPS (Computer Oracle and Password System), tigre, crack, Tripwire, chkwtmp, chklastlog, spar, Isof (List Open Files), cpm (Check Promiscuous Modé), ifstatus, osh (Operator Shell), noshell.

La instalación de tarjetas de acceso remoto, módems, RDSI, routers o cualquier otro dispositivo de comunicaciones debe ser hecha por el personal del Grupo de Tecnología, Conectividad y Comunicaciones o los contratistas debidamente autorizados e identificados.

Ninguna dependencia podrá instalar dispositivos de red sin el consentimiento y supervisión previa del administrador de la red, esto a fin de no alterar o inferir con dispositivos ya instalados y de no propiciar brechas de seguridad.

Todos los usuarios que tengan acceso a los equipos de comunicaciones deben estar autorizados y tener perfiles estrictamente definidos.

Asegurar que la totalidad del tráfico entrante y saliente de la red interna, sea filtrado y controlado por un elemento de seguridad (físico y lógico) prohibiendo de esta forma el paso de todo el tráfico que no se encuentre autorizado.

Utilizar cortafuegos para controlar el acceso de agentes externos que deseen ingresar a la red privada, utilizando software de seguridad o programas desarrollados para este fin.

No utilizar el cortafuego para el almacenamiento de archivos de propósito general o para ejecutar programas, excepto los que necesite el cortafuego.

Combinar diferentes técnicas de seguridad ya que el cortafuego por sí solo no puede garantizar o satisfacer todas las necesidades de seguridad.

El administrador de la red está obligado a revisar el registró de todas las incidencias producidas en los cortafuegos (archivos log's)) para asegurar el control y gestión adecuados, adicionalmente debe llevar una bitácora de las eventualidades se presenten y las acciones que se realicen para controlarlas.

Configurar los cortafuegos con base en decisiones corporativas acerca del tipo de accesos que mantendrán tanto los usuarios de la red local en internet como los accesos que se tendrán desde afuera a los datos de la red interna.

De haber una falla en el cortafuego, debe ser una "falla segura'', lo que significa que todos los accesos al servidor de Internet deben bloquearse.

Con el fin de disminuir la posibilidad de spoofing (falsificación de la dirección IP de una máquina de la red interna por un atacante externo) el cortafuego deberá denegar el acceso a cualquier tráfico de red externo que posea una dirección fuentes que debería estar en el interior de la red corporativa.

Mantener cerrados los puertos de comunicación que no se estén utilizando para impedir el acceso a intrusos.

Implementar herramientas de escaneo de puertos y vulnerabilidades, que permitan conocer el estado de la red en cuanto a su atacabilidad, es decir, que encuentren las vulnerabilidades e informen sobre las puertas que este n abiertas.

Implementar software tal como plataformas como Strobe, Nrnap, Portscanner, Saint, Nessus, entre otras permiten a los administradores verificar que puertos están siendo utilizados en la red y bajo que protocolos, para proceder a la aplicación de permisos para la utilización y justificación de estos puertos.

Monitorear el tráfico de la red corporativa de la Gobernación del Huila por medio de herramientas informáticas que faciliten dicha labor. Utilizar herramientas de monitoreo de tráfico con el fin de:

* Determinar qué servicios están siendo usados en cada uno de los puertos.
* Rastrear cambios en los registros del sistema que puedan ser realizados por actividades maliciosas.
* Detectar intrusos.
* Garantizar la integridad de los archivos que viajan por la red en busca de modificaciones no autorizadas.
* Detectar los usos indebidos del sistema.
* Las herramientas de monitoreo brindan al personal encargado una serie de estadísticas, por interface de red en la máquina, con las cuales los administradores pueden verificar el número de paquetes que se envían y reciben, y de qué tipo son.

Cuando un usuario se conecta a un servidor, se produce un intercambio de información entre ambos; es vital garantizar que los datos que recibe el cliente del servidor sean los mismos que se están enviando, esto es que no sufran modificaciones de terceros y también garantizar que la información que el usuario envía hacia el servidor no sea capturada, destruida o modificada por un atacante.

Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo un abuso, fraude u otro crimen que involucre los sistemas informáticos.

Los archivos de bitácora (loqs) y los registros de auditoría que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dichos archivos son importantes para la detección de intrusos brechas en la seguridad, investigaciones y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y solo los puedan leer las personas autorizadas.

# POLITICA DE TRANSFERENCIA DE INFORMACIÓN

**Objetivo:** Establecer lineamientos para mantener la seguridad de la información gestionada por la Gobernación del Huila, incluyendo información asociada a personas naturales determinadas o determinables o aquella que no tenga relación con personas determinadas, y que es transferida dentro de la Gobernación del Huila, y entre la Gobernación del Huila y cualquier otra entidad externa, a través de los canales autorizados para tal fin, y que son administrados y facilitados por la entidad (correo electrónico institucional, sistema de comunicaciones oficiales, FTP).

**Alcance:** Esta política aplica para toda la Administración Central Departamental de la Gobernación del Huila, todos sus funcionarios (personal de planta administrativa, personal de libre nombramiento y remoción, y contratistas de prestación de servicios), terceros, aprendices, practicantes, proveedores y ciudadanía en general, que realizan intercambio de información, a través de los canales autorizados para tal fin, y que son administrados y facilitados por la entidad (correo electrónico institucional, sistema de comunicaciones oficiales, FTP).

**Responsabilidades:**

* El Grupo de Tecnología es el responsable de poner a disposición los servicios a través de los cuales se disponen los canales autorizados para la transferencia de información dentro y fuera de la Gobernación del Huila, de acuerdo con los lineamientos de la presente política, mediante la administración de la plataforma que soporta el acceso a servicios tecnológicos asociados (correo electrónico, sistema de comunicaciones oficiales, FTP) para los funcionarios que desempeñen sus labores y/o actividades en la entidad.
* El jefe de dependencia y/o el supervisor del contrato, es el responsable de velar que el cumplimiento de la presente política se lleve a cabo por parte del personal a su cargo, de acuerdo con los lineamientos de seguridad establecidos. Así mismo, es el responsable de solicitar al Grupo de Tecnología la creación, modificación o cancelación de las cuentas de acceso a servicios tecnológicos, entre ellos el servicio de correo electrónico institucional, sistema de comunicaciones oficiales, y FTP, para los contratistas que por su objeto contractual necesiten acceso a éstos.
* El área de Talento Humano es la responsable de solicitar al Grupo TIC la creación, modificación o cancelación de las cuentas de acceso a servicios tecnológicos, entre ellos el servicio de correo electrónico institucional, para los funcionarios de planta, provisionalidad, y de libre nombramiento y remoción. Si se detecta que se solicita una cuenta institucional y que no se hace uso de ella, el Grupo TIC podrá eliminar dicha cuenta.
* Los funcionarios de la Gobernación del Huila son responsables de dar cumplimiento a la presente política y a las demás políticas plasmadas en el “*MANUAL DE POLÍTICAS DE USO, SEGURIDAD Y ADMINISTRACIÓN DE ACTIVOS TECNOLÓGICOS Y DE INFORMACIÓN DE LA GOBERNACIÓN DEL HUILA / Código: SGN-C043-M806 / Versión: 5*”, así como por las acciones u omisiones, y las respectivas consecuencias, sobre la transferencia de información dentro y fuera de la entidad, de acuerdo a las labores, funciones, responsabilidades del cargo que desempeña, y las autorizaciones y/o permisos pertinentes.

**Directrices Generales**

* La Gobernación del Huila realizará transferencia e intercambio de información con organizaciones gubernamentales, públicas y privadas, basados en la necesidad de la entidad que permita automatizar servicios y desarrollar proyectos y estrategias institucionales, fortaleciendo la gestión de la Administración Central Departamental.
* El Grupo de Tecnología de la Secretaría General implementará las herramientas y servicios tecnológicos de manera segura para la transferencia de información al interior y al exterior de la Gobernación del Huila, respetando la libertad y demás garantías constitucionales como consecuencia de la interoperabilidad que permita el pleno desarrollo de la función administrativa de la entidad, propendiendo a evitar la interceptación, copiado, modificación, enrutado y destrucción de ésta.
* De conformidad con la Ley 1581 de 2012 y la Política Institucional de Tratamiento de Datos Personales, la Gobernación del Huila podrá intercambiar y facilitar información sin autorización del titular en los casos indicados en el artículo 10 de la Ley 1581 de 2012 (*Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; Datos de naturaleza pública; Casos de urgencia médica o sanitaria; Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; Datos relacionados con el Registro Civil de las Personas.*) y a las personas a quienes se les puede suministrar la información (*A los Titulares, sus causahabientes(cuando aquellos falten) o sus representantes legales; A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial; A los encargado del tratamiento con un contrato de Transmisión de Datos personales de conformidad al artículo 25 del Decreto 1377 de 2013; A los terceros autorizados por el Titular o por la ley*).
* Los funcionarios de la Gobernación del Huila que traten temas o información clasificada como información reservada o información clasificada, deberán hacerlo en lugares seguros y/o por medios de comunicación seguros establecidos por la entidad, como el correo electrónico y el sistema de comunicaciones oficiales de la Extranet Corporativa.
* **Transferencia de información al exterior de la Gobernación del Huila**
  + La transferencia de información al exterior de la Gobernación del Huila deberá determinarse, ya sea a través de un convenio interadministrativo o contrato, siguiendo los lineamientos establecidos en el *Manual Módulo Contratación / SGN-C043-M816 / v.1*, definiendo claramente el tipo de información que se va a intercambiar entre la Gobernación y la entidad externa, incluyendo obligaciones o cláusulas de transferencia, confidencialidad y no divulgación de la información proporcionada, que establezcan las herramientas a utilizar para asegurar esta transferencia y cumplir la normatividad vigente nacional e internacional para el tratamiento de la información.
  + La transferencia de información al exterior de la Gobernación del Huila puede ser realizada por necesidad de alguna de sus dependencias, requerimiento y/o solicitud de un organismo externo, o incluso de un tercero que, ante disposiciones legales o directrices nacionales, hacen necesaria dicha interoperabilidad.
  + Las entidades receptoras de la información transferida por la Gobernación del Huila, deben salvaguardar a un nivel igual o mayor que el aplicado por la Gobernación al originar el documento, y cumplir con obligaciones de protección y garantía constitucionales, así como los principios de finalidad, utilidad y circulación restringida, en virtud de la política de interoperabilidad, las cuales deben quedar suscritas en los contratos y/o convenios que se suscriban, de acuerdo con lo establecido en la Ley 1581 de 2012.
  + Para el envío de información al exterior de la Gobernación del Huila, se utilizarán los servicios tecnológicos de correo electrónico institucional y sistema de comunicaciones oficiales, además de los servicios de mensajería física que sean contratados por la entidad y/o que sean necesarios para el envío de la información en medio físico.
* **Transferencia de información al interior de la Gobernación del Huila**
  + La transferencia y/o circulación de la información al interior de la Gobernación del Huila se realizará a través de los servicios tecnológicos dispuestos para tal fin: correo electrónico institucional, sistema de comunicaciones oficiales, y FTP, y ésta debe corresponder a información relacionada con las actividades a ejecutar en el ejercicio de sus labores.
  + Para el caso de funcionarios, contratistas de prestación de servicios, aprendices, practicantes, proveedores, y terceros en general vinculados a la Gobernación del Huila, siempre que se realice transferencia de información catalogada como clasificada o reservada, éste debe ser aprobado por el jefe directo o el supervisor de contrato.
* **Transferencia de información digital** 
  + La elaboración de las condiciones y estudios previos para el convenio interadministrativo o contrato que incluyan la transferencia de información digital con entidades u organizaciones externas, deberá realizarse de acuerdo al *Manual Módulo Contratación / SGN-C043-M816 / v.1*.
  + Las diferentes dependencias de la Gobernación del Huila serán las encargadas de transferir la información digital que requieran en el ejercicio de sus labores y desarrollo de proyectos y estrategias institucionales, siguiendo los lineamientos generales descritos en la presente política.
* **Transferencia de información Física**
  + El intercambio y/o transferencia de información en medios físicos durante cada uno de los procesos de gestión documental (producción, gestión y trámite, organización, transferencia, disposición de los documentos, preservación a largo plazo y valoración) se realizará de acuerdo a lo establecido por la Gobernación del Huila en el documento “*Política y Objetivos de Gestión Documental / DGO-C006-P816-F08 / v.2*”, y sus documentos relacionados.
  + La transferencia de información que se encuentre en formatos físicos debe estar debidamente etiquetada. En caso de que sea catalogada como información clasificada o información reservada, la transferencia debe realizarse en sobres o recipientes sellados para ser enviada a sus respectivos destinatarios, y propender que, a través de las empresas de mensajería que sean contratadas, se garantice que en su desplazamiento no sea intervenida o alterada por terceros ni afectada por amenazas de origen natural.
* **Transferencia de información vía correo electrónico institucional**
  + Toda información enviada desde la Gobernación del Huila, a través de correos electrónicos institucionales, al interior o al exterior de la entidad, deberá incluir en su pie de página la siguiente advertencia:

*\*\*\*\*\*\*\*\*\*\*\*\*\**

*AVISO LEGAL: La información enviada en este correo electrónico es confidencial y sólo puede ser utilizada por el destinatario del mismo. Está prohibida su divulgación o hacer público su contenido sin la debida autorización para ello. Si usted no es el destinatario del correo, tendrá prohibido darlo a conocer a persona alguna, así como reproducirlo o copiarlo. Si recibe este mensaje por error, deberá notificarlo inmediatamente al remitente, borrarlo de su sistema y/o buzón de correo electrónico de inmediato.*

*En consecuencia, le recordamos su deber de mantener la reserva sobre el contenido, los datos o información de contacto del remitente y en general sobre la información de este documento y/o archivos adjuntos. De esta manera, se deberá atender lo dispuesto en las normas pertinentes, entre ellas, la Ley 1581 de 2012 y la Ley 1712 de 2014.*

*\*\*\*\*\*\*\*\*\*\*\*\*\**

**Requerimientos Mínimos**

* Equipo de cómputo personal o corporativo.
* Correo electrónico institucional.
* Acceso al servicio de FTP en equipo de cómputo personal o corporativo.
* Credenciales de usuario y acceso a Extranet corporativa – Sistema de Comunicaciones Oficiales.
* Servicio de conectividad en red y conexión a internet en las instalaciones de la Gobernación del Huila.

**Violaciones y Consecuencias de Incumplimiento:** El incumplimiento a la política de transferencia de información de la Gobernación del Huila, podrá traer consigo la pérdida de confidencialidad, integridad y disponibilidad de información gestionada por la entidad, y necesaria para el cumplimiento de las diferentes actividades enmarcadas en los distintos procesos de gestión de la entidad, y la prestación de los diferentes trámites y servicios a usuarios. Igualmente, podrá traer consecuencias legales que apliquen a la normativa de la entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere (Ley 1273 de 2009 de Delitos Informáticos, Ley 1581 de 2012 de Habeas Data, Ley 734 de 2002 “Código Disciplinario Único”, entre otras).

# POLÍTICAS DE CORREO ELECTRONICO

**Objetivo:**

* Definir los lineamientos y/o directrices generales para la adecuada protección, en el uso del servicio eficiente del correo institucional

**Generalidades y Directrices:**

* El uso del correo electrónico será primordial para el apoyo en el desempeño de las labores inherentes a cada cargo y facilitará la comunicación y conectividad institucional.
* La asignación de usuarios para el correo electrónico se realiza únicamente para los funcionarios de planta, provisionalidad y libre nombramiento y remoción, y en casos excepcionales a los contratistas que por el desarrollo de sus funciones deban tener una cuenta en el correo corporativo.
* Los funcionarios a los cuales se les ha autorizado el uso de correo electrónico son responsables de todas las actividades realizadas con sus usuarios de acceso al correo, así como de mantener un comportamiento ético y evitar prácticas o usos que puedan comprometer la seguridad de la información de la Gobernación del Huila.
* Todo usuario del correo electrónico deberá leer y responder oportunamente los mensajes y citaciones que se les envíen por este medio; con el fin de aprovechar el mayor beneficio que ofrece la rapidez y la efectividad de las comunicaciones.
* La contraseña o clave de acceso al correo electrónico es la mejor defensa contra el uso no autorizado del mismo y/o de la red de datos de la Gobernación del Huila, por lo tanto, se requiere que se mantenga con la mayor reserva, no debe suministrarse a otras personas o exhibirse en público.
* Informar al Grupo TIC sobre mensajes sospechosos de SPAM, suplantación de identidad, u otras prácticas que puedan estar relacionadas con delitos informáticos, a fin de bloquear dicho remitente y evitar que esos mensajes lleguen a más funcionarios. Igualmente se deben marcar estos mensajes como no deseados desde la cuenta del usuario del correo.
* La Gobernación del Huila se reserva el derecho de monitorizar el correo electrónico, con fines de control, gestión y seguridad.

**Responsabilidades:**

* El área de Talento Humano es la responsable de solicitar al Grupo TIC la creación, modificación o cancelación de las cuentas de acceso a servicios tecnológicos, entre ellos el servicio de correo electrónico institucional, para los funcionarios de planta, provisionalidad, y de libre nombramiento y remoción. Si se detecta que se solicita una cuenta institucional y que no se hace uso de ella, el Grupo TIC podrá eliminar dicha cuenta.
* El jefe de dependencia o el supervisor del contrato, es el responsable de solicitor al Grupo TIC la creación, modificación o cancelación de las cuentas de acceso a servicios tecnológicos, entre ellos el servicio de correo electrónico institucional, para los contratistas que por su objeto contractual necesiten acceso a éstos.
* El usuario es responsable por las acciones u omisiones, y las respectivas consecuencias, sobre los asuntos que a través del correo electrónico institucional deba atender, de acuerdo a las labores, funciones y responsabilidades del cargo que desempeña en la entidad.
* El Grupo TIC es el responsable de administrar la plataforma tecnológica que soporta el acceso al servicio de correo electrónico institucional para los funcionarios que desempeñen labores o actividades en la Gobernación del Huila.

**Prohibiciones y usos no aceptables:**

Se prohíbe rotundamente usar el correo electrónico, para el envío de cualquier mensaje de correo a través del servidor de la entidad y que lleve consigo el nombre de la Gobernación del Huila, en alguna de las siguientes actividades:

* Difundir al interior o al exterior de la entidad material fotográfico que contenga escenas de sexo, nudismo, violencia o cualquier otra que atente contra la integridad de las personas o instituciones.
* Enviar información confidencial o reservada de la Gobernación del Huila a personas u organizaciones externas, salvo en los casos expresamente previstos en la Constitución Política y en la Ley, y por parte de los funcionarios autorizados internamente para ello.
* Utilizar el correo para hacer promociones y propagandas comerciales, así como responder mensajes donde le solicitan información personal o financiera, para participar en sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Este tipo de mensajes fomentan cadenas o correo spam, tanto al interior como al exterior de la entidad, ya que atentan contra la seguridad y el buen rendimiento de la red y del servicio de correo electrónico.
* Divulgar información de instituciones políticas, militares o con ánimo de lucro, ya que esta herramienta es de uso exclusivo para fines institucionales.
* Servir de mecanismo para la difusión de virus informáticos enviando archivos de dudosa procedencia y que no tienen nada que ver con las funciones de la institución.
* Enviar correos a más de un destinatario de la red sin que su fin no sea difundir una directriz de tipo administrativa o cualquier otra que no vaya estrictamente ligada al cumplimiento de la misión institucional.
* No se permite el uso del correo electrónico para envío de tarjetas de felicitaciones o motivos especiales, invitaciones particulares, negocios personales y en general comunicaciones de tipo personal.
* El uso de la correspondencia en forma electrónica, permite disminuir costos, por lo cual no se deberá imprimir lo recibido por e-mail mientras no sea necesario o autorizado, pues esto generaría un costo adicional para la Entidad.

Por último, es de recordar la atención primordial que se debe realizar al correo electrónico institucional, dispuestos en el portal web de la Gobernación del Huila como canales de atención a organismos judiciales y entes de control ([notificaciones.judiciales@huila.gov.co](mailto:notificaciones.judiciales@huila.gov.co)).

# POLÍTICAS DEL USUARIO FINAL

**Objetivo:**

* Garantizar el uso eficiente de los correos electrónicos y de dominio institucionales.

**Aplicabilidad:**

Estas son políticas que aplican usuarios (funcionarios, contratistas y cualquier otra persona o entidad) que por razón de su trabajo se le permita acceso o tenga relación con la Gobernación del Huila.

**Directrices:**

* El correo electrónico se presenta de una manera explícita como un recurso de la Gobernación para el uso institucional, no para uso personal, por lo cual no se debe utilizar el correo electrónico interno con fines personales, solo con miras a aumentar la efectividad y productividad de la organización. El propósito del correo es proporcionar una herramienta que permita facilitar y agilizar la comunicación entre los usuarios del sistema, en cualquier momento y desde cualquier lugar.
* Esta total mente prohibido transmitir a través del correo electrónico información sensible de la Gobernación del Huila sin previa autorización.
* Es importante tener en cuenta que el uso del Correo electrónico es exclusivamente para los funcionarios de la Gobernación del Huila que se encuentren registrados en la base de datos de Personal Administrativo. Aquellas personas que no pertenecen a este grupo no podrán hacer uso del sistema de Correo Electrónico.
* El correo electrónico, es de uso personal, por lo tanto, para acceder al mismo se ha configurado un nombre de usuario y clave con anticipación. El adecuado uso del sistema, así como su operación, son de exclusiva responsabilidad del usuario titular del mismo. En este sentido, y tal como sucede con cualquier sistema, se recomienda cambiar la contraseña con regularidad y una vez sea entregada esta cuenta oficialmente por un miembro del grupo de Tecnología, Conectividad y Comunicaciones.
* La configuración es la siguiente: primernombre.primerapellido. Clave inicial: gobernación.
* Con el fin de garantizar el óptimo desempeño del sistema de Correo Electrónico, cada usuario tiene asignado un espacio ilimitado en su buzón, dicho espacio corresponde a la suma de todos los elementos de correo: mensajes entrantes, mensajes salientes, contactos, elementos del calendario, tareas, y otros.
* El uso del sistema de correo electrónico para la distribución de información no solicitada o propaganda no relacionada a las actividades normales y asuntos de la Gobernación, no está permitido. Mandar y/o contestar cadenas de correo, ya que hacen perder el tiempo y copan el tráfico en la red, haciendo más lento el servicio.
* El correo electrónico no se debe utilizar para transmitir mensajes despectivos, difamatorios, comentarios acerca de raza o religión, edad, incapacidad, política, atributos físicos o preferencias sexuales de las personas. Transmitir mensajes con contenido ofensivo, amenazante, vulgar o pornográfico.

## Procedimientos Para El Uso Y El Manejo Del Sistema

Como todo sistema, el Correo Electrónico tiene asignado un administrador quien se encarga de administrar y dar cumplimiento a las políticas definidas.

Para solicitar el Cambio de Atributos:

Por razones de seguridad toda nueva cuenta de correo se crea con los atributos mencionados en las políticas citadas anteriormente. Para e cambio de un atributo especial, se deberá hacer la solicitud mediante al Grupo de Tecnología, Conectividad y Comunicaciones quien dará su visto bueno en la aceptación de dicho atributo.

En Caso de Olvido de la Contraseña:

Para el caso de olvido de la contraseña y por tratarse de un sistema que debe garantizar la seguridad a todo nivel, el usuario deberá enviar la solicitud Por medio de su cuenta y por el correo institucional le será notificada su nueva contraseña.

Administración del Espacio de Almacenamiento para cada Buzón:

Aunque cada buzón tiene un número ilimitado de almacenamiento de información, se hace necesario depurarlo, se les recomienda revisar permanentemente los mensajes nuevos, almacenar los que se consideren estrictamente necesarios y borrar los atendidos. De esta manera siempre su buzón estará disponible. Depurar los contenidos del buzón, esto es, examinar y eliminar diariamente los mensajes que ya no sean necesarios.

## Políticas Operativas

**Objetivo:**

* Mantener las directrices mediante el uso óptimo de las actividades operativas.

**Aplicabilidad:**

Estas son políticas que aplican usuarios (funcionarios, contratistas y cualquier otra persona o entidad) que por razón de su trabajo se le permita acceso o tenga relación con la Gobernación del Huila.

**Directrices:**

* Para la mejor administración y por lo tanto optimización de los servicios ofrecidos en la entidad es necesario que los usuarios finales tengan en cuenta las siguientes recomendaciones y políticas de uso:
* Se deja patente la posibilidad de sanción por el uso indebido, y se establece un estamento organizativo responsable de controlar el uso correcto representado por el Grupo de Tecnología, Conectividad y Comunicaciones.
* Se apela al sentido común de los funcionarios para que comprendan que cuando usan un recurso de la entidad, como es el correo electrónico, con un fin empresarial, la privacidad no puede ser plena.
* A ningún miembro de la Gobernación, le será permitido interceptar, leer, copiar o modificar datos electrónicos privados (ya sea en tránsito a través de la red o almacenados dentro de una computadora) sin el consentimiento escrito del propietario legítimo.
* Cuando no se esté haciendo uso de sistemas en red (aplicativos, Internet o correo), se deben cerrar y salir de ellos, para evitar trafico innecesario en la red.
* El usuario no debe guardar su contraseña en una forma legible en archivos, en discos, tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarse inmediatamente. No deben usarse contraseñas previamente empleadas.
* Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con ella.
* La contraseña inicial emitida a un nuevo usuario solo es válida para la primera sesión. En ese momento, el usuario debe cambiar la contraseña.
* Está prohibido alterar el software o la configuración del hardware de cualquier dispositivo sin la respectiva autorización.
* El usuario será responsable por el cuidado de los elementos de la infraestructura informática puesta a su disposición e informará oportunamente cualquier novedad al respecto.
* Los usuarios deben ser responsables de cumplir con todas las políticas de la Gobernación del Huila relativas a la seguridad informática.
* Cuando un usuario reciba una nueva cuenta, debe firmar un documento donde declarara conocer las políticas y procedimientos de seguridad y aceptar sus responsabilidades con relación al uso de esa cuenta.
* Los usuarios deben desconectarse o bloquear el equipo cuando se vayan a ausentar de la estación de trabajo. (control+alt+supr)
* Debe respetarse y no modificar la configuración de hardware y software establecida por el Grupo de Tecnología, Conectividad y Telecomunicaciones.
* No se permite la instalación y utilización de software no licenciado previamente ya que esta acción puede acarrear sanciones penales y disciplinarias.
* No divulgar información confidencial de la Gobernación a personas no autorizadas.
* No permitir y no facilitar el uso de los sistemas informáticos en la Gobernación a personas no autorizadas.
* No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Gobernación.

# CONFIDENCIALIDAD

Debido al carácter confidencial de la información, el personal de la Gobernación del Huila deberá de conducirse de acuerdo a los códigos de ética profesional, normas y procedimientos.

El propietario de los activos de información debe estar claramente identificado.

Toda la información debe ser clasificada de acuerdo a su confidencialidad.

La información confidencial debe estar físicamente guardada de manera segura.

El responsable de la información debe establecer los permisos adecuados de acceso a la misma.

En el caso de terceros que por motivos relacionados con actividades propias de la entidad necesiten acceso a la información deberán firmar un acuerdo de no difusión y confidencialidad.

Las llaves de cifrado son confidenciales y personales, así como los passwords de acceso a equipos, software y aplicaciones, no se permiten su difusión y de ser así es bajo responsabilidad del propietario.

El personal ocasional y los usuarios externos aun no contemplados en un contrato formalizado (que contenga el acuerdo de confidencialidad) deberán firmar el acuerdo mencionado antes de que se les otorgue acceso a las instalaciones de procesamiento de información.

Los acuerdos de confidencialidad deben ser revisados cuando se producen cambios en los términos y condiciones de empleo o del contrato, en particular cuando el empleado está próximo a desvincularse de la organización o el plazo del contrato está por finalizar.

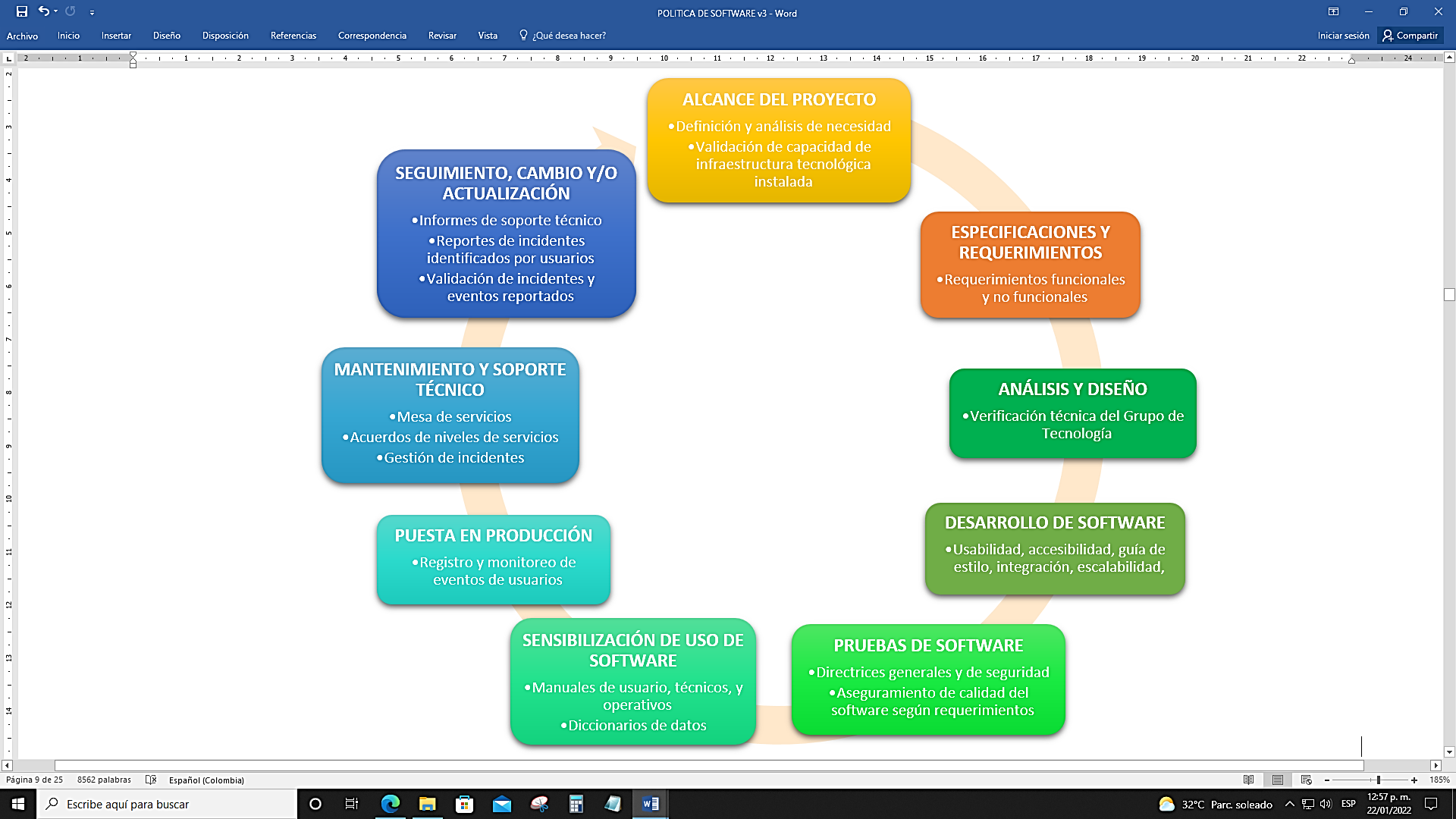
# CAPITULO 8:

# ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

# ADQUISICIÓN, DESARROLLO, SOPORTE, MANTENIMIENTO, RETIRO, CAMBIO Y/O ACTUALIZACIÓN DE SOFTWARE

## Ciclo De Vida De Un Software, Aplicativo Y/O Sistema De Información

Como punto de partida para establecer los diferentes procedimientos que se deben abarcar frente a la gestión de software en la Administración Central, en la siguiente figura se presenta el ciclo de vida de un sistema de información, con sus respectivas etapas, a partir de los lineamientos y directrices establecidos en la Política de Gobierno Digital del Estado Colombiano, el Marco de Referencia de Arquitectura Empresarial, y la Norma Técnica ISO/IEC 12207:2017.



* **Alcance del Proyecto – Fase Planeación**

En esta etapa las dependencias de la Gobernación del Huila expresan la necesidad de apoyar mediante software, aplicativos y/o sistemas de información el cumplimiento de sus funciones, tareas, procesos y/o procedimientos a partir de la normatividad pertinente como leyes, decretos, resoluciones, políticas, directrices, planes de desarrollo, auditorias, planes de mejoras entre otros que sustenten esta necesidad.

Uno de los requisitos de esta etapa es contemplar una planeación de dicha adquisición, cambio, desarrollo, acceso, soporte técnico, mantenimiento y/o actualización de software, teniendo en cuenta la alineación estratégica de los proyectos de software con los procesos y planes de TI de la Entidad de tal forma que exista coherencia entre las metas de alto nivel y los esfuerzos que hace cada una de las áreas y de los funcionarios.

A través de la mesa de servicios TIC (correo electrónico [soporte.tic@huila.gov.co](mailto:soporte.tic@huila.gov.co) – teléfono 608 8671300 extensión 1107), los jefes de las dependencias o los líderes de procesos deben solicitar de manera oficial al Grupo de Tecnología acompañamiento y/o asesoría frente a adquisición, cambio, desarrollo, acceso, soporte técnico, mantenimiento y/o actualización de software, aplicaciones y sistemas de información de propiedad o candidatos a implementar en la Entidad.

* **Especificaciones y Requerimientos – Fase Planeación**

En esta etapa, los jefes de dependencias, responsables funcionales y responsables técnicos designados establecen las especificaciones y requerimientos que soportan las necesidades expresadas para la adquisición, desarrollo, mantenimiento y/o actualización, cambio y/o retiro de software. Se establecen requerimientos funcionales y no funcionales, (es decir los requerimientos técnicos adoptados por la Entidad).

Estos requerimientos se consignan en el ***Formato de recolección y especificación de requerimientos / SGN-C043-P808-F01 / v1***. Los requerimientos funcionales serán diligenciados y aprobados por el responsable funcional o líder del proceso en donde se va a adelantar un proceso de adquisición, desarrollo, mantenimiento y/o actualización, cambio y/o retiro de software. Para llevar a cabo esta tarea se debe documentar el ***Formato de recolección y especificación de requerimientos / SGN-C043-P808-F01 / v1,*** debidamente aprobado y validado por todos los roles que en el intervienen.

Los responsables técnicos del Grupo de TIC harán un revisión y acompañamiento si es el caso a la recolección de estos requerimientos funcionales.

Los requerimientos no funcionales, características de plataforma tecnológica a adquirir (software y hardware), de modo que se valide la disponibilidad y la capacidad instalada en el Centro de Datos de la Gobernación para soportar el nuevo software.

En esta etapa el Grupo de Tecnología emite un concepto sobre la capacidad tecnológica existente instalada en el Centro de Datos y la verificación de los respectivos requerimientos técnicos adoptados para la gestión de software en la Administración Central Departamental, dando cumplimiento a estándares de Política de Gobierno Digital del Estado Colombiano, el Marco de Referencia de Arquitectura Empresarial, y la Norma Técnica ISO/IEC 12207:2017.De modo que, si es necesario, se incluyan dentro las especificaciones y requerimientos la adquisición de la infraestructura tecnológica (Hardware y/o software: licenciamiento de motores de base de datos, sistemas operativos entre otros) necesarios para el desarrollo y/o puesta en producción del software.

El resultado de las especificaciones y requerimientos técnicos debe plasmarse en los estudios y/o documentos previos del Proceso de Contratación y de la misma manera servir de insumo para el estudio de mercado.

De igual forma, la Etapa de **Especificaciones y Requerimientos** se deben considerar e incluir las siguientes exigencias mínimas, políticas y lineamientos adoptados por la Entidad y que son transversales a cualquier proceso de adquisición, desarrollo, mantenimiento y/o actualización, cambio y/o retiro de software, y que deberán ser exigidos a los proveedores, clasificados en los siguientes componentes:

* Dentro de los requisitos funcionales deben adicionarse como mínimo: Módulos de configuración y parametrización del software y Módulos para la disposición de auditoría, registro y monitoreo de eventos de usuarios.
* Lineamientos de usabilidad, accesibilidad e interoperabilidad para que el software cumpla con las expectativas de la organización en términos de la generación de valor.
* Usabilidad y accesibilidad de nivel A y AA de conformidad, definidos en la Norma Técnica NTC5854, en la interfaz web del software.
* Asegurar la visualización y acceso de la solución de software mediante diferentes navegadores web y a través de pantallas de dispositivos móviles (Smartphone y/o tabletas).
* Las directrices generales y de seguridad establecidas en la ***Política General de Seguridad y Privacidad de la Información / SGN-C043-POL01 / v.1,*** asegurando la calidad y el cumplimiento de los requerimientos funcionales y no funcionales del software. y otras adicionales como el Top 10 de vulnerabilidades de OWASP, validando la aplicación de controles de acceso al software, mediante la autenticación de usuarios dentro y fuera del servidor de dominio de la entidad.
* Aplicación de guía de estilo, especificaciones y lineamientos de usabilidad definidos por el MinTIC en el documento “*Anexo 1. Lineamientos para estandarizar las ventanillas únicas, portales de programas específicos de programas transversales del Estado y sedes electrónicas”*, disponible en <https://gobiernodigital.mintic.gov.co/692/articles-161264_Anexo_1_Resolucion_2893_2020.pdf>).
* Estructuración de datos e integración del software mediante webservices usando arquitecturas SOAP o REST, cuando se requieran integraciones con otros sistemas de información.
* Entregar el diseño descriptivo de la arquitectura de la solución de software. (En caso de venta de licencia de software)
* Entregar el diccionario de datos de la solución de software.
* Entregar el procedimiento de backups de información y datos de la solución de software.
* Entregar el código fuente del software desarrollado. (En caso que sea desarrollo propio por parte de la Entidad)
* Tramitar la cesión de derechos de autor como requisito de recibido del software desarrollado (En caso que sea desarrollo propio por parte de la Entidad)
* Entregar el licenciamiento a nombre de la Entidad (Gobernación del Huila) en caso de adquisición de software de terceros, debidamente soportado con registro de derechos de autor a nombre del Fabricante/proveedor.
* Si se trata de un proceso de cambio de software se debe incluir plan de migración de la información y los datos, para ser costeado por las partes intervinientes tanto del software de salida y software de entrada. Dentro de la planificación de la puesta en producción, debe incluirse la migración de bases de datos actuales, en caso de que corresponda a cambio o reemplazo del software.
* Habilitar ambientes de pruebas antes de paso a producción.
* Realizar un plan de pruebas para la realización de casos o escenarios de prueba, que permitan evaluar las funcionalidades y verificar los resultados esperados, teniendo en cuenta no utilizar para ello datos sensibles y/o datos personales en este proceso.
* Realizar pruebas de carga, estrés y rendimiento del software, con el fin de evaluar la cantidad de peticiones que puede soportar.
* Realizar pruebas de regresión, posterior a las anteriores pruebas descritas, con el fin de verificar la no existencia de defectos o errores en el software, producto de las pruebas o modificaciones que se realicen sobre éste.
* Realizar las pruebas de aplicación del procedimiento de backup programados para el respaldo y restauración del software, validando la información almacenada y restaurada.
* Entregar los manuales de usuario, administración, técnicos y los que sean necesarios, de acuerdo con los roles y responsabilidades establecidos para el uso y administración del software.
* Entregar el plan de capacitación teniendo en cuenta las temáticas, cantidad de usuarios a capacitar, los roles y responsabilidades establecidos para el uso y administración del software.
* Incluir dentro de las condiciones del soporte técnico a fallas y soporte post implementación como mínimo los siguientes términos: alcance, duración y costo.

Una vez diligenciado el Formato de recolección y especificación de requerimientos, el responsable funcional debe verificar, en coordinación con el Grupo de Tecnología, el cumplimiento de los requisitos mínimos generales y de seguridad establecidos en la **Política General de Seguridad y Privacidad de la Información / SGN-C043-POL01/v.1** y de esta forma, desarrollar o contratar la adquisición, diseño e implementación de éste, teniendo en cuenta las etapas del ciclo de vida de software para la Entidad.

* **Análisis y Diseño – Fase de ejecución**

Una vez definidos las especificaciones y requerimientospara la adquisición, desarrollo, mantenimiento y/o actualización, cambio y/o retiro de software, los cuales deben ser consignados y aprobados en el ***Formato de recolección y especificación de requerimientos / SGN-C043-P808-F01 / v1***, los jefes de dependencias y/o responsables técnicos y funcionales de la Entidad deben adelantar el proceso contractual correspondiente.

Siendo el ***Formato de recolección y especificación de requerimientos / SGN-C043-P808-F01 / v1,*** el insumo principal para que los proveedores de soluciones de software y/o fábrica de software contratados adelanten la fase de análisis y diseño de la solución.

* **Desarrollo de Software – Fase de Ejecución**

Una vez definidos las especificaciones y requerimientospara la adquisición, desarrollo, mantenimiento y/o actualización, cambio y/o retiro de software, los cuales deben ser consignados y aprobados en el ***Formato de recolección y especificación de requerimientos / SGN-C043-P808-F01 / v1***, los jefes de dependencias y/o responsables técnicos y funcionales de la Entidad deben adelantar el proceso contractual correspondiente.

Siendo el ***Formato de recolección y especificación de requerimientos / SGN-C043-P808-F01 / v1,*** y los documentos técnicos que corresponden a la etapa de análisis y diseño detallado los insumos para que los proveedores de soluciones de software y/o fábrica de software contratados adelanten la fase de desarrollo de software.

* **Pruebas de Software y validación de requerimientos.**

En esta etapa, la supervisión asignada, los responsables técnicos y responsables funcionales junto con los proveedores contratados, deben velar por el cumplimiento de las especificaciones del producto de software desarrollado/implementado, realizando el seguimiento de las pruebas en los ambientes de pruebas y producción respectivamente, hasta obtener la funcionalidad y operación adecuada.

Siendo el ***Formato de recolección y especificación de requerimientos / SGN-C043-P808-F01 / v1***, los documentos técnicos de la etapa de análisis y diseño detallado y las demás obligaciones estipuladas en los documentos contractuales los insumos para la verificación y ejecución de las pruebas.

Todas las pruebas que se realicen deben documentarse en un informe, que incluya al menos la siguiente información:

* Nombre del software y/o sistema de información objeto de la prueba.
* Fecha de realización.
* Ambiente en el que se desarrolló la prueba.
* Resultados obtenidos.
* Observaciones y opciones de mejora si aplican.
* Participantes y/o asistentes.
* **Sensibilización de Uso de Software**

En esta etapa, la supervisión asignada, los responsables técnicos y responsables funcionales junto con los proveedores contratados deben adelantar y dar cumplimento al plan de capacitación y la entrega del material (manuales de usuario, manuales técnicos, manuales de administración y configuración y/o video tutoriales) de la solución de software estipulados en el ***Formato de recolección y especificación de requerimientos / SGN-C043-P808-F01 / v1.***

Esta etapa debe cumplir con la socialización, capacitación y transferencia de conocimiento a todos los funcionarios que serán usuarios de la solución de software abarcando los diferentes roles y coordinar con el Grupo de Tecnología, la capacitación al personal encargado de atención de la mesa de servicios TIC de la Entidad, en caso de que se integre el servicio de soporte técnico de este software a los servicios TIC gestionados por el Grupo de Tecnología de la Secretaría General.

Estas capacitaciones y sensibilizaciones deben ser documentadas, incluyendo las memorias con las temáticas incluidas y el listado de asistencia a cada jornada de capacitación y sensibilización que se realice. Igualmente documentar el formato ***Asistencia a Formaciones y Capacitaciones/SGN-C043-F07/ v.1*** del Proceso Gestión y seguridad de tecnologías de la Información de MIPG

Los manuales de usuario, manuales técnicos, manuales de administración y/o configuración debe ser debidamente codificados e ingresados como tipo de documento: Manual al Proceso de Calidad que corresponda la misión que cubre el sistema de información/software.

* **Puesta en Producción**

En esta etapa, el supervisor del contrato debe coordinar con el Grupo de Tecnología de la Entidad, el proceso de puesta en producción y despliegue del software en el Centro de Datos, y suscribir acta de entrega al Grupo de Tecnología del software y hardware pertinente, si es el caso.

Cabe recordar que, dentro de la planificación de la puesta en producción, debe incluirse la migración de bases de datos actuales, en caso de que corresponda a cambio o reemplazo del software y la configuración y parametrización del software para entrar en producción.

* **Mantenimiento y Soporte Técnico**

Para las soluciones nuevas a adquirir a través de licenciamiento y/o desarrollo a la medida a través de fábrica de software, los jefes de dependencias, responsables funcionales y/o responsables técnicos deben hacer cumplir las condiciones y el alcance del mantenimiento y soporte técnico exigido al contratista y las cuales fueron estipuladas en ***Formato de recolección y especificación de requerimientos / SGN-C043-P808-F01 / v1***.

Para las soluciones existentes y en producción en la Entidad los jefes de dependencias, responsables funcionales y/o responsables técnicos deben definir y establecer las necesidades de mantenimiento y soporte técnico para las mismas y estos serán insumos para los contratos de soporte técnico y mantenimiento que se adelanten con proveedores externos. Para lo cual se debe diligenciar el Formato ***Cronograma: Mantenimiento de Equipos Tecnológicos; Soporte de Sistemas de Información, y Soporte, Administración y Seguridad Informática / SGN-C043- F02 / v.2*** del Proceso **Gestión y seguridad de tecnologías de la Información** de MIPG

En los contratos de soporte con proveedores externos se deben definir como mínimo los acuerdos de niveles de servicios, en los que se definan las características del servicio, personal requerido, límites y umbrales de servicios, tiempos de atención, tiempos máximos de indisponibilidad, niveles de impacto, niveles de prioridad, tipos de soporte, tipos de atención, datos de contacto de agentes del servicio, metas del servicio. Toda solicitud de mantenimiento y soporte técnico debe ser registrada en la **MESA DE SERVICIOS TIC** para llevar su respectiva trazabilidad y los proveedores deben hacer uso de esta herramienta.

Para el caso que se registren requerimientos de desarrollo de mejoras/actualización del software por parte de los usuarios en la **MESA DE SERVICIOS TIC,** el responsable técnico y/o responsable funcional debe realizar la identificación de necesidades y requerimientos legales, normativos, de planes de mejora y/o reglamentarios que obliguen a la Entidad a realizar ajustes, cambios, y/o mejoras correspondientes a una contratación de mejora o actualización del software. Para lo cual se debe diligenciar el Formato ***Cronograma: Mantenimiento de Equipos Tecnológicos; Soporte de Sistemas de Información, y Soporte, Administración y Seguridad Informática / SGN-C043- F02 / v.2*** delproceso **Gestión y seguridad de tecnologías de la Información** de MIPG.

En caso tal de que se haya realizado una transferencia de conocimiento al personal de mesa de servicios TIC (Personal del grupo TIC) para la atención y soporte técnico del software, se deben llevar a cabo los ajustes al software que se encuentren dentro del alcance de las responsabilidades del personal de atención de mesa de servicios, que sean producto de eventos y/o incidentes del software, o labores de mantenimiento solicitados por parte de las dependencias usuarias de éste. Toda solicitud de mantenimiento y soporte técnico debe ser registrada en la **MESA DE SERVICIOS TIC** para llevar su respectiva trazabilidad.

En general todos los eventos y/o incidentes identificados por parte de los usuarios del software, y la validación, tanto de incidentes y eventos reportados por los usuarios, como de las labores de soporte técnico, mantenimiento, y ajustes realizados en la ejecución de contratos de soporte y mantenimiento deben ser gestionados a través de la **MESA DE SERVICIOS TIC**.

* **Seguimiento, Cambio y/o registro de actualización**

En esta etapa, los supervisores de contratos de soporte técnico a las soluciones de software que se encuentran en producción en la Entidad y el Grupo de Tecnología son los encargados de registrar el seguimiento a los mismos para lo cual debe mantenerse actualizada la Hoja de Vida de cada Sistema de Información/software que se encuentre en uso en la Entidad mediante el formato ***Hoja de Vida Sistemas de Información/Software/Aplicaciones / SGN-C043-P808-F02 / v1***, delproceso **Gestión y seguridad de tecnologías de la Información** de MIPG.

Los insumos para alimentar el formato ***Hoja de Vida Sistemas de Información/Software/Aplicaciones / SGN-C043-P808-F02 / v1*** serán:

* Información de los contratos de soporte/actualizaciones suscritas con el valor de la inversión.
* Los informes de soporte técnico y mantenimiento presentados por parte del desarrollador/proveedor.
* Los registros de despliegues/ Paso a producción de actualizaciones.
* La instalación de nuevas versiones y registro de principales cambios documentados en el certificado de derechos de autor para las soluciones con licenciamiento.
* El registro de la actualización de derechos de autor a nombre de la Gobernación del Huila en caso de ser solución desarrollada para la Entidad.
* Registrar las situaciones presentadas en el comportamiento o funcionamiento del software por los usuarios finales o responsables funcionales que no hayan sido solucionadas dentro de los contratos de mantenimiento y soporte técnico del sistema de información/software.

Lo anterior, con el fin de realizar el respectivo seguimiento y realimentación del ciclo de vida de un sistema de información/software, para los casos que se necesite hacer análisis ya sea en mejoras y actualizaciones del software o en retiro y cambio de éste, en caso de que no se cumplan las expectativas ni los objetivos deseados.

En el caso de que se registren solicitudes de retiro y/o cambio del software en la **MESA DE SERVICIOS TIC**, los responsables técnicos, funcionales y/o usuarios finales deben revisar los registros realizados en la hoja denominada ***“Situaciones – Seguimiento***” del formato ***Hoja de Vida Sistemas de Información/Software/Aplicaciones / SGN-C043-P808-F02 / v1,*** frente a las situaciones presentadas en el comportamiento o funcionamiento del software por los usuarios finales o responsables funcionales que no hayan sido solucionadas dentro de los contratos de mantenimiento y soporte técnico del sistema de información/software.

Para los casos que no se encuentre documentadas las situaciones mencionadas y se solicite un cambio de software, todos los usuarios finales deberán diligenciar la hoja denominada ***“Situaciones – Seguimiento***” del formato ***Hoja de Vida Sistemas de Información/Software/Aplicaciones / SGN-C043-P808-F02 / v1,*** donde se registren las situaciones presentadas en el comportamiento o funcionamiento del software que no hayan sido solucionadas dentro de los contratos de mantenimiento y soporte técnico del sistema de información/software.

Una vez registradas las situaciones, se procederá a hacer el respectivo análisis técnico a cada una de las situaciones reportadas en la hoja denominada ***“Situaciones – Seguimiento***” del formato ***Hoja de Vida Sistemas de Información/Software/Aplicaciones / SGN-C043-P808-F02 / v1,*** verificando las evidencias reportadas y veracidad de las mismas. Posteriormente el Grupo de TIC emitirá un concepto de viabilidad técnica del cambio, o la formulación de un plan de mejora requerido para el Sistema de información/software existente.

Si el análisis técnico resulta en que se requiere un cambio de software, se debe realizar un análisis comparativo entre las funcionalidades, ventajas, beneficios, utilidades y costos de los softwares existentes en el mercado, con respecto al software que posee actualmente la entidad, para subsanar las situaciones encontradas. con el fin de con el fin de evaluar su disponibilidad, reputación, idoneidad, eficacia, ajustes a las necesidades, y requerimientos funcionales y no funcionales de la Gobernación del Huila para encontrar la mejor alternativa frente a calidad y precio.

Este análisis será el insumo para el componente económico y jurídico de la futura contratación., así como también estudios de mercado para comparar el software, y/o sistemas de información existentes.

# CAPITULO 9:

# GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

# COMUNICACIÓN DE INCIDENTES EN MATERIA DE SEGURIDAD

Se debe concienciar a todos los funcionarios y contratistas acerca de los procedimientos de comunicación de los diferentes tipos de incidentes (violaciones, amenazas, debilidades o anomalías en materia de seguridad) que podrían producir un impacto en la seguridad de los activos de la Organización.

El mecanismo implementado para comunicación de incidentes debe permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información debe utilizarse para identificar incidentes o anomalías recurrentes o de alto impacto. Esto puede señalar la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros, o de tomarlos en cuenta en el proceso de revisión de la política de seguridad y administración de recursos.

Se debe requerir que los usuarios (funcionarios y contratistas) comuniquen cualquier incidente advertido o supuesto al punto de contacto o responsable designado tan pronto como sea posible. Los usuarios deben advertir, registrar y comunicar las debilidades o amenazas supuestas u observadas en materia de seguridad, con relación a sistemas o servicios.

El principal medio de comunicación de anomalías debe contener procesos de realimentación para garantizar que los usuarios que comunicaron incidentes sean notificados de los resultados una vez tratados y resueltos los mismos, se debe realizar por medio telefónico o correo electrónico.

Se debe informar a los usuarios que ellos no deben, bajo ninguna circunstancia, intentar probar una supuesta debilidad. Esto se lleva a cabo para su propia protección, debido a que el intentar probar debilidades puede ser interpretado corno un potencial mal manejo del sistema.

Los usuarios no deben quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados por el responsable del recurso del Grupo de Tecnología, Conectividad y Comunicaciones. La recuperación debe ser realizada por personal adecuadamente capacitado y experimentado.

# CAPITULO 10:

# DISPONIBILIDAD DE SERVICIOS E INFORMACIÓN

# POLÍTICA DE SERVICIOS TIC

**Alcance:** Esta política aplica a la Administración Central Departamental de la Gobernación del Huila, todos sus funcionarios (personal de planta administrativa, personal de libre nombramiento y remoción, y contratistas de prestación de servicios), terceros, aprendices, practicantes, proveedores y ciudadanía en general, que en su calidad de usuarios y beneficiarios de servicios tecnológicos establecidos en el catálogo de servicios TIC incluido en el Plan Estratégico de Tecnologías de la Información -PETI- de la Gobernación del Huila, reportan incidentes y requerimientos, realizan solicitudes de servicios de TIC a través de la mesa de servicios, y evalúan el servicio a través encuestas de satisfacción y calidad.

**Objetivo:** Gestionar y entregar servicios TIC eficientes y de calidad al talento humano de la Gobernación del Huila, para su uso y apropiación en el desarrollo de los diferentes planes, programas, proyectos e iniciativas, que permitan la toma de decisiones para el cumplimiento de los objetivos estratégicos de la entidad.

**Responsabilidades:** Con el fin de realizar la debida gestión y prestación de servicios de TIC en la Gobernación del Huila, a continuación, se describen los roles de los funcionarios encargados de la atención de la mesa de servicios de TIC:

* + *Personal de Planta* 
    - *Técnico Operativo*
    - *Profesional Universitario*
    - *Profesional Especializado*
  + *Contratistas*
    - *Profesional de Apoyo*
    - *Prestadores de Servicios de Soporte Especializados*
    - *Proveedores de Servicios*

**Responsabilidades de los usuarios:**

* + Realizar sus requerimientos o solicitudes de servicios de TIC a la mesa de servicios, usando para ello los diferentes canales provistos para tal fin (teléfono fijo, correo electrónico, comunicación interna generada en el sistema de comunicaciones oficiales).
  + Incluir en el contenido de sus requerimientos o solicitudes, información detallada de sus datos de contacto (dependencia, usuario, número telefónico) y de la situación que origina la solicitud.
  + Prestar el acompañamiento y facilitar al personal de soporte técnico asignado, el acceso a los equipos, impresoras y hardware en general, a través de los cuales se proporcionarán los servicios de TIC solicitados a la mesa de servicios.
  + Estar atento a las respuestas y comunicaciones que emita el personal de soporte técnico, a través de los diferentes canales descritos, relacionados con ampliación de información de la solicitud, respuestas parciales o totales a las solicitudes y requerimientos presentados.
  + Evaluar y calificar la calidad, oportunidad y eficiencia de servicios de TIC prestados a través de la encuesta facilitada para tal fin por la mesa de servicios TIC.

**Directrices:**

* Registro, Clasificación y Análisis: Toda solicitud de servicios TIC debe ser registrada en el software de mesa de servicios vigente y dispuesto para tal fin, teniendo como canales de atención: teléfono fijo, correo electrónico, y comunicación interna generada en el sistema de comunicaciones oficiales. Cuando una solicitud sea reportada, se deberán desarrollar las siguientes etapas:
  + - **Registro:** Deberá realizarse de inmediato en el aplicativo vigente de mesa de servicios, para no incurrir en costos posteriormente y generar demoras indefinidas en la aparición de nuevas incidencias. Deberá garantizarse que se disponga como mínimo de la siguiente información: número de solicitud, tipo, prioridad, fecha y hora de registro, usuario que hace la solicitud, datos de contacto para notificaciones, y descripción de la solicitud.
    - **Clasificación:** Se define la categorización, nivel de prioridad, Asignación de Recursos y Monitorización.
    - **Análisis:** Se identifica si el incidente o requerimiento corresponde a una incidencia ya resuelta y se procede a aplicar el procedimiento asignado. Si la resolución no está dentro de las posibilidades de solución de la mesa de ayuda, redireccionar a un nivel superior.
    - **Solución:** En esta etapa se deberá confirmar con los usuarios la solución satisfactoria del mismo, incorporar el proceso de resolución, reclasifica el incidente si fuera necesario, actualizar la información sobre los elementos de configuración implicados en el incidente y cerrar el incidente.
* Evaluación: Se debe realizar evaluación de los requerimientos y solicitudes para determinar un posible rechazo en caso de que no aplique el tipo de solicitud a un servicio de TIC. Si se rechaza, se debe comunicar al solicitante o usuario, vía correo electrónico que su solicitud fue rechazada, con la respectiva justificación.
* Medios de Contacto:
  + - La Secretaría General de la Gobernación del Huila deberá disponer de una línea o extensión telefónica de contacto para atención de solicitudes y requerimientos de servicios TIC.
    - El Grupo TIC de la Gobernación del Huila deberá disponer de un correo electrónico de contacto y de un aplicativo de gestión de servicios, para atención de solicitudes y requerimientos de servicios TIC.
* Catálogo de servicios: Los servicios TIC que ofrezca el Grupo TIC de la Gobernación del Huila, deben estar publicados en el catálogo de servicios TIC de la entidad, con sus respectivos acuerdos de niveles de servicios, tiempos de ejecución y resolución de actividades y solicitudes de servicios.
* Base de datos de incidentes: Adicionalmente al registro, y una vez finalizada la atención de las solicitudes de servicios TIC, se debe generar y alimentar una base de datos de incidentes y requerimientos con información sobre el tipo de requerimiento, área encargada de prestar el servicio, solución aplicada, nivel de satisfacción del usuario, entre otros datos e información que permita generar análisis y mejoramiento de los procesos y servicios de TI.
* Tipos de requerimientos o solicitudes: El Grupo TIC debe definir los tipos de solicitud o reporte que se recibirán a través de la mesa de servicios.
* Niveles de criticidad, disponibilidad e impacto: El Grupo TIC debe definir los niveles de criticidad de cada uno de los servicios incluidos en el catálogo de servicios TIC de la entidad, así como los niveles de disponibilidad mínima de éstos.
* Niveles de soporte y atención a requerimientos: El Grupo TIC debe definir los niveles de soporte y atención que se pueden realizar a cada uno de los requerimientos y solicitudes de servicios de TIC, y de esta forma asignar los recursos que sean necesarios para la óptima solución de los requerimientos.

**Requerimientos mínimos:**

* Herramientas – Software y Hardware
  + - Correo electrónico asignado para la recepción de solicitudes en la mesa de servicios.
    - Teléfono o extensión telefónica asignado para la recepción de solicitudes en la mesa de servicios.
    - Aplicativo o herramienta de gestión de servicios de TI para la gestión de solicitudes de servicios TIC.
    - Servicio de conectividad en red y conexión a internet en las instalaciones de la Gobernación del Huila.
* Personal
  + - Agentes de Primer Nivel (Grupo de soporte - técnicos)
    - Agentes de Segundo Nivel (Profesionales analistas)
    - Agentes de Tercer Nivel (Personal Especializado para atender incidentes especializados)

**Acuerdos de Nivel de Servicio**

Periodo de validez: 09/10/2020 – 09/10/2022

Líder de Gestión de Niveles de Servicio:

* Coordinador de Tecnología, Conectividad y Telecomunicaciones
* PBX (57-8) 8671300 Ext. 1104
* Alcance de soporte técnico de incidencias y requerimientos

Los funcionarios con contrato vigente con la Gobernación del Huila cuentan con varios canales de comunicación para la solución de incidencias, con un equipo técnico para atención que provee soluciones a problemas con excelentes tiempos de respuesta y con personal especializado para visitas en sitio, en casos en que sea requerido.

La Mesa de Ayuda, atenderá los incidentes y peticiones necesarios para el normal funcionamiento de los activos y servicios de TI. Las incidencias registradas por persona no pueden ser superiores a DOS (02) incidencias diarias, en el caso de que sean de causas diferentes. Si se registran más de DOS (02) incidentes, éstos se informarán al usuario para priorizar su atención.

Las solicitudes registradas como incidentes, en caso de que sean repetitivas y requieran un cierre definitivo de su causa, serán atendidas a través de un plan de acción para identificar y cerrar la causa raíz que lo ocasiona.

Con el fin de garantizar una buena comunicación entre usuarios y proveedores del servicio, es necesario tener en cuenta los siguientes aspectos que se deben detallar al momento de registrar un incidente:

* + Descripción del problema (¿Qué ocurre? ¿Cómo ocurre?)
  + Sitio donde se presenta el problema (Físico o digital -sistema operativo o redes internas y externas-)
  + Resultado esperado

La prestación del servicio de incidentes y peticiones se atenderá por medio del correo electrónico [soporte.tic@huila.gov.co](mailto:soporte.tic@huila.gov.co), y del PBX (57-8) 8671300 Ext. 1104, en los horarios descritos a continuación:

* + Horario laboral: Corresponde a cinco (05) días a la semana, de 7:00 am – 12:00 m y 2:00 pm – 6:00 p.m. (lunes a jueves) y de 7:00 am – 12:00 m y 2:00 pm – 5:00 p.m. (viernes)

La disponibilidad de atención del servicio de soporte técnico en horario laboral será del 99,9%, frente a su horario de atención 5x8, según la siguiente disponibilidad:

|  |  |  |  |
| --- | --- | --- | --- |
| Disponibilidad | Horario de Atención | Fiabilidad | Indisponibilidad |
| 99,9% | 8 horas diarias  5 días de la semana | 8 horas y 30 minutos de disponibilidad diarios frente a las llamadas vía celular y teléfono fijo | 30 minutos diarios. |

Niveles de Servicio:

* Primer Nivel: Los incidentes son resueltos por el Operador de Primer Nivel durante la primera llamada del usuario, después del primer contacto vía e-mail, o mediante herramientas de soporte técnico remoto.
* Segundo Nivel: Los incidentes son resueltos durante la visita de personal de soporte técnico en sitio a la posición de trabajo del usuario, por medio de una llamada del operador de 2° nivel, o es escalado por la Mesa de Servicio a otras líneas de soporte para orientar una solución especializada.
* Tercer Nivel: Los incidentes son escalados a los proveedores y/o especialistas de soporte para su resolución.

Informes de Servicio:

En los primeros 8 días hábiles del mes vencido, se entrega al supervisor el informe del servicio con la siguiente información:

* + Reporte de casos del mes con los estados y tiempos de atención
  + Indicadores de uso, solución de incidentes y peticiones.
  + Propuestas para mejorar la prestación del servicio.

Contactos de la Mesa de Ayuda:

* Operador de Primer Nivel – Técnico de Soporte
  + PBX (57-8) 8671300 Ext. 1104
  + E-mail: [soporte.tic@huila.gov.co](mailto:soporte.tic@huila.gov.co)

Se cuenta además con un equipo de operadores en los niveles II y III, centralizados por el operador de primer nivel, quien además asignará los incidentes o requerimientos a los niveles correspondientes.

* Dueño del Servicio
  + Nombre: Profesional Especializado - Coordinadora TIC
  + PBX: (57-8) 8671300 Ext. 1104

Plazos de entrega del servicio:

|  |  |  |  |
| --- | --- | --- | --- |
| . | | | |
| Tipo de Solicitud | Nivel | SLA | Observaciones |
| Servicio 1: Internet | | | |
| Falla del servicio de internet | Alto | 4 horas máximo para entrega de solución | Ausencia total del servicio |
| Medio | 8 horas máximo para entrega de solución | Ausencia parcial del servicio |
| Bajo | 24 horas máximo para entrega de solución | Error que afecta el ingreso a un portal específico |
| Servicio 2: Soporte y asistencia técnica a usuarios | | | |
| Soporte en software básico, instalación de programas y configuración de red | Estándar | 8 horas máximo a partir del reporte | Soporte básico prestado sobre equipos dentro del inventario de la entidad |
| Mantenimiento preventivo y correctivo de equipos de cómputo y periféricos | Estándar | 72 horas máximo a partir del reporte | Sujeto a disponibilidad de suministros, partes y periféricos de repuesto. |
| Servicio 3: Conexión a redes WiFi | | | |
| Fallas de acceso a redes WiFi | Estándar | 8 horas máximo a partir del reporte | Se revisa la actividad de los equipos y se bloquean los no activos o que representen algún riesgo de seguridad |
| Servicio 4: Gestión de usuarios y correo electrónico | | | |
| Falla de acceso a dominio de la entidad | Estándar | 24 horas máximo para entrega de solución | El servicio se realiza desde el servidor de administrador de dominio |
| Falla de acceso al correo electrónico | Estándar | 12 horas máximo para entrega de solución | La contraseña de acceso debe ser renovada cada tres meses por directrices de seguridad |
| Servicio 5: Página web | | | |
| Caída de la página web | Externo | 24 horas máximo para entrega de solución | Se tiene ANS con proveedor |
| Publicación de documentos en página web | Alto | 4 horas máximo a partir del reporte | Documentos de extrema urgencia |
| Bajo | 24 horas máximo a partir del reporte | Documentos regulares |
| Servicio 6: Sistemas de información | | | |
| Incidentes y requerimientos de sistemas de información internos o externos que soportan procesos misionales | Externo | 24 horas máximo para entrega de solución | Se tiene ANS con proveedores |
| Servicio 7: Soporte a la operación del sistema financiero SIFA | | | |
| Creación de usuarios | Estándar | 8 horas máximo a partir del reporte | Autorizada por la Secretaría de Hacienda |
| Incidentes y requerimientos | Externo | 24 horas máximo para entrega de solución | Se tiene ANS con proveedor |
| Servicio 8: Soporte a la operación del sistema de Comunicaciones Oficiales | | | |
| Creación de usuarios y perfiles | Estándar | 8 horas máximo a partir del reporte | Se debe tener usuario de Extranet |
| Fallas en la creación y/o envío de comunicaciones | Externo | 24 horas máximo para entrega de solución | Se tiene ANS con proveedor |
| Incidentes y requerimientos | Externo | 24 horas máximo para entrega de solución | Se tiene ANS con proveedor |
| Servicio 9: Telefonía fija | | | |
| Programación de extensiones | Estándar | 8 horas máximo a partir del reporte | Ninguna |
| Mantenimiento de la red telefónica y de aparatos telefónicos | Alto | 4 horas máximo a partir del reporte | Atención urgente a Gestión del Riesgo y Atención al Ciudadano |
| Bajo | 72 horas máximo a partir del reporte | Atención estandarizada |
| Fallas del servicio | Externo | 24 horas máximo para entrega de solución | Se tiene ANS con proveedor |
| Servicio 10: Backup | | | |
| Almacenamiento de información de respaldo de los sistemas de información administrados por el Grupo TIC en el centro de datos | Estándar | 24 horas máximo a partir del reporte | Sujeto a Capacidad de almacenamiento del centro de datos |
| Pérdida de información de respaldo de los sistemas de información administrados por el Grupo TIC en el centro de datos | Estándar | 96 horas máximo para entrega de solución | Priorizado por el nivel de importancia de los procesos que lideran y la información que manejan |
| Servicio 11: Conceptos Técnicos | | | |
| Emisión de conceptos técnicos | Alto | 5 días hábiles máximo a partir del reporte | Proyectos o estudios previos que involucren la adquisición, renovación o modificación de infraestructura tecnológica de la entidad |
| Bajo | 15 días hábiles máximo a partir del reporte |
| Servicio 12: Extranet | | | |
| Falla de acceso a Extranet | Externo | 24 horas máximo para entrega de solución | Se tiene ANS con proveedor |
| Falla de acceso a módulos y sistemas de información | Externo | 24 horas máximo para entrega de solución | Se tiene ANS con proveedor |

Interrupción del servicio: Interrupción que permite realizar mantenimiento preventivo al servicio, con un mínimo impacto sobre los clientes, no puede ocurrir durante los horarios del servicio establecidas.

El horario establecido para la interrupción del servicio será desde las 06:00 AM del sábado hasta las 06:00 AM del siguiente día hábil. Dependiendo de los servicios que se inhabiliten, puede ajustarse y minimizarse el tiempo máximo de interrupción.

El procedimiento para cada tipo de interrupción será:

* El profesional de servicios notificará vía e-mail a la entidad que se presentará una interrupción del servicio.
* El profesional del servicio responsable mantendrá al tanto al cliente sobre los avances y resolución de la incidencia.

Los tipos de interrupciones podrán ser notificadas por parte del cliente o el proveedor del servicio, estas podrán ser:

* Interrupción planificada del servicio: Se requiere una notificación con una antelación mínima de 3 días antes de que ocurra una interrupción programada.
* Interrupciones no programadas: Una interrupción no planificada de un servicio será un corte inmediato en el servicio debido a un problema de “falla del sistema” y se notificará inmediatamente al cliente.

**Responsabilidades de los usuarios:**

* Entrega de los insumos necesarios para la atención oportuna del servicio (información exacta, completa y válida).
* Adoptar los niveles de seguridad para evitar el acceso de personal no autorizado a la información sensible.
* Responder a las encuestas que se enviaran por parte del proveedor del servicio, junto con el e-mail de entrega de la respuesta o solución al servicio requerido.

**Responsabilidades del proveedor del servicio:**

* Avisar con anticipación y oportunidad los hechos y factores que puedan afectar el cumplimiento de los términos del contrato.
* Rendir informes periódicos al supervisor del contrato sobre el avance y cumplimiento del cronograma presentado e informe final sobre la ejecución del contrato.
* Atender las solicitudes que haga el supervisor en procura del cumplimiento cabal y oportuno del contrato.
* Garantizar el cumplimiento de los SLA, realizando las mediciones necesarias a las metas del servicio.
* Entrega de informes en los periodos establecidos.
* Garantizar el cumplimiento de obligaciones contractuales pactadas.
* Garantizar los parámetros establecidos en este documento.

**Quejas y Reclamos**

Si en las actividades de seguimiento al servicio por parte del cliente o los auditores internos del servicio de soporte técnico, se encuentra una falta de cumplimiento de los acuerdos de niveles del servicio, el usuario tendrá el derecho de reportar una queja o insatisfacción del servicio, la cual podrá registrarse por medio de la mesa de servicios al correo [soporte.tic@huila.gov.co](mailto:soporte.tic@huila.gov.co), y por medio del sistema de comunicaciones oficiales.

Al identificar la no conformidad del servicio, se aplicará el procedimiento de acción de mejora, con el objetivo de garantizar que el servicio cumple con las expectativas requeridas. Posteriormente se socializará a los usuarios el plan de acción a ejecutar para su validación.

**Metas del Servicio:**

Mantener la atención oportuna en un rango entre el 90% - 100% de las solicitudes registradas y clasificadas como incidentes y requerimientos.

**Excepciones:**

* Los tiempos de atención no incluyen los que sean derivados por procedimientos internos, para la entrega de insumos, aprobaciones e implementación de cambios (configuraciones, pruebas de cambios, restauraciones, migraciones). Cuando esto sucede, el caso pasa a estado “Pendiente” mientras se recibe la confirmación de “Cerrado”.
* Sólo se dará trámite a peticiones sobre los servicios catalogados por el Grupo TIC de la Gobernación del Huila.
* El servicio no incluye mantenimiento preventivo, correctivo ni ventanas de mantenimiento programadas.

**Violaciones y consecuencias de incumplimiento de la política:**

El incumplimiento a la política de servicios TIC de la Gobernación del Huila, podrá traer consigo la no atención de la solicitudes y requerimientos de servicios necesarios para el cumplimiento de las diferentes actividades enmarcadas en los distintos procesos de gestión de la entidad, así como las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere (Ley 1273 de 2009 de Delitos Informáticos, Ley 1581 de 2012 de Habeas Data, Ley 734 de 2002 “Código Disciplinario Único”, entre otras).

# CAPITULO 11:

# CUMPLIMIENTO DE REQUISITOS LEGALES Y NORMATIVOS

# PROPIEDAD DE LA INFORMACIÓN

Con el fin de mejorar la productividad y competitividad de la Gobernación del Huila promueve el uso responsable de las comunicaciones y tareas en forma electrónica, La información generada en cada una de las secretarias, departamentos administrativos y oficinas asesoras se debe considerar como propiedad de la Gobernación del Huila y no propiedad de los funcionarios o contratistas usuarios de los servicios informáticos utilizados.

# POLITICAS SITIO WEB

**Objetivo:**

* Establecer los lineamientos de la página web institucional [www.huila.gov.co](http://www.huila.gov.co), como servicio tecnológico para la publicación y divulgación de información misional de la entidad, fomento de la transparencia, acceso a la información pública, participación ciudadana, e interacción con otras entidades y organizaciones, siendo ésta el principal medio de comunicación y divulgación de información pública generada por la Gobernación del Huila, referente al desarrollo de programas, proyectos, estrategias, iniciativas, trámites, servicios, noticias de actualidad, disposición de impuestos en línea, etc.

**Aplicabilidad:**

Estas son políticas que aplican usuarios (funcionarios, contratistas y cualquier otra persona o entidad) que por razón de su trabajo se le permita acceso o tenga relación con la Gobernación del Huila.

**Directrices:**

* Actualmente en El sitio web de la Gobernación del Huila, es fundamental la seguridad del funcionamiento de la plataforma de la entidad y su dominio reconocido se denomina así [www.huila.gov.co](http://www.huila.gov.co).
* Para realizar procesos de publicación en el sitio web de la entidad, se debe solicitar mediante herramientas institucionales (correo electrónico, PQRS, nota, extranet, etc.) dirigido al grupo de Tecnología, Conectividad y Telecomunicaciones de la Gobernación del Huila.
* Se deben implementar software de desarrollo en herramientas y/o administradores de contenido reconocidos, actualizados y licenciados de última Tecnología.
* El Grupo de Tecnología, Conectividad y Comunicaciones (es el encargado de coordinar el mantenimiento, soporte y actualización de la información publicada en el sitio Web oficial, con el apoyo de profesionales asignado con el propósito de brindar un adecuado servicio a la comunidad.
* Toda información de los sitios web de la Gobernación del Huila, se debe publicar en español usual y escrito; el lenguaje debe ser concreto, respetuoso y enfocado al público, permite a los visitantes consultar con facilidad y rapidez, la comprensión de la información y cumple con la finalidad de atender los requerimientos de la ciudadanía.
* Las relaciones entre los elementos que componen la estructura del sitio web (resultan del diseño y planeación), deben ser dinámicas y versátiles. Para comprenderlas en su funcionalidad se utilizan los criterios de usabilidad y de la información, conforme los criterios de: (rapidez-navegabilidad-interactividad-vínculos-vigencia-estructura-enfoque-relevancia-pertinencia)
* Los contenidos que ofrecen los sitios Web de la Gobernación del Huila, deben orientarse bajo los parámetros del gobierno en línea, y/o normas dictadas por el Ministerio de Tecnología de la Información y las comunicaciones.
* Los sitios Web de la Gobernación del Huila, deben estar alojados en sitios y/o servidores de alto desempeño protegidos por cortafuegos y/o firewall que le ofrezcan un alto nivel de seguridad.

# POLÍTICA DE DERECHOS DE AUTOR Y/O AUTORIZACIÓN DE USO SOBRE LOS CONTENIDOS DE LA SEDE ELECTRÓNICA

## Alcances Y Limites En El Uso

A través de nuestra sede electrónica, compuesta por la ventanilla única y los portales transversales y aplicativos informáticos, la Gobernación del Huila divulga los temas y actividades propias de su misión, visión, objetivos y funciones.

Al navegar y utilizar los sitios web asociados a cada uno de los servicios, el usuario acepta las políticas anteriormente mencionadas. Si el usuario no está de acuerdo con las políticas mencionadas, se sugiere que se abstenga de acceder o navegar por los sitios web de nuestra Entidad.

La Gobernación del Huila se reserva el derecho de actualizar, modificar en cualquier momento el presente contenido.

## Política De Derechos De Autor Y/O Autorización De Uso Sobre Los Contenidos

La Gobernación del Huila no busca recibir ganancias o interés comercial con los contenidos o enlaces que se publican los sitios web, ni en las demás adscritas o vinculadas a las que se accede a través de [www.huila.gov.co](http://www.huila.gov.co), portales transversales y aplicativos informáticos.

Al acceder al contenido de nuestros sitios web usted podrá usar la información con fines personales o profesionales, pero no para explotación comercial.

Es necesario reconocer la titularidad de la Gobernación del Huila sobre los derechos de Propiedad Industrial e Intelectual del contenido, diseño gráfico del sitio web con cada uno de los elementos que lo componen (por ejemplo: menús, botones de navegación, el código fuente, textos, imágenes, texturas, gráficos, etc.), salvo que en los mismos se indique titularidad distinta, en cuyo caso dicho derechos corresponden a los terceros que la Gobernación del Huila indique.

El acceso a los sitios web y sus contenidos por parte del usuario, en ningún caso implica que la Gobernación del Huila renuncie, transmite, ceda total o parcialmente los derechos, ni confiere ningún derecho de utilización, licencia, alteración, explotación, reproducción, distribución o comunicación pública de los contenidos, sin la previa y expresa autorización de la Gobernación del Huila.

Recuerde que para usar los contenidos de los sitios web, portales y aplicativos informáticos debe tener autorización expedida por la Gobernación del Huila, la autorización incluye:

* 1. Cesión parcial o total de derechos sobre los contenidos
  2. Derecho de utilización
  3. Derecho de alteración, explotación, reproducción, distribución o comunicación de los contenidos

## Materiales Suministrados A La Gobernación Del Huila

Los materiales suministrados incluyen cualquier marca y logotipo que aparezcan en los sitios web, éstas son marcas comerciales registradas. Las marcas comerciales son los nombres de compañías y productos reales mencionados en los sitios web pueden ser marcas comerciales de sus respectivos propietarios.

La Gobernación del Huila no reclama la propiedad de los materiales que el usuario suministre al realizar comentarios, sugerencias, anuncios, publicaciones, sin embargo, al anunciar, publicar, subir, escribir, el usuario está otorgando permiso a la Gobernación del Huila para publicar y eliminar la información que ha proporcionado.

El usuario al anunciar, subir, escribir, suministrar información garantiza que es el propietario o de alguna manera controla todos los derechos, como se describe en los términos y condiciones de uso.

## Política Datos Abiertos

Se podrá hacer uso, transformación, distribución, redistribución, reutilización, compilación, extracción, copia, difusión, modificación y/o adaptación de los datos y de la información publicados en formato de datos abiertos en este sitio web bajo los criterios establecidos en la Licencia Creative Commons Attribution 4.0, en todo caso debe citarse la fuente de los datos objeto del uso, rehúso y/o transformación, la entidad productora de los datos publicados no será responsable de la utilización que de sus datos hagan las personas que transformen y/o usen dichos datos, ni tampoco de los daños sufridos o pérdidas económicas que, de forma directa o indirecta, produzcan o puedan producir perjuicios económicos, materiales o sobre datos y aplicaciones, provocados por el uso y/o transformación de los datos. Esta licencia de uso se rige por la legislación colombiana, independientemente del entorno jurídico del usuario, cualquier disputa que llegue a surgir en la interpretación de estos términos se resolverá bajo el amparo de la Ley colombiana.

## Responsabilidades De Los Usuarios

La Gobernación del Huila no será responsable por el uso indebido que hagan los usuarios del contenido de su sitio web.

El usuario debe usar los contenidos de forma diligente, correcta y lícita, sin incurrir en actividades que infrinjan los derechos de la Gobernación del Huila o de terceros, o que puedan atentar contra la moral, las normas jurídicas, esto incluye los daños o ataques informáticos, interceptación de comunicaciones, infracciones al derecho de autor, usurpación de identidad, revelación de secretos o falsedad en los documentos.

El usuario se compromete a no realizar las siguientes acciones que atentan contra la reputación de la Gobernación del Huila:

* Copiar, duplicar, reproducir, prestar, vender, revender, republicar, transmitir cualquier parte de este sitio web o de su contenido para uso comercial.
* Emitir publicidad usando los contenidos e información del sitio web.
* Publicar, anunciar, subir, distribuir material o información, que sea inapropiada, indecente, transgresora, difamatoria, obscena o ilegal.
* Difamar, abusar, acosar, acechar, amenazar o de alguna forma violar los derechos de privacidad, y publicidad de otros.
* Suprimir, eludir, o manipular el copyright (derechos de autor) y demás datos que identifiquen a la Gobernación del Huila. Usar técnicas de embebido para esconder la marca, logo u otras porciones del sitio web sin la autorización previa y por escrito de la Gobernación del Huila.
* Subir archivos que contengan software, material protegido por leyes de propiedad intelectual, derechos de privacidad, o publicidad a menos que el usuario sea el propietario o controle los derechos respectivos, o haya recibido el necesario consentimiento expreso.
* Falsificar o eliminar cualquier referencia al autor, referencia legal o avisos o designaciones propietarias o rótulos del origen o fuente del software u otro material contenidos en un archivo que se sube.
* Subir archivos que contengan virus, archivos corruptos, o cualquier otro software o programas malicioso.
* Publicar, ofrecer a la venta o a la compra cualquier bien o servicio.
* Dirigir o reenviar encuestas, cadenas de cartas o esquemas piramidales. Recoger información incluyendo direcciones de correo electrónico sin su consentimiento.
* Restringir o inhibir que otros usuarios puedan usar y disfrutar de los servicios de comunicación.
* Usar software automatizado o proceso manual, así como robots o spiders para copiar o monitorizar el contenido de la sede electrónica de la Gobernación del Huila sin la autorización previa y por escrito de la Gobernación del Huila
* Decompilar, alquilar, vender, realizar ingeniería inversa, o crear obras derivadas de este sitio web o de su contenido.
* Realizar ataques de denegación de servicio (DDOS) en contra de la infraestructura tecnológica de la Gobernación del Huila que impida el correcto funcionamiento de la sede electrónica de la Gobernación del Huila.

## Notificaciones Y Procedimiento De Reclamos De Violación A Los Derechos De Propiedad

Cualquier notificación de reclamo o violación de los derechos de propiedad bajo la ley colombiana, debe ser enviada a cualquiera de los siguientes datos de contacto:

**Dirección**: Carrera 4 Calle 8 Esquina, Sede Principal, Neiva-Huila-Colombia

**Horario de Atención**: Lunes a Jueves de 7:00 a.m a 11:45 a.m y de 2:00 p.m a 5:30 p.m - Viernes de 7:00 a.m a 11:30 a.m y de 2:00 p.m a 4:30 p.m

**Línea Gratuita**: 01 8000 968 716

**PBX**: (57 + 8) 8671300

**PQRSFD**: <https://www.huila.gov.co/publicaciones/9535/pqrsfd/>

# TÉRMINOS Y CONDICIONES DE USO

## Alcances Y Limites En El Uso

Apreciado usuario, le damos la bienvenida a nuestra Sede Electrónica, por medio de la cual la Gobernación del Huila divulga los temas y actividades propias de su misión, visión, objetivos y funciones.

La Gobernación del Huila no persigue ningún lucro, ganancia o interés comercial con los contenidos y enlaces que se publican en su sede electrónica y en los portales transversales de los diferentes productos y servicios que son parte de la Entidad y a los cuales se accede a través de la diferente URL <https://www.huila.gov.co/publicaciones/10714/aplicaciones-digitales/>.

Todos los productos y servicios que ofrece la Gobernación del Huila, son gratuitos y no utiliza ningún tipo de intermediarios para acceder a ellos, por favor denuncie este tipo de irregularidades en nuestros canales de atención.

La Gobernación del Huila se compromete a proteger la privacidad de la información de los usuarios. Al utilizar nuestros sitios web, acepta las prácticas utilizadas por La Gobernación del Huila en relación con los datos personales.

Nos reservamos, en todos los sentidos, el derecho de actualizar, modificar en cualquier momento los presentes términos y condiciones de uso.

## Definiciones

Para facilitar la comprensión de estos Términos y condiciones de uso, aquí le aclaramos el significado:

* Contenidos. Son todas las formas de información o datos que se divulgan en la página web, entre los que se encuentran: textos, imágenes, fotos, logos, diseños, animaciones, etc.
* Derechos de Propiedad Intelectual: Hacen referencia a todos los derechos de propiedad de la información de la Gobernación del Huila o de cualquier persona que sea titular legítima, como: signos distintivos, marcas, lemas, enseñas, logos, nombres de dominio, bases de datos, diseños, contenidos o cualquier otra obra o creación intelectual vinculada con el objeto, operación o desempeño del sitio web de la Gobernación del Huila.
* Foro. Servicio automatizado de mensajes, a menudo moderado por un propietario, a través del cual los suscriptores reciben mensajes dejados por otros suscriptores por un tema dado. Los mensajes se envían por correo electrónico.
* Internet : una red global de redes de ordenadores cuya finalidad es permitir el intercambio libre de información entre todos sus usuarios. Sobre esta red se pueden utilizar múltiples servicios como por ejemplo correos electrónicos, www, etc.
* Página web: Es la unidad informativa de la web, son documentos compuestos por textos, imágenes, audios o videos a los que se puede acceder a través de www y se accede empleando un navegador. La información de las páginas web está generalmente en formato HTML. Su contenido puede ir desde un texto corto a un voluminoso conjunto de textos, gráficos estáticos o en movimiento, sonido, etc.
* Publicar. Hacer que un documento, video, audio, imágenes sean visibles desde los sitios web institucionales.
* Servicio de Comunicación: Áreas de chat, grupos de usuarios, foros de discusión, comunidades, calendarios, acceso a redes sociales y/o otras facilidades de mensajería o comunicación, diseñadas para permitirle a la Gobernación del Huila comunicarse con el público en general o con un grupo de personas.
* Servicios. Son las ayudas en línea que la Gobernación del Huila provee actualmente o que piensa proveer en el futuro a los usuarios, por medio de esta página web, como publicación de noticias o actividades propias de la gestión institucional; trámites en línea; consultas; foros y buzón de quejas y reclamos, entre otros.
* Sede electrónica: es el sitio oficial en internet de cada autoridad, al que se accede a través de una dirección electrónica en la que se dispone información, trámites, servicios y demás elementos ofertados por la autoridad y cuya titularidad, administración y gestión le corresponde.
* Sitio web: Incluye los portales web, sistemas de información y aplicativos.
* Términos y condiciones de uso: Acuerdo completo entre el usuario y La Gobernación del Huila respecto al uso del sitio web.
* Usuario. Es la persona que ingresa al sitio web de la Gobernación del Huila para buscar o consultar información de su interés; o para poner una queja mediante el registro de peticiones, quejas, reclamos, sugerencias y denuncias en el enlace: <https://www.huila.gov.co/publicaciones/9535/pqrsfd/>.
* Vínculo. [*Link* en inglés]. Enlaces que sirven para saltar de una información a otra, o de un servidor web a otro, cuando se navega por Internet.

## Condiciones De Uso

## Vínculos A Sitios De Terceros

Nuestros sitios web pueden contener vínculos a otros sitios web (“sitios vinculados”), que no están bajo nuestro control y por lo tanto no somos responsables de los contenidos. Proveemos estos vínculos solamente para accesibilidad de los usuarios y su inclusión no implica aprobación, ni asociación con sus operadores.

## Uso De Servicios De Comunicación

Nuestros servicios de comunicación son áreas de chat, grupos de usuarios, foros de discusión, comunidades, calendarios, acceso a redes sociales y/o otras facilidades de mensajería o comunicación, diseñadas que nos permiten la comunicación con el público en general o con un grupo de personas.

* Nosotros no tenemos la obligación de monitorear los servicios de comunicación. No obstante, reservamos el derecho de revisar los materiales anunciados en los servicios de comunicación y quitarlos a discreción.
* Reservamos el derecho de retirarles a los usuarios el acceso a los servicios de comunicación, en cualquier momento sin previo aviso.
* No controlamos o aprobamos el contenido, mensajes, o información encontrada en los Servicios de Comunicación y, por tanto, no somos responsables en relación con los mismos y con cualquier acción resultante de la participación de un usuario en los servicios de comunicación.

## Uso De “Cookies”

Los sitios de la Gobernación del Huila utilizan "cookies" para almacenar sus preferencias ayudándolo a personalizar su experiencia en línea. Una cookie es un archivo de texto que es grabado en su disco duro por un servidor de páginas Web. Las cookies no pueden ser utilizadas para ejecutar programas o distribuir virus informáticos a su computadora. Las cookies son asignadas al usuario por el servidor en relación uno-a-uno, y pueden ser leídas únicamente por un servidor miembro del dominio que emitió la cookie para el usuario.

Una de las principales ventajas de las cookies es que le ahorran tiempo al usuario, porque el propósito de una cookie es informarle al servidor Web que el usuario ha regresado a una página específica. Por ejemplo, cuando el usuario personaliza páginas en la Gobernación del Huila, o cuando se registra en los sitios de la Gobernación del Huila, la cookie grabada permite al servidor Web de la Gobernación recuperar su información específica en las subsiguientes visitas. La próxima vez que regrese al mimo sitio la información que el usuario suministró anteriormente puede ser recuperada de la cookie, y así las opciones que el usuario haya personalizado en su visita anterior a los sitios de la Gobernación del Huila estarán disponibles sin necesidad de que deba escribirlas nuevamente.

El usuario tiene la posibilidad de aceptar o rechazar cookies. La mayoría de los exploradores de Internet aceptan las cookies automáticamente, pero si lo prefiere Usted puede modificar la configuración para que las rechace. Si escoge que el navegador rechace cookies, es probable que no pueda aprovechar en su totalidad las características interactivas de los servicios ofrecidos en sitios de la Gobernación del Huila que visite el usuario.

## ***Seguridad De Su Información Personal***

La Gobernación del Huila asegura su información personal frente al acceso, uso o divulgación no autorizados. La Gobernación del Huila mantiene la información de identificación personal que Usted haya provisto, en servidores ubicados en un ambiente controlado y seguro, protegidos del acceso, uso o divulgación no autorizados. En caso de que información personal sea transmitida a otros sitios Web, ésta se protege mediante el uso de protocolos cifrados como el protocolo SSL (Secure Sockets Layer).

## Normas Aplicables

Los términos y condiciones de uso son gobernados por las leyes de la República de Colombia, para cualquier efecto legal o judicial, el lugar de las presentes condiciones es la ciudad de Bogotá y cualquier controversia que surja de su interpretación o aplicación se someterá a los jueces de la República de Colombia.

La Gobernación del Huila se reserva el derecho a revelar, editar o denegar información en cualquier momento cuando sea necesario cumplir con las leyes aplicables, regulaciones, procesos legales o pedidos del Gobierno nacional.

Nos reservamos el derecho en cualquier momento a revelar, editar o denegar información cuando sea necesario cumplir con las leyes aplicables, regulaciones, procesos legales o pedidos del Gobierno Nacional.

De acuerdo con el máximo alcance permitido por las leyes aplicables, en ningún caso la Gobernación del Huila será responsable daños directos, indirectos ocasionados por el rendimiento de los sitios web, demoras, imposibilidad del uso del sitio o servicios relacionados, falla en la provisión de servicios, o por cualquier información, software, productos, servicios y gráficos obtenidos a través de los sitios web.

## Renuncia De Obligación

La información, software, productos y servicios incluidos o disponibles a través de nuestros sitios web pueden contener inexactitudes o errores tipográficos. Periódicamente modificamos y agregamos a la información aquí contenida. Nosotros podemos realizar en cualquier momento modificaciones o mejoras al sitio web.

## Deberes De Los Usuarios

No somos responsables del uso indebido que hagan los usuarios del contenido de nuestro sitio web. Los usuarios deben usar los contenidos de forma diligente, correcta y lícita, sin incurrir en actividades que infrinjan los derechos de la Gobernación del Huila o de terceros, o que puedan atentar contra la moral, las normas jurídicas, esto incluye los daños o ataques informáticos, interceptación de comunicaciones, infracciones al derecho de autor, usurpación de identidad, revelación de secretos o falsedad en los documentos.

Al ingresar a nuestro sitio web los usuarios se compromete a no realizar las siguientes acciones:

* Copiar, duplicar, reproducir, prestar, vender, revender, republicar, transmitir cualquier parte de este sitio web o de su contenido para uso comercial.
* Emitir publicidad usando los contenidos e información del sitio web.
* Publicar, anunciar, subir, distribuir material o información, que sea inapropiada, indecente, transgresora, difamatoria, obscena o ilegal.
* Difamar, abusar, acosar, acechar, amenazar o de alguna forma violar los derechos de privacidad, y publicidad de otros.
* Suprimir, eludir, o manipular el copyright (derechos de autor) y demás datos que identifiquen a la Gobernación del Huila. Usar técnicas de embebido para esconder la marca, logo u otras porciones del sitio web sin la autorización previa y por escrito de la Gobernación del Huila.
* Subir archivos que contengan software, material protegido por leyes de propiedad intelectual, derechos de privacidad, o publicidad a menos que el usuario sea el propietario o controle los derechos respectivos, o haya recibido el necesario consentimiento expreso.
* Falsificar o eliminar cualquier referencia al autor, referencia legal o avisos o designaciones propietarias o rótulos del origen o fuente del software u otro material contenidos en un archivo que se sube.
* Subir archivos que contengan virus, archivos corruptos, o cualquier otro software o programas malicioso.
* Publicar, ofrecer a la venta o a la compra cualquier bien o servicio.
* Dirigir o reenviar encuestas, cadenas de cartas o esquemas piramidales. Recoger información incluyendo direcciones de correo electrónico sin su consentimiento.
* Restringir o inhibir que otros usuarios puedan usar y disfrutar de los servicios de comunicación.
* Usar software automatizado o proceso manual, así como robots o spiders para copiar o monitorizar el contenido del sitio web sin la autorización previa y por escrito de la Gobernación del Huila
* Decompilar, alquilar, vender, realizar ingeniería inversa, o crear obras derivadas de este sitio web o de su contenido.

## Política Comentarios

Los usuarios son responsables de sus comentarios en cualquier foro, u otro espacio de participación de los sitios web por lo que nosotros no garantizamos la calidad, idoneidad y/o consecuencias que pudieren acarrear a favor y/o en contra de otros usuarios o de terceros.

De esta manera, cada usuario acepta y nos faculta expresa e irrevocablemente a la Gobernación del Huila para revisar los comentarios u opiniones escritos y el administrador de sitio web se reserva el derecho de ocultar cualquier comentario ofensivo, amenazante, xenófobo, pedófilo, que esté en contra de las libertades políticas, religiosas, preferencias sexuales, que promueva el racismo, la xenofobia entre otros que se puedan considerar insultantes o provocativos.

Le invitamos a conocer nuestros “Términos y condiciones de uso”, para la participación en los comentarios y foros del sitio, ya que se asume su aceptación, así como el compromiso irrevocable de cada uno, de respetarlas, por lo cual nosotros estamos eximidos ante cualquier responsabilidad que se derive de su incumplimiento, incluidos daños y perjuicios causados a otros usuarios y/o cualquier tercero afectado.

## Contacto Para Asuntos Relacionados Con Los Términos Y Condiciones

Sus sugerencias para mejorar nuestros contenidos, información y servicios son bienvenidas, comuníquese con nosotros a través de:

**Dirección**: Carrera 4 Calle 8 Esquina, Sede Principal, Neiva-Huila-Colombia

**Horario de Atención**: Lunes a Jueves de 7:00 a.m a 11:45 a.m y de 2:00 p.m a 5:30 p.m - Viernes de 7:00 a.m a 11:30 a.m y de 2:00 p.m a 4:30 p.m

**Línea Gratuita**: 01 8000 968 716

**PBX**: (57 + 8) 8671300

**PQRSFD**: <https://www.huila.gov.co/publicaciones/9535/pqrsfd/>

# GLOSARIO

***Activo:*** Cualquier cosa que tenga valor para la organización.

***Administración de Redes****:* Es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

***Amenaza:*** Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir daño (material o inmaterial) sobre los elementos (activos, recursos) de un sistema.

***Comunicación:*** Es cuando se transmite información desde un equipo a cualquier otro. Para que se pueda realizar una transmisión de información, son necesarios tres elementos: El emisor, quien origina la información; el medio de transmisión, que permite la transmisión de esa información; el receptor, quien recibe la información.

***Confidencialidad:*** Propiedad que determina que la información no esté disponible ni sea revelada a los individuos, entidades o procesos no autorizados.

***Correo electrónico:*** También conocido como “E-MAIL”. Es un software que puede utilizarse para el envío y recepción de mensajería entre usuarios, entendiendo por mensajería cualquier texto, archivo, programa, etc.

***Disponibilidad:*** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

***Dominio:*** Es el término que se emplea para indicar que en una organización existe un sistema en red al cual se encuentran conectados todos los ordenadores o computadores de la entidad. Este sistema administra la información de sus usuarios a través de un servidor principal o servidor de dominio, desde el cual es posible establecer políticas de acceso, restricciones y privilegios para los usuarios en de la red.

***Firewall:*** Mecanismo de seguridad en internet frente a accesos no autorizados.

***Hardware:*** El hardware está formado por los componentes físicos. Es la parte "dura", es decir, las partes que configuran la máquina y que le dan una serie de características.

***Política:*** Es un documento que articula los lineamientos o principios básicos que sirven de medio para alcanzar los objetivos de la entidad y sobre los cuales debe asentarse, las normas, instrucciones, procedimientos.

***Política de seguridad:*** Es un documento que articula la filosofía, los requerimientos reglamentarios y las creencias que la Organización tiene en relación con la protección de los recursos de información, tecnológicos y telecomunicaciones.

***Privacidad:*** El derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y que información referente a ellos serán difundidas o trasmitidas a otras.

***Red de computadoras****:* A nivel más elemental una red no es más que un conjunto de máquinas (computadoras, impresoras y otros recursos), un medio compartido (tal como un cable con el que se interconectan todas las computadoras y las impresoras), junto con una serie de reglas (protocolo) que rigen el acceso a dicho medio.

***Red Internet:*** Conjunto de computadores y entidades alrededor del mundo, interconectadas entre sí, con el propósito de intercambiar correo e información de carácter general.

***Servicio:*** Son programas que están disponibles en los servidores y que son utilizados por los usuarios de la red bajo una solicitud.

***Software****:* El software está compuesto por los programas que dirigen el funcionamiento de un ordenador. Es la "parte lógica" de la máquina que permite enlazar todos los elementos de [hardware](http://www.ciudadfutura.com/mundopc/glosario/h/hardware.htm) de la manera más efectiva posible, permitiéndole realizar cualquier tipo de trabajo.

***Usuarios:*** Se refiere a todos los funcionarios, contratistas y cualquier otra persona o entidad que por razón de su trabajo se le permita acceso, se le asigne derecho de uso y utilice los medios electrónicos de almacenamiento y transmisión de datos de la entidad.

***Virus:*** Son pequeños programas de computadora cuya principal cualidad es la de poder auto replicarse, está escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este para producir efectos dañinos.

# CONTROL DE CAMBIOS

| **Versión** | **Vigencia** | **Identificación de los cambios** | **Responsable** |
| --- | --- | --- | --- |
| 1 | 23 de septiembre de 2010 | Primera versión | Coordinadora Grupo de tecnología, Conectividad y comunicaciones |
| 2 | 20 de diciembre de 2014 | * Se modificó el alcance del manual. * Se actualizaron los objetos. * Se incluyó el ítem de estructura documental y diagnóstico inicial. * Se modificaron los ítems de descripción de actividades, documentos y registros. * Se incluyó el glosario. | Coordinadora Grupo de tecnología, Conectividad y comunicaciones |
| 3 | 20 de octubre de 2020 | * Se actualizó nombres de procesos en el ítem 12.1.1 Procesos Estratégicos, en el ítem 12.1.3 Procesos Misionales, y en el ítem 12.1.4 Procesos de Apoyo * Se actualizó el ítem 24 “Política de Correo Electrónico” * Se actualizó objetivo de la Política Sitio Web en el ítem 25 * Se incluyó ítem 26 “Política de Servicios TIC” * Se incluyó ítem 27 “Política de Respaldo de Información” * Se modificó numeración de Políticas de Usuario Final, de Glosario, y de Control de Cambios, a 28, 29 y 30 respectivamente | Coordinador Grupo de Tecnología, Conectividad y Telecomunicaciones |
| 4 | 02 de junio de 2021 | * Se incluyó ítem 28 “Política de Dispositivos Móviles” * Se modificó numeración de Políticas de Usuario Final, de Glosario, y de Control de Cambios, a 28, 29 y 30 respectivamente | Coordinador Grupo de Tecnología, Conectividad y Telecomunicaciones |
| 5 | 06 de junio de 2022 | * Se incluyó ítem 20.1.1. “Limpieza de puestos de trabajo” * Se ajustaron los ítems 19.5.1 “Creación cuentas usuarios de planta Gobernación del Huila”, 19.5.1.1 “Creación cuentas usuario para contratistas de la Gobernación del Huila”, y 19.6.2.3 "Identificación de Estaciones de Trabajo" | Coordinador Grupo de Tecnología, Conectividad y Telecomunicaciones |
| 6 | 15 de agosto de 2022 | * Se actualizó ítem 18 “Uso, Clasificación y Control de Activos de TI” (nombre y lineamientos) * Se incluyó ítem 30 “Política de Transferencia de Información” * Se modificó numeración de Glosario, y de Control de Cambios, a 31 y 32 respectivamente. | Coordinador Grupo de Tecnología, Conectividad y Telecomunicaciones |
| 7 | 28 de septiembre de 2022 | * Se actualiza nombre del documento a “Manual de Políticas de Uso, Seguridad y Administración de Activos Tecnológicos y de Información”. * Se ajusta el orden del documento, reorganizando las diferentes políticas por capítulos, y se ajusta numeración. * Se añade el ítem 17 “Metodología de Gestión de Activos de Seguridad Digital” * Se añade el ítem 31 “Separación de Ambientes de Desarrollo, Pruebas y Operación”“ * Se añade el ítem 41 “Adquisición, desarrollo, soporte, mantenimiento, retiro, cambio y/o actualización de software”. * Se añade el ítem 46 “Política de Derechos de Autor y/o Autorización de Uso Sobre los Contenidos de la Sede Electrónica” * Se añade el ítem 47 “Términos y Condiciones de Uso” | Coordinador Grupo de Tecnología, Conectividad y Telecomunicaciones |